

IGEL OS

Exported on 10/25/2021



## Table of Contents

<b>1</b>	<b>Partner Solutions .....</b>	<b>56</b>
1.1	Crossmatch / Digital Persona .....	56
1.2	Diktamen Compatibility.....	56
1.3	Imprivata OneSign Compatibility.....	57
1.3.1	IGEL Devices .....	57
1.3.2	IGEL Software Clients.....	58
1.4	Jabra Handsets / Headsets.....	58
1.4.1	Tested by IGEL.....	58
1.5	Nuance Compatibility .....	59
1.6	Olympus Compatibility .....	59
1.7	Poly Headsets.....	61
1.8	EPOS/Sennheiser Compatibility .....	61
1.8.1	Tested by IGEL.....	61
1.8.2	Tested by EPOS/Sennheiser .....	61
	Wired Headsets .....	61
	Wireless Headsets .....	62
	Speakerphones .....	62
1.9	Signotec Compatibility .....	62
1.10	StepOver Signature Pads Compatibility .....	63
1.11	Wacom Compatibility .....	63
1.12	deviceTrust.....	64
1.13	Philips Speech .....	64
<b>2</b>	<b>IGEL OS Articles .....</b>	<b>66</b>
2.1	Overview: First Steps with IGEL OS 11 .....	66
2.2	Update and Upgrade.....	68
2.2.1	Adapting IGEL OS 11.04 or Higher for Devices with Small Storage .....	69
	Environment.....	69
	Overview .....	69
	Determining Which Features to Deactivate .....	69
	Reducing the Feature Set .....	69
2.2.2	Upgrading UDC3 or UD Pocket from IGEL OS 10.06 to IGEL OS 11 via Universal Firmware Update .....	71



Devices That Can Be Upgraded to IGEL OS 11 .....	71
Important! Consider This Before Upgrading .....	78
Getting the UMS Ready .....	80
Deploying the Licenses .....	80
Creating the Universal Firmware Update .....	81
Creating an Upgrade Profile .....	91
Assigning the Upgrade Profile and the Universal Firmware Update to the Test Devices.....	100
Testing the Upgrade .....	104
Unassigning the Upgrade Profile and the Universal Firmware Update .....	106
If Applicable: Restoring Custom Partition and Custom Applications.....	107
Upgrading All Devices .....	107
2.2.3    Upgrading from IGEL OS 10 to IGEL OS 11 .....	114
Upgrading UDC3 Devices from IGEL OS 10 to IGEL OS 11 .....	114
Upgrading IGEL Devices from IGEL OS 10 to IGEL OS 11 .....	174
2.2.4    Buddy Update .....	221
TechChannel .....	222
Configuring the Buddy Update Server .....	223
Configuring the Buddy Update Client .....	224
2.2.5    Firmware Update .....	225
Downloading Updates and Storing them on an FTP Server .....	226
Executing an Update Process.....	227
2.2.6    Updating the Firmware using a USB Storage Device .....	228
2.2.7    Updating the Firmware using the Linux Console .....	229
Issue .....	229
Solution .....	229
2.2.8    Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher .....	231
Symptom .....	231
Problem .....	231
Environment.....	231
Solution .....	231
2.2.9    Error: "legacy ICG Root (CA) certificate" When Updating to Igel OS 11.04 on Devices Connected via ICG....	232
Possible Problem .....	232
Environment.....	233
Diagnosis .....	233
Solution .....	234
2.2.10   Device Does Not Connect to ICG after Update to IGEL OS 11.04 or Higher .....	235



Symptom .....	235
Environment.....	235
Problem/Possible Cause.....	235
Diagnosis .....	235
Solution .....	236
2.2.11 IGEL OS Automatic Update Service for Device Evaluation.....	237
Overview.....	237
Environment.....	237
Configuring the Automatic Update Service .....	237
2.3 Citrix.....	238
2.3.1 Performance.....	238
Poor Performance: Black Blocks and Stripes in Citrix Sessions .....	238
Poor Performance with Citrix XenDesktop 7.6 Deep Compression.....	239
Citrix Receiver: Grey Blocks in Excel 2013.....	240
Bar Code Scanning is Slow via Citrix .....	240
Slow Performance of Citrix Session in a Cloud Environment .....	241
2.3.2 Mouse.....	242
Changing Middle Mouse Button Function for Citrix Session and Local Firefox Browser.....	242
How to Connect a SpaceMouse with a Citrix Session.....	243
Solve SpaceMouse USB Reset Problem .....	245
Wireless Mouse Keyboard Set Logitech k520 Freezes in Citrix Session.....	246
Black Box Next to the Mouse Cursor .....	246
2.3.3 How to Configure Citrix Native USB Redirection.....	247
2.3.4 Citrix Fabulatech Scanner Redirection .....	248
Enabling Fabulatech Scanner Redirection .....	248
2.3.5 Mapping USB Storage Media into Citrix Sessions.....	249
Basic Configuration of the Client .....	250
Additional Parameters to Check .....	250
Assigning a Drive Letter within the Session (Optional) .....	251
Configuration on the Server Side .....	251
2.3.6 Auto-Hide Toolbar in Appliance Mode.....	251
Environment.....	251
Problem .....	251
Solution .....	251
2.3.7 Create a Seamless, Transparent User Experience with Appliance Mode.....	252



2.3.8	Connecting to a Citrix Farm .....	252
	Citrix StoreFront.....	253
	Citrix Self-Service .....	253
	Appliance Mode.....	255
2.3.9	Create a Self-Service Setup for the User with Quick Settings.....	255
2.3.10	Login Failed because of the Expired AD Password.....	257
	Problem .....	257
	Solution .....	257
	Changing an Expired Active Directory Password.....	257
2.3.11	Configuring Auto Logon for Citrix Virtual Desktops .....	258
	Steps .....	258
2.3.12	Force Citrix Logout Using Hotkey.....	262
2.3.13	Citrix: Freeze at Logout.....	263
	Symptom .....	263
	Solution .....	263
	Workaround.....	263
2.3.14	Warning Message: [Citrix Store] Could Not Connect to the Citrix Server .....	264
	Environment.....	264
	Symptom .....	264
	Problem .....	265
	Solution .....	265
2.3.15	Setting up Citrix Sessions with Hardware-Accelerated H.264 Deep Compression Codec .....	265
	Prerequisites .....	265
	Activating the Codec .....	266
2.3.16	Using Font Smoothing (ClearType) in Citrix Sessions.....	266
	Symptom .....	266
	Problem .....	266
	Solution .....	266
2.3.17	Highly Secured XenServer has Problems with LD_BIND_NOW Workaround.....	267
	Problem .....	267
	Solution .....	267
2.3.18	Workaround for Citrix Receiver X Error .....	268
	Problem .....	268
	Environment.....	268
	Solution .....	268
2.3.19	Citrix HTML5 Receiver Issue.....	268



Affected Versions.....	268
Issue .....	268
Solution .....	269
2.3.20 Macbook Keyboard Layout inside Citrix Session.....	269
2.3.21 Citrix Feature Matrix.....	269
2.3.22 Using Lync / Skype for Business with Citrix HDX RealTime Optimization Pack.....	273
Issue .....	273
Solution .....	273
2.4 RDP .....	274
2.4.1 Mapping USB Storage Media into RDP Sessions .....	274
Solution: .....	274
Basic Configuration of the Client .....	275
Additional Parameters to Check .....	275
Configuration on the Server Side .....	276
2.4.2 What Is the String for Token-Based Load Balancing? .....	276
Environment.....	276
Question .....	276
Answer .....	277
2.4.3 RDP Fabulatech Scanner Redirection .....	277
Enabling Fabulatech Scanner Redirection .....	277
2.4.4 RDP RemoteApp Parameter Settings.....	278
Symptom .....	278
Problem .....	278
Solution .....	278
2.4.5 RDP Performance Enhancements .....	279
Symptom .....	279
Problem .....	279
Solution .....	280
2.4.6 RDP Session playing Sound: Error RDPSND_NEGOTIATE .....	280
Symptom .....	280
Problem .....	280
Solution .....	281
2.4.7 Crackling and Audio Dropouts in RDP Sessions .....	281
Symptom .....	281
Environment.....	281



Problem .....	281
Solution .....	281
2.4.8 Login Failed Because of Expired AD Password .....	282
Issue .....	282
Solution .....	283
Changing an Expired Active Directory Password.....	283
2.4.9 User Has to Provide Credentials Twice for RDP Logon .....	283
Issue .....	283
Cause .....	284
Solution .....	285
2.5 VMware Horizon .....	285
2.5.1 Setting up VMware Blast Sessions.....	285
Prerequisites .....	285
2.5.2 Use NLA (Network Layer Authentication) for Logon with Horizon Client Sessions .....	285
2.5.3 Workaround for Hotkeys in Horizon Sessions .....	286
Issue .....	286
Solution .....	286
2.5.4 Multimedia Acceleration with VMware Horizon View in VESA Mode .....	286
Symptom .....	286
Problem .....	286
Solution .....	286
2.5.5 Horizon Feature Matrix .....	287
2.5.6 Troubleshooting the Horizon Client.....	291
Symptom .....	291
Environment.....	291
Problem .....	291
Solution .....	291
2.6 Microsoft Azure Virtual Desktop (AVD) .....	292
2.6.1 Importance of Keeping IGEL OS Firmware Up-to-Date for Microsoft AVD and Windows 365 CloudPC .....	292
Why Is It Important to Keep Your Igel OS Firmware Updated? .....	292
IGEL Environment .....	292
How to Check for the Latest IGEL OS Firmware Version .....	293
How to Check If the IGEL OS Version Is Out-of-Date .....	294
How to Update IGEL OS Endpoint Devices to the Latest Firmware Version .....	298
2.7 Evidian .....	305



2.7.1	Authenticating with Evidian Authentication Manager .....	305
	Prerequisites .....	305
	Configuring an Evidian Authentication Manager Session.....	305
	Configuring Citrix/RDP/VMware Horizon Sessions.....	306
	Custom Commands .....	307
	Debugging and Troubleshooting .....	307
2.8	IBM iAccess .....	308
2.8.1	Editing the List of Visible Menu Entries for IBM iAccess .....	308
	Removing Menu Items .....	308
2.8.2	Key Mapping for IBM iAccess Client.....	309
	Problem .....	309
	Environment/Prerequisites .....	309
	Solution .....	310
	Editing the Key Mappings .....	310
2.9	Imprivata .....	322
2.9.1	Imprivata: Clear the Imprivata Data Partition .....	323
2.9.2	Imprivata: Session Customization .....	323
	Imprivata_VMware Session .....	324
2.10	Azure Virtual Desktop .....	324
2.10.1	Feature Matrix: AVD (RDP3) for IGEL OS 11 .....	324
2.10.2	How to Connect IGEL OS to Azure Virtual Desktop .....	327
	Quick Start Guide .....	327
2.11	SSH.....	331
2.11.1	Enable Weaker Algorithms in the Built-in OpenSSH Server.....	332
	Problem .....	332
	Solution .....	332
2.11.2	Enable Weaker Algorithms in the SSH Client.....	332
	Environment.....	332
	Problem .....	332
	Solution .....	332
2.11.3	SSH: Deprecation of Weak Algorithms as of IGEL Linux 10.04.100 .....	333
2.12	Amazon WorkSpaces – Teradici PCoIP Sessions .....	333
2.12.1	Connecting IGEL OS Devices with Amazon WorkSpaces via PCoIP .....	334
	Set Up the Device Connection .....	334
	Connecting to Amazon WorkSpaces .....	335



2.12.2	Use IGEL Setup for Configuration – Connecting with AWS via PCoIP .....	337
	Configuring in the IGEL Setup .....	337
	Connecting to Amazon WorkSpaces .....	338
2.12.3	Broker Types – Amazon WorkSpaces .....	338
	PCoIP Broker .....	338
	Direct Hardhost .....	339
2.12.4	How Can I Use H.264 Acceleration in a Teradici PCoIP Session? .....	339
	Question .....	339
	Environment .....	339
	Answer .....	339
2.13	Login Enterprise Configuration .....	340
2.13.1	Login Enterprise Launcher in IGEL OS .....	340
	Requirements .....	340
	Uploading the SSL Certificate .....	340
	Configuration of Login Enterprise Launcher .....	342
	Starting the Login Enterprise Launcher from the UMS .....	343
2.13.2	Getting the Secret for Login Enterprise Launcher .....	344
2.13.3	Using the Login Enterprise Launcher within a VMware Horizon Session .....	347
2.14	Nutanix .....	351
2.14.1	Frame on Nutanix .....	351
	Setting Up Frame Connection .....	351
2.14.2	Running the Nutanix Test Drive on IGEL .....	352
2.15	Browser .....	355
2.15.1	Define Multiple Start Pages for Your Browser .....	355
	Firefox .....	355
	Chromium .....	355
2.15.2	Touchscreen: Multitouch/Gesture Support for Firefox .....	356
2.15.3	Set Advanced User Preferences for the Browser .....	357
2.15.4	Use the Firefox Browser in Kiosk Mode .....	358
	Settings under Sessions > Firefox Browser > Firefox Browser Sessions > [Session Name] .....	358
	Settings under Sessions > Firefox Browser > Firefox Browser Sessions > [Session Name] > Settings .....	359
	Settings under Sessions > Firefox Browser > Firefox Browser Global .....	359
	Settings under Sessions > Firefox Browser > Firefox Browser Global > Tabs .....	360
	Settings under Sessions > Firefox Browser > Firefox Browser Global > Content .....	360
	Settings under Sessions > Firefox Browser > Firefox Browser Global > Privacy .....	361



Settings under Sessions > Firefox Browser > Firefox Browser Global > Security .....	362
Settings under Sessions > Firefox Browser > Firefox Browser Global > Restart.....	362
Settings under Sessions > Firefox Browser > Firefox Browser Global > Window .....	363
Settings under Sessions > Firefox Browser > Firefox Browser Global > Menus & Toolbars.....	363
Settings under Sessions > Firefox Browser > Firefox Browser Global > Context.....	364
Disabling Access to Developer Tools.....	364
Disabling Crash Reports.....	364
2.15.5 SSL/TLS Error with Firefox in Appliance Mode .....	365
Symptom .....	365
Problem .....	365
Solution .....	365
2.15.6 Browser Cannot Download Files .....	366
Symptom .....	366
Problem .....	366
Solution .....	366
2.15.7 Some PDFs are not opened by Firefox .....	366
Symptom .....	366
Problem .....	366
Solution .....	366
2.15.8 Can I Install Firefox Extensions? .....	367
Question .....	367
Answer .....	367
2.16 System .....	367
2.16.1 Resetting a Device with Unknown Administrator Password .....	368
Symptom .....	368
Problem .....	368
Solution .....	368
2.16.2 Error: "Unknown filesystem..." .....	369
Symptom .....	369
Environment.....	370
Problem .....	370
Solution .....	370
2.16.3 Custom Boot Commands Are Still Active after Factory Reset .....	370
Symptom .....	370
Problem .....	370



Solution .....	371
2.16.4 Solving Issues with Signed Partitions .....	371
Error: "Partition couldn't be loaded due to invalid signature" .....	371
Error: Device Plays a Beep Code Instead of Booting .....	372
Error: "The new firmware is not signed. Update not allowed." .....	374
Error: "Invalid signature - Failed to read from partition".....	375
2.16.5 How to Show the Boot Mode of IGEL OS.....	375
2.16.6 Disabling Features to Reduce Firmware Size .....	376
Symptom .....	376
Problem .....	376
Solution .....	376
2.16.7 Fabulatech USB Redirection Server Component .....	376
Issue.....	376
Problem .....	377
Solution .....	377
2.16.8 Which Features of IGEL OS Will Be Affected If the UMS Is Down? .....	377
Overview .....	377
Productivity Features That Are Affected If the UMS Is Down .....	377
Administration Functions That Are Affected If the UMS Is Down .....	377
2.17 Network .....	378
2.17.1 Configuring Open VPN Sessions.....	378
Prerequisites .....	378
Authenticating with TLS Certificates .....	379
Authenticating with Name/Password .....	379
Authenticating with Name/Password with TLS Certificates.....	380
Authenticating with Static Key .....	381
Options and TLS Options.....	382
DNS and Routing Options.....	382
Proxy .....	383
Checking the VPN Connection.....	383
Automatically Starting the VPN During Boot.....	384
Further Information .....	384
Securely Distributing Keys and Certificates for OpenVPN .....	385
2.17.2 Running the OpenVPN Client with a Preconfigured Configuration File .....	386
Environment.....	386



Setting up an OpenVPN Connection with a Preconfigured Configuration File.....	386
Removing the OpenVPN Connection .....	387
2.17.3 How Can I Configure OpenVPN with an .ovpn or .conf File? .....	387
Overview .....	387
Creating a Profile.....	387
Creating the Certificate/Key Files.....	390
Transferring the Files to the UMS .....	392
Adjust the Profile.....	392
2.17.4 Configuring Wi-Fi Network Roaming.....	393
Issue .....	393
Solution .....	393
2.17.5 Connecting to a Wi-Fi Network with Hidden SSID.....	395
Symptom .....	395
Problem .....	395
Solution .....	395
2.17.6 Improving WiFi Connectivity .....	395
Problem .....	395
Environment.....	396
Possible Causes and Solutions.....	396
2.17.7 Preventing Permanent Storage of Wireless Network Keys .....	398
2.17.8 Using WPA Enterprise / WPA2 Enterprise with TLS Client Certificates.....	399
Via SCEP (NDES) .....	399
Via Files Served from UMS .....	399
Deploying Client Certificates and Keys .....	399
Configuring the Network Interface.....	400
2.17.9 IPv6 Settings.....	401
Application Scenario .....	401
Available Configurations .....	402
Timeouts in Automatic Configuration .....	403
2.17.10 Extended Logging With Syslog, Tcpdump and Netlog .....	403
Debuglog Partition.....	403
Syslog.....	405
Tcpdump .....	405
Netlog .....	407
2.17.11 Making a Telnet Connection from IGEL Linux.....	413
Issue .....	413



Solution .....	413
2.17.12 Configuring Dynamic DNS Updates via DDNS .....	414
2.17.13 Changing the SMB protocol version.....	416
2.17.14 How to Launch the Wireless Manager within IGEL OS when the Taskbar Is Hidden .....	416
Problem .....	416
Environment.....	416
Solution .....	416
2.18 Security.....	418
2.18.1 Securing IGEL OS Endpoints.....	418
Introduction .....	418
Setting Passwords.....	419
Keeping the System Up-To-Date .....	422
Disabling Access to Components .....	426
Minimizing the Attack Surface.....	429
Configuring Remote Access and Management.....	434
Wi-Fi and Bluetooth .....	438
Using UD Pocket for BYOD Devices .....	439
2.18.2 Secure Shell (SSH) Access to IGEL OS with Keys .....	439
Generating the SSH Key Pair .....	440
Distributing the Public Key with UMS .....	441
Configuring SSH Access on the Device.....	442
2.18.3 Secure Terminal (Telnet with TLS/SSL) .....	443
2.18.4 Secure Shadowing (VNC with TLS/SSL).....	443
Basic Principles and Requirements.....	444
Shadow Devices Securely .....	445
VNC Logging .....	445
2.18.5 Cherry eGK Channel Substitution .....	446
Using the G87-1504/ST-1503 with firmware version 10.05.100 and higher: .....	446
2.18.6 Single Sign-on for the Browser Proxy .....	448
2.18.7 Limiting the Number of Permitted Login Attempts.....	452
Symptom .....	452
Problem .....	452
Solution .....	452
2.18.8 How to Deploy Device Encryption.....	452
Overview .....	452



Instructions .....	452
2.18.9 Security: Timeout for Secure Shadowing and Secure Terminal.....	456
Overview.....	456
Configuring the Timeout.....	456
2.19 Certificates .....	457
2.19.1 Certificate Enrollment and Renewal with SCEP (NDES).....	457
Requirements.....	457
Technical Background .....	458
Client Enrollment Details.....	460
Configuration of the SCEP Client.....	461
Files Involved.....	467
Troubleshooting.....	468
2.19.2 Deploying Trusted Root Certificates .....	470
Purpose.....	470
Requirements.....	470
Solution .....	470
Deploying Certificates via UMS.....	471
Installing Certificates Manually .....	472
2.19.3 Which CA Certificates Are Contained in IGEL OS?.....	474
2.20 Smartcard.....	484
2.20.1 Authentication with IGEL Smartcard .....	485
Prerequisites .....	485
Creating IGEL Smartcard Folders .....	486
Folder "Smartcard Operation" .....	486
Folder "Smartcard Creation".....	487
Writing the IGEL Smartcard .....	487
Smartcard Readers Supported by IGEL Smartcards .....	491
2.20.2 Smartcard Authentication .....	492
Certificate Authentication .....	492
Smartcard Readers .....	492
PC/SC Resource Manager .....	492
Smartcard Middleware .....	493
Active Directory Logon with Smartcard .....	494
Citrix StoreFront.....	494
RDP Sessions .....	495



Horizon Sessions .....	496
Smartcard Authentication in Browser .....	497
Local Login with Smartcard Certificate .....	498
2.21 Desktop and Display .....	512
2.21.1 Display Configuration for Shared Workplace (SWP) .....	512
Best practice.....	513
2.21.2 Display Switch .....	513
Configure a Starter for the Display Switch.....	513
Configure the Display Switch .....	514
Use the Display Switch.....	515
2.21.3 Multimonitor .....	517
Automatic Configuration .....	517
Manual Configuration .....	518
Additional Settings.....	521
Auto Switch Monitor Configuration for Laptops .....	524
2.21.4 Showing and Hiding the On-Screen Software Keyboard Automatically .....	526
Showing Automatically.....	526
Hiding Automatically .....	526
2.21.5 Overcoming the Restrictions of a Full-Screen Session with the in-Session Control Bar .....	527
Activating the in-session control bar: .....	527
Using the in-session control bar:.....	527
2.21.6 Screen Issues When Redocking Notebook.....	528
2.21.7 Using an External NVIDIA Graphics Card.....	528
Goal.....	528
Environment.....	528
Solution .....	529
2.22 Customizing.....	529
2.22.1 Custom Partition Tutorial.....	529
A First Simple Custom Partition .....	530
Packaging the Custom Partition .....	537
A Real-World CP: Chromium .....	549
Zoom as a Custom Partition .....	558
Microsoft Teams as a Custom Partition .....	573
2.22.2 Using a Custom PKCS#11 Library .....	588
Issue .....	588



Problem .....	588
Solution .....	589
2.22.3 Adding an Icon for Browsing Removable Storage .....	590
Symptom .....	590
2.22.4 Adding an Icon for the Image Viewer .....	591
Symptom .....	591
Problem .....	591
Solution .....	591
2.22.5 Creating a Timed Command (Cron Replacement) .....	593
2.22.6 Customizing IGEL OS Desktop .....	594
Introduction .....	595
Creating Your Own Wallpaper .....	597
Creating a New Bootsplash .....	599
Creating Your Own Screensaver .....	600
Assigning Your Own Company Logos .....	602
Creating Your Own Taskbar .....	604
Customizing Desktop Icons .....	604
2.22.7 How to Change the Font Color of the Desktop Icons .....	605
Overview .....	605
Environment .....	606
Instructions .....	606
2.22.8 How to Set up a Screensaver Countdown .....	607
Setting up a Countdown .....	607
Configuring a Conditional Countdown and Command .....	610
2.22.9 Installing a Calculator on IGEL Linux .....	611
2.22.10 Keyboard Shortcuts for Managing Windows .....	612
2.22.11 Make Frequent User Actions Easier by Defining Hotkeys .....	612
2.22.12 Shutdown/Suspend Devices Automatically at the End of a Session .....	614
Issue .....	614
Solution .....	614
2.22.13 Suspend to RAM - Wake Up by USB Mouse .....	615
Setting System Suspend as the Default Action .....	615
Configuring the BIOS for PS/2 Mouse and Keyboard .....	615
Configuring the BIOS for USB Mouse and Keyboard .....	616
Enabling the Wake-Up Functionality .....	616
2.22.14 Taking Screenshots on IGEL Linux .....	616



Issue .....	616
Solution .....	616
2.22.15 Setting the Device's System Time .....	617
Issue .....	617
Solution .....	617
2.22.16 Updating Timezone Information (Daylight Saving Time, DST).....	618
Symptom .....	618
Problem .....	618
Solution .....	618
2.22.17 Adding or Changing a MIME Type Handler.....	620
Symptom .....	620
Problem .....	620
Solution .....	620
2.22.18 Regional Settings in Sessions.....	623
Symptom .....	623
Problem .....	624
Solution .....	624
2.23 Devices.....	624
2.23.1 Monitor .....	625
Touchscreen Calibration .....	625
Touchscreen in Multimonitor Environment .....	636
USB-Powered ASUS Monitor and IGEL OS 11 .....	636
Solving Hotplugging Issues with DisplayPort Monitors .....	637
No Sound When Using a DisplayPort Monitor .....	637
Connecting Three DVI Monitors to UD7 with Passive DisplayPort Adapters.....	639
2.23.2 Using a Cherry SECURE BOARD .....	640
Overview .....	640
Prerequisites .....	640
Getting the Cherry SECURE BOARD to Work in Secure Mode .....	640
Getting the Certificates .....	640
Setting Up the Personalization Machine.....	653
Personalizing the Cherry SECURE BOARD .....	654
Setting Up the Endpoints.....	658
Resetting the Cherry SECURE BOARD to Its Original State .....	662
2.23.3 Webcam Redirection and Optimization.....	663



Overview .....	663
General Recommendations .....	664
Citrix .....	665
VMware Horizon .....	669
RDP .....	671
2.23.4 Webcam Information .....	673
2.23.5 Bluetooth Tool .....	674
2.23.6 How to Deploy a Jabra Xpress Package .....	677
Making the Jabra Xpress Package Available for Download .....	677
Configuring the Source URL .....	678
Triggering the Deployment Process .....	679
2.23.7 Connecting Signature Pads .....	681
2.23.8 Using a Kofax / Wacom Signature Pad .....	681
On the Device .....	681
On the VDI Server (Windows) .....	682
2.23.9 Using a StepOver Signature Pad .....	682
With StepOver TCP Client .....	682
With StepOver Signature Pad Channel .....	685
2.23.10 eGK/KVK - Card Reader .....	685
Cherry G80-1502 at the Serial Port .....	686
Cherry ST-2052 .....	687
Cherry ST-1503 und G87-1504 (USB) .....	688
Orga 910/920 M .....	689
Orga 6041 L eGK eHealth-BC S .....	690
celectronic CARD STAR / medic2 .....	691
celectronic CARD STAR/ memo3 .....	692
2.23.11 Using Mobile Device Access .....	692
Environment .....	693
Enabling Mobile Device Access .....	693
Disabling Mobile Device Access .....	694
Mapping a Mobile Device for a Session .....	694
Connecting Your Mobile Device .....	695
Accessing the Mobile Device USB Window from a Session .....	695
Viewing the Files and Directories Locally .....	696
Safely Removing the Mobile Device .....	697
2.23.12 Swapping Function of Mouse Buttons (e.g. When Using an Evoluent Mouse) .....	698



Problem .....	698
Solution A. To manually analyze the assignment and determine how it needs to be adjusted: .....	698
2.23.13 Connecting a Serial Barcode Scanner.....	699
Connecting Barcode Scanner via COM Port .....	699
Connecting Barcode Scanner via USB .....	700
2.23.14 Using DriveLock with IGEL Devices .....	701
Issue.....	701
Problem.....	701
Solution .....	701
2.23.15 Restricting the Mounting of Hotplug Storage Devices on IGEL Linux.....	702
Goal:.....	702
Solution: .....	702
2.23.16 When to Use USB Redirection .....	703
Document Purpose .....	703
Best Practices for USB Redirection .....	703
Example: Redirecting a Nuance Powermic (Dictaphone) .....	704
2.23.17 How to Configure USB Access Control .....	706
Enable USB Access Control.....	706
Create a Class Rule.....	707
Create a Device Rule .....	707
Example .....	707
2.23.18 Issues with USB IDs in USB Devices Rules.....	708
Symptom .....	708
Problem .....	708
Solution .....	709
2.23.19 How Can I Fix Touchpad Issues? .....	710
Overview .....	710
Issues and Solutions .....	710
2.24 Printer .....	712
2.24.1 CUPS: Mapping Local Printer to Citrix or RDP Sessions .....	712
Issue.....	712
Problem .....	712
Solution .....	712
2.24.2 Print Server Configuration.....	712
Prerequisites .....	712



Recommendation .....	713
Instructions .....	713
2.24.3 Installing a Custom CUPS Driver .....	714
Environment.....	714
Issue.....	714
Solution .....	714
2.25 UD Pocket .....	715
2.25.1 Running IGEL OS from UD Pocket on a Dell WYSE ZX0D (aka 7010) Device .....	715
2.25.2 Running UD Pocket on an Acer Chromebook C910 .....	716
Enabling Your Device to Boot from UD Pocket.....	716
2.25.3 UD Pocket Seems to Break Microsoft Surface .....	717
Tested Environment .....	717
Issue.....	717
Solution .....	717
2.25.4 How to Boot from the UD Pocket on Mac mini, MacBook Air 2018, MacBook Pro.....	719
Environment.....	719
Problem .....	719
Solution .....	719
2.26 Miscellaneous.....	719
2.26.1 Sending Device Log Files to IGEL Support .....	720
With UMS .....	720
Without UMS.....	725
2.26.2 Exporting the Local Device Configuration .....	727
Issue .....	727
Solution .....	727
2.26.3 Which Unified Communication Solutions Does IGEL OS Support? .....	729
Hardware .....	729
Virtual Desktop Optimizations .....	729
Local Installation on the Endpoint Device with a Custom Partition .....	730
2.26.4 Passthrough Authentication.....	730
Introduction .....	730
Basic configuration .....	732
Session Configuration.....	735
2.26.5 Hardware Video Acceleration on IGEL OS.....	736
Question .....	736



Answer .....	736
2.26.6 Running Commands before or after a Session .....	739
2.26.7 Copy Sessions in Setup or UMS .....	741
2.26.8 IZ1 and UD2-MM Usage of RAM.....	742
2.26.9 Using Symantec Ghost to Deploy IGEL OS.....	742
Topic of discussion/Issue.....	742
Firmware version .....	742
UMS version.....	742
Description .....	742
Solution .....	742
2.26.10 Starting UMS Console Crashes NX Session .....	744
2.26.11 Accessing IGEL Setup within Appliance Mode.....	744
Symptom .....	744
Problem .....	744
Solution .....	744
2.26.12 Application Is Terminated with Message "Low memory! Killing process ..." .....	745
Symptom .....	745
Environment.....	745
Problem .....	745
Solution .....	745
2.26.13 An Application Window Cannot Be Repositioned .....	745
Symptom .....	745
Problem .....	746
Solution .....	746
2.26.14 Updating IGEL UMD: Error "not compatible with System5" .....	747
Symptom .....	747
Solution .....	748
2.26.15 Using Natural Scrolling (reverse Scrolling Direction).....	748
Issue.....	748
Problem .....	748
Solution .....	748
2.26.16 IGEL Third-party Endpoint Partners: Ensuring Image Integrity with a Checksum .....	749
Overview .....	749
Requirements.....	749
Instructions .....	749



<b>3</b>	<b>IGEL OS Reference Manual .....</b>	<b>750</b>
3.1	What Is New in 11.06.100? .....	750
3.1.1	Login with Local User Password.....	750
3.1.2	Names of Ethernet and WLAN Interfaces Changed .....	750
3.1.3	Automatic Switch between LAN/Wi-Fi .....	750
3.1.4	Support for EAP-FAST .....	751
3.1.5	Proxy Settings .....	751
3.1.6	A Post-Session Command for Multiple Sessions .....	751
3.1.7	Remote Management.....	751
3.1.8	AVD: CUPS Printer Redirection .....	751
3.1.9	TLS Encryption for Remote Syslog .....	751
3.1.10	AppliDis Sessions .....	751
3.1.11	Amazon WorkSpaces Sessions .....	751
3.1.12	Parallels Client .....	752
3.1.13	Imprivata .....	752
3.1.14	RD Web Access.....	752
3.1.15	Chromium Browser .....	752
3.1.16	Device Encryption .....	752
3.1.17	Security: Timeout for Port 30022 (Secure Shadowing and Secure Terminal) .....	752
3.1.18	Configurable Default Web Browser .....	752
3.1.19	Conky System Monitor Added .....	752
3.1.20	Suppressing Enterprise Management Pack Expiration Warnings .....	753
3.1.21	Zoom Client Selection .....	753
3.1.22	Cisco WebEx Meetings VDI Client Selection .....	753
3.1.23	Wildcard in Horizon Client USB Redirection Rules.....	753
3.1.24	Registry Parameters for Fixing Touchpad Issues .....	753
3.1.25	Automatic Update Service for Evaluation Purposes .....	753
3.2	IGEL Workspace Edition.....	753
3.2.1	Supported Formats and Codecs.....	754
3.2.2	IGEL Devices Supported by IGEL OS 11.....	755
	IGEL UD (Universal Desktop) .....	755
	IGEL Zero .....	755
3.3	Bluetooth Assistant.....	756
3.3.1	Bluetooth Tool: .....	756
3.3.2	USB Access Control:.....	756



3.3.3	Bluetooth.....	756
3.4	Setup Assistant.....	757
3.4.1	Overview.....	757
3.4.2	Buttons .....	757
3.4.3	Language .....	757
3.4.4	Keyboard Layout.....	758
3.4.5	Time Zone Continent/Area .....	758
3.4.6	Time and Date .....	758
3.4.7	Mobile Broadband.....	758
3.4.8	Wireless.....	759
3.4.9	Connectivity .....	759
3.4.10	Local Logon .....	759
3.4.11	Activate Your IGEL OS .....	760
	Install License via UMS/ICG .....	760
	Manual License Deployment .....	760
	Register for Demo License .....	761
	Troubleshooting: Proxy Configuration .....	761
3.4.12	ICG Agent Setup .....	761
3.4.13	Finish .....	762
3.5	Boot Procedure .....	762
3.5.1	Boot Menu .....	762
	Quiet Boot .....	762
	Verbose Boot .....	762
	Emergency Boot.....	763
	Failsafe Boot - CRC Check.....	763
	Reset to Factory Defaults.....	763
	Custom Boot Command .....	764
3.5.2	Network Integration.....	765
3.5.3	X-Server .....	765
3.6	The IGEL OS Desktop .....	765
3.6.1	Application Launcher.....	768
3.6.2	Sessions .....	770
3.6.3	System .....	770
3.6.4	License.....	771
3.6.5	About Window .....	771



3.6.6	Restart and Shutdown .....	772
3.7	Setup.....	772
3.7.1	Starting the Setup .....	772
3.7.2	End the Setup .....	773
3.7.3	Quick Setup .....	773
3.7.4	Setup Search .....	774
3.8	Sessions .....	774
3.8.1	Copy Session .....	775
3.8.2	Global Session Options.....	775
3.8.3	Citrix.....	776
	Citrix Client Selection.....	776
	Citrix Global .....	776
	Citrix StoreFront.....	798
	Citrix Self-Service .....	807
3.8.4	RDP Global.....	811
	Gateway .....	811
	Local Logon .....	812
	Window .....	813
	Keyboard .....	815
	Mapping .....	815
	Performance.....	820
	Options .....	823
	Native USB Redirection.....	823
	Fabulatech USB Redirection.....	825
	Fabulatech Scanner Redirection .....	827
	Multimedia .....	827
3.8.5	RDP Session.....	828
	Server.....	828
	Gateway .....	829
	Logon .....	830
	Window .....	830
	Keyboard .....	831
	Mapping .....	832
	Performance.....	833
	Options .....	834



USB Redirection .....	834
Multimedia .....	834
Desktop Integration .....	835
3.8.6 Remote Desktop Web Access .....	837
Starting Methods for Session .....	837
Server .....	839
Authentication .....	842
Appearance .....	843
Logoff .....	843
Desktop Integration .....	845
3.8.7 Horizon Client Global .....	847
Server Options .....	848
Local Logon .....	849
Window .....	850
USB Redirection .....	851
Fabulatech USB Redirection .....	852
Fabulatech Scanner Redirection .....	855
Serial Port Redirection .....	855
Drive Mapping .....	855
Multimedia .....	856
Performance .....	857
Smartcard .....	857
Unified Communications .....	858
3.8.8 Horizon Client Session .....	860
Starting Methods for Session .....	860
Connection Settings .....	862
Window .....	863
Mouse and Keyboard .....	864
Mapping .....	864
Performance .....	865
Options .....	866
Multimedia .....	866
Proxy .....	867
Desktop Integration .....	867
3.8.9 Appliance Mode .....	869
VMware Horizon .....	870



Browser.....	871
Citrix Self-Service .....	871
RHEV/Spice.....	872
Imprivata .....	872
RDP MultiPoint Server.....	874
XDMCP for This Display .....	875
3.8.10 AppliDis.....	875
Connection .....	875
Options .....	876
Desktop Integration.....	878
3.8.11 Evidian AuthMgr .....	880
Evidian AuthMgr Global .....	880
Evidian AuthMgr Session .....	882
3.8.12 NoMachine NX Client .....	887
Starting Methods for Session .....	887
Server.....	889
Unix Desktop .....	890
Unix Display.....	891
Windows Desktop .....	892
Windows Display .....	893
VNC Desktop.....	894
VNC Display .....	894
Shadow Display.....	895
Logon .....	896
Advanced .....	897
Services.....	898
Desktop Integration.....	898
3.8.13 X Sessions .....	901
Starting Methods for Session .....	901
Server.....	903
Desktop Integration .....	904
3.8.14 Parallels Client Global.....	907
Keyboard .....	907
USB Redirection .....	907
3.8.15 Parallels Client Session.....	908
Starting Methods for Session .....	909



Connection .....	911
Display .....	912
Local Resources .....	913
Experience .....	914
Network .....	915
Advanced .....	915
Desktop Integration .....	916
3.8.16 PowerTerm Selection .....	918
3.8.17 PowerTerm Session .....	919
Desktop Integration .....	919
3.8.18 IBM iAccess Client.....	921
iAccess Global.....	921
IBM iAccess Session.....	923
3.8.19 ThinLinc Global .....	933
Server.....	933
Window .....	933
Options .....	934
Optimization .....	935
VNC Optimization.....	935
3.8.20 ThinLinc Session .....	936
Starting Methods for Session .....	936
Server.....	938
Login .....	939
Window .....	940
Options .....	941
Optimization .....	942
VNC Optimization.....	942
User Interface .....	943
Desktop Integration .....	944
3.8.21 SSH Session .....	946
Starting Methods for Session .....	946
Command .....	948
Options .....	949
Desktop Integration .....	949
3.8.22 VNC Viewer Sessions .....	951
Starting Methods for Session .....	952



Connection .....	954
Compression .....	954
Input .....	954
Misc .....	955
Desktop Integration .....	955
3.8.23 Firefox Browser Global.....	957
Tabs .....	958
Content.....	959
Print .....	960
Proxy .....	961
Privacy .....	963
Security.....	965
Advanced.....	965
Encryption .....	968
Certificates .....	968
Smartcard Middleware .....	969
Restart .....	970
Window.....	970
Menus & Toolbars.....	971
Hotkeys.....	974
Context .....	975
Commands .....	976
3.8.24 Firefox Browser Session.....	978
Starting Methods for Session .....	978
Settings.....	980
Desktop Integration .....	980
Plugins .....	982
3.8.25 Chromium Browser Global .....	982
General .....	983
Content.....	984
Proxy .....	984
Privacy .....	985
Security.....	987
Encryption .....	987
Menus & Toolbars.....	987
Window.....	988



Custom Setup.....	988
Smartcard Middleware .....	989
3.8.26 Chromium Sessions .....	990
Starting Methods for Session .....	990
Settings.....	992
Desktop Integration .....	992
3.8.27 Media Player Global .....	994
Window.....	994
Playback .....	995
Video .....	996
Options .....	996
3.8.28 Media Player Session .....	997
Starting Methods for Session .....	997
Playback .....	999
Options .....	1000
Desktop Integration .....	1000
3.8.29 VoIP Client .....	1002
Starting Methods for Session .....	1002
Account.....	1004
Audio.....	1006
SIP .....	1007
H.323.....	1007
Call Options.....	1008
Phone Book .....	1008
Preferences.....	1009
Desktop Integration .....	1009
3.8.30 Teradici PCoIP Session .....	1011
Connection Settings.....	1012
Login .....	1012
Window .....	1012
Desktop Integration .....	1013
3.8.31 AVD Global .....	1015
Plugins .....	1015
3.8.32 AVD Session .....	1018
Starting Methods for Session .....	1018
Logon .....	1020



Options .....	1021
Proxy .....	1022
Display .....	1022
Printing .....	1023
Plugins .....	1024
Desktop Integration .....	1024
3.8.33 Amazon WorkSpaces .....	1026
Starting Methods for Session .....	1027
Connection Settings.....	1029
Local Settings.....	1029
Network Settings.....	1029
Window.....	1029
Desktop Integration .....	1030
3.8.34 deskMate Session.....	1032
Starting Methods for Session .....	1032
Provider .....	1034
Options .....	1034
Network .....	1035
Desktop Integration .....	1035
3.8.35 Unified Communications.....	1037
Zoom Client Selection .....	1037
Cisco WebEx Meetings VDI Selection.....	1037
3.9 Accessories .....	1038
3.9.1 ICA Connection Center.....	1038
Starting Methods for Session .....	1039
Using ICA Connection Center .....	1041
3.9.2 Terminals.....	1042
Starting Methods for Session .....	1042
Using Local Terminal .....	1044
3.9.3 Change Smartcard Password .....	1044
Starting Methods for Session .....	1045
Using Change Smartcard Password Function .....	1046
3.9.4 Change Password.....	1047
Starting Methods for Session .....	1047
Using Change Password Function.....	1049



3.9.5	Setup.....	1049
	Starting Methods for Session .....	1049
	Setup User Permissions.....	1051
	Setup Administrator Permissions .....	1052
	Options .....	1053
3.9.6	Quick Settings .....	1053
	Starting Methods for Session .....	1053
	Setup User Permissions.....	1055
3.9.7	Display Switch .....	1055
	Starting Methods for Session .....	1055
	Options .....	1057
	Minimal Dialog.....	1059
	Advanced Dialog .....	1060
	Using Display Switch.....	1061
3.9.8	Application Launcher.....	1063
	Starting Methods for Session .....	1063
	Application Launcher Configuration.....	1065
3.9.9	Sound Preferences.....	1066
	Starting Methods for Session .....	1066
	Options .....	1069
	Using Sound Preferences Function .....	1070
3.9.10	System Log Viewer .....	1070
	Starting Methods for Session .....	1071
	Options .....	1073
	Using System Log Viewer Function .....	1073
3.9.11	UMS Registration.....	1073
	Starting Methods for Session .....	1074
	Using UMS Registration Function.....	1075
3.9.12	Touchscreen Calibration .....	1076
	Starting Methods for Session .....	1076
	Using Touchscreen Calibration .....	1078
3.9.13	Task Manager .....	1078
	Starting Methods for Session .....	1079
	Using Task Manager .....	1081
3.9.14	Screenshot Tool .....	1084
	Starting Methods for Session .....	1085



Special Hotkeys.....	1087
Using Screenshot Tool .....	1087
3.9.15 On-Screen Keyboard.....	1088
Starting Methods for Session .....	1088
Appearance .....	1089
Application Integration.....	1090
3.9.16 Monitor Calibration.....	1091
Starting Methods for Session .....	1091
3.9.17 Commands .....	1093
3.9.18 Network Tools .....	1095
Starting Methods for Session .....	1096
Using Network Tools Function .....	1099
3.9.19 Bluetooth Tool .....	1100
Starting Methods for Session .....	1100
Using Bluetooth Tool .....	1102
3.9.20 System Information .....	1105
Starting Methods for Session .....	1106
Using System Information Function .....	1108
3.9.21 Disk Utility .....	1109
Starting Methods for Session .....	1109
Using Disk Utility .....	1111
3.9.22 Disk Removal.....	1112
Starting Methods for Session .....	1112
3.9.23 Mobile Device Access .....	1114
Starting Methods for Session .....	1114
3.9.24 Firmware Update .....	1116
Starting Methods for Session .....	1117
Using Firmware Update Function .....	1119
3.9.25 Smartcard Personalization.....	1119
Starting Methods for Session .....	1119
Using Smartcard Personalization Function.....	1121
3.9.26 Identify Monitors.....	1122
Starting Methods for Session .....	1122
Using Identify Monitors Function.....	1124
3.9.27 Webcam Information .....	1125
Starting Methods for Session .....	1125



Using Webcam Information .....	1127
3.9.28 ICG Agent Setup .....	1127
Starting Methods for Session .....	1128
Using ICG Agent Setup .....	1130
3.9.29 Licensing .....	1130
3.9.30 Login Enterprise .....	1133
Login Enterprise Launcher .....	1133
3.9.31 Connector ID Key Software .....	1133
3.9.32 OS 11 Upgrade .....	1134
3.9.33 Conky System Monitor .....	1136
Starting Methods for Session .....	1137
Options .....	1139
Custom Setup .....	1140
3.10 User Interface .....	1142
3.10.1 Display .....	1142
Screen Configuration .....	1142
Advanced .....	1143
Power Options .....	1144
Access Control .....	1144
Gamma Correction .....	1145
Options .....	1145
3.10.2 Desktop .....	1146
Desktop fonts .....	1146
Background .....	1147
Taskbar .....	1149
Taskbar Background .....	1151
Taskbar Items .....	1151
Pager .....	1152
Start Menu .....	1153
In-Session Control Bar .....	1154
3.10.3 Language .....	1155
3.10.4 Screenlock / Screensaver .....	1155
Starting Methods for Session .....	1155
Options .....	1157
Taskbar .....	1159



Screensaver .....	1160
3.10.5 Input .....	1161
Keyboard .....	1161
Additional Keyboard Layouts .....	1162
Mouse .....	1162
Touchpad .....	1163
Touchscreen .....	1165
Signature Pad .....	1167
3.10.6 Hotkeys .....	1167
Commands .....	1167
3.10.7 Font Services .....	1170
XC Font Service .....	1170
NFS Font Service .....	1171
3.11 Network .....	1171
3.11.1 LAN Interfaces .....	1172
Individual Interface .....	1173
Wireless .....	1178
3.11.2 Mobile Broadband .....	1186
3.11.3 DHCP Client .....	1187
Default Options .....	1188
User-Defined Options .....	1188
3.11.4 VPN .....	1189
OpenVPN .....	1189
NCP VPN Client .....	1197
OpenConnect VPN .....	1199
genucard .....	1202
3.11.5 SCEP Client (NDES) .....	1207
Certificate .....	1208
Certification Authority .....	1209
SCEP .....	1209
3.11.6 Routing .....	1210
Routing [1-5] .....	1211
3.11.7 Hosts .....	1211
Add .....	1212
3.11.8 Network Drives .....	1212



NFS.....	1212
Windows Drive.....	1213
3.11.9 Proxy .....	1214
3.12 Devices.....	1215
3.12.1 Printer.....	1216
CUPS .....	1216
LPD.....	1222
TCP/IP .....	1222
ThinPrint.....	1225
PrinterLogic.....	1226
3.12.2 Storage Devices.....	1228
Storage Hotplug.....	1228
Options .....	1230
DriveLock.....	1231
3.12.3 Bluetooth.....	1231
3.12.4 USB Access Control .....	1231
Class Rules.....	1232
Device Rules .....	1232
3.12.5 Unified Communications.....	1233
Jabra.....	1233
EPOS Audio.....	1234
3.13 Security.....	1235
3.13.1 Device Encryption .....	1235
3.13.2 Password .....	1236
Administrator .....	1237
Setup Administrator .....	1238
Setup User .....	1238
User.....	1238
User account for remote access .....	1239
3.13.3 Logon .....	1239
IGEL Smartcard .....	1239
Taskbar .....	1240
Active Directory/Kerberos .....	1242
Shared Workplace .....	1244
Local User .....	1246



3.13.4	Active Directory/Kerberos .....	1247
	Domain 1 ... Domain 4.....	1248
	Domain Realm Mapping .....	1248
3.13.5	Smartcard.....	1249
	Services.....	1249
	Middleware.....	1250
3.14	System .....	1251
3.14.1	Time and Date .....	1252
3.14.2	Update .....	1252
	Firmware Update .....	1252
	Buddy Update .....	1254
3.14.3	Remote Management.....	1254
	Options .....	1256
3.14.4	Remote Access .....	1256
	SSH Access.....	1257
	Shadow.....	1258
	Secure Terminal .....	1259
3.14.5	Logging .....	1259
	Remote Mode Switched to "Server" .....	1260
	Remote Mode Switched to "Client" .....	1260
3.14.6	Power Options.....	1261
	System .....	1261
	Battery .....	1262
	Screen .....	1263
	Shutdown .....	1263
3.14.7	Firmware Customization .....	1264
	Custom Partition .....	1264
	Custom Application .....	1267
	Custom Commands .....	1272
	Corporate Design .....	1275
	Environment Variables .....	1280
	Features .....	1281
3.14.8	Registry .....	1282
4	UD Pocket (UDP) Reference Manual.....	1284
4.1	IGEL TechChannel .....	1284



4.2	General Information.....	1284
4.3	Devices Supported by OSC and UD Pocket.....	1284
4.3.1	Core Requirements .....	1284
4.3.2	Devices Officially Supported by OSC and UD Pocket with IGEL OS 11 .....	1285
	ADS-Tec .....	1285
	Advantech.....	1286
	Advantech-DLoG .....	1286
	Dell / Wyse .....	1286
	Elo .....	1287
	Fujitsu .....	1287
	HP .....	1287
	Intel.....	1288
	Lenovo .....	1288
	LG .....	1288
	OnLogic.....	1289
	Onyx Healthcare.....	1289
	Rein Medical .....	1289
	Secunet.....	1290
	Toshiba .....	1290
4.3.3	USB Memory Sticks That Can Be Used as Alternative UD Pocket Hardware .....	1290
	DIGITTRADE .....	1290
4.3.4	Officially Supported Virtual Environments.....	1291
4.4	Setup and Startup .....	1291
4.4.1	Requirements.....	1291
4.4.2	Boot Settings.....	1291
4.4.3	Starting Your UD Pocket .....	1292
	The First Boot Procedure.....	1292
	Should the UD Pocket Boot-Up Fail .....	1292
	After the First Boot-Up .....	1292
5	IGEL OS Creator.....	1293
5.1	IGEL OS Creator Manual.....	1293
5.1.1	General Information.....	1293
5.1.2	Devices Supported by IGEL OS 11 .....	1293
	IGEL Devices .....	1293
	IGEL UD (Universal Desktop) .....	1293



IGEL Zero .....	1294
Third-Party Devices.....	1295
5.1.3 Licensing.....	1295
5.1.4 Installation .....	1295
Create USB installation medium (Windows) .....	1295
Create USB installation medium (Linux).....	1298
Create DVD installation medium .....	1299
Boot Settings.....	1299
Installation Procedure .....	1302
Installation Procedure for Factory Images .....	1314
5.2 IGEL OS Creator Articles.....	1328
5.2.1 Café Wireless (Wi-Fi).....	1328
5.2.2 Reduce CPU Power Consumption .....	1332
5.2.3 Installing UDC3 on Secunet SINA Workstation .....	1333
5.2.4 Setting up UDC3 on Mobile Devices .....	1335
Multi Monitor Environment .....	1335
Presentation Mode.....	1335
Display Brightness.....	1336
Power Management.....	1337
Wireless Manager (Café Wireless).....	1338
Shortening Network Timeouts in Mobile Scenarios.....	1339
Battery Level Control .....	1340
<b>6 IGEL OS Creator for Windows (OSCW).....</b>	<b>1342</b>
6.1 IGEL OS Creator for Windows (OSCW) on Windows 7/10 Workstations .....	1342
6.1.1 Introduction .....	1342
6.1.2 Video .....	1342
Part I.....	1342
Part II.....	1343
6.1.3 Prerequisites .....	1343
Hardware.....	1343
Software .....	1343
Network .....	1343
Next Step .....	1343
6.1.4 Getting the Required Software.....	1343
IGEL Universal Management Suite (UMS) 6.04.120 or Higher .....	1344



OSCW Files.....	1344
Check List .....	1344
Next Step .....	1344
6.1.5    Transferring the IGEL OSC File to the UMS .....	1344
Next Step .....	1345
6.1.6    Deploying the OSCW Installer on the Target Machines.....	1345
Check List .....	1345
Next Step .....	1345
6.1.7    Installing the OSCW Installer.....	1345
OSCW Installer Has Been Deployed via SCCM or Group Policy.....	1345
OSCW Installer Has Been Deployed from a File .....	1346
Check List .....	1348
Next Step .....	1348
6.1.8    Registering the Target Machines to the UMS.....	1348
Registering by a UMS Scan .....	1349
Registering by Automatic Registration .....	1350
Check List .....	1350
Next Step .....	1350
6.1.9    Configuring the OSCW Installer.....	1351
Configuring the OSCW Installer in Normal Mode .....	1351
Configuring the OSCW Installer in Buddy Mode .....	1364
6.1.10   Starting the Conversion.....	1381
6.2    IGEL OS Creator for Windows (OSCW) on IGEL Windows Embedded 7/7+.....	1382
6.2.1   Prerequisites .....	1383
Network .....	1383
Next Step .....	1383
6.2.2   Getting the Required Software.....	1383
IGEL Universal Management Suite (UMS) 6.04.120 or Higher .....	1383
IGEL OS 11 .....	1383
IGEL WES 7/7+ .....	1383
Check List .....	1383
Next Step .....	1383
6.2.3   Updating the IGEL WES7/7+ Devices.....	1384
Transferring the Snapshot File to the UMS.....	1384
Creating an Update Profile .....	1384



Starting the Update .....	1386
Check List .....	1389
Next Step .....	1389
6.2.4 Transferring the IGEL OS 11 Firmware to the UMS.....	1389
Check List .....	1389
Next Step .....	1389
6.2.5 Configuring the OSCW Installer.....	1389
Configuring the OSCW Installer in Normal Mode .....	1390
Configuring the OSCW Installer in Buddy Mode .....	1394
6.2.6 Starting the Conversion.....	1400
6.3 IGEL OS Creator for Windows (OSCW) on IGEL Windows 10 IoT .....	1401
6.3.1 Prerequisites .....	1402
Network .....	1402
Next Step .....	1402
6.3.2 Getting the Required Software.....	1402
IGEL Universal Management Suite (UMS) .....	1402
IGEL Windows 10 IoT .....	1402
Check List .....	1402
Next Step .....	1402
6.3.3 Starting the Conversion by Updating the Devices.....	1402
Transferring the Snapshot File to the UMS.....	1403
Creating an Update Profile .....	1403
Starting the Update .....	1405
6.4 IGEL OS SCCM Add-On .....	1408
6.4.1 Overview .....	1408
6.4.2 Short Video Summary .....	1408
6.4.3 Prerequisites .....	1408
6.4.4 Installing the IGEL OS SCCM Add-On.....	1409
6.4.5 Verifying the Installation.....	1412
6.4.6 Provisioning IGEL OS via a PXE Boot Environment .....	1413
6.4.7 Deploying an Alternative IGEL OS Image .....	1419
<b>7 IGEL OS Release Notes.....</b>	<b>1422</b>
7.1 Notes for Release 11.06.100.....	1422
7.1.1 IGEL OS 11 .....	1423
Supported Devices 11.06.100 .....	1423



Component Versions 11.06.100 .....	1425
General Information 11.06.100 .....	1432
Known Issues 11.06.100 .....	1432
Security Fixes 11.06.100 .....	1436
New Features 11.06.100 .....	1440
Resolved Issues 11.06.100 .....	1461
CA Certificates Contained in IGEL OS 11.06 .....	1467
7.1.2 IGEL OS Creator (OSC) .....	1477
Supported Devices .....	1477
Component Versions 11.06.100 .....	1477
New Features 11.06.100 .....	1479
Resolved Issues 11.06.100 .....	1479
7.2 Notes for Release 11.05.133 .....	1480
7.2.1 Supported Devices 11.05.133 .....	1480
7.2.2 Component Versions 11.05.133 .....	1481
Clients .....	1481
Dictation .....	1482
Signature .....	1483
Smartcard .....	1483
System Components .....	1484
VM Guest Support Components .....	1486
Features with Limited IGEL Support .....	1486
Services .....	1486
7.2.3 General Information 11.05.133 .....	1488
7.2.4 Known Issues 11.05.133 .....	1488
7.2.5 Security Fixes 11.05.133 .....	1491
7.2.6 New Features 11.05.133 .....	1491
7.2.7 Resolved Issues 11.05.133 .....	1493
7.3 Notes for Release 11.05.120 .....	1494
7.3.1 IGEL OS 11 .....	1495
Supported Devices 11.05.120 .....	1495
Component Versions 11.05.120 .....	1496
General Information 11.05.120 .....	1503
Known Issues 11.05.120 .....	1503
New Features 11.05.120 .....	1506



Resolved Issues 11.05.120 .....	1508
7.3.2 IGEL OS Creator (OSC).....	1510
Supported Devices.....	1510
Component Versions 11.05.120.....	1511
New Features 11.05.120.....	1512
Resolved Issues 11.05.120 .....	1512
7.4 Notes for Release 11.05.100.....	1512
7.4.1 IGEL OS 11 .....	1513
Supported Devices 11.05.100 .....	1513
Component Versions 11.05.100.....	1514
General Information 11.05.100.....	1520
Known Issues 11.05.100.....	1521
Security Fixes 11.05.100.....	1523
New Features 11.05.100.....	1527
Resolved Issues 11.05.100 .....	1538
CA Certificates Contained in IGEL OS 11.05 .....	1546
7.4.2 IGEL OS Creator (OSC).....	1554
Supported Devices .....	1554
Component Versions 11.05.100.....	1555
New Features 11.05.100 .....	1557
Resolved Issues 11.05.100 .....	1557
7.5 Notes for Release 11.04.270.....	1557
7.5.1 Supported Devices 11.04.270 .....	1558
7.5.2 Component Versions 11.04.270.....	1558
Clients.....	1558
Dictation .....	1560
Signature .....	1560
Smartcard .....	1560
System Components.....	1561
VM Guest Support Components .....	1563
Features with Limited IGEL Support .....	1563
Services.....	1564
7.5.3 General Information 11.04.270.....	1565
7.5.4 Known Issues 11.04.270 .....	1565
7.5.5 Security Fixes 11.04.270.....	1569



7.5.6	New Features 11.04.270 .....	1569
7.5.7	Resolved Issues 11.04.270 .....	1570
7.6	Notes for Release 11.04.240.....	1572
7.6.1	Supported Devices 11.04.240 .....	1572
7.6.2	Component Versions 11.04.240.....	1573
	Clients .....	1573
	Dictation .....	1575
	Signature .....	1575
	Smartcard.....	1575
	System Components.....	1576
	VM Guest Support Components .....	1578
	Features with Limited IGEL Support .....	1578
	Services.....	1578
7.6.3	General Information 11.04.240.....	1580
7.6.4	Known Issues 11.04.240 .....	1580
7.6.5	Security Fixes 11.04.240.....	1583
7.6.6	New Features 11.04.240 .....	1584
7.6.7	Resolved Issues 11.04.240 .....	1585
7.7	Notes for Release 11.04.200.....	1588
7.7.1	Supported Devices 11.04.200 .....	1588
7.7.2	Component Versions 11.04.200.....	1589
	Clients .....	1589
	Dictation .....	1590
	Signature .....	1591
	Smartcard.....	1591
	System Components.....	1592
	VM Guest Support Components .....	1593
	Features with Limited IGEL Support .....	1593
	Services.....	1594
7.7.3	General Information 11.04.200.....	1595
7.7.4	Known Issues 11.04.200 .....	1595
7.7.5	Security Fixes 11.04.200.....	1599
7.7.6	New Features 11.04.200 .....	1599
7.7.7	Resolved Issues 11.04.200 .....	1601
7.8	Notes for Release 11.04.100.....	1603



7.8.1	IGEL OS 11 .....	1603
	Supported Devices 11.04.100 .....	1604
	Component Versions 11.04.100 .....	1604
	General Information 11.04.100 .....	1610
	Known Issues 11.04.100 .....	1611
	Security Fixes 11.04.100 .....	1614
	New Features 11.04.100 .....	1615
	Resolved Issues 11.04.100 .....	1631
	CA Certificates Contained in IGEL OS 11.04.100 .....	1638
7.8.2	IGEL OS Creator (OSC) .....	1646
	Supported Devices .....	1646
	Component Versions 11.04.100 .....	1647
	General Information 11.04.100 .....	1653
	Known Issues 11.04.100 .....	1653
	Security Fixes 11.04.100 .....	1656
	New Features 11.04.100 .....	1657
	Resolved Issues 11.04.100 .....	1673
7.9	Notes for Release 11.03.500 .....	1680
7.9.1	IGEL OS 11 .....	1680
	Supported Devices 11.03.500 .....	1681
	Component Versions 11.03.500 .....	1681
	General Information 11.03.500 .....	1686
	Security Fixes 11.03.500 .....	1686
	Known Issues 11.03.500 .....	1687
	New Features 11.03.500 .....	1689
	Resolved Issues 11.03.500 .....	1693
7.9.2	IGEL OS Creator (OSC) .....	1696
	Supported Devices .....	1696
	Component Versions 11.03.500 .....	1697
	New Features 11.03.500 .....	1698
	Resolved Issues 11.03.500 .....	1698
7.10	Notes for Release 11.03.110 .....	1699
7.10.1	IGEL OS 11 .....	1699
	Supported Devices 11.03.110 .....	1700
	Component Versions 11.03.110 .....	1700



General Information 11.03.110.....	1705
Known Issues 11.03.110 .....	1705
Security Fixes 11.03.110.....	1708
New Features 11.03.110 .....	1708
Resolved Issues 11.03.110 .....	1709
7.10.2 IGEL OS Creator (OSC).....	1709
Supported Devices .....	1709
Component Versions 11.03.110 .....	1710
Resolved Issues 11.03.110 .....	1712
7.11 Notes for Release 11.03.100.....	1712
7.11.1 IGEL OS 11 .....	1712
Supported Devices 11.03.100 .....	1713
Component Versions 11.03.100.....	1713
General Information 11.03.100.....	1718
Security Fixes 11.03.100.....	1718
Known Issues 11.03.100 .....	1721
New Features 11.03.100 .....	1723
Resolved Issues 11.03.100 .....	1731
CA Certificates Contained in IGEL OS 11.03 .....	1733
7.11.2 IGEL OS Creator (OSC).....	1741
Supported Devices .....	1741
Component Versions 11.03.100.....	1741
New Features 11.03.100 .....	1743
7.12 Notes for Release 11.02.150.....	1743
7.12.1 Supported Devices 11.02.150 .....	1743
7.12.2 Component Versions 11.02.150.....	1744
7.12.3 General Information 11.02.150.....	1748
7.12.4 Security Fixes 11.02.150.....	1749
7.12.5 Known Issues 11.02.150.....	1752
7.12.6 New Features 11.02.150 .....	1754
7.12.7 Resolved Issues 11.02.150 .....	1754
7.13 Notes for Release 11.02.130.....	1755
7.13.1 Supported Devices 11.02.130 .....	1756
7.13.2 Component Versions 11.02.130.....	1756
7.13.3 General Information 11.02.130.....	1761



7.13.4	Security Fixes 11.02.130.....	1761
7.13.5	Known Issues 11.02.130 .....	1764
7.13.6	Resolved Issues 11.02.130 .....	1766
7.14	Notes for Release 11.02.100.....	1766
7.14.1	IGEL OS 11 .....	1766
	Supported Devices 11.02.100 .....	1767
	Component Versions 11.02.100.....	1767
	General Information 11.02.100.....	1772
	Security Fixes 11.02.100.....	1772
	Known Issues 11.02.100 .....	1775
	New Features 11.02.100.....	1777
	Resolved Issues 11.02.100 .....	1801
	CA Certificates Contained in IGEL OS 11.02.100 .....	1811
7.14.2	IGEL OS Creator (OSC).....	1814
	Supported Devices .....	1814
	Component Versions 11.02.100 .....	1815
	New Features 11.02.100 .....	1816
7.15	Notes for Release 11.01.130.....	1817
7.15.1	Supported Devices 11.01.130 .....	1817
7.15.2	Component Versions 11.01.130.....	1818
7.15.3	General Information 11.01.130.....	1822
7.15.4	Known Issues 11.01.130.....	1822
7.15.5	Security Fixes 11.01.130.....	1823
7.15.6	New Features 11.01.130 .....	1824
7.15.7	Resolved Issues 11.01.130 .....	1824
7.16	Notes for Release 11.01.120.....	1825
7.16.1	Supported Devices 11.01.120 .....	1825
7.16.2	Component Versions 11.01.120.....	1826
7.16.3	General Information 11.01.120.....	1830
7.16.4	Security Fixes 11.01.120.....	1830
7.16.5	New Features 11.01.120 .....	1830
7.16.6	Resolved Issues 11.01.120 .....	1831
7.17	Notes for Release 11.01.110.....	1832
7.17.1	Supported Devices 11.01.110 .....	1833
7.17.2	Component Versions 11.01.110.....	1833



7.17.3	General Information 11.01.110.....	1837
7.17.4	Security Fixes 11.01.110.....	1837
7.17.5	Known Issues 11.01.110.....	1838
7.17.6	New Features 11.01.110.....	1839
7.17.7	Resolved Issues 11.01.110 .....	1847
7.18	Notes for Release 11.01.100.....	1853
7.18.1	IGEL OS 11 .....	1854
	Supported Devices .....	1854
	Component Versions 11.01.100 .....	1854
	General Information 11.01.100.....	1859
	Known Issues 11.01.100 .....	1859
	New Features 11.01.100.....	1860
	CA Certificates Contained in IGEL OS 11.01.100 .....	1865
7.18.2	IGEL OS Creator (OSC).....	1869
	Supported Devices .....	1869
	General Information 11.01.100.....	1869
	Component Versions 11.01.100 .....	1869
7.19	Notes for Release 10.06.190.....	1871
7.20	Notes for Release 10.06.170.....	1871
7.20.1	IGEL Linux Universal Desktop.....	1871
	Supported Devices .....	1871
	Component Versions 10.06.170 .....	1872
	General Information 10.06.170.....	1877
	Security Fixes 10.06.170.....	1878
	Known Issues 10.06.170 .....	1878
	New Features 10.06.170.....	1880
	Resolved Issues 10.06.170 .....	1881
7.20.2	IGEL Universal Desktop OS 3 .....	1883
	Supported Hardware .....	1883
	Component Versions 10.06.170 .....	1883
	General Information 10.06.170.....	1887
	Security Fixes 10.06.170.....	1888
	Known Issues 10.06.170 .....	1889
	New Features 10.06.170.....	1890
	Resolved Issues 10.06.170 .....	1891



7.21 Notes for Release 10.06.130.....	1893
7.21.1 IGEL Linux Universal Desktop.....	1893
Supported Devices .....	1893
Component Versions 10.06.130 .....	1895
General Information 10.06.130.....	1899
Security Fixes 10.06.130.....	1900
Known Issues 10.06.130.....	1900
Resolved Issues 10.06.130 .....	1901
7.21.2 IGEL Universal Desktop OS 3 .....	1903
Component Versions 10.06.130.....	1903
General Information 10.06.130.....	1908
Security Fixes 10.06.130.....	1909
Known Issues 10.06.130.....	1909
New Features 10.06.130.....	1910
Resolved Issues 10.06.130 .....	1911
7.22 Notes for Release 10.06.120.....	1912
7.22.1 IGEL Linux Universal Desktop.....	1913
Supported Devices .....	1913
Component Versions 10.06.120 .....	1914
General Information 10.06.120.....	1918
Security Fixes 10.06.120.....	1919
Known Issues 10.06.120.....	1923
New Features 10.06.120.....	1925
Resolved Issues 10.06.120 .....	1925
7.22.2 IGEL Universal Desktop OS 3 .....	1925
Component Versions 10.06.120.....	1926
General Information 10.06.120.....	1930
Security Fixes 10.06.120.....	1931
Known Issues 10.06.120.....	1935
New Features 10.06.120.....	1937
Resolved Issues 10.06.120 .....	1937
7.23 Notes for Release 10.06.110.....	1938
7.23.1 IGEL Linux Universal Desktop.....	1938
Supported Devices .....	1938
Component Versions 10.06.110 .....	1939



General Information 10.06.110.....	1943
Known Issues 10.06.110 .....	1944
Security Fixes 10.06.110.....	1946
New Features 10.06.110 .....	1946
Resolved Issues 10.06.110 .....	1947
7.23.2 IGEL Universal Desktop OS 3 .....	1947
Component Versions 10.06.110.....	1947
General Information 10.06.110.....	1952
Known Issues 10.06.110 .....	1953
Security Fixes 10.06.110.....	1954
New Features 10.06.110 .....	1955
Resolved Issues 10.06.110 .....	1955
7.24 Notes for Release 10.06.100.....	1955
7.24.1 IGEL Linux Universal Desktop.....	1956
Supported Devices .....	1956
Component Versions 10.06.100 .....	1957
General Information 10.06.100.....	1961
Security Fixes 10.06.100.....	1962
Known Issues 10.06.100 .....	1966
New Features 10.06.100 .....	1967
Resolved Issues 10.06.100 .....	1988
7.24.2 IGEL Universal Desktop OS 3 .....	1996
Component Versions 10.06.100.....	1996
General Information 10.06.100.....	2000
Security Fixes 10.06.100.....	2001
Known Issues 10.06.100 .....	2005
New Features 10.06.100 .....	2007
Resolved Issues 10.06.100 .....	2029
7.25 Notes for Release 10.05.830.....	2036
7.25.1 IGEL Linux Universal Desktop.....	2036
Supported Devices .....	2036
Component Versions 10.05.830.....	2038
General Information 10.05.830.....	2042
Known Issues 10.05.830 .....	2043
New Features 10.05.830 .....	2044



Resolved Issues 10.05.830 .....	2053
Security Fixes 10.05.830.....	2057
7.25.2 IGEL Universal Desktop OS 3 .....	2057
Component Versions 10.05.830.....	2058
General Information 10.05.830.....	2062
Known Issues 10.05.830.....	2063
New Features 10.05.830.....	2064
Resolved Issues 10.05.830 .....	2073
Security Fixes 10.05.830.....	2077
7.26 Notes for Release 10.05.800.....	2078
7.26.1 IGEL Linux Universal Desktop.....	2078
Supported Devices .....	2078
Component Versions 10.05.800.....	2079
General Information 10.05.800.....	2083
Known Issues 10.05.800.....	2084
New Features 10.05.800 .....	2086
Resolved Issues 10.05.800 .....	2089
7.26.2 IGEL Universal Desktop OS 3 .....	2092
Component Versions 10.05.800.....	2092
General Information 10.05.800.....	2096
Known Issues 10.05.800.....	2097
New Features 10.05.800 .....	2099
Resolved Issues 10.05.800 .....	2106
7.27 Notes for Release 10.05.700.....	2110
7.27.1 IGEL Linux Universal Desktop.....	2111
Supported Devices .....	2111
Component Versions 10.05.700.....	2112
General Information 10.05.700.....	2116
Known Issues 10.05.700.....	2117
New Features 10.05.700 .....	2118
Resolved Issues 10.05.700 .....	2125
7.28 Notes for Release 10.05.500.....	2128
7.28.1 IGEL Linux Universal Desktop.....	2129
Supported Devices .....	2129
Component Versions 10.05.500 .....	2130



General Information 10.05.500.....	2134
Known Issues 10.05.500 .....	2135
New Features 10.05.500 .....	2136
Resolved Issues 10.05.500 .....	2143
7.28.2 IGEL Universal Desktop OS3/IGEL UD Pocket.....	2146
Component Versions 10.05.500 .....	2146
General Information 10.05.500.....	2151
Known Issues 10.05.500 .....	2151
New Features 10.05.500 .....	2153
Resolved Issues 10.05.500 .....	2159
7.28.3 IGEL Universal Desktop Converter (UDC3).....	2163
Component Versions 10.05.500 .....	2163
New Features 10.05.500 .....	2164
7.29 Notes for Release 10.05.100.....	2164
7.29.1 IGEL Linux Universal Desktop.....	2165
Supported Devices .....	2165
Component Versions 10.05.100 .....	2166
General Information 10.05.100.....	2171
Security Fixes 10.05.100.....	2171
Known Issues 10.05.100 .....	2176
New Features 10.05.100 .....	2177
Resolved Issues 10.05.100 .....	2205
7.29.2 IGEL Universal Desktop OS3/IGEL UD Pocket.....	2212
Versions 10.05.100.....	2212
General Information 10.05.100.....	2217
Security Fixes 10.05.100.....	2217
Known Issues 10.05.100 .....	2222
New Features 10.05.100 .....	2223
Resolved Issues 10.05.100 .....	2251
7.29.3 IGEL Universal Desktop Converter (UDC3).....	2258
Versions 10.05.100.....	2258
New Features 10.05.100 .....	2260
7.30 Notes for Release 10.04.100.....	2260
7.30.1 IGEL Linux Universal Desktop 10.04.100 .....	2261
Supported Devices .....	2261



Versions for Release 10.04.100 .....	2262
General Information 10.04.100.....	2266
Security Fixes 10.04.100.....	2267
Known Issues 10.04.100 .....	2270
New Features 10.04.100 .....	2271
Resolved Issues 10.04.100 .....	2283
7.30.2 IGEL Universal Desktop OS3/IGEL UD Pocket 10.04.100.....	2286
Versions for Release 10.04.100 .....	2286
General Information 10.04.100.....	2290
Security Fixes 10.04.100.....	2291
Known Issues 10.04.100 .....	2294
New Features 10.04.100 .....	2296
Resolved Issues 10.04.100 .....	2308
7.30.3 IGEL Universal Desktop Converter (UDC3) 10.04.100.....	2310
Versions for Release 10.04.100 .....	2311
New Features 10.04.100 .....	2312
7.31 Notes for Release 10.03.570.....	2324
7.31.1 IGEL Universal Desktop LX / IGEL Zero 10.03.570.....	2325
Supported Devices .....	2325
Versions for Release 10.03.570 .....	2326
Security Fixes 10.03.570.....	2329
General Information 10.03.570.....	2330
Known Issues 10.03.570 .....	2331
7.31.2 IGEL Universal Desktop OS 3 / IGEL UD Pocket 10.03.570.....	2332
Versions for Release 10.03.570 .....	2332
Security Fixes 10.03.570.....	2336
General Information 10.03.570.....	2336
Known Issues 10.03.570 .....	2337
7.32 Notes for Release 10.03.550.....	2338
7.32.1 IGEL Universal Desktop / IGEL Zero 10.03.550.....	2338
Versions for Release 10.03.550 .....	2340
Security Fixes 10.03.550.....	2343
General Information 10.03.550.....	2343
Known Issues 10.03.550 .....	2344
New Features 10.03.550 .....	2345



Resolved Issues 10.03.550 .....	2345
7.32.2 IGEL Universal Desktop OS 3 / IGEL UD Pocket 10.03.550.....	2346
Versions for Release 10.03.550 .....	2346
Security Fixes 10.03.550.....	2350
General Information 10.03.550.....	2351
Known Issues 10.03.550.....	2351
New Features 10.03.550.....	2352
Resolved Issues 10.03.550 .....	2352
7.33 Notes for Release 10.03.500.....	2353
7.33.1 IGEL Universal Desktop / IGEL Zero 10.03.500.....	2354
Supported Devices .....	2354
Versions for 10.03.500 .....	2355
Security Fixes 10.03.500.....	2358
General Information 10.03.500.....	2364
Known Issues 10.03.500 .....	2365
New Features 10.03.500 .....	2366
Resolved Issues 10.03.500 .....	2378
7.33.2 IGEL Universal Desktop OS3 / IGEL UD Pocket 10.03.500 .....	2381
Versions 10.03.500.....	2381
Security Fixes 10.03.500.....	2385
General Information 10.03.500.....	2390
Known Issues 10.03.500 .....	2391
New Features 10.03.500 .....	2392
Resolved Issues 10.03.500 .....	2404
7.33.3 IGEL Universal Desktop Converter (UDC3) 10.03.500 .....	2407
Versions 10.03.500.....	2407
New Features 10.03.500 .....	2409
Resolved Issues 10.03.500 .....	2421



- Partner Solutions(see page 56)
- IGEL OS Articles(see page 66)
- IGEL OS Reference Manual(see page 750)
- UD Pocket (UDP) Reference Manual(see page 1284)
- IGEL OS Creator(see page 1293)
- IGEL OS Creator for Windows (OSCW)(see page 1342)
- IGEL OS Release Notes(see page 1422)



## 1 Partner Solutions

- [Crossmatch / Digital Persona](#)(see page 56)
- [Diktamen Compatibility](#)(see page 56)
- [Imprivata OneSign Compatibility](#)(see page 57)
- [Jabra Handsets / Headsets](#)(see page 58)
- [Nuance Compatibility](#)(see page 59)
- [Olympus Compatibility](#)(see page 59)
- [Poly Headsets](#)(see page 61)
- [EPOS/Sennheiser Compatibility](#)(see page 61)
- [Signotec Compatibility](#)(see page 62)
- [StepOver Signature Pads Compatibility](#)(see page 63)
- [Wacom Compatibility](#)(see page 63)
- [deviceTrust](#)(see page 64)
- [Philips Speech](#)(see page 64)

### 1.1 Crossmatch / Digital Persona

Users can authenticate to a Citrix server using a Crossmatch / DigitalPersona fingerprint reader. For this purpose, the associated server software must be integrated into the server.

The following Crossmatch / Digital Persona fingerprint readers are supported (for Citrix only):

- U.are.U 4500
- Eikon Touch 510
- Eikon Touch 710

► To use the fingerprint readers in Citrix sessions, enable the **Crossmatch DigitalPersona fingerprint channel**; see [Device Support](#)(see page 784).

### 1.2 Diktamen Compatibility

As of IGEL OS 10, the following devices with Diktamen dictation solutions are supported:

<b>Dictation devices</b>	<b>Vendor ID</b>	<b>Product ID</b>
Grundig SonicMic EU	0x15d8	0x0025
Grundig SonicMic US	0x15d8	0x0026
Grundig SonicMic US	0x15d8	0x002A
Grundig Cordex	0x15d8	0x0020
Philips 32xx, 35xx, 37xx	0x0911	0x0c1c



<b>Dictation devices</b>	<b>Vendor ID</b>	<b>Product ID</b>
Philips 52xx	0x0911	0x149a
Philips 6264	0x0911	0x1878
Philips 6274	0x0911	0x2512
Olympus DR 2000	0x07b4	0x0216
Olympus DR 2100	0x07b4	0x0253
<b>Foot pedals</b>	<b>Vendor ID</b>	<b>Product ID</b>
VEC	0x05f3	0x00ff
Philips, old version	0x0911	0x184c
Philips	0x0911	0x1844
Infinity	0x0e0f	0x0003
Grundig	0x15d8	0x0024
Olympus	0x07b4	0x0218
DictaPhone	0x04b4	0x0100

## 1.3 Imprivata OneSign Compatibility

The following IGEL devices are officially supported as of Imprivata OneSign Embedded.

### 1.3.1 IGEL Devices

<b>IGEL Device</b>	<b>IGEL Firmware</b>	<b>Imprivata Ready</b>	<b>Citrix Receiver Support</b>	<b>VMware Horizon Support</b>
UD2 LX	11.01.x	✓	✓	✓
UD3 LX	11.01.x	✓	✓	✓



<b>IGEL Device</b>	<b>IGEL Firmware</b>	<b>Imprivata Ready</b>	<b>Citrix Receiver Support</b>	<b>VMware Horizon Support</b>
UD5 LX	11.01.x	✓	✓	✓
UD6 LX	11.01.x	✓	✓	✓
UD7 LX	11.01.x	✓	✓	✓
UD9 LX	11.01.x	✓	✓	✓
UD9 LX Touch	11.01.x	✓	✓	✓

### 1.3.2 IGEL Software Clients

<b>IGEL Device</b>	<b>IGEL Firmware</b>	<b>Imprivata Ready</b>	<b>Citrix Receiver Support</b>	<b>VMware Horizon Support</b>
UDC3	11.01.x	✓	✓	✓
UD Pocket	11.01.x	✓	✓	✓

The compatibility matrix can also be found on the Imprivata documentation. Log in to the Imprivata website and search for "Imprivata Supported Components".

## 1.4 Jabra Handsets / Headsets

IGEL OS integrates remote call control (RCC) for Jabra headsets. The Jabra RCC is intended to control state of radio connection in Bluetooth headsets.

To save battery power, the connection must be closed after every call.

IGEL OS supports the following Jabra handsets and headsets (verified with Citrix and enabled [HDX RTME](#)(see page 796)):

### 1.4.1 Tested by IGEL

<b>Jabra model</b>	<b>IGEL OS 11.05.100 and higher</b>
Jabra Engage 50	✓
Jabra Engage 65	✓



Jabra model	IGEL OS 11.05.100 and higher
Jabra Engage 75	✓
Jabra Evolve 30 II (Ver. B)	✓
Jabra Evolve 30 II (Ver. C)	✓
Jabra Evolve 40 (Ver. B) - USB-C	✓
Jabra Evolve 40 (Ver. D)	✓
Jabra Evolve 65	✓
Jabra Evolve2 65	✓
Jabra Evolve 75	✓
Jabra Evolve2 85 (verified with Microsoft Teams optimization only; based on test results from the field)	✓
Jabra Handset 450	✓
Jabra Pro 9470	✓

For more information on the configuration of Jabra headsets, see [Jabra \(see page 1233\)](#) and [How to Deploy a Jabra Xpress Package \(see page 677\)](#).

## 1.5 Nuance Compatibility

IGEL OS 10.03.100 or higher contains Nuance Citrix Client Audio Extension.

Nuance Citrix Client Audio Extension configures audio redirection on a Linux device in a Citrix environment to provide optimal support for speech recognition.

For further information, see the [Readme for IGEL<sup>1</sup>](#) by Nuance.

## 1.6 Olympus Compatibility

IGEL OS 10.04 and higher supports the following Olympus dictation devices:

Desktop Dictation Devices	RDP (from version 2012)	Citrix (current version)
DR-1200		✓

<sup>1</sup> [https://kb.igel.com/download/attachments/49586590/README\\_NUANCE\\_IGEL.htm?  
api=v2&modificationDate=1585920382109&version=1](https://kb.igel.com/download/attachments/49586590/README_NUANCE_IGEL.htm?api=v2&modificationDate=1585920382109&version=1)



<b>Desktop Dictation Devices</b>	<b>RDP (from version 2012)</b>	<b>Citrix (current version)</b>
DR-2200		✓
DR-2300		✓
RM-4000P		✓
RM-4010P		✓
RM-4015P		✓
RM-4100		✓
RM-4110		✓
<b>Mobile Devices</b>	<b>RDP (from version 2012)</b>	<b>Citrix (current version)</b>
DS-3500	✓	✓
DS-7000	✓	✓
<b>Foot Pedals</b>	<b>RDP (from version 2012)</b>	<b>Citrix (current version)</b>
RS-27		✓
RS-28		✓
RS-31		✓
RS-27H	✓	✓
RS-28H	✓	✓
RS-31H	✓	✓



## 1.7 Poly Headsets

IGEL OS supports the following Poly (former Plantronics) headsets (verified with Citrix and enabled [HDX RTME](#)(see page 796)):

- Blackwire 325 (wired)
- Blackwire 5210
- C320 (wired)
- Savi 8220
- Savi 8245 Office
- Voyager 5200 UC
- Voyager 5200 UC B5200 (Bluetooth)
- Voyager 6200 UC
- Voyager 8200 UC
- Voyager Focus UC B825

## 1.8 EPOS/Sennheiser Compatibility

The following EPOS/Sennheiser headsets are supported (verified with Citrix and enabled [HDX RTME](#)(see page 796)):

With IGEL OS 11.04.200 or higher, EPOS Connect is integrated. For more information, see [EPOS Connect](#)(see page 1234).

### 1.8.1 Tested by IGEL

- EPOS/Sennheiser DW Pro USB
- EPOS/Sennheiser MB Pro
- EPOS/Sennheiser MB 660
- EPOS/Sennheiser SC 45
- EPOS/Sennheiser SC 70
- EPOS/Sennheiser SC 160
- EPOS/Sennheiser SC 260
- EPOS/Sennheiser SC 630

### 1.8.2 Tested by EPOS/Sennheiser

#### Wired Headsets

- Culture Series:
  - SC 30 USB ML
  - SC 60 USB ML
- Culture Plus Series:
  - SC 40 USB MS BLACK



- SC 70 USB MS BLACK
- Culture Plus Mobile Series:
  - SC 45 USB MS
  - SC 75 USB MS
- Circle Series:
  - SC 230 USB MS II
  - SC 260 USB MS II
  - SC 230 with USB-ED CC 01 MS
  - SC 260 with USB-ED CC 01 MS
- Century Series:
  - SC 630 USB ML
  - SC 660 USB ML
  - SC 630 with USB-ED CC 01 MS
  - SC 660 with USB-ED CC 01 MS

## Wireless Headsets

- Bluetooth headsets:
  - MB Pro 1 UC ML
  - MB Pro 2 UC ML
  - Presence UC ML
  - MB 660 UC MS
- DECT headsets:
  - DW Office ML
  - DW Pro 1 ML
  - DW Pro 2 ML
  - SD Office ML
  - SD Pro 1 ML
  - SD Pro 2 ML
  - D 10 USB ML

## Speakerphones

- SP 10 ML
- SP 20 ML
- SP 220 MS

## 1.9 Signotec Compatibility

The following Signotec devices are supported:



Signotec Device	IGEL Firmware from	Citrix Receiver Support	RDP Support	VMware Horizon (RDP) Support
Signotec LCD Signature Pad Alpha	IGEL Linux 5.08.x	✓	✓	✓
Signotec LCD Signature Pad Gamma	IGEL Linux 5.09.x	✓	✓	✓
Signotec LCD Signature Pad Sigma	IGEL Linux 5.08.x	✓	✓	✓
Signotec LCD Signature Pad Omega	IGEL Linux 5.08.x	✓	✓	✓

## 1.10 StepOver Signature Pads Compatibility

As of IGEL OS 11.02.100, the StepOver TCP Client supports the applications eSignatureOffice, SimpleSigner, and StepOver APIs with the following devices:

### duraSign pads:

- duraSign Pad Brilliance
- duraSign Pad 10.0

### naturaSign pads:

- Standard 1 (FW 1.x)
- Standard 2
- Standard 2.5
- Classic
- Biometric
- Mobile
- Flawless
- Comfort
- ColourPad

The legacy models +Pad and BlueMobile are not supported.

Learn more in the how-to document "[Using a StepOver Signature Pad](#)(see page 682)".

## 1.11 Wacom Compatibility

IGEL OS 11 supports the following Wacom devices (for Citrix only):



- DTU-1141B
- STU-500
- STU-520
- STU-530
- STU-300
- STU-430

## 1.12 deviceTrust

The deviceTrust client, which first comes with IGEL OS 10, adds context awareness to an endpoint. Access to a remote session can be granted or denied, depending on the device's location, network connection, hardware, or according to other criteria. For further information, see <https://www.igel.com/ready/showcase-products/devicetrust><sup>2</sup>.

## 1.13 Philips Speech

The following dictation and accessory devices have been tested with IGEL OS by Philips Speech.

Device Category	Device Type	Officially tested by IGEL
SpeechAir	PSP1100 PSP2100	
Digital PocketMemo 4	DPM8000 DPM8200 DPM8500	✓
SpeechOne	PSM6000	
SpeechMike Premium Air	SMP4000 SMP4010	
SpeechMike Premium Touch	SMP3810 SMP3800 SMP3710 SMP3700	

---

<sup>2</sup><https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.igel.com%2Fready%2Fshowcase-products%2FdeviceTrust%2F&data=04%7C01%7Cloew%40igel.com%7C17f55dbdebb343b3204208d8f0423240%7C3f04441122ea4ba182dfd85e25879b4f%7C0%7C0%7C637523514995310251%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBtil6Ik1haWwiLCJXVCi6Mn0%3D%7C1000&sdata=0%2FZ0VHPstSTCXMidmv33CtvM1yUD%2BQ0l9oDkT0UiIpA%3D&reserved=0>



Device Category	Device Type	Officially tested by IGEL
SpeechMike Premium	LFH3610 LFH3600 LFH3520 LFH3510 LFH3500	✓
SpeechMike 3	LFH3310 LFH3300 LFH3220 LFH3210 LFH3200	✓
Foot Control	ACC2330 ACC2320 ACC2310 LFH2330 LFH2320 LFH2310	✓
AirBridge	ACC4100	



## 2 IGEL OS Articles

- [Overview: First Steps with IGEL OS 11](#)(see page 66)
- [Update and Upgrade](#)(see page 68)
- [Citrix](#)(see page 238)
- [RDP](#)(see page 274)
- [VMware Horizon](#)(see page 285)
- [Microsoft Azure Virtual Desktop \(AVD\)](#)(see page 292)
- [Evidian](#)(see page 305)
- [IBM iAccess](#)(see page 308)
- [Imprivata](#)(see page 322)
- [Azure Virtual Desktop](#)(see page 324)
- [SSH](#)(see page 331)
- [Amazon WorkSpaces – Teradici PCoIP Sessions](#)(see page 333)
- [Login Enterprise Configuration](#)(see page 340)
- [Nutanix](#)(see page 351)
- [Browser](#)(see page 355)
- [System](#)(see page 367)
- [Network](#)(see page 378)
- [Security](#)(see page 418)
- [Certificates](#)(see page 457)
- [Smartcard](#)(see page 484)
- [Desktop and Display](#)(see page 512)
- [Customizing](#)(see page 529)
- [Devices](#)(see page 624)
- [Printer](#)(see page 712)
- [UD Pocket](#)(see page 715)
- [Miscellaneous](#)(see page 719)

### 2.1 Overview: First Steps with IGEL OS 11

The following article provides a short overview of how to get started with an IGEL device or a third-party device that you want to convert to IGEL OS. The steps are generally the same, but in the case of a third-party device you will need to use the IGEL OS Creator.



IGEL Device	3d-Party Device
<b>Step 1: Download and install the UMS</b> <ul style="list-style-type: none"> <li>IGEL Download Server<sup>3</sup></li> <li>Instruction: Installing a UMS Server<sup>4</sup></li> <li>Video: UMS installation on a Windows Server<sup>5</sup></li> <li>Video: UMS installation on a Linux operating system<sup>6</sup></li> </ul>	<b>Step 1: Download and install the UMS</b> <ul style="list-style-type: none"> <li>IGEL Download Server<sup>16</sup></li> <li>Instruction: Installing a UMS Server<sup>17</sup></li> <li>Video: UMS installation on a Windows Server<sup>18</sup></li> <li>Video: UMS installation on a Linux operating system<sup>19</sup></li> </ul>
<b>Step 2: Activate your IGEL OS 11</b> <p><b>with the Setup Assistant (free evaluation license):</b></p>	<b>Step 2: Download IGEL OS 11</b> <ul style="list-style-type: none"> <li>IGEL Download Server<sup>20</sup>, section <b>OS 11 &gt; OS Creator</b></li> </ul>
<p>Instruction: Activate Your IGEL OS(see page 760), section "Register for Demo License". See also Getting a Demo License<sup>7</sup>.</p> <p>Video: Acquire a Demo License Including Workspace Edition and Enterprise Management Pack<sup>8</sup></p> <p><b>via UMS (purchased license):</b></p> <ul style="list-style-type: none"> <li>Deploy licenses using automatic or manual license deployment method.<sup>9</sup></li> <li>Video: Register an endpoint in the UMS and assign a license to it<sup>10</sup></li> </ul>	<b>Step 3: Convert your device to IGEL OS 11</b> <ul style="list-style-type: none"> <li>IGEL OS Creator Manual(see page 1293)</li> <li>Video: Converting an x86-Endpoint Using the IGEL OS Creator<sup>21</sup></li> </ul> <p><b>Step 4: Activate your IGEL OS 11</b></p> <p><b>with the Setup Assistant (free evaluation license):</b></p> <ul style="list-style-type: none"> <li>Instruction: Activate Your IGEL OS(see page 760), section "Register for Demo License". See also Getting a Demo License<sup>22</sup>.</li> </ul>
<b>Step 3: Configure your device</b> <p><b>with the UMS:</b></p> <ul style="list-style-type: none"> <li>Create a profile<sup>11</sup> with the required settings and assign it to the device<sup>12</sup>. See also Profiles<sup>13</sup>.</li> </ul>	

<sup>7</sup> <https://kb.igel.com/display/licensesmoreigelos11/Getting+a+Demo+License>

<sup>8</sup> <https://www.youtube.com/watch?v=j31c8dzBMAg>

<sup>9</sup> <https://kb.igel.com/display/licensesmoreigelos11/Deploying+Licenses>

<sup>10</sup> <https://www.youtube.com/watch?v=01N-9b3P4wo>

<sup>11</sup> <https://kb.igel.com/display/endpointmgmt606/Creating+Profiles>

<sup>12</sup> <https://kb.igel.com/display/endpointmgmt606/Allocating+Profiles>

<sup>13</sup> <https://kb.igel.com/display/endpointmgmt606/Profiles>

<sup>16</sup> <https://www.igel.com/software-downloads/workspace-edition/>

<sup>17</sup> <https://kb.igel.com/display/endpointmgmt606/Installing+a+UMS+server>

<sup>18</sup> <https://www.youtube.com/watch?v=3YJnFiE7y5w>

<sup>19</sup> [https://www.youtube.com/watch?v=p52CxtB\\_0ok](https://www.youtube.com/watch?v=p52CxtB_0ok)

<sup>20</sup> <https://www.igel.com/software-downloads/workspace-edition/>

<sup>21</sup> <https://www.youtube.com/watch?v=xVqcX6QTZ5g>

<sup>22</sup> <https://kb.igel.com/display/licensesmoreigelos11/Getting+a+Demo+License>



IGEL Device	3rd-Party Device
<ul style="list-style-type: none"> <li>Video: <a href="#">Configure an endpoint in the UMS using profiles<sup>14</sup></a></li> </ul> <p><b>without the UMS:</b></p> <ul style="list-style-type: none"> <li>Use the IGEL Setup on the device, e.g. to configure <a href="#">User Interface</a>(see page 1142) and <a href="#">Sessions</a>(see page 774).</li> <li>Video: <a href="#">Configuring an Endpoint with IGEL OS 11<sup>15</sup></a></li> </ul>	<ul style="list-style-type: none"> <li>Video: <a href="#">Acquire a Demo License Including Workspace Edition and Enterprise Management Pack<sup>23</sup></a></li> </ul> <p><b>via UMS (purchased license):</b></p> <ul style="list-style-type: none"> <li>Deploy licenses using automatic or manual license deployment method.<sup>24</sup></li> <li>Video: <a href="#">Register an endpoint in the UMS and assign a license to it<sup>25</sup></a></li> </ul> <p><b>Step 5: Configure your device</b></p> <p><b>with the UMS:</b></p> <ul style="list-style-type: none"> <li>Create a profile<sup>26</sup> with the required settings and assign it to the device<sup>27</sup>. See also <a href="#">Profiles<sup>28</sup></a>.</li> <li>Video: <a href="#">Configure an endpoint in the UMS using profiles<sup>29</sup></a></li> </ul> <p><b>without the UMS:</b></p> <ul style="list-style-type: none"> <li>Use the IGEL Setup on the device, e.g. to configure <a href="#">User Interface</a>(see page 1142) and <a href="#">Sessions</a>(see page 774)</li> <li>Video: <a href="#">Configuring an Endpoint with IGEL OS 11<sup>30</sup></a></li> </ul>

## 2.2 Update and Upgrade

- Adapting IGEL OS 11.04 or Higher for Devices with Small Storage(see page 69)
- Upgrading UDC3 or UD Pocket from IGEL OS 10.06 to IGEL OS 11 via Universal Firmware Update(see page 71)
- Upgrading from IGEL OS 10 to IGEL OS 11(see page 114)
- Buddy Update(see page 221)
- Firmware Update(see page 225)
- Updating the Firmware using a USB Storage Device(see page 228)
- Updating the Firmware using the Linux Console(see page 229)
- Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher(see page 231)
- Error: "legacy ICG Root (CA) certificate" When Updating to Igel OS 11.04 on Devices Connected via ICG(see page 232)
- Device Does Not Connect to ICG after Update to IGEL OS 11.04 or Higher(see page 235)
- IGEL OS Automatic Update Service for Device Evaluation(see page 237)

<sup>14</sup> <https://www.youtube.com/watch?v=Sc38mRv5Z1s>

<sup>15</sup> <https://www.youtube.com/watch?v=6WfLVgYBTHg>



## 2.2.1 Adapting IGEL OS 11.04 or Higher for Devices with Small Storage

### Environment

This article is valid for the following environment:

- IGEL OS 11.04 or higher
- UMS 6.05 or higher (recommended)
- Endpoint device that is supported by IGEL OS 11.04.100 or higher but the free storage is lesser than required by the full feature set

### Overview

For IGEL OS 11.04.100 or higher with the full feature set, a minimum of 2 GB storage is required. If your device has less free storage than required, e.g. because of large custom partitions, you can reduce the feature set so that the firmware fits on your device's storage.

Perform these two steps:

1. [Determining Which Features to Deactivate](#)(see page 69)
2. Reducing the feature set by one of the following methods:
  - [Using a UMS Profile](#)(see page 69)
  - [Using the Preconfigured Reduced INF File](#)(see page 70)
  - [Customizing the INF File](#)(see page 70)

### Determining Which Features to Deactivate

► Determine the storage requirements of the individual IGEL OS features using one of these methods:

- Go to [IGEL OS Release Notes](#)(see page 1422), select the "Notes for Release" of your firmware version, then select "Component Versions...", and go to the "Services" section. The "Reduced Firmware" column indicates for each feature whether it is included in the preconfigured reduced feature set or not.
- Open the `readme[version].txt` in your update source directory and search for "Reduced Firmware".

### Reducing the Feature Set

#### Using a UMS Profile

##### **Buddy Update Server**

When you download a firmware that has been reduced with the UMS (or the device's Setup) on a buddy update server, the buddy server itself will have the full feature set anyway. Hence, all devices that are used as update servers must have sufficient free storage.



1. Choose an appropriate profile that is assigned to all relevant devices, or create a new profile. For further information, see [Creating Profiles](#)<sup>31</sup>.
2. Go to **System > Firmware Customization > Features** and deactivate all features that are not needed.

Using the Preconfigured Reduced INF File

#### **Reduced Feature Set Cannot Be Changed by Setup/UMS**

When you have reduced the firmware using this method, you cannot reactivate features via the Setup resp. the UMS configuration dialog. To recover the complete feature set, you must copy `lxos-full.inf` to `lxos.inf` and then start the firmware update.

#### **Buddy Update Server**

When you have downloaded a reduced firmware on a buddy update server, also the buddy server itself has the reduced feature set. To recover the complete feature set on the buddy server, you must copy `lxos-full.inf` to `lxos.inf` in the update source and then update the buddy update server again.

Replace the `lxos.inf` file as follows:

1. Go to the directory that contains the source files for the firmware update. If you use the WebDav capability of the UMS, this is `<UMS installation directory>\rmguiserver\webapps\ums_filetransfer\<firmware version>`; example: `C:\Program Files\IGEL\RemoteManager\rmguiserver\webapps\ums_filetransfer\IGEL_OS_11-11.04.100`
2. Delete `lxos.inf`

It is safe to delete `lxos.inf` because there is a backup file named `lxos-full.inf`
3. Copy `lxos-reduced.inf` to `lxos.inf`
4. Start the firmware update as usual.

Customizing the INF File

#### **Reduced Feature Set Cannot Be Changed by Setup/UMS**

When you have reduced the firmware using this method, you cannot reactivate features via the Setup resp. the UMS configuration dialog. To recover the complete feature set, you must copy `lxos-full.inf` to `lxos.inf` and then start the firmware update.

<sup>31</sup> <https://kb.igel.com/display/endpointmgmt605/Creating+Profiles>



### Buddy Update Server

When you have downloaded a reduced firmware on a buddy update server, also the buddy server itself has the reduced feature set. To recover the complete feature set on the buddy server, you must copy `lxos-full.inf` to `lxos.inf` in the update source and then update the buddy update server again.

To customize the INF file:

1. Open `lxos.inf`
2. In the `[INFO]` section, add the following line:  
`custom="true"`
3. Delete the `[PART]` section of every partition you want to exclude, but do this ONLY IF the section has both of the following entries:  
`disposable="true"`  
`type="squashfs-auto"`
4. Save `lxos.inf` and start the firmware update as usual.

## 2.2.2 Upgrading UDC3 or UD Pocket from IGEL OS 10.06 to IGEL OS 11 via Universal Firmware Update

This document describes how to upgrade UDC3 or UD Pocket devices from IGEL OS 10.06 to IGEL OS 11 via the Universal Firmware Update feature of the UMS (Universal Management Suite).

Since a new licensing model has been introduced with IGEL OS 11, a license from an IGEL Workspace Edition Product Pack must be available for each device. If you have valid maintenance for your devices, you can convert your existing UDC3 or UD Pocket Product Packs to Workspace Edition (WE) Product Packs; see [Converting UDC3 or UD Pocket Licenses for Upgrading to IGEL OS 11](#)<sup>32</sup>.

Read all the following chapters in the order given and follow the instructions.

1. [Devices That Can Be Upgraded to IGEL OS 11](#)(see page 71)
2. [Important! Consider This Before Upgrading](#)(see page 78)
3. [Getting the UMS Ready](#)(see page 80)
4. [Deploying the Licenses](#)(see page 80)
5. [Creating the Universal Firmware Update](#)(see page 81)
6. [Creating an Upgrade Profile](#)(see page 91)
7. [Assigning the Upgrade Profile and the Universal Firmware Update to the Test Devices](#)(see page 100)
8. [Testing the Upgrade](#)(see page 104)
9. [Unassigning the Upgrade Profile and the Universal Firmware Update](#)(see page 106)
10. [If Applicable: Restoring Custom Partition and Custom Applications](#)(see page 107)
11. [Upgrading All Devices](#)(see page 107)

### Devices That Can Be Upgraded to IGEL OS 11

In this section, you find the general hardware requirements for IGEL OS 11 and a list of third-party devices officially supported by IGEL OS 11.

---

<sup>32</sup> <https://kb.igel.com/display/licensesmoreigelos11/Converting+UDC3+or+UD+Pocket+Licenses+for+Upgrading+to+IGEL+OS+11>



## Core Requirements

- CPU with 64-bit support
- CPU speed  $\geq 1$  GHz
- $\geq 2$  GB memory (RAM)

With devices that have 2 GB RAM and shared video memory, a maximum of 512 MB may be used as video memory.

- Recommended:  $\geq 4$  GB; minimum 2 GB storage

### Storage Requirements for IGEL OS 11.04 or Higher

IGEL OS 11.04.100 or higher requires at least 2.4 GB storage if the full feature set is applied. Thus, the feature set must be modified accordingly; for more information, see Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher(see page 231).

- No VIA graphic adapter; VIA graphics support is discontinued in IGEL OS.
- Legacy Bios and EFI/UEFI are supported.

## Devices Officially Supported by OSC and UD Pocket with IGEL OS 11

The following list only includes those devices that are **tested by IGEL** (with each major release of IGEL OS). By no means it implies that the devices which are not included in this list but meet the [core requirements](#)(see page 72) will not function with IGEL OS.

Further supported devices can be found on the [IGEL Ready<sup>33</sup>](#) Showcase at <https://www.igel.com/ready/showcase-categories/endpoints/>.

Integrated drivers and supported peripherals are listed in the [Third-Party Hardware Database<sup>34</sup>](#). For more solutions compatible with IGEL OS, see [Partner Solutions<sup>35</sup>](#).

For some of the devices listed here, Flash memory must be extended to  $\geq 2$  GB. For these devices, an appropriate note is added.

<sup>33</sup> <https://www.igel.com/technology-partners/>

<sup>34</sup> <https://www.igel.com/linux-3rd-party-hardware-database/>

<sup>35</sup> <https://kb.igel.com/display/igelos1105/Partner+Solutions>



## ADS-Tec

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
VMT9000	Industrial PC/Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100

## Advantech

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
POC-W213L	Medical All in One	4 GB	128 GB	Intel Core i7-7300U	11.01.100
POC-W243L*(see page 78)	Medical All in One	4 GB	32 GB	Intel Kaby Lake Core i5-7300U	11.01.110
POC-W243L*(see page 78)	Medical All in One	4 GB	128 GB	Intel Core i7-7300U	11.01.100

## Advantech-DLoG

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
DLT-V6210	Industrial PC/Terminal	4 GB	32 GB	Intel Atom	11.01.100
DLT-V7210 K	Industrial PC/Terminal	4 GB	4 GB	Intel Atom E3845	11.01.100

## Dell / Wyse

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
(AiO) 5040 / 5212	All in One	2 GB	2 GB	AMD G-T48E	11.01.100
3040	Thin Client	2 GB	8 GB	Intel Atom x5-Z8350	11.01.100
5020	Thin Client	2 GB	8 GB	AMD G-Series SoC	11.02.140



Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
5060	Thin Client	4 GB	8 GB	AMD GX-424CC	11.01.100
5070	Thin Client	8 GB	32 GB	Intel Celeron J4105	11.01.100
Latitude 5510	Laptop/Notebook	8 GB	256 GB	Intel Core i5-10210U	11.05.100

Elo

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
(AiO) i2 Touch (15 and 22 inches)	All in One	8 GB	128 GB	Intel Core i3-8100T	11.05.100

Fujitsu

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
Q957	Desktop PC	8 GB	500 GB	Intel Core i3-6100	11.02.100
FUTRO S740	Thin Client	4 GB	8 GB	Intel Celeron J4105	11.04.100

HP

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
t420	Thin Client	2 GB	8 GB	AMD Embedded G-Series GX-209JA	11.02.100
t430	Thin Client	2 GB	16 GB	Intel®Celeron® N4000	11.01.110
t530	Thin Client	4 GB	8 GB	AMD GX-215JJ Dual-Core	11.01.100
t630	Thin Client	4 GB	8 GB	AMD GX-420GI	11.01.100
t730	Thin Client	16 GB	8 GB	AMD RX-427BB APU	11.01.100
t820	Thin Client	16 GB	16 GB	Intel Core i5-4570S	11.01.100



Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
t640	Thin Client	4 GB	16 GB	AMD Ryzen R1505G	11.04.100
t540	Thin Client	16 GB	16 GB	AMD Ryzen Embedded R1305G	11.06.100

## Intel

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
NUC 5i5MYHE	Desktop PC	2 GB	32 GB	Intel i5-5300U	11.01.100
NUC 5i3RYH	Desktop PC	2 GB	2 GB	Intel i3-5010U	11.01.100
NUC 7CJYH	Desktop PC	2 GB	4 GB	Intel Celeron J4005	11.01.100

## Lenovo

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
ThinkCentre M625q	Desktop PC	4 GB	32 GB	AMD E2-9000e	11.04.100
ThinkCentre M75n	Desktop PC	8 GB	128 GB	AMD Ryzen 3 Pro 3300U	11.05.100
ThinkCentre M70q	Desktop PC	8 GB	500 GB	Intel Pentium Gold G6400T	11.05.100
L14	Laptop/Notebook	64 GB	1000 GB	AMD Ryzen 7 Pro 4750	11.05.100
14w	Laptop/Notebook	8 GB	128 GB	AMD A6	11.05.100

## LG

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
(AiO) 24CK550N **(see page 78)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
(AiO) 24CK550W **(see page 78)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100



Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
(AiO) 24CK560N **(see page 78)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
CK500W	Thin Client	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
(AiO) 38CK950N	All in One	8 GB	128 GB	AMD Ryzen 3	11.02.100
(AiO) 38CK900N	All in One	8 GB	128 GB	AMD Ryzen 3	11.02.100
CL600N	Thin Client	4 GB	16 GB	Intel® Celeron J4105	11.03.100
CL600W	Thin Client	8 GB	128 GB	Intel® Celeron J4105	11.03.100
(AiO) 34CN650N	All in One	4 GB	16 GB	Intel® Celeron J4105	11.05.100

## OnLogic

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
CL210G-10	Industrial PC/Terminal	4 GB	32 GB	Intel Celeron N3350	11.04.100
KARBON 300	Desktop PC	4 GB	32 GB	Intel Atom x5-E3930	11.04.100

## Onyx Healthcare

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
Venus 223	Medical All in One	4 GB	128 GB	Intel Quad-Core J1900	11.01.100

## Rein Medical

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
Silenio C122	All in One	8 GB	128 GB	Intel® Core™ i5 – 6th Generation	11.01.110



Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
Silenio C124	All in One	8 GB	128 GB	Intel® Core™ i5 – 6th Generation	11.01.110
Clinio S 522TCT	Medical All in One	8 GB	16 GB	Intel® Pentium® Silver J5005	11.04.100
Clinio S 524TCT	Medical All in One	8 GB	16 GB	Intel® Pentium® Silver J5005	11.04.100

Secunet

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
SINA Workstation S EliteDesk 800 G2	Workstation	16 GB	256 GB	Intel Core i7-6700	11.01.100

Toshiba

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
Portégé X20W-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7200U	11.01.100
Portégé X30-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7300U	11.01.100
Tecra C50	Laptop/ Notebook	4 GB	500 GB	Intel i5-4210U	11.01.100
Tecra Z50-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7200U	11.01.100
SATELLITE R50	Laptop/ Notebook	4 GB	500 GB	Intel i3-6006U	11.01.100

USB Memory Sticks That Can Be Used as Alternative UD Pocket Hardware

DIGITTRADE

Name	Storage	Supported from IGEL OS Version
Kobra Stick	≥ 4GB	11.05.133



## Officially Supported Virtual Environments

- Tested with Ubuntu (64-bit) and default settings

Note that the use of a UD Pocket within a virtual machine is **not** supported by IGEL.

Name	Memory (RAM)	Storage	Type	Supported from IGEL OS Version
Oracle VM VirtualBox	≥ 2 GB	≥ 4 GB	Linux	11.04.100
VMware Workstation	≥ 2 GB	≥ 4 GB	Linux	11.04.100

\* Delock Adapter DP 1.2 to DVI does not work.

\*\* When using an additional 4k screen with this device, please edit the BIOS settings as follows:

- Go to the **Chipset** screen.
- Set **Integrated Graphics** to “Force”.
- Set **UMA Frame Buffer Size** to “256M” or higher.

## Check List

- The devices you want to upgrade meet the hardware requirements for IGEL OS 11.

## Next Step

>> [Important! Consider This Before Upgrading](#)(see page 78)

## Important! Consider This Before Upgrading

To make sure that your upgrade can be successful, check the following warnings and notes; a warning symbol indicates that irreversible damage can be done to your devices.

**Existing partitions:** Any existing partition on the target drive of your device will be deleted. The installer will repartition the target device. The overall size of the newly created partitions will be calculated based on the available disk space. The minimum disk usage is 2 GB, the maximum is 16 GB.

### No Downgrade

You cannot restore your IGEL OS 10 system once you have migrated to IGEL OS 11. The device storage is overwritten completely with a new partitioning scheme.



### Features (e.g. Clients)

IGEL OS 11 does not have the complete feature set of IGEL OS 10. Make sure that the current version of IGEL OS 11 meets your requirements. For details, refer to the appropriate release notes.

### Custom Partitions

The contents of Custom Partitions will be deleted by the upgrade. Make sure that the Custom Partition is restored after the upgrade has finished. Besides becoming dysfunctional after the upgrade, applications and kernel drivers in a Custom Partition might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device.

### Custom Commands

The persistence of custom commands cannot be guaranteed. Besides becoming dysfunctional after the upgrade, custom commands might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device. In general, custom commands must be adapted for IGEL OS 11. We recommend that you disable custom commands when upgrading; you can enable them once the upgrade has been successfully completed.

### Power Supply

Ensure that the device is not running on battery power, i.e. it must be connected to a power supply during the complete upgrade process.

### Network

All devices must be connected to a LAN or WLAN. LAN is the recommended option. The device will not be upgraded if OpenVPN, OpenConnect, mobile broadband, or genucard is configured. To be sure, check if the following parameters are deactivated resp. no session is configured:

- **Network > VPN Open VPN** (registry: sessions.openvpn%)
- **Network > VPN > OpenConnect VPN** (registry: sessions.openconnect%)
- **Network > Mobile Broadband**, checkbox **Enable Mobile Broadband** (registry: network.interfaces.mobile\_broadband.enabled)
- **Network > VPN > genucard** (registry: network.interfaces.genucard\_vpn\_connector.autostart\_enabled)

When you have changed the settings, restart the device to enable the upgrade.

### Check List

- The limitations and conditions are understood and do not constitute a problem.

### Next Step

>> [Getting the UMS Ready\(see page 80\)](#)



## Getting the UMS Ready

To upgrade your devices to IGEL OS 11, you need the appropriate version of the UMS. Also, the devices must be registered with the UMS to receive their licenses.

1. If you have not already done so, update your UMS to version 6.01.130 or higher. For instructions, see [Updating a UMS Installation<sup>36</sup>](#).
2. Make sure that your devices are registered with the UMS. For more information, see the chapter [Registering Devices on the UMS Server<sup>37</sup>](#) in the UMS Manual.

### Check List

- Your Universal Management Suite (UMS) version is 6.01.130 or higher.
- All devices that will be upgraded are registered in the UMS.

### Next Step

>> [Deploying the Licenses\(see page 80\)](#)

## Deploying the Licenses

### Checking If the Required Licenses Are Available

- Ensure that you have the following licenses:
- A valid license from an IGEL Workspace Edition (WE) Product Pack for each device.
  - Depending on the features you want to use, you might need IGEL Enterprise Management (EMP) licenses in addition. For further information, see [IGEL Software License Overview<sup>38</sup>](#).

### Deploying the Licenses

- Choose one of the following methods:
- If you want to deploy a license quickly on a single device: See [Manual License Deployment for IGEL OS without UMS<sup>39</sup>](#); start from step 5.
  - If you have a smaller or medium number of devices and want to control exactly which device should get a license: See [Manual License Deployment for IGEL OS<sup>40</sup>](#).
  - If you have a medium or greater number of devices, and you are planning to add new devices/licenses regularly: See [Set up Automatic License Deployment \(ALD\) with ALD Token<sup>41</sup>](#).

---

<sup>36</sup> <https://kb.igel.com/display/endpointmgmt601/Updating+a+UMS+Installation>

<sup>37</sup> <https://kb.igel.com/display/endpointmgmt601/Registering+devices+on+the+UMS+Server>

<sup>38</sup> <https://kb.igel.com/display/licensesmoreigelos11/IGEL+Software+License+Overview>

<sup>39</sup> <https://kb.igel.com/display/licensesmoreigelos11/Manual+License+Deployment+without+UMS>

<sup>40</sup> <https://kb.igel.com/display/licensesmoreigelos11/Manual+License+Deployment+without+UMS>

<sup>41</sup> <https://kb.igel.com/pages/viewpage.action?pageId=26029121>



- If you have a medium or greater number of devices, and you are planning to add new devices/licenses frequently (licensing can be managed completely in the IGEL License Portal): See [Setting up Automatic License Deployment \(ALD\)](#)<sup>42</sup>.

#### Check List

- ✓ The licenses have been purchased.
- ✓ License deployment is set up.

#### Next Step

>> [Creating the Universal Firmware Update\(see page 81\)](#)

### Creating the Universal Firmware Update

In this step, we will create a Universal Firmware Update that will be used for testing the upgrade and for rolling out the upgrade on all relevant machines.

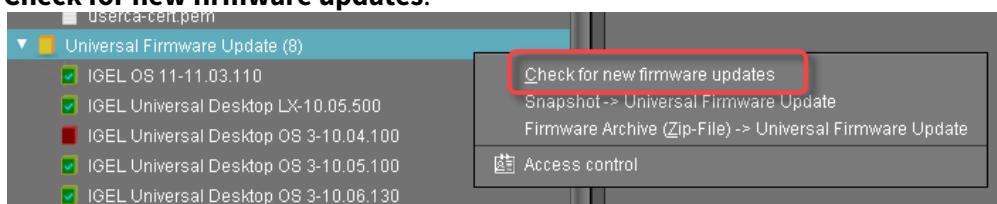
If you use the [High Availability Extension](#)<sup>43</sup>, note that Universal Firmware Updates are NOT synchronized, that is why you have to either download them to all HA nodes or configure an external (FTP) server.

Choose the procedure that suits your needs:

- [Configuring the Universal Firmware Update with Files Hosted by the UMS\(see page 81\)](#)
- [Configuring the Universal Firmware Update with Files Hosted by FTP Server \(Required for ICG\)\(see page 85\)](#)

#### Configuring the Universal Firmware Update with Files Hosted by the UMS

1. Go to **Server - [UMS address] > Universal Firmware Update** and in the context menu, select **Check for new firmware updates.**



<sup>42</sup> <https://kb.igel.com/pages/viewpage.action?pageId=10325058>

<sup>43</sup> <https://kb.igel.com/display/endpointmgmt604/High+Availability+HA>



2. Select the entry for the IGEL OS 11 firmware and then select **Download**. (In the example, IGEL OS 11.03.110 is used.)

**Universal Firmware Updates**

Include	Model	Version	Target directory	Release Notes	Release Notes
<input type="checkbox"/>	IGEL Zero	10.06.130	https://DokuW10hs.IGEL.LOCAL:8443/ums_filetransfer/	<a href="#">HTML</a>	<a href="#">Text</a>
<input type="checkbox"/>	IGEL UD LX (IGEL M330C, IGEL M340C)	10.06.130	https://DokuW10hs.IGEL.LOCAL:8443/ums_filetransfer/	<a href="#">HTML</a>	<a href="#">Text</a>
<input type="checkbox"/>	IGEL UD OS 3 (Legacy x86 system)	10.06.830	https://DokuW10hs.IGEL.LOCAL:8443/ums_filetransfer/	<a href="#">HTML</a>	<a href="#">Text</a>
<input checked="" type="checkbox"/>	IGEL OS 11 (IGEL D220, IGEL H850C)	11.03.110	https://DokuW10hs.IGEL.LOCAL:8443/ums_filetransfer/	<a href="#">HTML</a>	<a href="#">Text</a>

Show only latest firmware versions (hides already downloaded versions)

**Download** **Cancel**

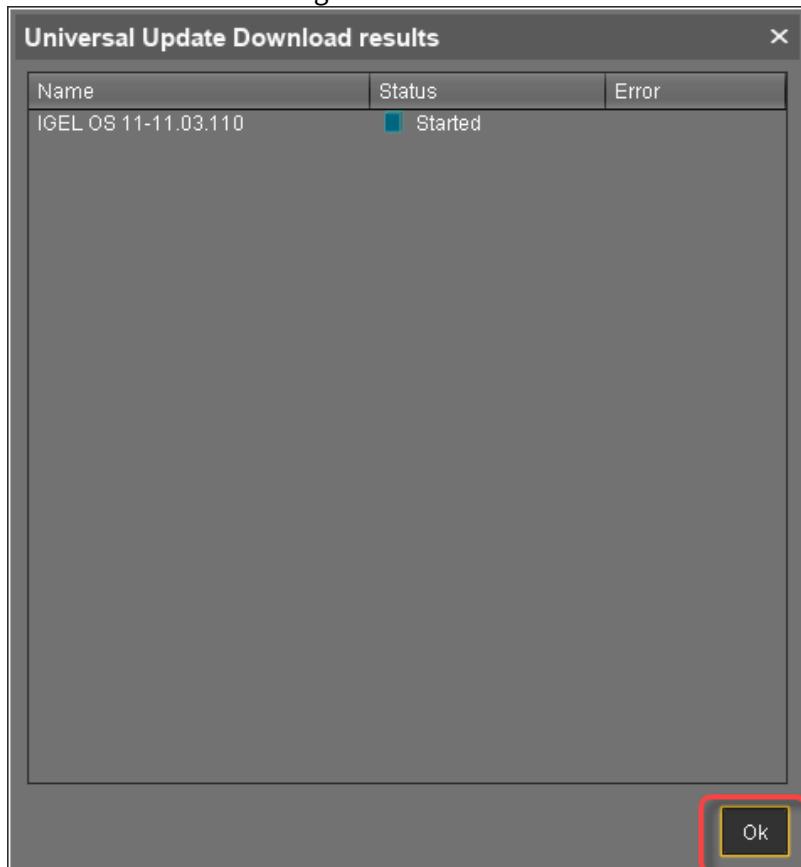


3. Read and confirm the disclaimer. (IGEL OS 11.03.100 or higher only)





4. Confirm the status message.



In the main window, you can monitor the download process.



/Universal Firmware Update/IGEL OS 11-11.03.110

Product	IGEL OS 11
Version	11.03.110
Release Notes	<a href="#">HTML Text</a>
<b>Firmware Update Settings</b>	
User	IGEL_INTERNAL_FIRMWAREUPDATE_USER
Password	*****
Host	DokuW10hs.IGEL.LOCAL
Port	8443
Protocol	HTTPS
Target URL	/ums_filetransfer/IGEL_OS_11-11.03.110
Snapshot file	
<b>Download Status</b>	
Status	Started <div style="width: 50%; background-color: #ffcc00; display: inline-block;"></div> <a href="#">Download the firmware update...</a>
Error	

When the status is **Finished**, your Universal Firmware Update is ready for use.

/Universal Firmware Update/IGEL OS 11-11.03.110

Product	IGEL OS 11
Version	11.03.110
Release Notes	<a href="#">HTML Text</a>
<b>Firmware Update Settings</b>	
User	IGEL_INTERNAL_FIRMWAREUPDATE_USER
Password	*****
Host	DokuW10hs.IGEL.LOCAL
Port	8443
Protocol	HTTPS
Target URL	/ums_filetransfer/IGEL_OS_11-11.03.110
Snapshot file	
<b>Download Status</b>	
Status	OK <div style="width: 100%; background-color: #2e6b2e; display: inline-block;"></div> <b>Finished</b>
Error	

#### Configuring the Universal Firmware Update with Files Hosted by FTP Server (Required for ICG)

You can use an FTP server instead of the UMS to host the firmware files. If you are using IGEL Cloud Gateway (ICG), an FTP server is required.



To configure an FTP server as update source:

1. In the UMS, go to **UMS Administration > Universal Firmware Update** and click **Edit**.
2. Enter the data required for accessing the FTP server and click **Save**.

**Edit FTP Server Configuration**

**Universal update settings**  
The IGEL Universal Firmware files are downloaded from: 'fwu.igel.com'.

Proxy Server [ ]

**The FTP server settings where the files are downloaded to (optional).**

Host	ftpServername
Port	21
User name	ftp
Password	***
Directory	directory/subdir

**Save** **Cancel**

3. Click **Test server connection** to test your settings.  
If everything went well, a success message is shown both for the IGEL download server and for the FTP server:

**Universal Firmware Update**

**Edit...** **Edit proxy configuration** **Test server connection**

**Universal update settings**  
The IGEL Universal Firmware files are downloaded from: 'fwus.igel.com'.

Proxy Server [ ]

Connection test **Connection successfully tested.**

**The FTP server settings where the files are downloaded to (optional).**

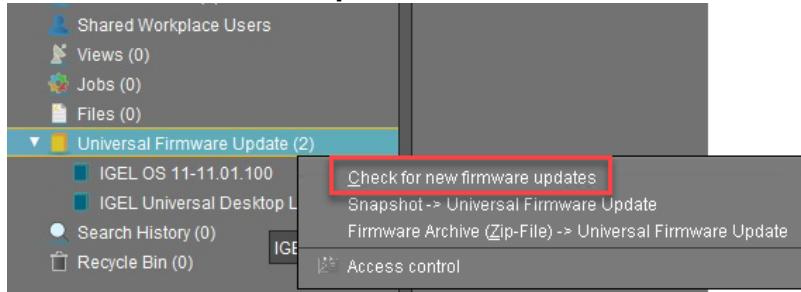
Protocol  FTP  FTP passive  FTPS  FTPS passive  SFTP

Host	localhost
Port	21
User name	ufu
Password	*****
Directory	[ ]

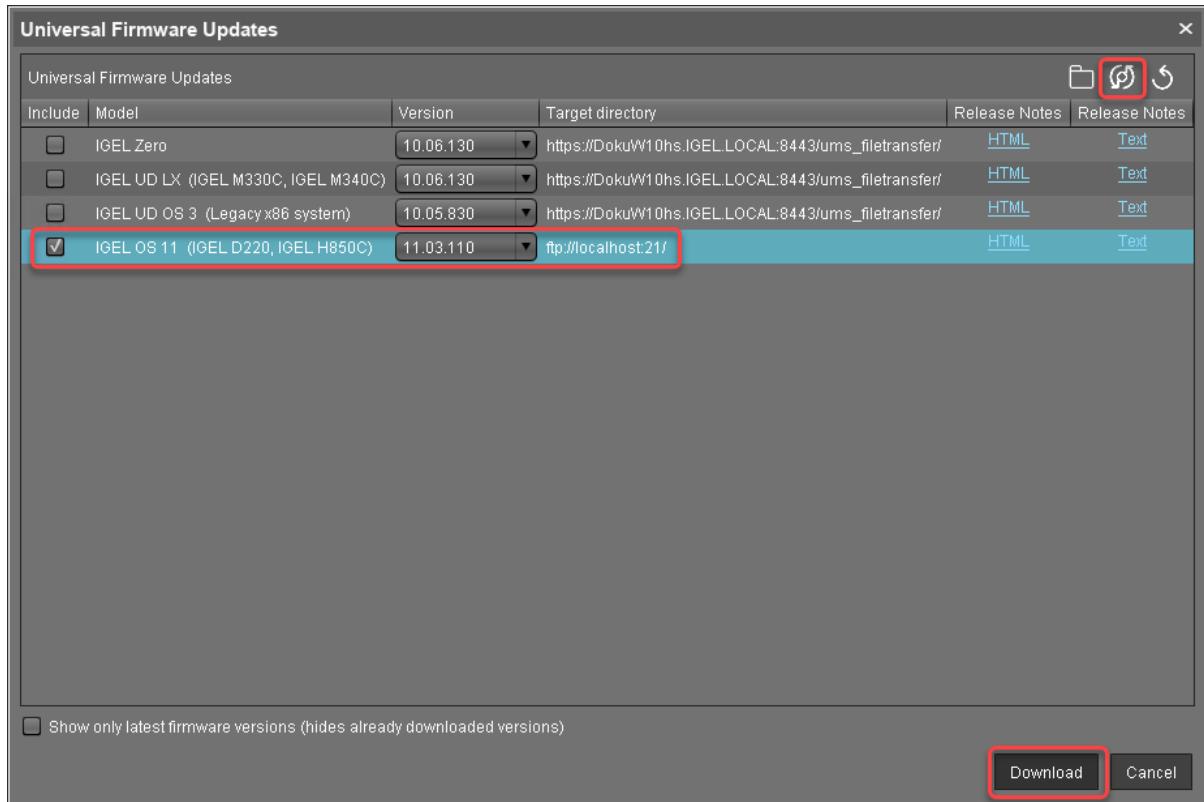
Connection test **Connection successfully tested.**



4. Go to **Server - [UMS address] > Universal Firmware Update** and in the context menu, select **Check for new firmware updates**.

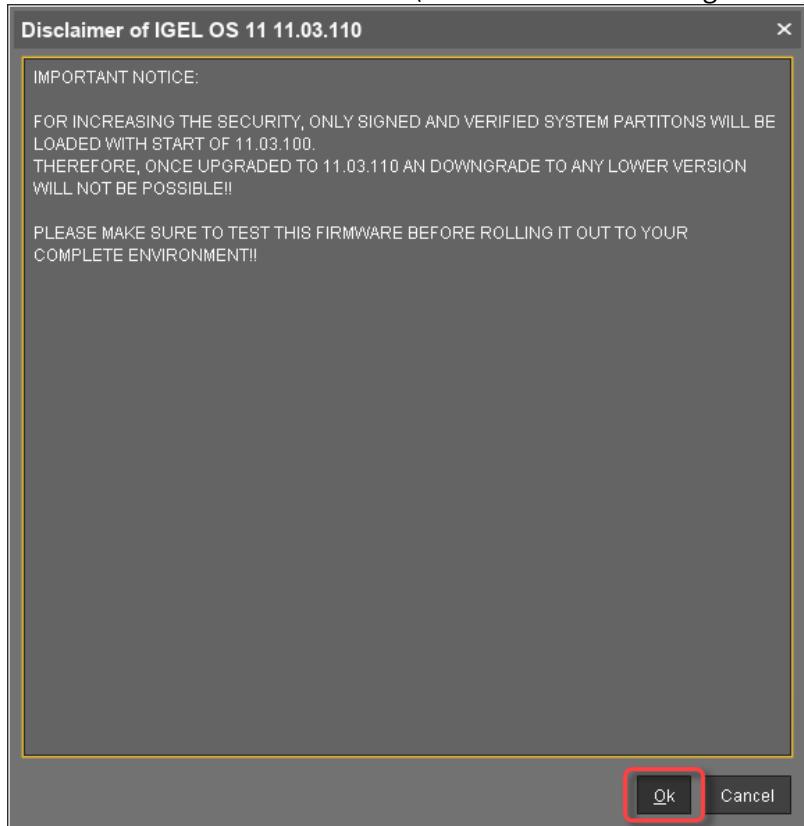


5. Select the entry for the IGEL OS 11 firmware, click to select the FTP server selected in step 2 and then select **Download**.



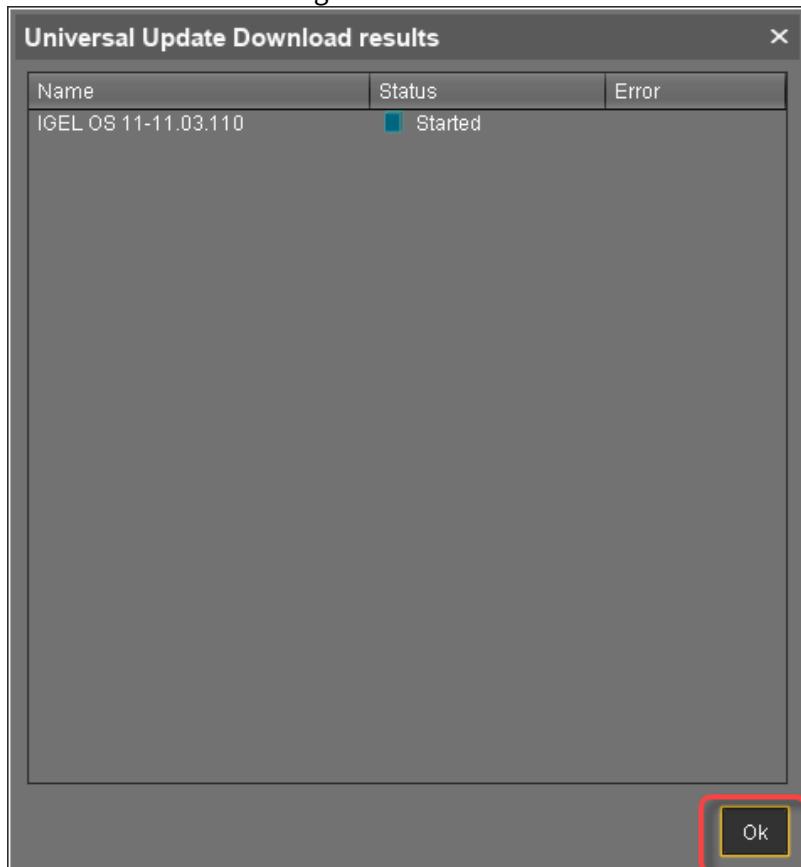


6. Read and confirm the disclaimer. (IGEL OS 11.03.100 or higher only)





7. Confirm the status message.



The firmware is transferred to the FTP server. In the main window, you can monitor the download process.



/Universal Firmware Update/IGEL OS 11-11.03.110

Product: IGEL OS 11  
Version: 11.03.110  
Release Notes: [HTML](#) [Text](#)

**Firmware Update Settings**

User: ufu  
Password: \*\*\*\*\*  
Host: localhost  
Port: 21  
Protocol: FTP  
Target URL: IGEL\_OS\_11-11.03.110  
Snapshot file:

**Download Status**

Status: Started Download the firmware update...

Error:

When the status is **Finished**, your Universal Firmware Update is ready for use.



/Universal Firmware Update/IGEL OS 11-11.03.110

Product	IGEL OS 11
Version	11.03.110
Release Notes	<a href="#">HTML</a> <a href="#">Text</a>
<b>Firmware Update Settings</b>	
User	ufu
Password	*****
Host	localhost
Port	21
Protocol	FTP
Target URL	IGEL_OS_11-11.03.110
Snapshot file	
<b>Download Status</b>	
Status	OK
	<div style="width: 100%;"><div style="width: 100%;"> </div></div> Finished
Error	

#### Check List

- The Universal Firmware Update has been created successfully.

#### Next Step

>> [Creating an Upgrade Profile](#)(see page 91)

### Creating an Upgrade Profile

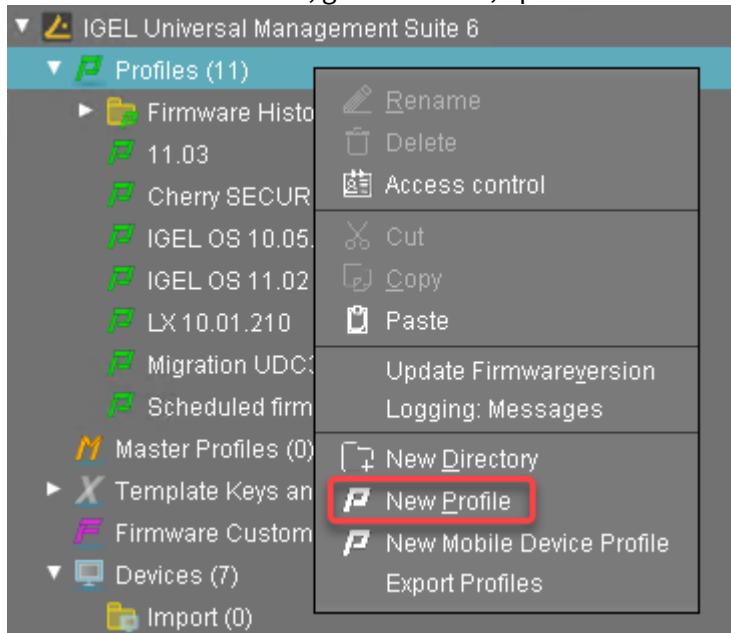
The upgrade profile varies, depending on whether the devices are in the same network as the UMS or connected via ICG. Choose the appropriate procedure:

- [For Devices that Are in the UMS Network](#)(see page 92)
- [For Devices that Are Connected via ICG](#)(see page 96)



## For Devices That Are in the UMS Network

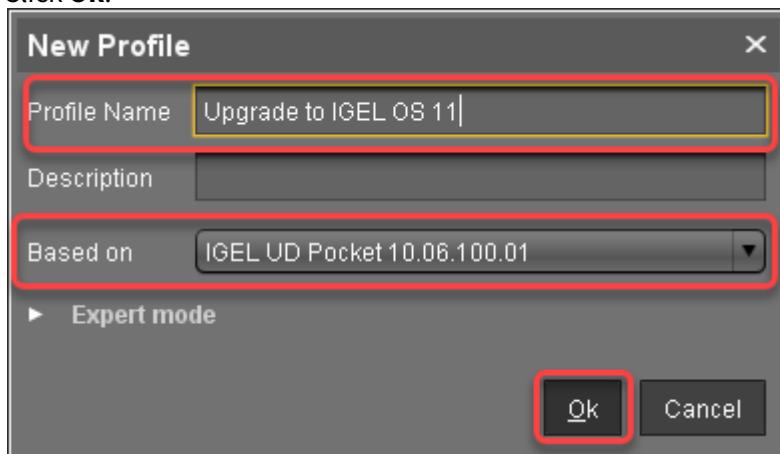
1. In the UMS structure tree, go to **Profiles**, open the context menu and select **New Profile**.



2. Enter the following data:

- **Profile Name:** Name for the profile, e. g. "Upgrade to IGEL OS 11".
- **Description:** Optional description for the profile.
- **Based on:** Firmware version for the profile; select the current firmware of your devices, that is, "IGEL UD Pocket 10.06.100".

3. Click **Ok**.

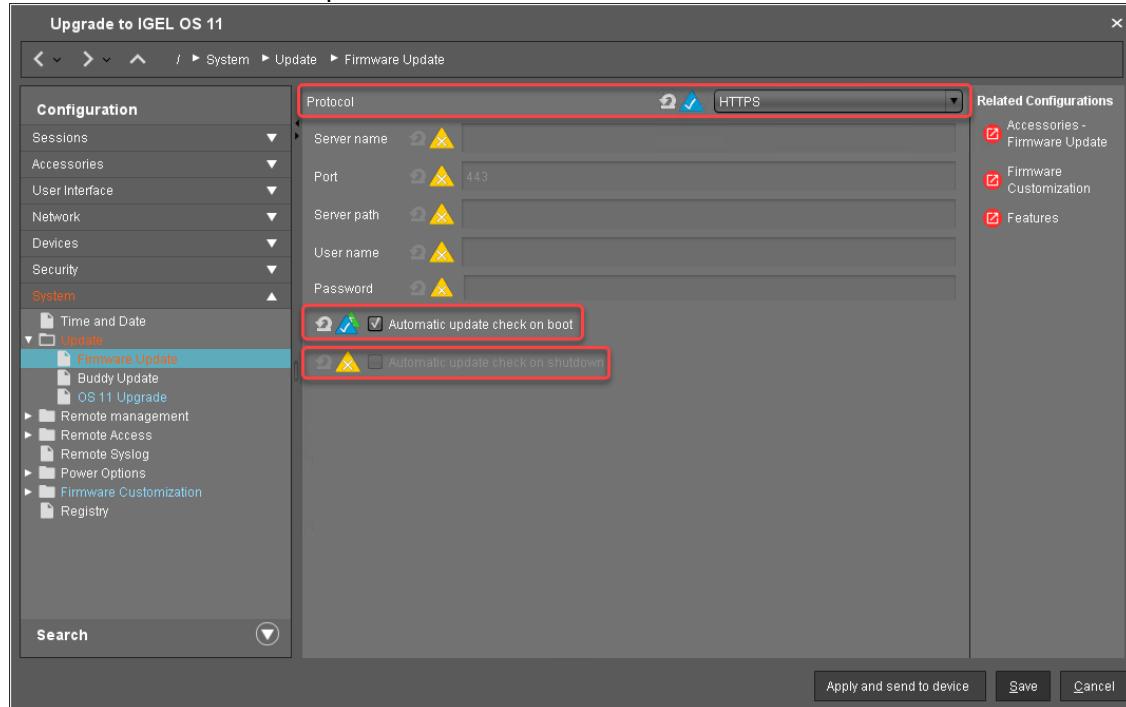


4. Go to **System > Update > Firmware Update** and change the settings as follows:

- Select "HTTPS" as the **Protocol**.
- Activate **Automatic update check on boot**.



- Ensure that **Automatic update check on shutdown** is deactivated. Otherwise, the device will shut down when the update is finished.



5. Go to **System > Update > Firmware Update > OS 11 Upgrade**.

6. Activate **Upgrade to OS 11**.

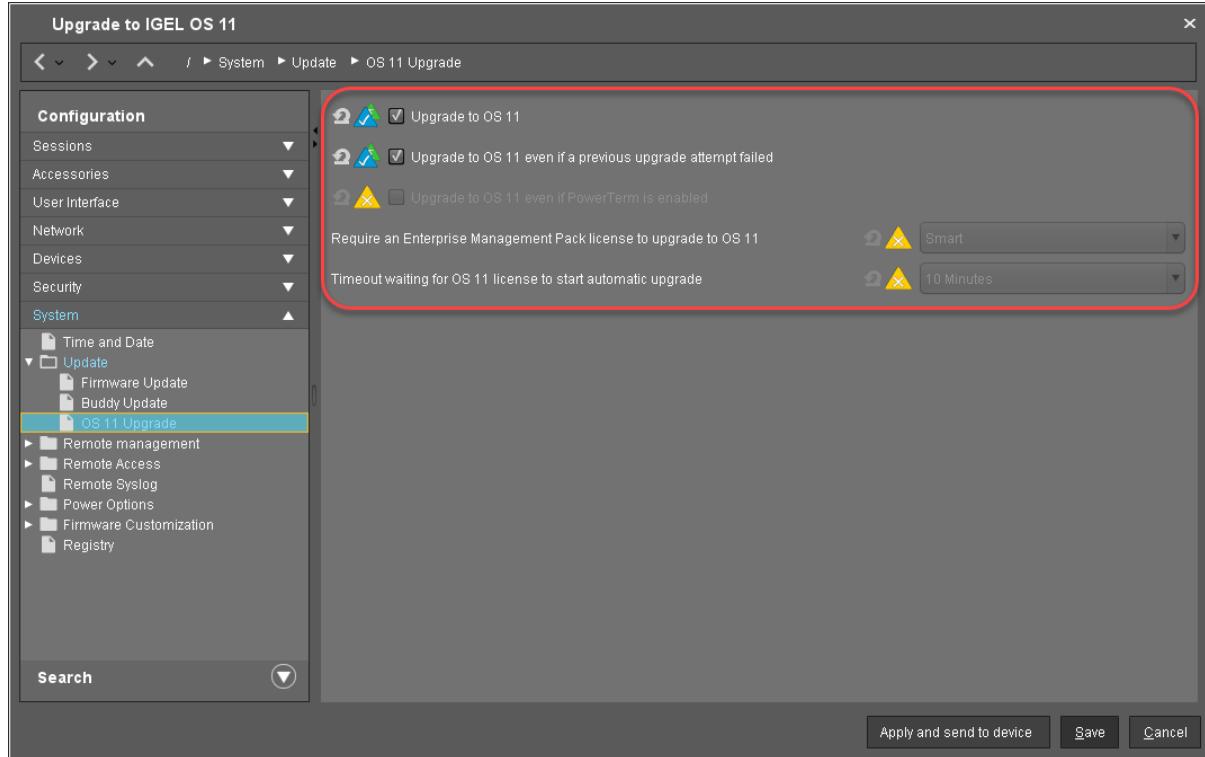
7. Make the following settings according to your needs:

- If you want the device to retry the upgrade immediately after a failed attempt, activate **Upgrade to OS 11 even if a previous upgrade attempt failed**. With this setting, the device will retry the upgrade 5 times. When the 5th attempt has failed, a message will be shown in the upgrade tool window.
- If your device has a PowerTerm license, and you want to upgrade to IGEL OS 11 even though IGEL OS 11 does not support PowerTerm, you must activate **Upgrade to OS 11 even if PowerTerm is enabled**.
- Under **Require an Enterprise Management Pack license to upgrade to OS 11**, select the appropriate option:
  - If you are using IGEL Cloud Gateway (ICG) or Shared Workplace (SWP) or a Custom Partition and want to make sure that the upgrade is performed only if these features can be used furthermore, select **Smart**. When **Smart** is selected, and one of these features is activated, the upgrade is performed only if the device succeeded in fetching a license from an Enterprise Management Pack.
  - If you want to force the device to fetch a license from an Enterprise Management Pack and make sure that the upgrade is performed only if this license has been fetched, select **Always**.
  - If you want the device to upgrade to IGEL OS 11 without fetching a license from an Enterprise Management Pack, disregarding the features, select **Never**.

8. Under **Timeout waiting for OS 11 license to start automatic upgrade**, set the time period the device will wait for a license in a mass deployment scenario. This setting prevents the device from

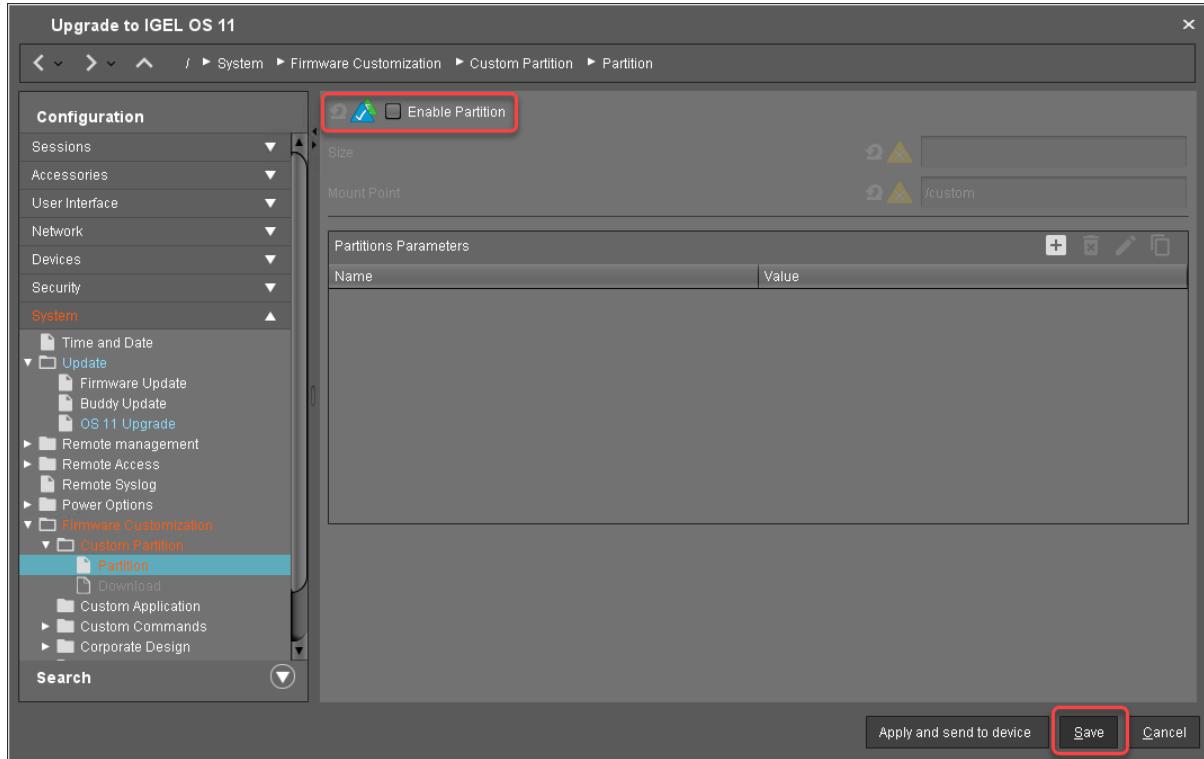


starting the upgrade at an inappropriate time as a result of the license just being deployed. This way, the setting prevents unwanted interruptions at work. For a mass deployment scenario, the default value **10 Minutes** is recommended.

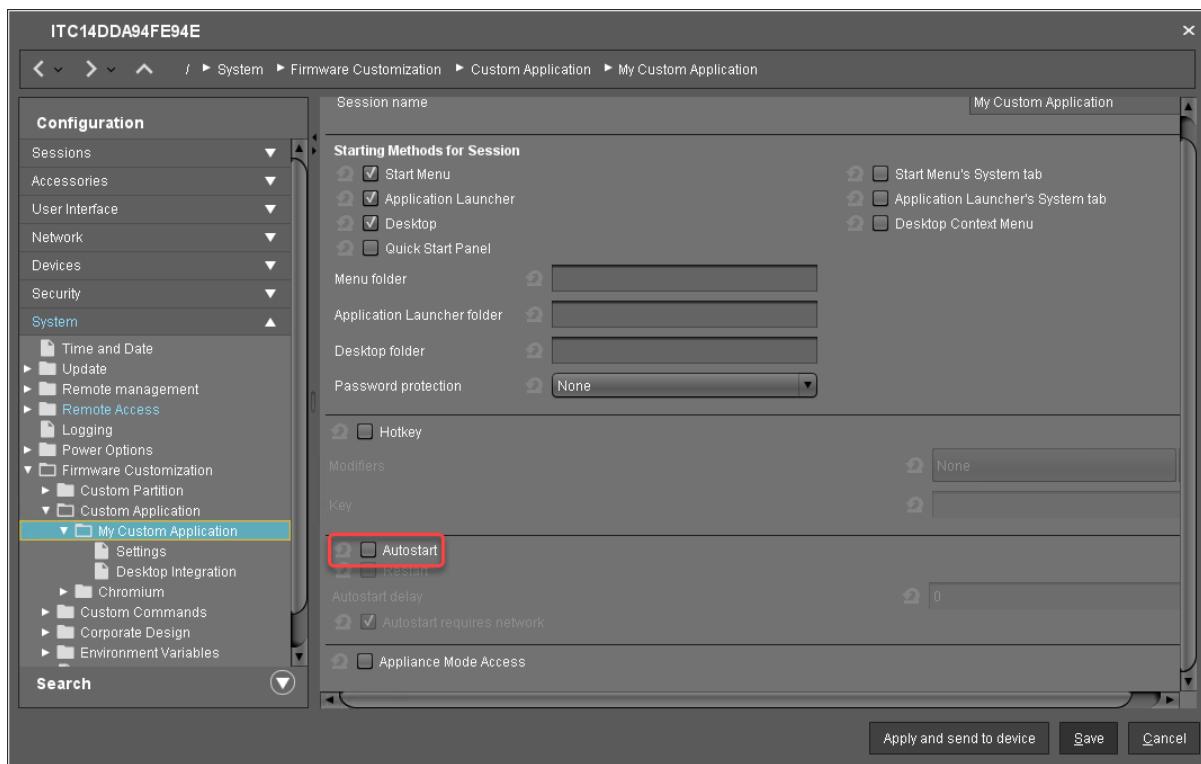




9. If you have a Custom Partition, go to **Firmware Customization > Custom Partition > Partition** and deactivate **Enable Partition**.



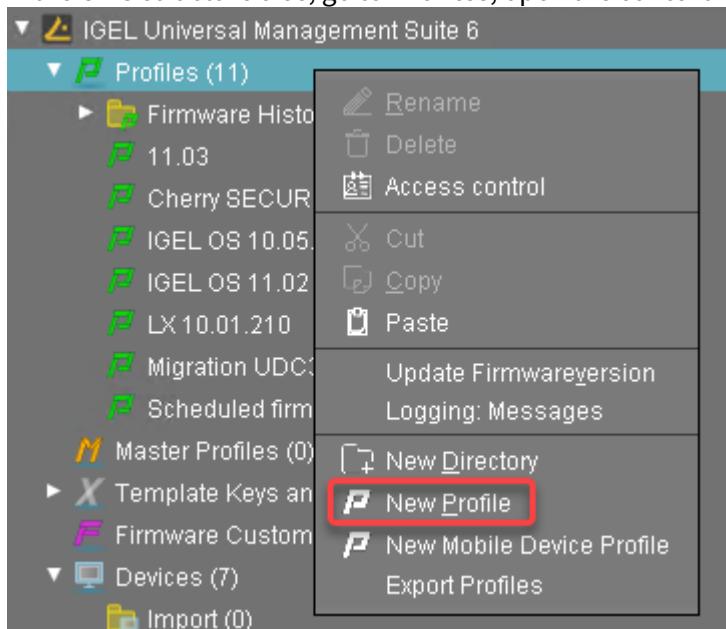
10. If you have custom applications, go to **Firmware Customization > Custom Application** and, for each custom application, deactivate **Autostart**. This is to prevent the custom application from interfering with the device's system before it can be tested properly.



**11. Click **Save**.**

For Devices That Are Connected via ICG

- In the UMS structure tree, go to **Profiles**, open the context menu and select **New Profile**.

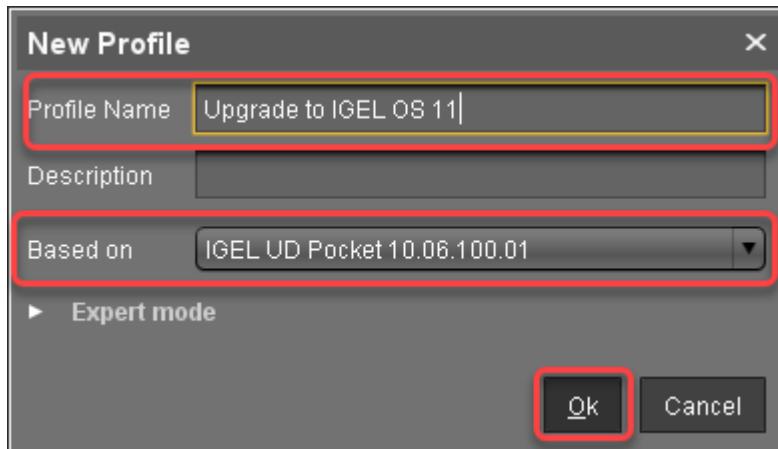


- Enter the following data:



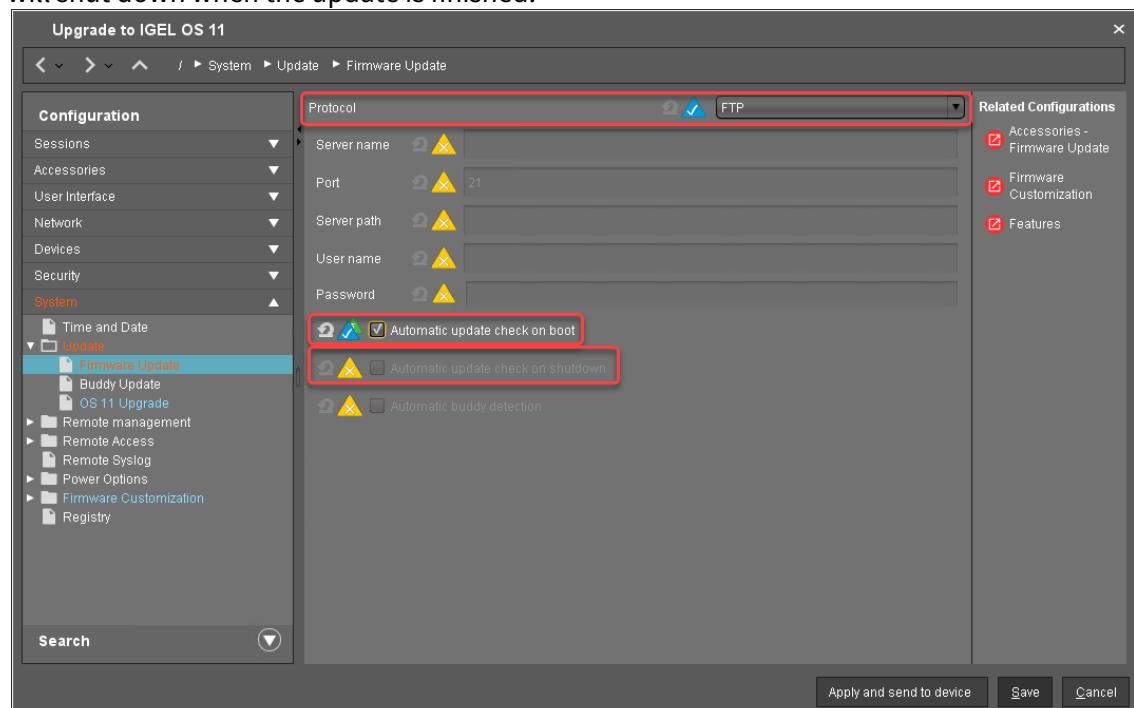
- **Profile Name:** Name for the profile, e. g. "Upgrade to IGEL OS 11".
- **Description:** Optional description for the profile.
- **Based on:** Firmware version for the profile; select the current firmware of your devices, that is, "IGEL UD Pocket 10.06.100".

3. Click **Ok**.



4. Go to **System > Update > Firmware Update** and change the settings as follows:

- Select "FTP" as Protocol.
- Activate **Automatic update check on boot**.
- Ensure that **Automatic update check on shutdown** is deactivated. Otherwise, the device will shut down when the update is finished.



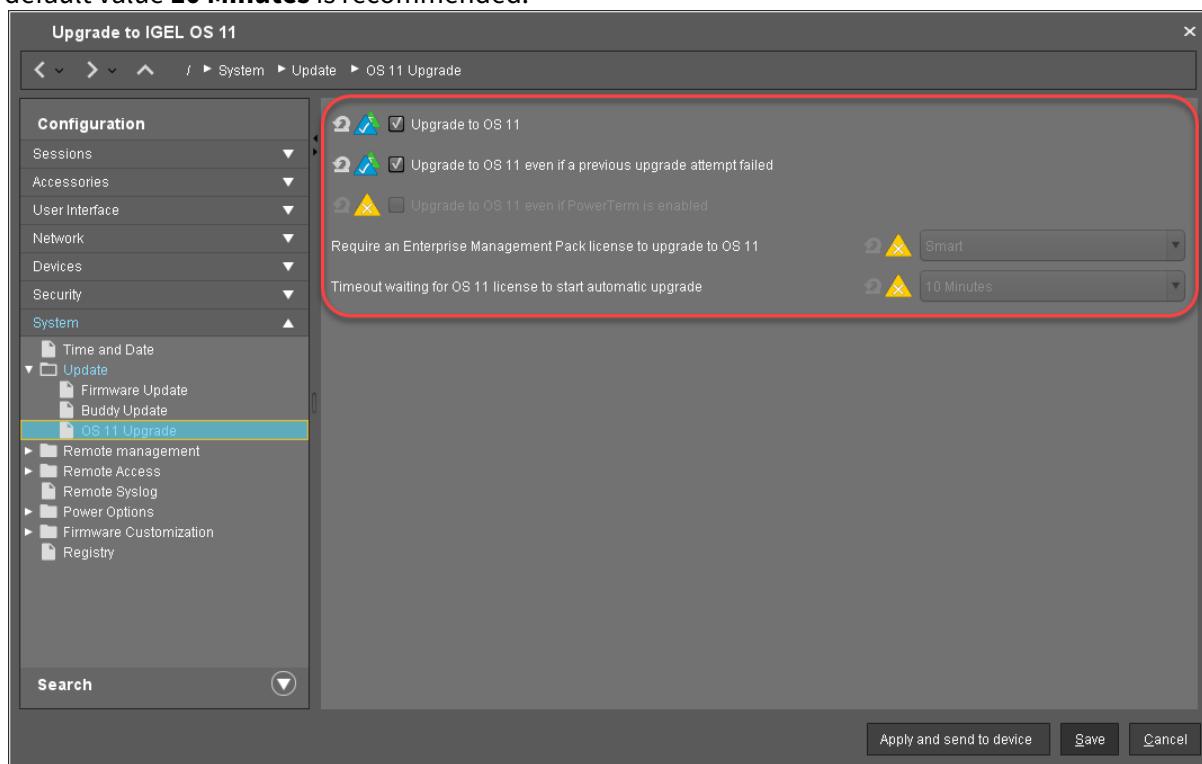
5. Go to **System > Update > Firmware Update > OS 11 Upgrade**.

6. Activate **Upgrade to OS 11**.

7. Make the following settings according to your needs:



- If you want the device to retry the upgrade immediately after a failed attempt, activate **Upgrade to OS 11 even if a previous upgrade attempt failed**. With this setting, the device will retry the upgrade 5 times. When the 5th attempt has failed, a message will be shown in the upgrade tool window.
  - If your device has a PowerTerm license, and you want to upgrade to IGEL OS 11 even though IGEL OS 11 does not support PowerTerm, you must activate **Upgrade to OS 11 even if PowerTerm is enabled**.
  - Under **Require an Enterprise Management Pack license to upgrade to OS 11**, select the appropriate option:
    - If you are using IGEL Cloud Gateway (ICG) or Shared Workplace (SWP) or a Custom Partition and want to make sure that the upgrade is performed only if these features can be used furthermore, select **Smart**. When **Smart** is selected, and one of these features is activated, the upgrade is performed only if the device succeeded in fetching a license from an Enterprise Management Pack.
    - If you want to force the device to fetch a license from an Enterprise Management Pack and make sure that the upgrade is performed only if this license has been fetched, select **Always**.
    - If you want the device to upgrade to IGEL OS 11 without fetching a license from an Enterprise Management Pack, disregarding the features, select **Never**.
8. Under **Timeout waiting for OS 11 license to start automatic upgrade**, set the time period the device will wait for a license in a mass deployment scenario. This setting prevents the device from starting the upgrade at an inappropriate time as a result of the license just being deployed. This way, the setting prevents unwanted interruptions at work. For a mass deployment scenario, the default value **10 Minutes** is recommended.



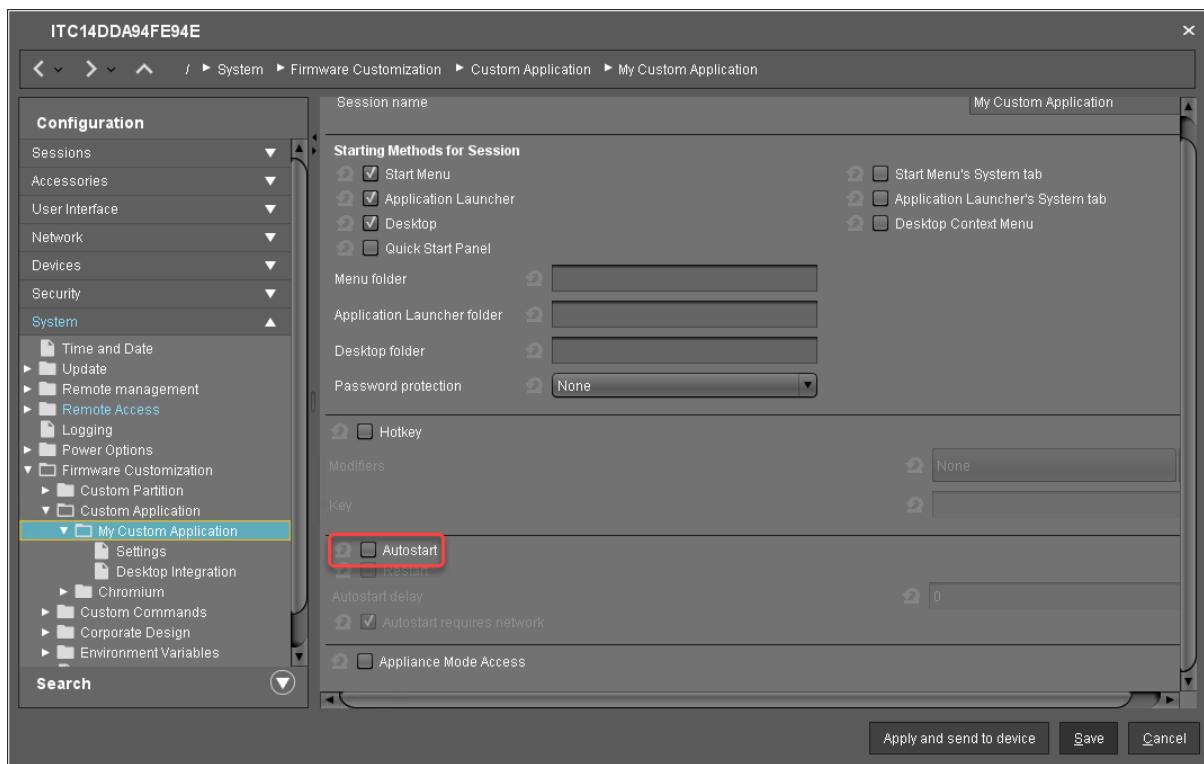


9. If you have a Custom Partition, go to **Firmware Customization > Custom Partition > Partition** and deactivate **Enable Partition**.

A screenshot of the IGEL Firmware Customization interface. The window title is "ITC14DDA94FE94E". The left sidebar shows a tree view of configuration categories: Sessions, Accessories, User Interface, Network, Devices, Security, and System. Under System, there are several sub-options like Time and Date, Update, Remote management, and Firmware Customization. Under Firmware Customization, there is a "Custom Partition" section which is expanded, showing "Partition" and "Download" as sub-options. The main panel has a message "This feature requires an active Enterprise Management Pack subscription." followed by a checkbox labeled "Enable Partition" which is unchecked. Below this are fields for "Size" (set to 250M) and "Mount Point" (set to /custom). A table titled "Partitions Parameters" is present but empty. At the bottom right are buttons for "Apply and send to device", "Save", and "Cancel".

This feature requires an active Enterprise Management Pack subscription.  
 Enable Partition  
Size: 250M  
Mount Point: /custom  
Partitions Parameters  
Name Value  
Apply and send to device Save Cancel

10. If you have custom applications, go to **Firmware Customization > Custom Application** and, for each custom application, deactivate **Autostart**. This is to prevent the custom application from interfering with the device's system before it can be tested properly.



11. Click **Save**.

#### Check List

- The upgrade profile is configured properly for your needs.

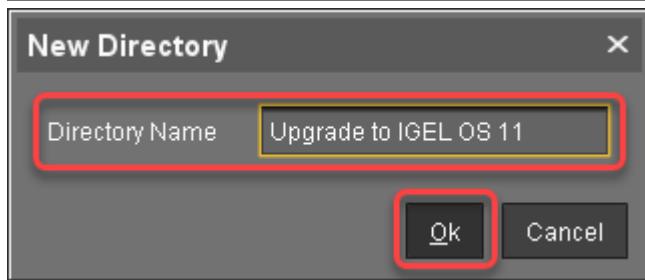
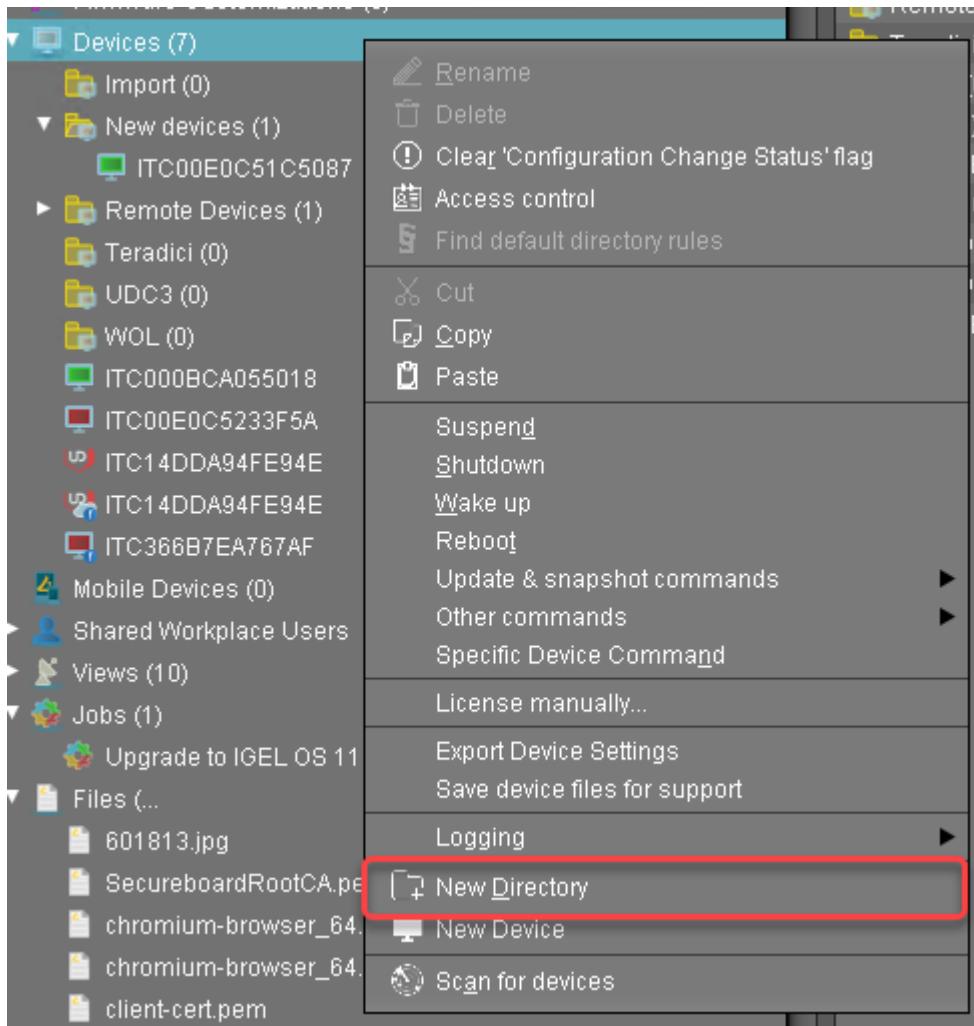
#### Next Step

>> [Assigning the Upgrade Profile and the Universal Firmware Update to the Test Devices](#)(see page 100)

### Assigning the Upgrade Profile and the Universal Firmware Update to the Test Devices

1. If you have not already created a directory as a distribution condition while setting up Automatic License Deployment (ALD): In the **Devices** node of the UMS structure tree, create a directory and name it "Upgrade to IGEL OS 11", for instance. For more information about distribution conditions, see [Configuring the Distribution Conditions](#)<sup>44</sup>, section "Distributing Licenses to Devices in a Specified Directory".

<sup>44</sup> <https://kb.igel.com/display/licensesmoreigelos11/Configuring+the+Distribution+Conditions>

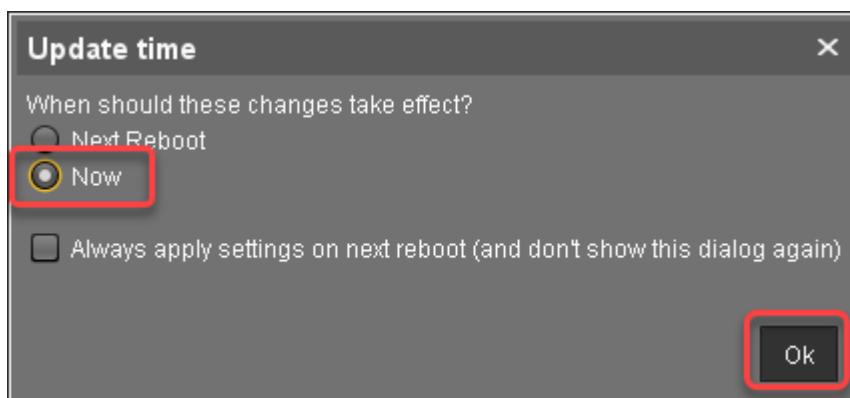




2. Put the devices that are to be updated into the new directory. You can use drag & drop.

3. In the **Update time** dialog, select **Now** and click **Ok**.

The directory change is communicated immediately to the device.

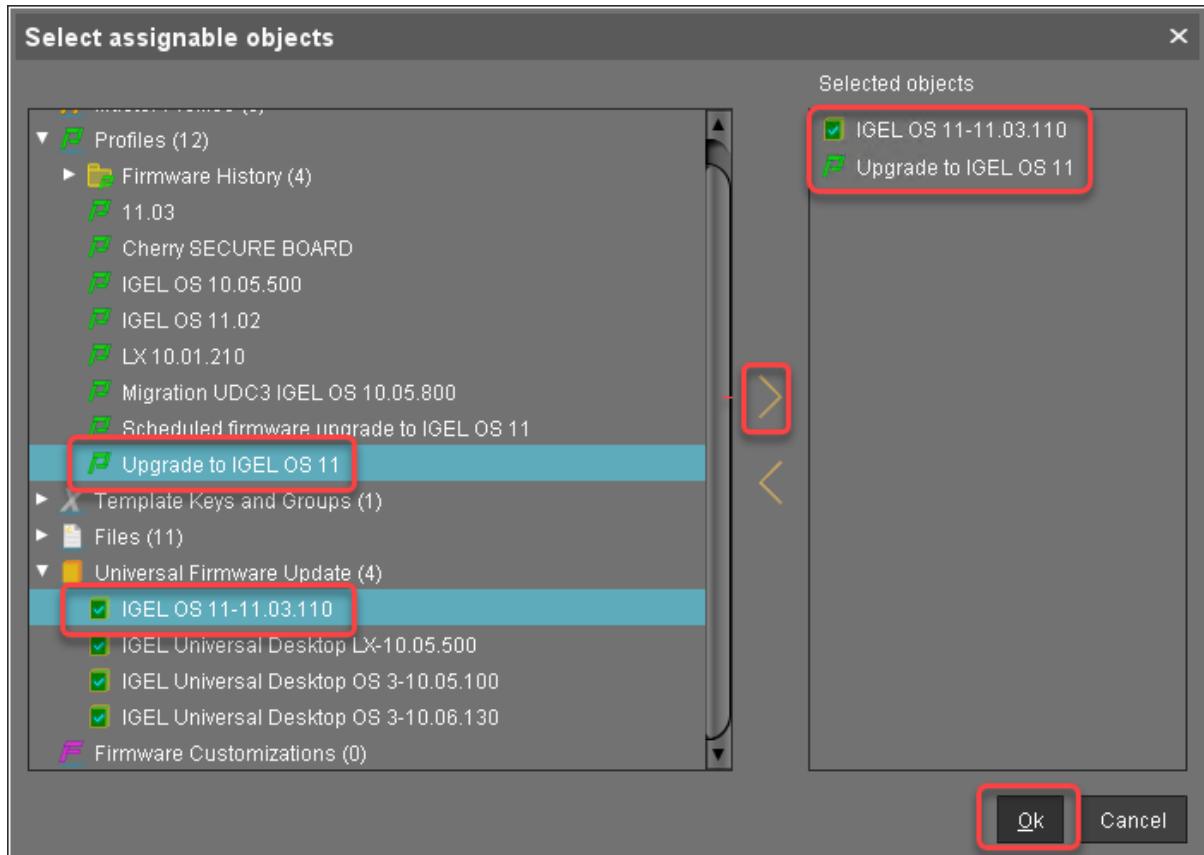


4. Select the directory and in the **Assigned objects** area, click **+**.

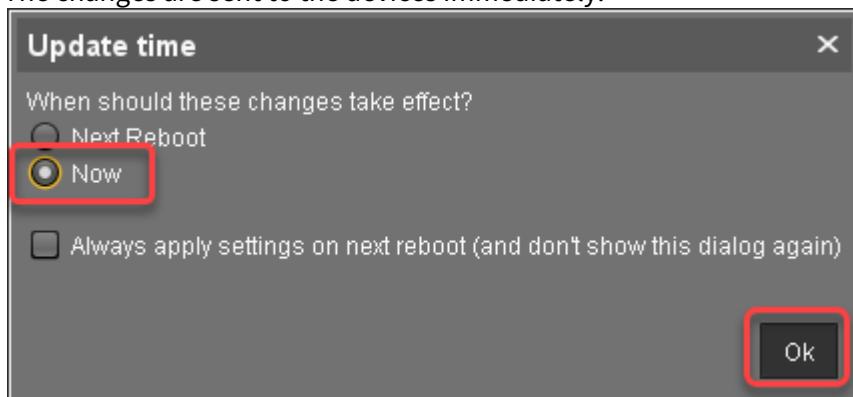
Name	Last known...	MAC Adr...	Product	Ver...
ITC14...	172.30.9...	14DD...	IGEL...	10.0...



5. Assign the upgrade profile and the Universal Firmware Update for IGEL OS 11.03 to the directory and click **Ok**.



6. In the **Update time** dialog, select **Now** and click **Ok**.  
The changes are sent to the devices immediately.





In the **Assigned objects** area, the profile and the Universal Firmware Update are shown:

A screenshot of a software interface titled "Assigned objects". At the top, there are four icons: a pencil, a clipboard, a plus sign, and a minus sign. Below the title is a table with a single column labeled "Name". Two items are listed: "Upgrade to IGEL OS 11" and "IGEL OS 11-11.03.110". The first item has a red rectangular box drawn around it, highlighting it.

If you are using Automatic License Deployment (ALD), it might be feasible to confine the distribution of licenses to the current directory. For more information, see [Configuring the Distribution Conditions<sup>45</sup>](#), section "Distributing Licenses to Devices in a Specified Directory".

#### Check List

- ✓ The test devices are in a directory to which the upgrade profile and the Universal Firmware Update are assigned.

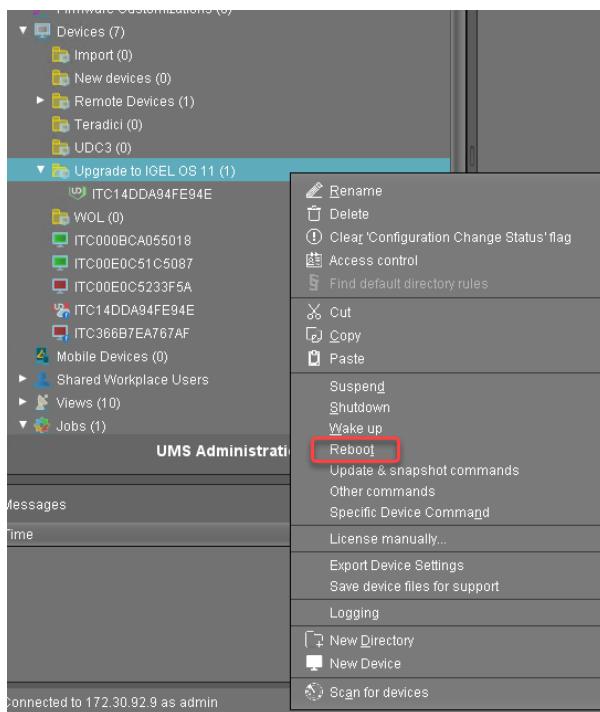
#### Next Step

>> [Testing the Upgrade](#)(see page 104)

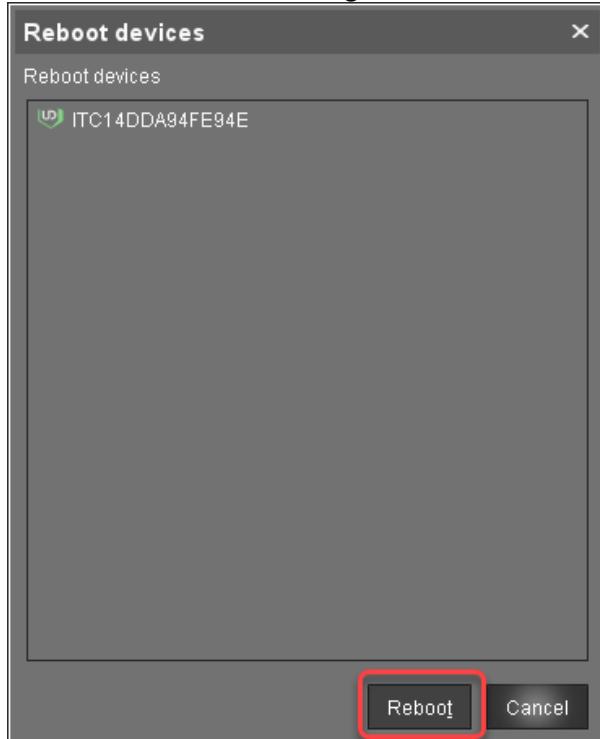
#### Testing the Upgrade

1. In the UMS, select the directory containing the test devices and select **Reboot**.

<sup>45</sup> <https://kb.igel.com/display/licensesmoreigelos11/Configuring+the+Distribution+Conditions>



2. In the **Reboot devices** dialog, click **Reboot**.



If no IGEL OS 11 licenses have been deployed on the devices yet, the licenses are deployed within a few minutes. The upgrade will be started when the licenses are deployed. The maximum time period the device will wait for a license is configured by the parameter **Timeout waiting for OS 11**



**license to start automatic upgrade;** for details, see [Creating an Upgrade Profile\(see page 91\)](#), step 8. The parameter **Automatic update check on boot** makes the devices look for new firmware again. Although two Universal Firmware Updates are assigned to the devices, the UMS offers the IGEL OS 11 firmware, because the ID of the IGEL OS 11 firmware is higher than the ID of the IGEL OS 10 firmware.

The upgrade is completed.

3. Check whether all features and functions of your test devices are working as expected.

#### Check List

- ✓ All features and functions of your test devices are working as expected.

#### Next Step

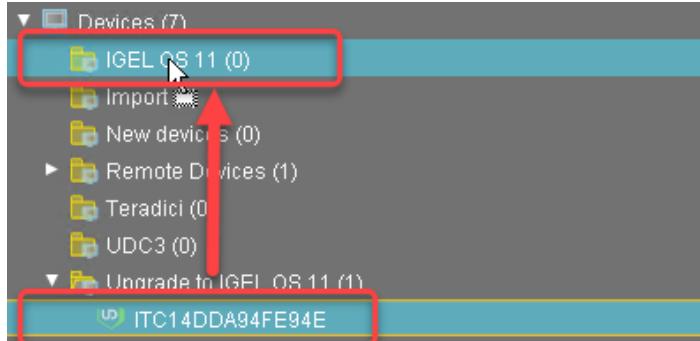
>> [Unassigning the Upgrade Profile and the Universal Firmware Update\(see page 106\)](#)

### Unassigning the Upgrade Profile and the Universal Firmware Update

The upgrade profile and the Universal Firmware Update should be unassigned from the devices after they have been upgraded to IGEL OS 11 successfully.

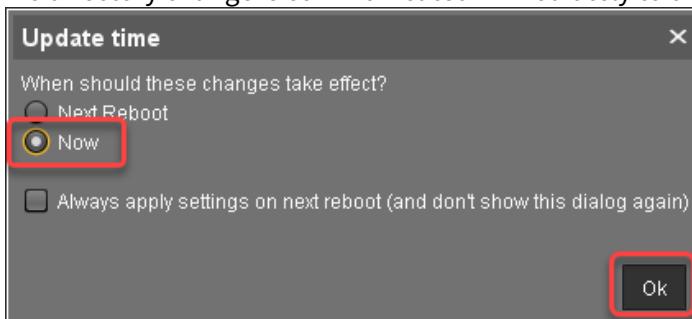
To unassign upgrade profile and the Universal Firmware Update:

1. Move the devices to a different folder.



2. In the **Update time** dialog, select **Now** and click **Ok**.

The directory change is communicated immediately to the devices.



If a device had a Custom Partition before, it will be downloaded by the device and activated again.



## Check List

If a device had a Custom Partition before:

- The Custom Partition has been downloaded by the device and activated.

## Next Step

If some devices have a Custom Partition:

>> [If Applicable: Restoring Custom Partition and Custom Application\(see page 107\)](#)

If no device has a Custom Partition:

>> [Upgrading All Devices\(see page 107\)](#)

## If Applicable: Restoring Custom Partition and Custom Applications

If a device had a custom partition before the upgrade, it has been downloaded and activated again after the upgrade profile has been unassigned; see [Unassigning the Upgrade Profile and the Universal Firmware Update\(see page 106\)](#). It cannot be ruled out that custom commands and the applications and drivers of a Custom Partition disturb your device's system. Therefore, it is very important to check the Custom Partition, the custom applications, and the device's basic functionality.

1. Test the Custom Partition and the custom applications. If errors should occur, modify the Custom Partition and the custom applications accordingly.
2. Check if all other functions are still working properly.

## Check List

- The Custom Partition and the custom applications are enabled and can be used.
- All other functions are working properly.

## Next Step

>> [Upgrading All Devices\(see page 107\)](#)

## Upgrading All Devices

### Assigning the Upgrade Profile and the Universal Firmware Update to the Devices

1. Put the devices that are to be upgraded into the directory you have created for the test devices. It is recommended to use cut and paste.



The screenshot shows the IGEL OS interface with a context menu open over a selected device. The device name, "ITC000BCA055018", is highlighted with a red box. The context menu options are:

- Edit Configuration
- Rename
- Delete
- Clear 'Configuration Change Status' flag
- Access control

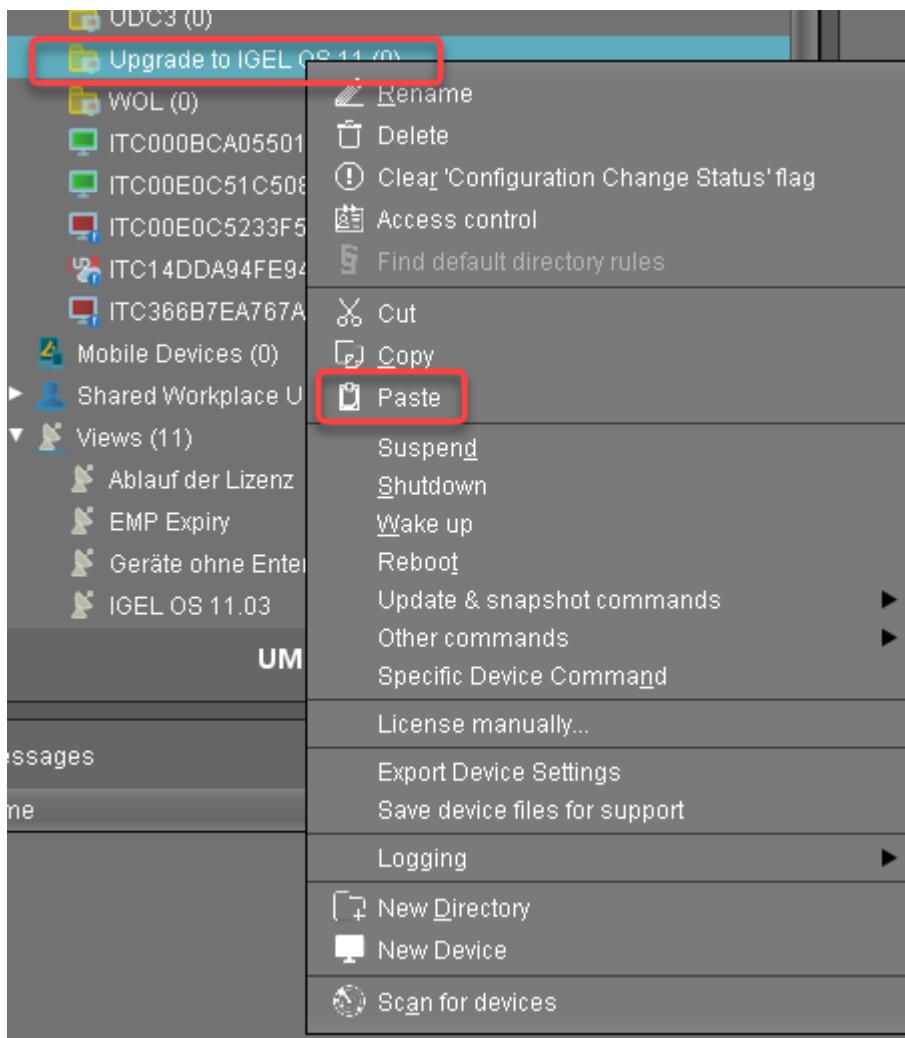
Below these are additional options:

- Cut (highlighted with a red box)
- Copy
- Paste
- Shadow
- Secure Terminal
- Suspend
- Shutdown
- Wake up
- Reboot
- Update & snapshot commands
- Other commands
- Specific Device Command

At the bottom of the menu are:

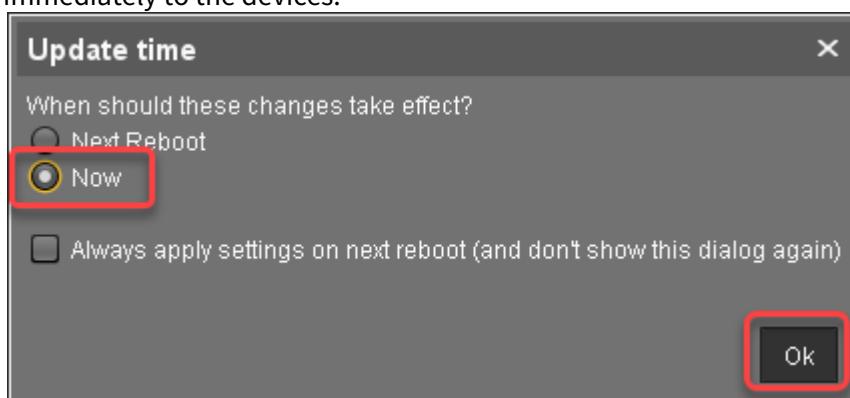
- Take over settings from ...
- Export Device Settings
- Save device files for support
- Release IGEL Cloud Gateway license

On the left side of the interface, there are navigation sections for Teradici, UDC3, Upgrade to IGEL OS 11, WOL, Mobile Devices, Shared Workplaces, and Views (11). The Views section is expanded, showing sub-options like Ablauf der Li, EMP Expiry, Geräte ohne, and IGEL OS 11. The status bar at the bottom indicates "Connected to 172.30.92".



2. In the **Update time** dialog, select **Now** and click **Ok**.

The directory change, the upgrade profile and the Universal Firmware Update are communicated immediately to the devices.



3. In the UMS, select the directory with the devices and select **Reboot**.



The screenshot shows the UMS Administration interface with a context menu open over a device entry in the list. The device entry is titled "Upgrade to IGEL OS 11 (1)" and contains several items: ITC14DDA94FE94E, WOL (0), ITC000BCA055018, ITC00E0C51C5087, ITC00E0C5233F5A, ITC14DDA94FE94E, ITC366B7EA767AF, Mobile Devices (0), Shared Workplace Users, Views (10), and Jobs (1).

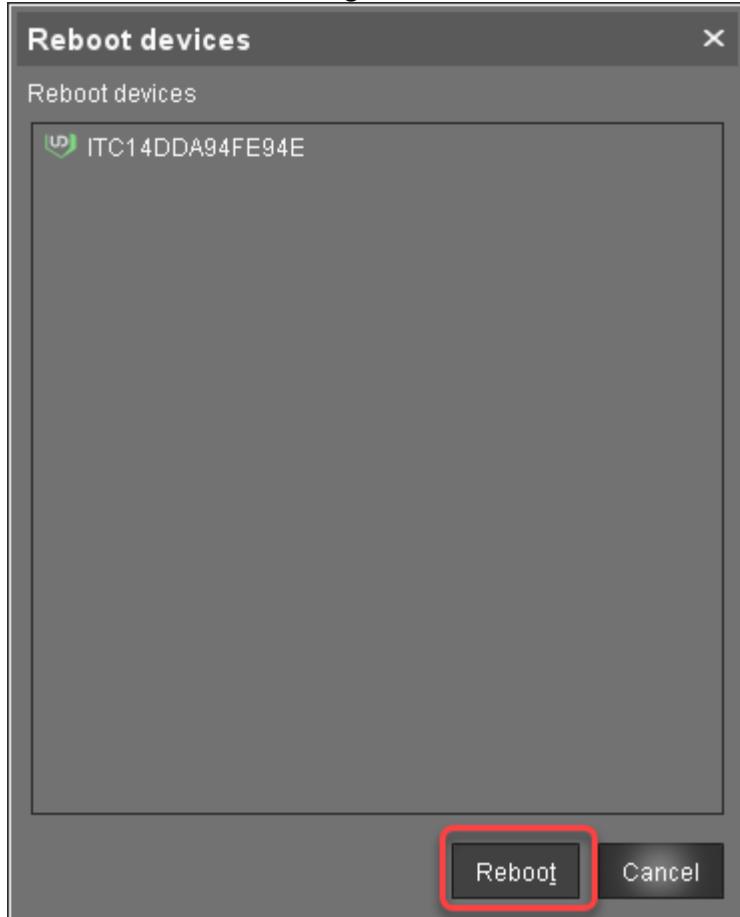
The context menu options are:

- Rename
- Delete
- Clear 'Configuration Change Status' flag
- Access control
- Find default directory rules
- Cut
- Copy
- Paste
- Suspend
- Shutdown
- Wake up
- Reboot** (highlighted with a red box)
- Update & snapshot commands
- Other commands
- Specific Device Command
- License manually...
- Export Device Settings
- Save device files for support
- Logging
- New Directory
- New Device
- Scan for devices

At the bottom left of the interface, it says "Connected to 172.30.92.9 as admin".



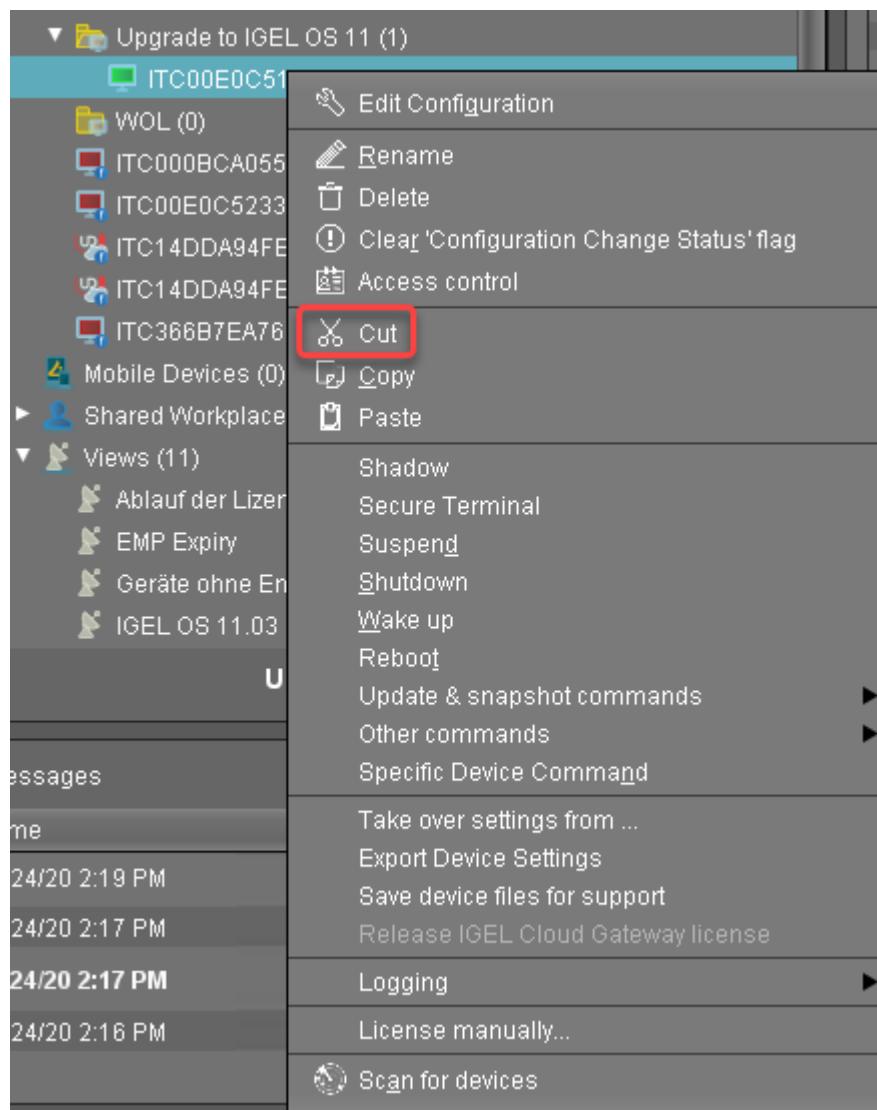
4. In the **Reboot devices** dialog, click **Reboot**.

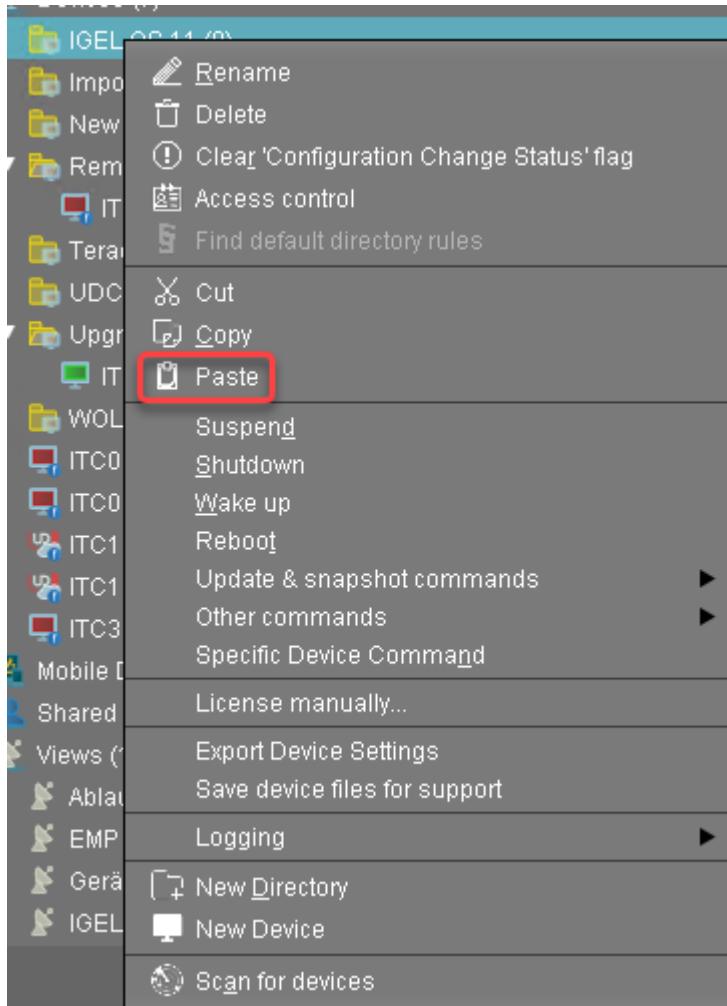


If no IGEL OS 11 licenses have been deployed on the devices yet, the licenses are deployed within a few minutes. The upgrade will be started when the licenses are deployed. The maximum time period a device will wait for a license is configured by the parameter **Timeout waiting for OS 11 license to start automatic upgrade**; for details, see [Creating an Upgrade Profile](#)(see page 91), step 8. The parameter **Automatic update check on boot** makes the devices look for new firmware again. Although two Universal Firmware Updates are assigned to the devices, the UMS offers the IGEL OS 11 firmware, because the ID of the IGEL OS 11 firmware is higher than the ID of the IGEL OS 10 firmware.

#### Unassigning the Upgrade Profile and the Universal Firmware Update

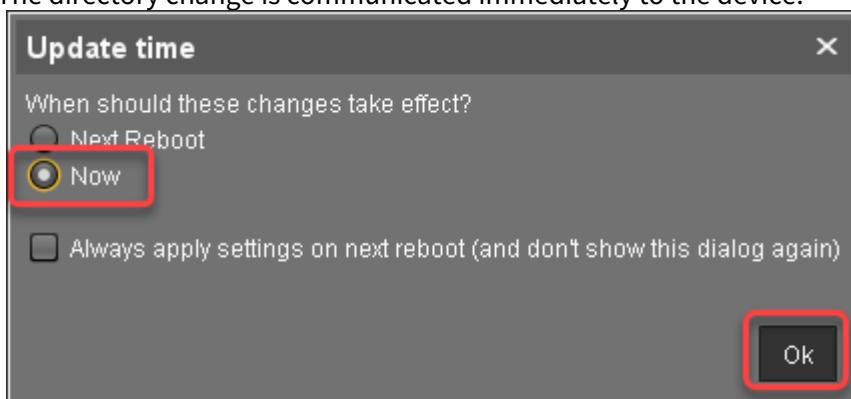
1. To unassign the upgrade profile and the Universal Firmware Update, move the devices to a different folder.





2. In the **Update time** dialog, select **Now** and click **Ok**.

The directory change is communicated immediately to the device.



If a device had a Custom Partition before the upgrade, it has been downloaded and activated again after the upgrade profile has been unassigned.

3. If applicable, restore the required custom applications; see [If Applicable: Restoring Custom Partition and Custom Applications](#)(see page 107).



### Update Can Be Canceled After Timeout

An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

### Check List

- All devices have been upgraded to IGEL OS 11.
- All required functionality is available, including custom applications.

### 2.2.3 Upgrading from IGEL OS 10 to IGEL OS 11

- [Upgrading UDC3 Devices from IGEL OS 10 to IGEL OS 11](#)(see page 114)
- [Upgrading IGEL Devices from IGEL OS 10 to IGEL OS 11](#)(see page 174)

#### Upgrading UDC3 Devices from IGEL OS 10 to IGEL OS 11

This document describes how to upgrade any number of devices (UDC3) from IGEL OS 10 to IGEL OS 11.

IGEL OS 10.05.800 or higher is required for upgrading to IGEL OS 11. If you have an older version of IGEL OS 10, you need to update to version 10.05.800 or a higher version first.

Since a new licensing model has been introduced with IGEL OS 11, a license from an IGEL Workspace Edition Product Pack must be available for each device. If you have a valid maintenance for your devices, you can convert your existing UDC3 or UD Pocket Product Packs to Workspace Edition (WE) Product Packs; see [Converting UDC3 or UD Pocket Licenses for Upgrading to IGEL OS 11](#)<sup>46</sup>.

The following methods of mass deployment are described here:

- [Zero-Touch Deployment Using Universal Firmware Update](#)(see page 115): Mass upgrade from any version of IGEL OS 10 to IGEL OS 11 in one step using Universal Firmware Update. This method can be started immediately or as a scheduled job (wake up or reboot).
- [Zero-Touch Deployment Using Buddy Update](#)(see page 141): Mass upgrade from any version of IGEL OS 10 to IGEL OS 11 in one step using two devices as update buddies. This method can be started immediately or as a scheduled job (wake up or reboot).
- [Zero-Touch Deployment Using a Scheduled Job](#)(see page 158): Upgrade devices that are already running IGEL OS 10.05.800 (or higher) using a specific scheduled job.

---

<sup>46</sup> <https://kb.igel.com/display/licensesmoreigelos11/Converting+UDC3+or+UD+Pocket+Licenses+for+Upgrading+to+IGEL+OS+11>



## Zero-Touch Deployment Using Universal Firmware Update

This method is the most convenient way to upgrade from IGEL OS 10 to IGEL OS 11. The method uses the Universal Firmware Update feature of the UMS (Universal Management Suite) and a profile.

Read all the following chapters carefully and follow the instructions.

1. Devices That Can Be Upgraded to Igel OS 11(see page 115)
2. Important! Consider This Before Upgrading(see page 121)
3. Preparing the Upgrade(see page 122)
4. Testing the Upgrade(see page 124)
5. Checking the Requirements(see page 128)
6. Creating the Universal Firmware Updates(see page 129)
7. Creating a Profile(see page 133)
8. Deploying the Licenses(see page 137)
9. Putting It All Together(see page 138)
10. Executing the Upgrade(see page 140)

### Devices That Can Be Upgraded to Igel OS 11

#### Core Requirements

- CPU with 64-bit support
- CPU speed  $\geq$  1 GHz
- $\geq$  2 GB memory (RAM)

With devices that have 2 GB RAM and shared video memory, a maximum of 512 MB may be used as video memory.

- Recommended:  $\geq$  4 GB; minimum 2 GB storage

#### Storage Requirements for IGEL OS 11.04 or Higher

IGEL OS 11.04.100 or higher requires at least 2.4 GB storage if the full feature set is applied. Thus, the feature set must be modified accordingly; for more information, see Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher(see page 231).

- No VIA graphic adapter; VIA graphics support is discontinued in IGEL OS.
- Legacy Bios and EFI/UEFI are supported.

### Devices Officially Supported by OSC and UD Pocket with IGEL OS 11



The following list only includes those devices that are **tested by IGEL** (with each major release of IGEL OS). By no means it implies that the devices which are not included in this list but meet the [core requirements](#)(see page 115) will not function with IGEL OS.

Further supported devices can be found on the [IGEL Ready<sup>47</sup>](#) Showcase at <https://www.igel.com/ready/showcase-categories/endpoints/>.

Integrated drivers and supported peripherals are listed in the [Third-Party Hardware Database<sup>48</sup>](#). For more solutions compatible with IGEL OS, see [Partner Solutions<sup>49</sup>](#).

For some of the devices listed here, Flash memory must be extended to  $\geq 2$  GB. For these devices, an appropriate note is added.

#### ADS-Tec

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
VMT9000	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100

#### Advantech

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
POC-W213L	Medical All in One	4 GB	128 GB	Intel Core i7-7300U	11.01.100
POC-W243L*(see page 121)	Medical All in One	4 GB	32 GB	Intel Kaby Lake Core i5-7300U	11.01.110
POC-W243L*(see page 121)	Medical All in One	4 GB	128 GB	Intel Core i7-7300U	11.01.100

#### Advantech-DLoG

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
DLT-V6210	Industrial PC/ Terminal	4 GB	32 GB	Intel Atom	11.01.100

<sup>47</sup> <https://www.igel.com/technology-partners/>

<sup>48</sup> <https://www.igel.com/linux-3rd-party-hardware-database/>

<sup>49</sup> <https://kb.igel.com/display/igelos1105/Partner+Solutions>



Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
DLT-V7210 K	Industrial PC/Terminal	4 GB	4 GB	Intel Atom E3845	11.01.100

Dell / Wyse

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
(AiO) 5040 / 5212	All in One	2 GB	2 GB	AMD G-T48E	11.01.100
3040	Thin Client	2 GB	8 GB	Intel Atom x5-Z8350	11.01.100
5020	Thin Client	2 GB	8 GB	AMD G-Series SoC	11.02.140
5060	Thin Client	4 GB	8 GB	AMD GX-424CC	11.01.100
5070	Thin Client	8 GB	32 GB	Intel Celeron J4105	11.01.100
Latitude 5510	Laptop/Notebook	8 GB	256 GB	Intel Core i5-10210U	11.05.100

Elo

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
(AiO) i2 Touch (15 and 22 inches)	All in One	8 GB	128 GB	Intel Core i3-8100T	11.05.100

Fujitsu

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
Q957	Desktop PC	8 GB	500 GB	Intel Core i3-6100	11.02.100
FUTRO S740	Thin Client	4 GB	8 GB	Intel Celeron J4105	11.04.100

HP

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
t420	Thin Client	2 GB	8 GB	AMD Embedded G-Series GX-209JA	11.02.100
t430	Thin Client	2 GB	16 GB	Intel® Celeron® N4000	11.01.110



Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
t530	Thin Client	4 GB	8 GB	AMD GX-215JJ Dual-Core	11.01.100
t630	Thin Client	4 GB	8 GB	AMD GX-420GI	11.01.100
t730	Thin Client	16 GB	8 GB	AMD RX-427BB APU	11.01.100
t820	Thin Client	16 GB	16 GB	Intel Core i5-4570S	11.01.100
t640	Thin Client	4 GB	16 GB	AMD Ryzen R1505G	11.04.100
t540	Thin Client	16 GB	16 GB	AMD Ryzen Embedded R1305G	11.06.100

Intel

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
NUC 5i5MYHE	Desktop PC	2 GB	32 GB	Intel i5-5300U	11.01.100
NUC 5i3RYH	Desktop PC	2 GB	2 GB	Intel i3-5010U	11.01.100
NUC 7CJYH	Desktop PC	2 GB	4 GB	Intel Celeron J4005	11.01.100

Lenovo

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
ThinkCentre M625q	Desktop PC	4 GB	32 GB	AMD E2-9000e	11.04.100
ThinkCentre M75n	Desktop PC	8 GB	128 GB	AMD Ryzen 3 Pro 3300U	11.05.100
ThinkCentre M70q	Desktop PC	8 GB	500 GB	Intel Pentium Gold G6400T	11.05.100
L14	Laptop/Notebook	64 GB	1000 GB	AMD Ryzen 7 Pro 4750	11.05.100
14w	Laptop/Notebook	8 GB	128 GB	AMD A6	11.05.100

LG



Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
(AiO) 24CK550N **(see page 121)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
(AiO) 24CK550W **(see page 121)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
(AiO) 24CK560N **(see page 121)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
CK500W	Thin Client	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
(AiO) 38CK950N	All in One	8 GB	128 GB	AMD Ryzen 3	11.02.100
(AiO) 38CK900N	All in One	8 GB	128 GB	AMD Ryzen 3	11.02.100
CL600N	Thin Client	4 GB	16 GB	Intel® Celeron J4105	11.03.100
CL600W	Thin Client	8 GB	128 GB	Intel® Celeron J4105	11.03.100
(AiO) 34CN650N	All in One	4 GB	16 GB	Intel® Celeron J4105	11.05.100

## OnLogic

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
CL210G-10	Industrial PC/Terminal	4 GB	32 GB	Intel Celeron N3350	11.04.100
KARBON 300	Desktop PC	4 GB	32 GB	Intel Atom x5-E3930	11.04.100

## Onyx Healthcare

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
Venus 223	Medical All in One	4 GB	128 GB	Intel Quad-Core J1900	11.01.100

## Rein Medical



Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
Silenio C122	All in One	8 GB	128 GB	Intel® Core™ i5 – 6th Generation	11.01.110
Silenio C124	All in One	8 GB	128 GB	Intel® Core™ i5 – 6th Generation	11.01.110
Clinio S 522TCT	Medical All in One	8 GB	16 GB	Intel® Pentium® Silver J5005	11.04.100
Clinio S 524TCT	Medical All in One	8 GB	16 GB	Intel® Pentium® Silver J5005	11.04.100

## Secunet

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
SINA Workstation S EliteDesk 800 G2	Workstation	16 GB	256 GB	Intel Core i7-6700	11.01.100

## Toshiba

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
Portégé X20W-D	Laptop/Notebook	8 GB	256 GB	Intel Core i5-7200U	11.01.100
Portégé X30-D	Laptop/Notebook	8 GB	256 GB	Intel Core i5-7300U	11.01.100
Tecra C50	Laptop/Notebook	4 GB	500 GB	Intel i5-4210U	11.01.100
Tecra Z50-D	Laptop/Notebook	8 GB	256 GB	Intel Core i5-7200U	11.01.100
SATELLITE R50	Laptop/Notebook	4 GB	500 GB	Intel i3-6006U	11.01.100

USB Memory Sticks That Can Be Used as Alternative UD Pocket Hardware

DIGITTRADE

Name	Storage	Supported from IGEL OS Version
Kobra Stick	≥ 4GB	11.05.133

Officially Supported Virtual Environments

- Tested with Ubuntu (64-bit) and default settings



Note that the use of a UD Pocket within a virtual machine is **not** supported by IGEL.

Name	Memory (RAM)	Storage	Type	Supported from IGEL OS Version
Oracle VM VirtualBox	$\geq 2$ GB	$\geq 4$ GB	Linux	11.04.100
VMware Workstation	$\geq 2$ GB	$\geq 4$ GB	Linux	11.04.100

\* Delock Adapter DP 1.2 to DVI does not work.

\*\* When using an additional 4k screen with this device, please edit the BIOS settings as follows:

1. Go to the **Chipset** screen.
2. Set **Integrated Graphics** to “Force”.
3. Set **UMA Frame Buffer Size** to “256M” or higher.

When you have confirmed that your devices can be upgraded to IGEL OS 11, make sure to consider [Important! Consider This Before Upgrading](#)(see page 121).

#### Important! Consider This Before Upgrading

To make sure that your upgrade can be successful, check the following warnings and notes; a warning symbol indicates that irreversible damage can be done to your devices.

**Existing partitions:** Any existing partition on the target drive of your device will be deleted. The installer will repartition the target device. The overall size of the newly created partitions will be calculated based on the available disk space. The minimum disk usage is 2 GB, the maximum is 16 GB.

#### No Downgrade

You cannot restore your IGEL OS 10 system once you have migrated to IGEL OS 11. The device storage is overwritten completely with a new partitioning scheme.

#### Features (e.g. Clients)

IGEL OS 11 does not have the complete feature set of IGEL OS 10. Make sure that the current version of IGEL OS 11 meets your requirements. For details, refer to the appropriate release notes.

#### Custom Partitions

The contents of custom partitions will be deleted by the upgrade. Make sure to back up the contents and restore them after the upgrade has finished. Besides becoming dysfunctional after the upgrade, applications and kernel drivers in a custom partition might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device. We recommend that you disable custom partitions when upgrading; you can enable them once the upgrade has been successfully completed.



### Custom Commands

The persistence of custom commands cannot be guaranteed. Besides becoming dysfunctional after the upgrade, custom commands might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device. In general, custom commands must be adapted for IGEL OS 11. We recommend that you disable custom commands when upgrading; you can enable them once the upgrade has been successfully completed.

### Power Supply

Ensure that the device is not running on battery power, i.e. it must be connected to a power supply during the complete upgrade process.

### Network

All devices must be connected to a WLAN or LAN. LAN is the recommended option. The device will not be upgraded if connected to OpenVPN, OpenConnect, genucard or mobile broadband.

When you have considered everything that is relevant, continue with [Preparing the Upgrade](#)(see page 122).

## Preparing the Upgrade

This section describes the required preparations and tests before any productive devices can be updated. The testing should be done with at least one device that is characteristic of your environment. This device should have every custom partition and every custom command that may possibly exist in any of your devices.

To prepare the upgrade, perform the following steps:

1. [Preparing the UMS](#)(see page 122)
2. [Adjusting the Setup](#)(see page 122)
3. [Deploying a License](#)(see page 123)
4. [Configuring the Update Source](#)(see page 124)

### Preparing the UMS

To upgrade your devices to IGEL OS 11, you need the appropriate version of the UMS. Also, the devices must be registered with the UMS to receive their licenses.

1. If you have not already done so, update your UMS to version 6.01.130 or higher. For instructions, see [Updating UMS](#)<sup>50</sup>.
2. Make sure that your devices are registered with the UMS. For more information, see the chapter [Registering Devices on the UMS Server](#)<sup>51</sup> in the UMS Manual.

When the UMS is ready, continue with [Adjusting the Setup](#)(see page 122).

### Adjusting the Setup

Depending on the features that are in use now or will be used in the future, a specific set of parameters must be set in the device's Setup.

1. In the Setup, go to **System > Firmware Update > OS 11 Upgrade**.

<sup>50</sup> <https://kb.igel.com/display/endpointmgmt601/Updating+UMS>

<sup>51</sup> <https://kb.igel.com/display/endpointmgmt601/Registering+devices+on+the+UMS+Server>



2. Make your settings as appropriate:
  - Activate **Upgrade to OS 11**.

When **Upgrade to OS 11** is activated, the device checks for a Workspace Edition license and stops checking for a legacy UDC3 or UD Pocket license. Therefore, in the UMS, it is displayed as an unlicensed device until a Workspace Edition license has been deployed.

- If you want the device to retry the upgrade immediately after a failed attempt, activate **Upgrade to OS 11 even if a previous upgrade attempt failed**. The device will retry the upgrade 5 times. When the 5th attempt has failed, a message will be shown in the upgrade tool window.
- If your device has a PowerTerm license, and you want to upgrade to IGEL OS 11 even though it does not support PowerTerm, you must activate **Upgrade to OS 11 even if PowerTerm is enabled**.
- Under **Require an Enterprise Management Pack license to upgrade to OS 11**, select the appropriate option:
  - If you are using IGEL Cloud Gateway (ICG) or Shared Workplace (SWP) or a Custom Partition and want to make sure that the upgrade is performed only if these features can be used furthermore, select **Smart**. When this option is selected, and any of these features is activated, the upgrade is performed only if the device could fetch a license from an Enterprise Management Pack.
  - If you want to force the device to fetch a license from an Enterprise Management Pack and make sure that the upgrade is performed only if the license could be fetched, select **Always**.
  - If you want the device to upgrade to IGEL OS 11 without fetching an Enterprise Management Pack, disregarding the features that might be activated, select **Never**.
- Under **Timeout waiting for OS 11 license to start automatic upgrade**, set the time period the device will wait for a license in a mass deployment scenario (see [Zero-Touch Deployment Using Universal Firmware Update](#)(see page 115), [Zero-Touch Deployment Using Buddy Update](#)(see page 141) and [Mass Deployment Using a Scheduled Job](#)(see page 209)). This setting prevents the device from starting the upgrade at an inappropriate time as a result of the license just being deployed. This way, the setting prevents unwanted interruptions at work. For a mass deployment scenario, the default value **10 Minutes** is recommended.

### 3. Click **Apply**.

When the Setup is adjusted, continue with [Deploying a License](#)(see page 123).

#### Deploying a License

To upgrade from IGEL OS 10 to IGEL OS 11, you need an appropriate license. Depending on your requirements, one or more of these licenses will be needed for each device:

- One Workspace Edition license for basic functionality; see [Workspace Edition](#)<sup>52</sup>
- If one of the following features are used, one Enterprise Management Pack license is required (see [Enterprise Management Pack](#)<sup>53</sup>):
  - IGEL Cloud Gateway (ICG)

<sup>52</sup> <https://kb.igel.com/display/licensesmoreigelos11/Workspace+Edition>

<sup>53</sup> <https://kb.igel.com/display/licensesmoreigelos11/Enterprise+Management+Pack>



- Shared Workplace (SWP)
- Custom Partition if IGEL OS 11.03.100 or lower is the target version; if the target version is IGEL OS 11.03.500 or higher, the Custom Partition feature is included in the Workspace Edition.

Proceed as follows:

- Deploy the licenses for IGEL OS 11 using the method that suits your needs:
- Manual License Deployment: Licenses are created and deployed manually. For instructions, see [Manual License Deployment for IGEL OS<sup>54</sup>](#).
  - Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see [Setting up Automatic License Deployment \(ALD\)<sup>55</sup>](#).
  - Download three demo licenses from <https://www.igel.com/download/>.

When the device has a license, continue with [Configuring the Update Source](#)(see page 124).

#### Configuring the Update Source

1. In the Setup, go to **System > Update > Firmware Update** and configure the update source for IGEL OS 11. For more information, see the [Firmware Update](#)(see page 1252) chapter in the IGEL OS Manual.
2. Click **Ok**.

When the correct update source is configured, continue with [Testing the Upgrade](#)(see page 124).

#### Testing the Upgrade

1. Click System and then **Upgrade to OS 11**. The OS 11 Upgrade Tool starts and indicates whether all requirements are met.

You can change the starting methods for the OS 11 Upgrade Tool in the Setup under **Accessories > OS11 Upgrade**.

<sup>54</sup> <https://kb.igel.com/display/licensesmoreigelos11/Manual+License+Deployment+for+IGEL+OS>

<sup>55</sup> <https://kb.igel.com/pages/viewpage.action?pageId=10325058>

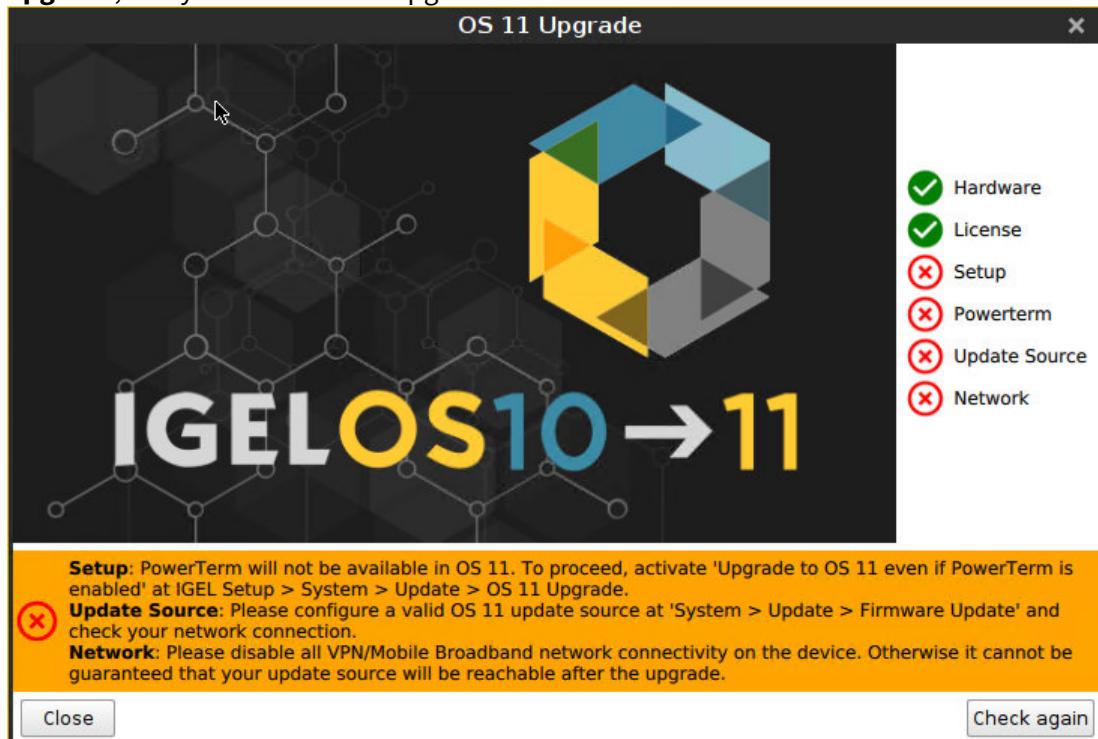


2. Check the output of the OS 11 Upgrade Tool and continue appropriately:

- If each requirement has an icon, click **OS Upgrade** to start the upgrade process.
- If one or more requirements have an icon, check the messages and resolve the issues. Afterwards, click **Check again**. If all requirements are met, the button changes to **OS Upgrade**.

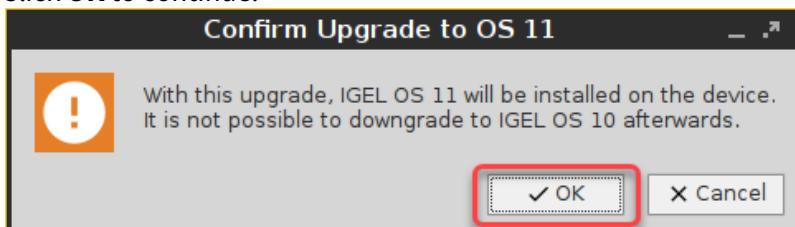


**Upgrade**, and you can start the upgrade.

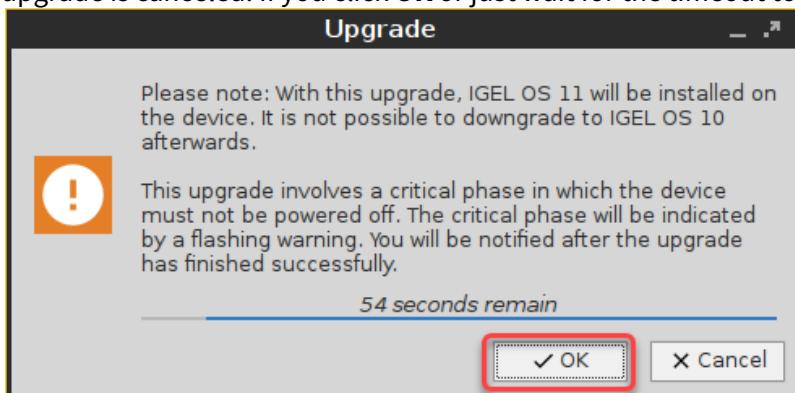


When you start the upgrade, a warning dialog is shown.

- Click **OK** to continue.



A warning dialog with a timeout is shown. If you click **Cancel** before the timeout expires, the upgrade is canceled. If you click **OK** or just wait for the timeout to expire, the upgrade is started



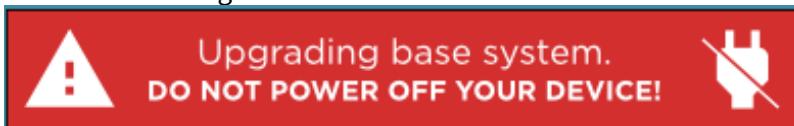
After the warning dialog has been confirmed or the timeout has expired, the device reboots into a special IGEL OS 10 environment, in which the system upgrade is executed. The **Upgrade** window



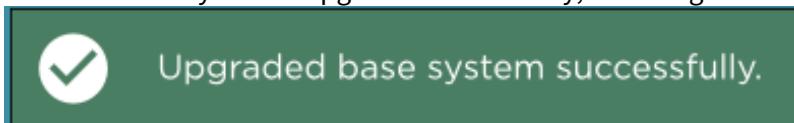
show the progress.



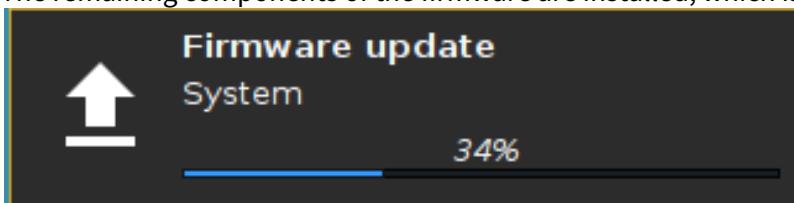
During the critical phase, the device must not be powered off. At this stage in the progress, an additional warning is shown.



When the base system is upgraded successfully, a message is shown.



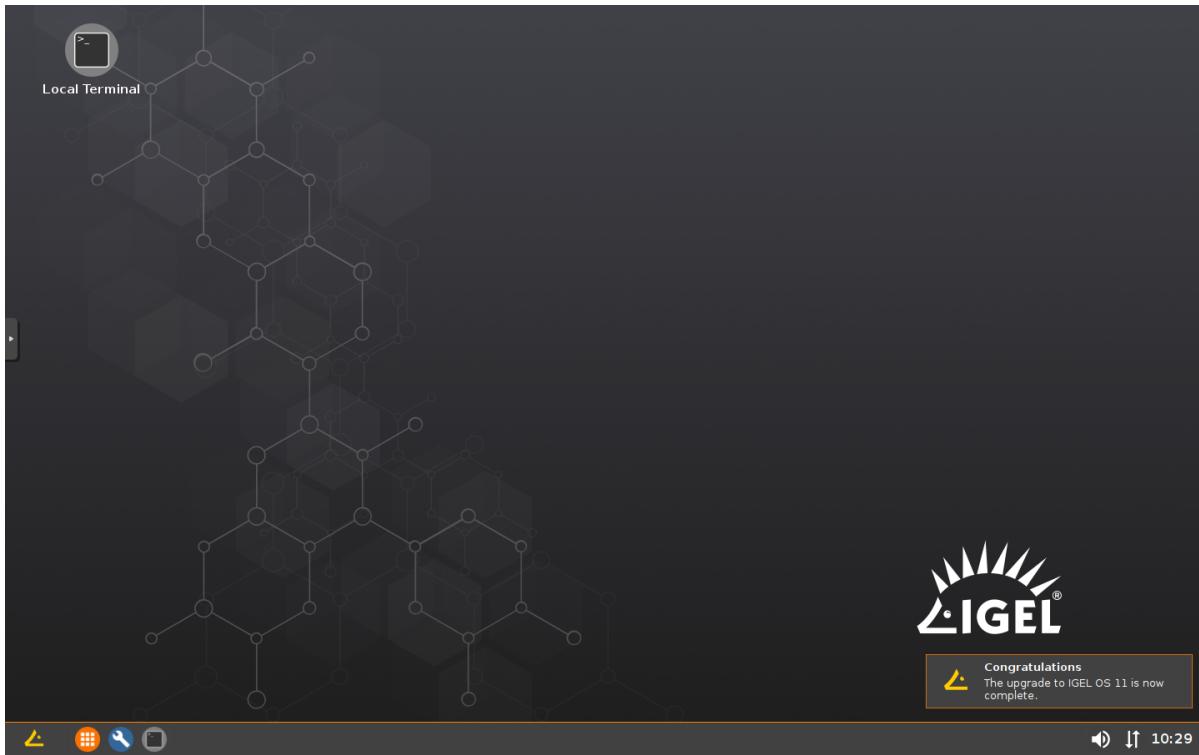
The remaining components of the firmware are installed, which is indicated by update messages.



When the installation is completed, the **Upgrade** window looks like this:



After a few seconds the device reboots into IGEL OS 11.



When the upgrade test has been successful, you are ready to set up the mass upgrade. Continue with [Checking the Requirements](#)(see page 128).

### Checking the Requirements

The following requirements must be met:

- The upgrade has been tested with characteristic devices.
- UMS 6.01.130 or higher is available.



- The firmware IGEL OS 10.05.800 (or higher) is known to the UMS. For this purpose, a device with this firmware version must be registered in the UMS. This is already the case if you tested the upgrade with the same UMS with which you are about to do the mass upgrade. If not, you must register a device with the appropriate firmware version now.
- All devices are connected to a regular LAN (not OpenVPN, OpenConnect, genucard, NCP VPN or mobile broadband).
- All devices are in a safe environment where the upgrade process cannot be disrupted, e.g. by powering off the devices.

When all requirements are met, continue with [Creating the Universal Firmware Updates](#)(see page 129).

#### Creating the Universal Firmware Updates

For detailed information, see the chapter [Universal Firmware Update<sup>56</sup>](#) in the UMS Manual.

If you use the [High Availability Extension<sup>57</sup>](#), note that Universal Firmware Updates are NOT synchronized, that is why you have to either download them to all HA nodes or configure an external (FTP) server.

1. Create a Universal Firmware Update for IGEL OS 10.05.800 (or higher).
2. After you have created the Universal Firmware Update for IGEL OS 10.05.800 (or higher), create a Universal Firmware Update for IGEL OS 11.

The order of creation is crucial because the IGEL OS 11 firmware must have a higher ID in order to be chosen by the device. For details, see [Executing the Upgrade](#)(see page 140).

#### Configuring the Universal Firmware Update for ICG

If you are using IGEL Cloud Gateway (ICG), an FTP server that is accessible to all devices must be configured as an update source.

To configure an FTP server as update source:

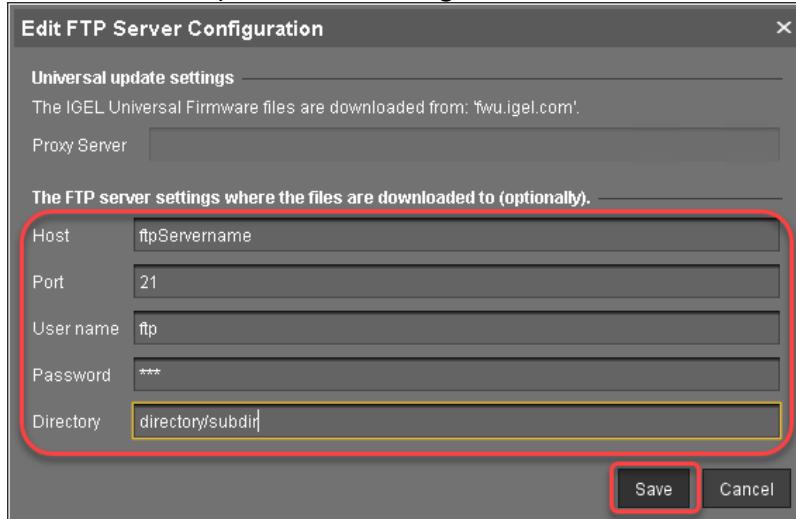
1. In the UMS, go to **UMS Administration > Universal Firmware Update** and click **Edit...**.

<sup>56</sup> <https://kb.igel.com/display/endpointmgmt601/Universal+Firmware+Update>

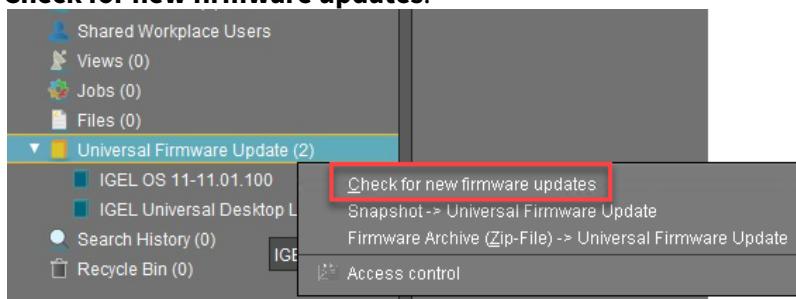
<sup>57</sup> <https://kb.igel.com/pages/viewpage.action?pageId=915787>



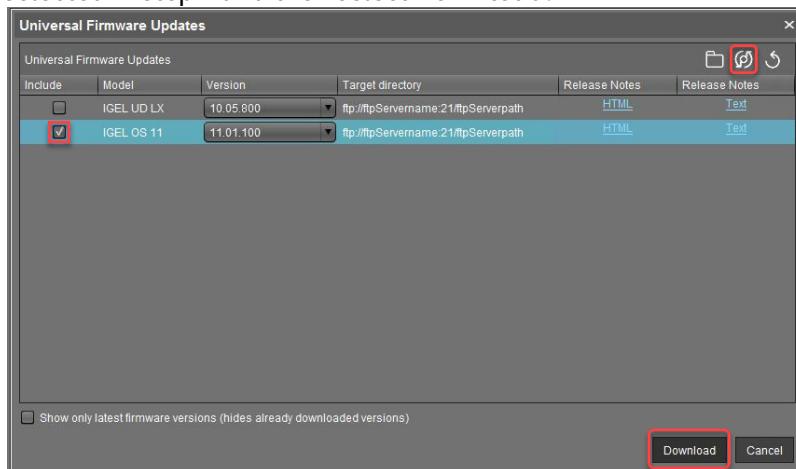
2. Enter the data required for accessing the FTP server and click **Save**.



3. Go to **Server - [UMS address] > Universal Firmware Update** and in the context menu, select **Check for new firmware updates**.



4. Select the entry for the IGEL OS 10.05.800 (or higher) firmware, click to select the FTP server selected in step 2 and then select **Download**.





5. The firmware is transferred to the FTP server.

A screenshot of a web-based configuration interface for an IGEL Universal Desktop LX. The page title is "/Universal Firmware Update/IGEL Universal Desktop LX-10.05.800".

- Product:** IGEL Universal Desktop LX
- Version:** 10.05.800
- Release Notes:** [HTML](#) [Text](#)
- Firmware Update Settings:**
  - User:** ftpUser
  - Password:** [REDACTED]
  - Host:** ftpServername
  - Port:** 21
  - Protocol:** ftp
  - Target URL:** /ftpServerpath/IGEL\_Universal/Desktop\_LX-10.05.800
  - Snapshot file:** [REDACTED]
- Download Status:**
  - Status:** Started
  - Progress:** Download the firmware update...
  - Error:** [REDACTED]

6. Under **Server - [UMS address] > Universal Firmware Update**, in the context menu, select **Check for new firmware updates** again.

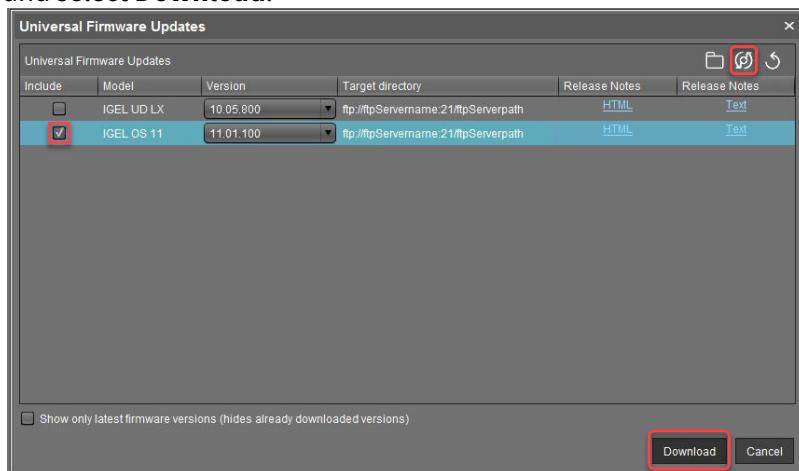
A screenshot of the UMS (Universal Management System) interface. The left sidebar shows various categories like Shared Workplace Users, Views, Jobs, Files, and Universal Firmware Update (2). The Universal Firmware Update item is selected and highlighted with a blue bar.

- Shared Workplace Users**
- Views (0)**
- Jobs (0)**
- Files (0)**
- Universal Firmware Update (2)**
  - IGEL OS 11-11.01.100**
  - IGEL Universal Desktop L**
  - Search History (0)**
  - Recycle Bin (0)**

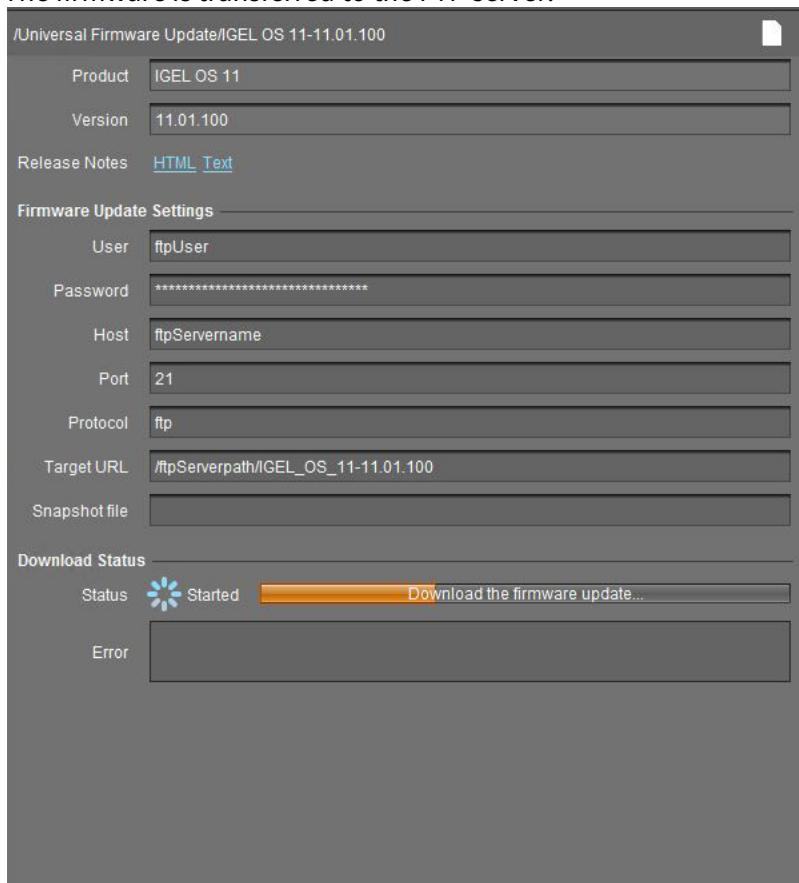
A context menu is open over the "Universal Firmware Update" item, with the "Check for new firmware updates" option highlighted by a red box. Other options in the menu include "Snapshot -> Universal Firmware Update", "Firmware Archive (.Zip-File) -> Universal Firmware Update", and "Access control".



7. Select the entry for the IGEL OS 11 firmware, click to select the FTP server selected in step 2 and select **Download**.



8. The firmware is transferred to the FTP server.



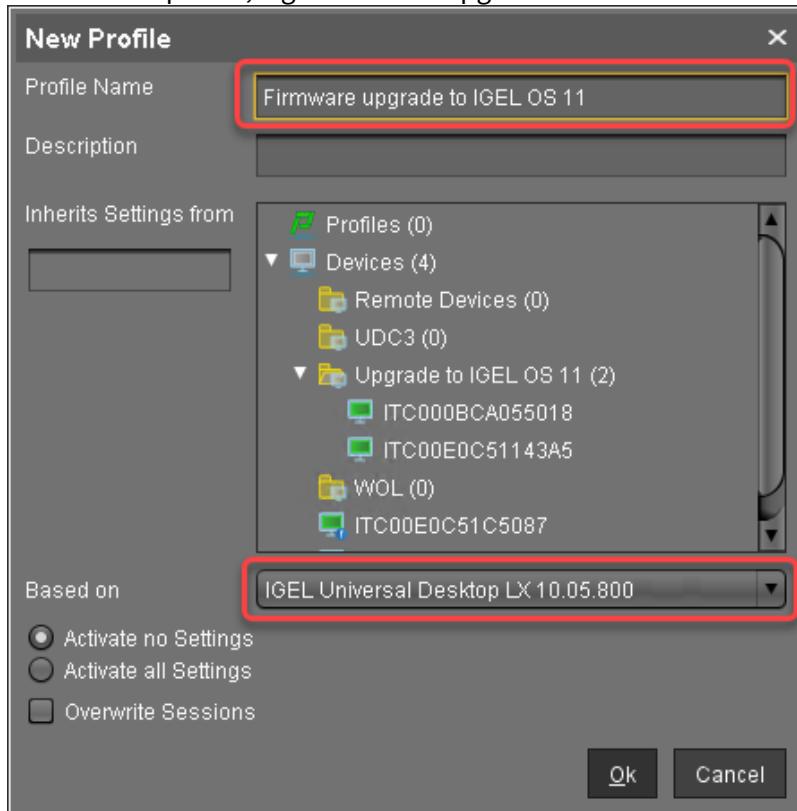
The devices can download the firmware from the FTP server,

When the Universal Firmware Update is ready, continue with [Creating a Profile](#)(see page 133).

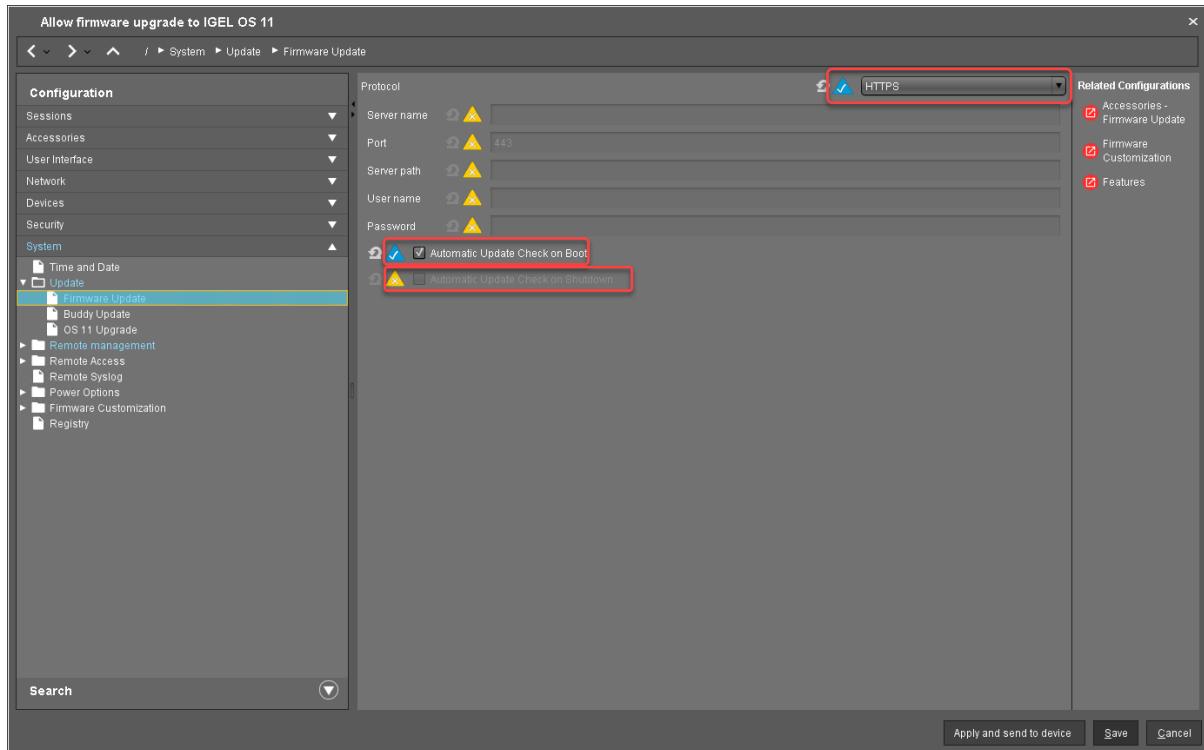


## Creating a Profile

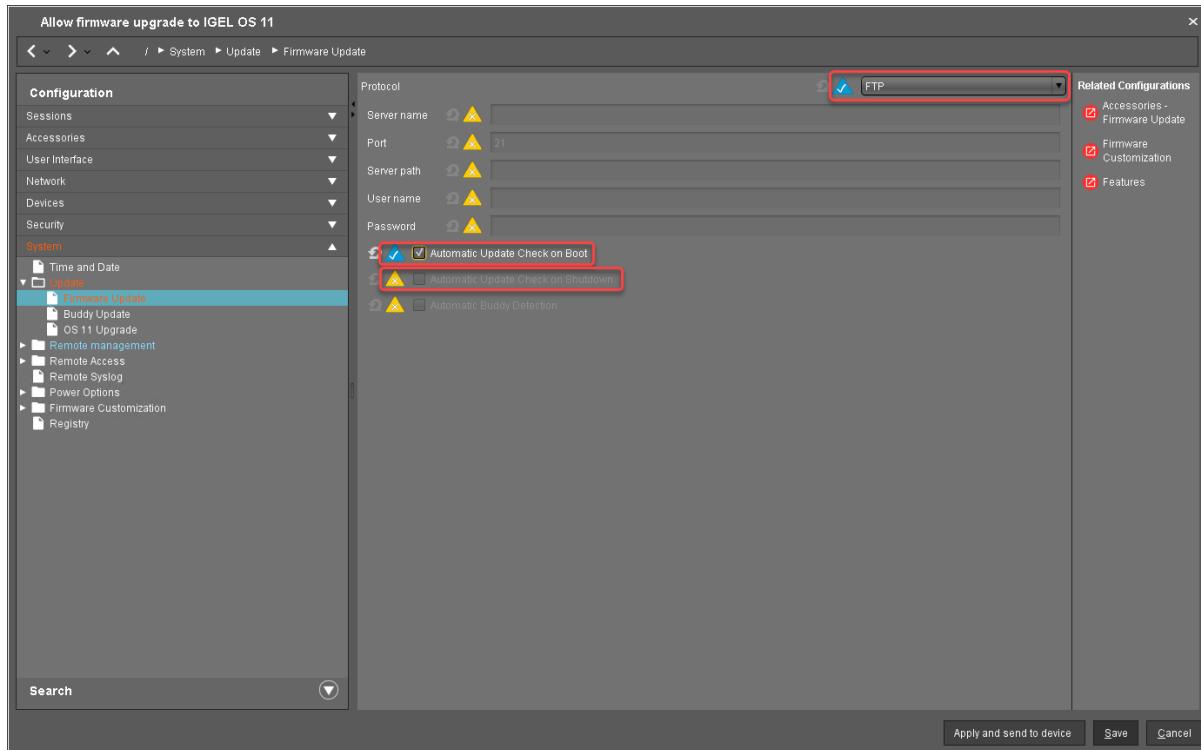
1. Create a profile that is based on the IGEL OS 10 firmware (10.08.800 or higher). Find a suitable name for the profile, e.g. "Firmware upgrade to IGEL OS 11".



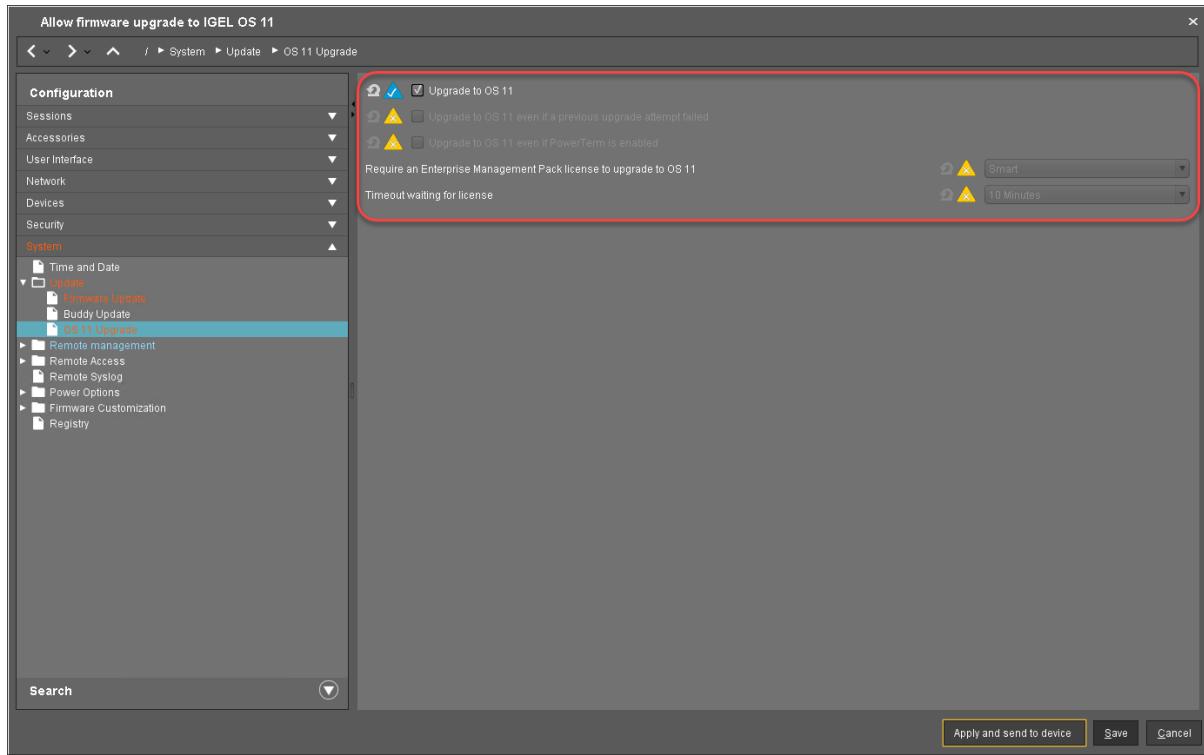
2. In the profile's configuration dialog, go to **System > Update > Firmware Update** and change the settings according to your environment:
  - If the UMS and the devices are in one and the same network and no IGEL Cloud Gateway (ICG) is used:
    - Select "HTTPS" as **Protocol**.
    - Activate **Automatic Update Check on Boot**.
    - Ensure that **Automatic Update Check on Shutdown** is deactivated. Otherwise, the device will shut down when the update is finished.



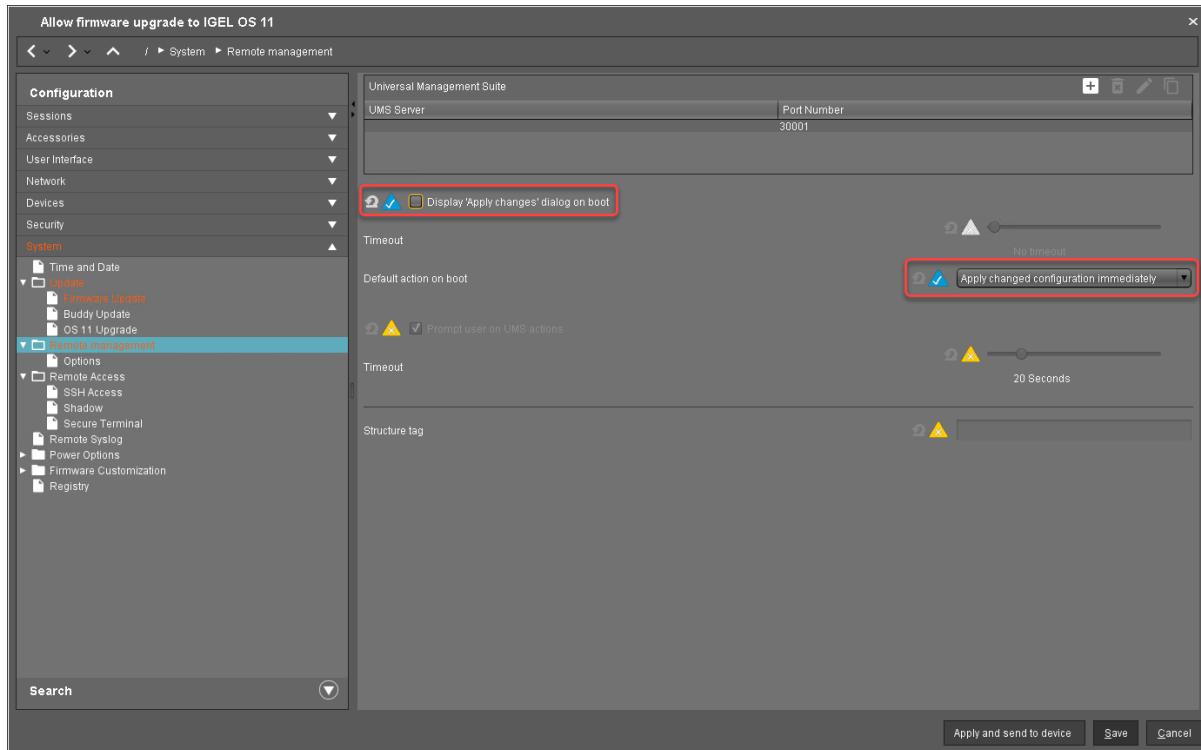
- If IGEL Cloud Gateway (ICG) is used:
  - Select "FTP" as **Protocol**.
  - Activate **Automatic Update Check on Boot**.
  - Ensure that **Automatic Update Check on Shutdown** is deactivated. Otherwise, the device will shut down when the update is finished.



3. Go to **System > Update > OS 11 Upgrade** and change the following settings according to your successful upgrade test (for details of the settings, see [Adjusting the Setup](#)(see page 122)):
  - Activate **Upgrade to OS 11**.
  - Set **Upgrade to OS 11 even if PowerTerm is enabled** according to your needs.
  - Set **Upgrade to OS 11 even if a previous upgrade attempt failed** according to your needs.
  - Set **Require an Enterprise Management Pack license to upgrade to OS 11** according to your needs.
  - Ensure that the **Timeout waiting for OS 11 license to start automatic upgrade** is set to **10 Minutes**.



4. Go to **System > Remote Management** and change the settings as follows:
  - Deactivate **Display 'Apply changes' dialog on boot**.
  - Set **Default action on boot** to **Apply changed configuration immediately**.



## 5. Click **Save**.

When the profile is created, continue with [Deploying the Licenses](#)(see page 137).

## Deploying the Licenses

Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see [Setting up Automatic License Deployment \(ALD\)](#)<sup>58</sup>.
- Manual License Deployment: Licenses are created and deployed manually. For instructions, see [Manual License Deployment for IGEL OS](#)<sup>59</sup>.

When the license deployment is set up, continue with [Putting It All Together](#)(see page 138).

---

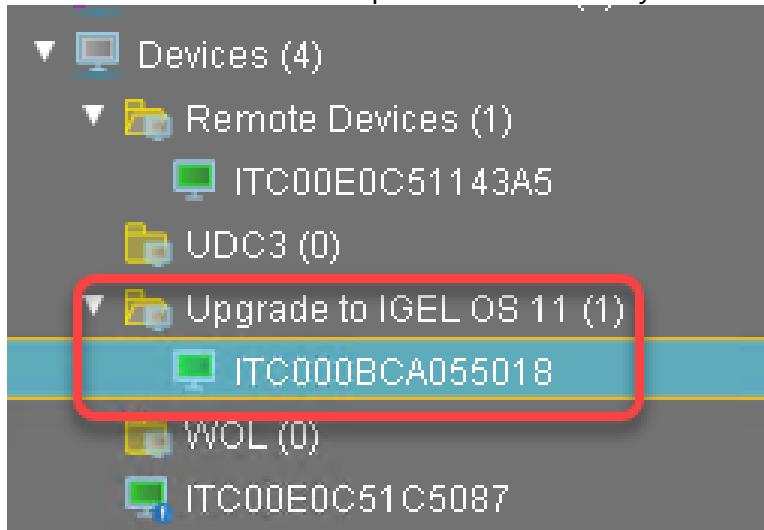
<sup>58</sup> <https://kb.igel.com/pages/viewpage.action?pageId=10325058>

<sup>59</sup> <https://kb.igel.com/display/licensesmoreigelos11/Manual+License+Deployment+for+IGEL+OS>

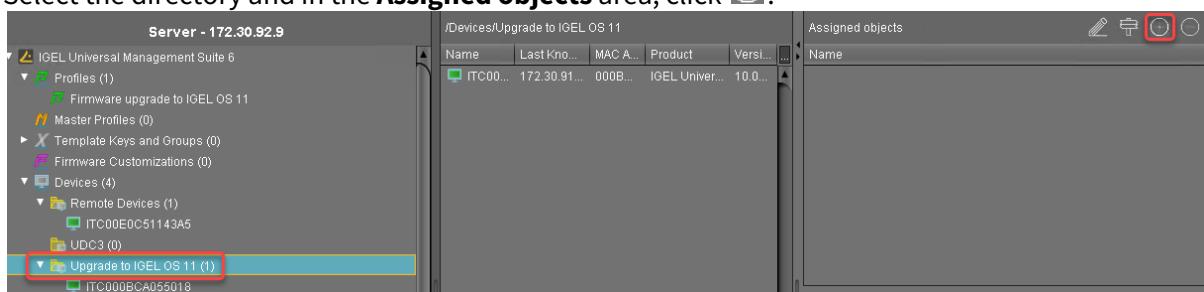


## Putting It All Together

1. Put all devices that are to be updated into a directory.

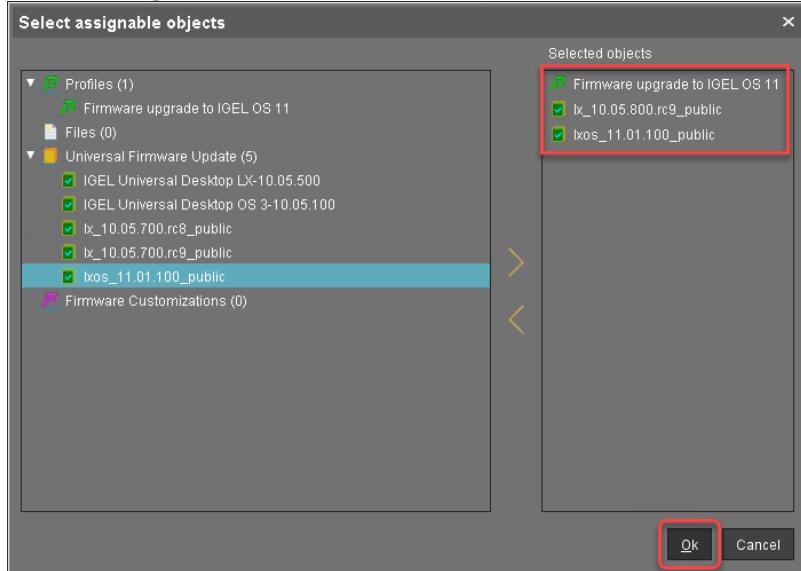


2. Select the directory and in the **Assigned objects** area, click .

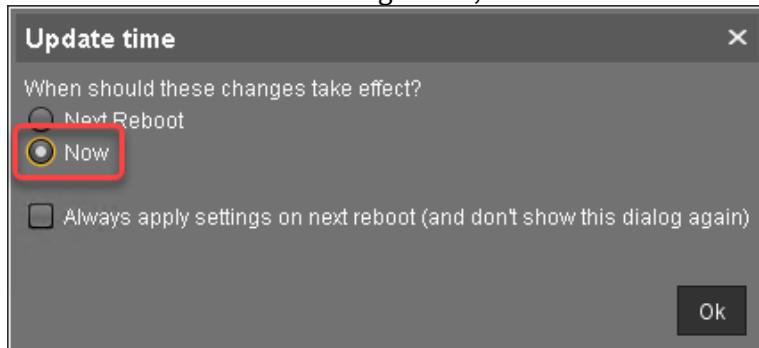




3. Assign the profile (see [Creating a Profile\(see page 133\)](#)) and the two Universal Firmware Updates (see [Creating the Universal Firmware Updates\(see page 129\)](#)) to the directory and click **Ok**.



4. In the context menu of the assignment, select **Now**.



In the **Assigned objects** area, the profile and the Universal Firmware Updates are shown:

Name
Firmware upgrade to IGEL OS 11
lxos_11.01.100_public
lx_10.05.700.rc8_public

5. If you are using Automatic License Deployment (ALD), it might be feasible to confine the distribution of licenses to the current directory. For more information, see [Configuring the Distribution Conditions](#)<sup>60</sup>, section "Distributing Licenses to Devices in a Specified Directory".

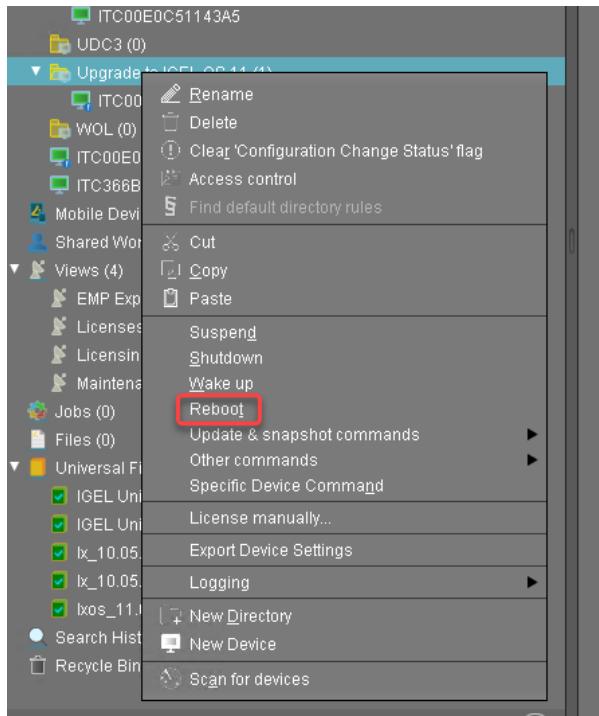
When everything is in place, continue with [Executing the Upgrade\(see page 140\)](#).

<sup>60</sup> <https://kb.igel.com/display/licensesmoreigelos11/Configuring+the+Distribution+Conditions>

## Executing the Upgrade

- In the UMS, select the directory containing all devices that are to be upgraded and reboot them.

Alternatively, you can create a scheduled job for reboot or wake up and assign it to the devices or the directory containing these devices. For more information, see [Jobs](#)<sup>61</sup>



On reboot or wake up, the devices update to the appropriate IGEL OS 10 firmware (10.05.800 or higher). With this version, the **Upgrade to OS 11** parameter is recognized by the devices; also, the devices request IGEL OS 11 licenses from the UMS (Workspace Edition and, if required, Enterprise Management Pack).

If no IGEL OS 11 licenses have been deployed on the devices yet, the licenses are deployed within a few minutes. The upgrade will be started when the licenses are deployed. The maximum time period the device will wait for a license is configured by the parameter **Timeout waiting for OS 11 license to start automatic upgrade**; for details, see [Adjusting the setup](#)(see page 122).

The parameter **Automatic update check on boot** causes the devices look for new firmware again. Although two Universal Firmware Updates are assigned to the devices, the UMS offers the IGEL OS 11 firmware, because the ID of the IGEL OS 11 firmware is higher than the ID of the IGEL OS 10 firmware.

---

<sup>61</sup> <https://kb.igel.com/display/endpointmgmt602/Jobs>

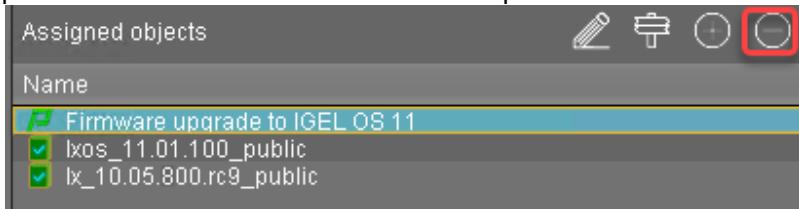


### Update Can Be Canceled After Timeout

An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

2. When all devices have been upgraded successfully, remove the "Firmware upgrade to IGEL OS 11" profile and the two Universal Firmware Updates from the directory.



The upgrade is completed.

### Zero-Touch Deployment Using Buddy Update

This method uses the buddy update feature of IGEL OS. One or more devices that are configured as an update buddy access the main server and download the firmware. The other devices are configured to download their firmware from an update buddy.

Read all the following chapters carefully and follow the instructions.

1. [Devices That Can Be Upgraded to IGEL OS 11](#)(see page 141)
2. [Important! Consider This Before Upgrading](#)(see page 147)
3. [Preparing the Upgrade](#)(see page 148)
4. [Testing the Upgrade](#)(see page 151)
5. [Checking the Requirements](#)(see page 154)
6. [Configuring Two Update Buddies](#)(see page 155)
7. [Creating a Profile](#)(see page 155)
8. [Deploying the Licenses](#)(see page 157)
9. [Putting It All Together](#)(see page 157)
10. [Executing the Upgrade](#)(see page 158)

### Devices That Can Be Upgraded to IGEL OS 11

#### Core Requirements

- CPU with 64-bit support
- CPU speed ≥ 1 GHz
- ≥ 2 GB memory (RAM)



With devices that have 2 GB RAM and shared video memory, a maximum of 512 MB may be used as video memory.

- Recommended: ≥ 4 GB; minimum 2 GB storage

#### **Storage Requirements for IGEL OS 11.04 or Higher**

IGEL OS 11.04.100 or higher requires at least 2.4 GB storage if the full feature set is applied. Thus, the feature set must be modified accordingly; for more information, see Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher(see page 231).

- No VIA graphic adapter; VIA graphics support is discontinued in IGEL OS.
- Legacy Bios and EFI/UEFI are supported.

#### Devices Officially Supported by OSC and UD Pocket with IGEL OS 11

The following list only includes those devices that are **tested by IGEL** (with each major release of IGEL OS). By no means it implies that the devices which are not included in this list but meet the [core requirements](#)(see page 141) will not function with IGEL OS.

Further supported devices can be found on the [IGEL Ready](#)<sup>62</sup> Showcase at <https://www.igel.com/ready/showcase-categories/endpoints/>.

Integrated drivers and supported peripherals are listed in the [Third-Party Hardware Database](#)<sup>63</sup>. For more solutions compatible with IGEL OS, see [Partner Solutions](#)<sup>64</sup>.

For some of the devices listed here, Flash memory must be extended to ≥ 2 GB. For these devices, an appropriate note is added.

#### ADS-Tec

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
VMT9000	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100

#### Advantech

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
POC-W213L	Medical All in One	4 GB	128 GB	Intel Core i7-7300U	11.01.100

<sup>62</sup> <https://www.igel.com/technology-partners/>

<sup>63</sup> <https://www.igel.com/linux-3rd-party-hardware-database/>

<sup>64</sup> <https://kb.igel.com/display/igelos1105/Partner+Solutions>



Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
POC-W243L*(see page 147)	Medical All in One	4 GB	32 GB	Intel Kaby Lake Core i5-7300U	11.01.110
POC-W243L*(see page 147)	Medical All in One	4 GB	128 GB	Intel Core i7-7300U	11.01.100

## Advantech-DLoG

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
DLT-V6210	Industrial PC/Terminal	4 GB	32 GB	Intel Atom	11.01.100
DLT-V7210 K	Industrial PC/Terminal	4 GB	4 GB	Intel Atom E3845	11.01.100

## Dell / Wyse

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
(AiO) 5040 / 5212	All in One	2 GB	2 GB	AMD G-T48E	11.01.100
3040	Thin Client	2 GB	8 GB	Intel Atom x5-Z8350	11.01.100
5020	Thin Client	2 GB	8 GB	AMD G-Series SoC	11.02.140
5060	Thin Client	4 GB	8 GB	AMD GX-424CC	11.01.100
5070	Thin Client	8 GB	32 GB	Intel Celeron J4105	11.01.100
Latitude 5510	Laptop/Notebook	8 GB	256 GB	Intel Core i5-10210U	11.05.100

## Elo

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
(AiO) i2 Touch (15 and 22 inches)	All in One	8 GB	128 GB	Intel Core i3-8100T	11.05.100

## Fujitsu



Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
Q957	Desktop PC	8 GB	500 GB	Intel Core i3-6100	11.02.100
FUTRO S740	Thin Client	4 GB	8 GB	Intel Celeron J4105	11.04.100

HP

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
t420	Thin Client	2 GB	8 GB	AMD Embedded G-Series GX-209JA	11.02.100
t430	Thin Client	2 GB	16 GB	Intel® Celeron® N4000	11.01.110
t530	Thin Client	4 GB	8 GB	AMD GX-215JJ Dual-Core	11.01.100
t630	Thin Client	4 GB	8 GB	AMD GX-420GI	11.01.100
t730	Thin Client	16 GB	8 GB	AMD RX-427BB APU	11.01.100
t820	Thin Client	16 GB	16 GB	Intel Core i5-4570S	11.01.100
t640	Thin Client	4 GB	16 GB	AMD Ryzen R1505G	11.04.100
t540	Thin Client	16 GB	16 GB	AMD Ryzen Embedded R1305G	11.06.100

Intel

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
NUC 5i5MYHE	Desktop PC	2 GB	32 GB	Intel i5-5300U	11.01.100
NUC 5i3RYH	Desktop PC	2 GB	2 GB	Intel i3-5010U	11.01.100
NUC 7CJYH	Desktop PC	2 GB	4 GB	Intel Celeron J4005	11.01.100

Lenovo



Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
ThinkCentre M625q	Desktop PC	4 GB	32 GB	AMD E2-9000e	11.04.100
ThinkCentre M75n	Desktop PC	8 GB	128 GB	AMD Ryzen 3 Pro 3300U	11.05.100
ThinkCentre M70q	Desktop PC	8 GB	500 GB	Intel Pentium Gold G6400T	11.05.100
L14	Laptop/Notebook	64 GB	1000 GB	AMD Ryzen 7 Pro 4750	11.05.100
14w	Laptop/Notebook	8 GB	128 GB	AMD A6	11.05.100

LG

Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
(AiO) 24CK550N **(see page 147)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
(AiO) 24CK550W **(see page 147)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
(AiO) 24CK560N **(see page 147)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
CK500W	Thin Client	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
(AiO) 38CK950N	All in One	8 GB	128 GB	AMD Ryzen 3	11.02.100
(AiO) 38CK900N	All in One	8 GB	128 GB	AMD Ryzen 3	11.02.100
CL600N	Thin Client	4 GB	16 GB	Intel® Celeron J4105	11.03.100
CL600W	Thin Client	8 GB	128 GB	Intel® Celeron J4105	11.03.100
(AiO) 34CN650N	All in One	4 GB	16 GB	Intel® Celeron J4105	11.05.100

OnLogic



Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
CL210G-10	Industrial PC/Terminal	4 GB	32 GB	Intel Celeron N3350	11.04.100
KARBON 300	Desktop PC	4 GB	32 GB	Intel Atom x5-E3930	11.04.100
Onyx Healthcare					
Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
Venus 223	Medical All in One	4 GB	128 GB	Intel Quad-Core J1900	11.01.100
Rein Medical					
Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
Silenio C122	All in One	8 GB	128 GB	Intel® Core™ i5 – 6th Generation	11.01.110
Silenio C124	All in One	8 GB	128 GB	Intel® Core™ i5 – 6th Generation	11.01.110
Clinio S 522TCT	Medical All in One	8 GB	16 GB	Intel® Pentium® Silver J5005	11.04.100
Clinio S 524TCT	Medical All in One	8 GB	16 GB	Intel® Pentium® Silver J5005	11.04.100
Secunet					
Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
SINA Workstation S EliteDesk 800 G2	Workstation	16 GB	256 GB	Intel Core i7-6700	11.01.100
Toshiba					
Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
Portégé X20W-D	Laptop/Notebook	8 GB	256 GB	Intel Core i5-7200U	11.01.100



Name	Endpoint Type	Memory (RAM)	Storage	Processor	Supported from IGEL OS Version
Portégé X30-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7300U	11.01.100
Tecra C50	Laptop/ Notebook	4 GB	500 GB	Intel i5-4210U	11.01.100
Tecra Z50-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7200U	11.01.100
SATELLITE R50	Laptop/ Notebook	4 GB	500 GB	Intel i3-6006U	11.01.100

USB Memory Sticks That Can Be Used as Alternative UD Pocket Hardware

DIGITTRADE

Name	Storage	Supported from IGEL OS Version
Kobra Stick	≥ 4GB	11.05.133

Officially Supported Virtual Environments

- Tested with Ubuntu (64-bit) and default settings

Note that the use of a UD Pocket within a virtual machine is **not** supported by IGEL.

Name	Memory (RAM)	Storage	Type	Supported from IGEL OS Version
Oracle VM VirtualBox	≥ 2 GB	≥ 4 GB	Linux	11.04.100
VMware Workstation	≥ 2 GB	≥ 4 GB	Linux	11.04.100

\* Delock Adapter DP 1.2 to DVI does not work.

\*\* When using an additional 4k screen with this device, please edit the BIOS settings as follows:

1. Go to the **Chipset** screen.
2. Set **Integrated Graphics** to “Force”.
3. Set **UMA Frame Buffer Size** to “256M” or higher.

When you have confirmed that your devices can be upgraded to IGEL OS 11, make sure to consider [Important! Consider This Before Upgrading](#)(see page 147).

#### Important! Consider This Before Upgrading

To make sure that your upgrade can be successful, check the following warnings and notes; a warning symbol indicates that irreversible damage can be done to your devices.



**Existing partitions:** Any existing partition on the target drive of your device will be deleted. The installer will repartition the target device. The overall size of the newly created partitions will be calculated based on the available disk space. The minimum disk usage is 2 GB, the maximum is 16 GB.

### No Downgrade

You cannot restore your IGEL OS 10 system once you have migrated to IGEL OS 11. The device storage is overwritten completely with a new partitioning scheme.

### Features (e.g. Clients)

IGEL OS 11 does not have the complete feature set of IGEL OS 10. Make sure that the current version of IGEL OS 11 meets your requirements. For details, refer to the appropriate release notes.

### Custom Partitions

The contents of custom partitions will be deleted by the upgrade. Make sure to back up the contents and restore them after the upgrade has finished. Besides becoming dysfunctional after the upgrade, applications and kernel drivers in a custom partition might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device. We recommend that you disable custom partitions when upgrading; you can enable them once the upgrade has been successfully completed.

### Custom Commands

The persistence of custom commands cannot be guaranteed. Besides becoming dysfunctional after the upgrade, custom commands might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device. In general, custom commands must be adapted for IGEL OS 11. We recommend that you disable custom commands when upgrading; you can enable them once the upgrade has been successfully completed.

### Power Supply

Ensure that the device is not running on battery power, i.e. it must be connected to a power supply during the complete upgrade process.

### Network

All devices must be connected to a WLAN or LAN. LAN is the recommended option. The device will not be upgraded if connected to OpenVPN, OpenConnect, genucard or mobile broadband.

When you have considered everything that is relevant, continue with [Preparing the Upgrade](#)(see page 148).

## Preparing the Upgrade

This section describes the required preparations and tests before any productive devices can be updated. The testing should be done with at least one device that is characteristic of your environment. This device should have every custom partition and every custom command that may possibly exist in any of your devices.



To prepare the upgrade, perform the following steps:

1. Preparing the UMS(see page 149)
2. Adjusting the Setup(see page 149)
3. Deploying a License(see page 150)
4. Configuring the Update Source(see page 150)

#### Preparing the UMS

To upgrade your devices to IGEL OS 11, you need the appropriate version of the UMS. Also, the devices must be registered with the UMS to receive their licenses.

1. If you have not already done so, update your UMS to version 6.01.130 or higher. For instructions, see [Updating UMS<sup>65</sup>](#).
2. Make sure that your devices are registered with the UMS. For more information, see the chapter [Registering Devices on the UMS Server<sup>66</sup>](#) in the UMS Manual.

When the UMS is ready, continue with [Adjusting the Setup\(see page 149\)](#).

#### Adjusting the Setup

Depending on the features that are in use now or will be used in the future, a specific set of parameters must be set in the device's Setup.

1. In the Setup, go to **System > Firmware Update > OS 11 Upgrade**.
2. Make your settings as appropriate:
  - Activate **Upgrade to OS 11**.

When **Upgrade to OS 11** is activated, the device checks for a Workspace Edition license and stops checking for a legacy UDC3 or UD Pocket license. Therefore, in the UMS, it is displayed as an unlicensed device until a Workspace Edition license has been deployed.

- If you want the device to retry the upgrade immediately after a failed attempt, activate **Upgrade to OS 11 even if a previous upgrade attempt failed**. The device will retry the upgrade 5 times. When the 5th attempt has failed, a message will be shown in the upgrade tool window.
- If your device has a PowerTerm license, and you want to upgrade to IGEL OS 11 even though it does not support PowerTerm, you must activate **Upgrade to OS 11 even if PowerTerm is enabled**.
- Under **Require an Enterprise Management Pack license to upgrade to OS 11**, select the appropriate option:
  - If you are using IGEL Cloud Gateway (ICG) or Shared Workplace (SWP) or a Custom Partition and want to make sure that the upgrade is performed only if these features can be used furthermore, select **Smart**. When this option is selected, and any of these features is activated, the upgrade is performed only if the device could fetch a license from an Enterprise Management Pack.
  - If you want to force the device to fetch a license from an Enterprise Management Pack and make sure that the upgrade is performed only if the license could be fetched, select **Always**.

<sup>65</sup> <https://kb.igel.com/display/endpointmgmt601/Updating+UMS>

<sup>66</sup> <https://kb.igel.com/display/endpointmgmt601/Registering+devices+on+the+UMS+Server>



- If you want the device to upgrade to IGEL OS 11 without fetching an Enterprise Management Pack, disregarding the features that might be activated, select **Never**.
- Under **Timeout waiting for OS 11 license to start automatic upgrade**, set the time period the device will wait for a license in a mass deployment scenario (see [Zero-Touch Deployment Using Universal Firmware Update](#)(see page 115), [Zero-Touch Deployment Using Buddy Update](#)(see page 141) and [Mass Deployment Using a Scheduled Job](#)(see page 209)). This setting prevents the device from starting the upgrade at an inappropriate time as a result of the license just being deployed. This way, the setting prevents unwanted interruptions at work. For a mass deployment scenario, the default value **10 Minutes** is recommended.

3. Click **Apply**.

When the Setup is adjusted, continue with [Deploying a License](#)(see page 150).

#### Deploying a License

To upgrade from IGEL OS 10 to IGEL OS 11, you need an appropriate license. Depending on your requirements, one or more of these licenses will be needed for each device:

- One Workspace Edition license for basic functionality; see [Workspace Edition](#)<sup>67</sup>
- If one of the following features are used, one Enterprise Management Pack license is required (see [Enterprise Management Pack](#)<sup>68</sup>):
  - IGEL Cloud Gateway (ICG)
  - Shared Workplace (SWP)
  - Custom Partition if IGEL OS 11.03.100 or lower is the target version; if the target version is IGEL OS 11.03.500 or higher, the Custom Partition feature is included in the Workspace Edition.

Proceed as follows:

► Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Manual License Deployment: Licenses are created and deployed manually. For instructions, see [Manual License Deployment for IGEL OS](#)<sup>69</sup>.
- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see [Setting up Automatic License Deployment \(ALD\)](#)<sup>70</sup>.
- Download three demo licenses from <https://www.igel.com/download/>.

When the device has a license, continue with [Configuring the Update Source](#)(see page 150).

#### Configuring the Update Source

1. In the Setup, go to **System > Update > Firmware Update** and configure the update source for IGEL OS 11. For more information, see the [Firmware Update](#)(see page 1252) chapter in the IGEL OS Manual.
2. Click **Ok**.

When the correct update source is configured, continue with [Testing the Upgrade](#)(see page 151).

---

<sup>67</sup> <https://kb.igel.com/display/licensesmoreigelos11/Workspace+Edition>

<sup>68</sup> <https://kb.igel.com/display/licensesmoreigelos11/Enterprise+Management+Pack>

<sup>69</sup> <https://kb.igel.com/display/licensesmoreigelos11/Manual+License+Deployment+for+IGEL+OS>

<sup>70</sup> <https://kb.igel.com/pages/viewpage.action?pageId=10325058>



## Testing the Upgrade

1. Click System and then **Upgrade to OS 11**. The OS 11 Upgrade Tool starts and indicates whether all requirements are met.

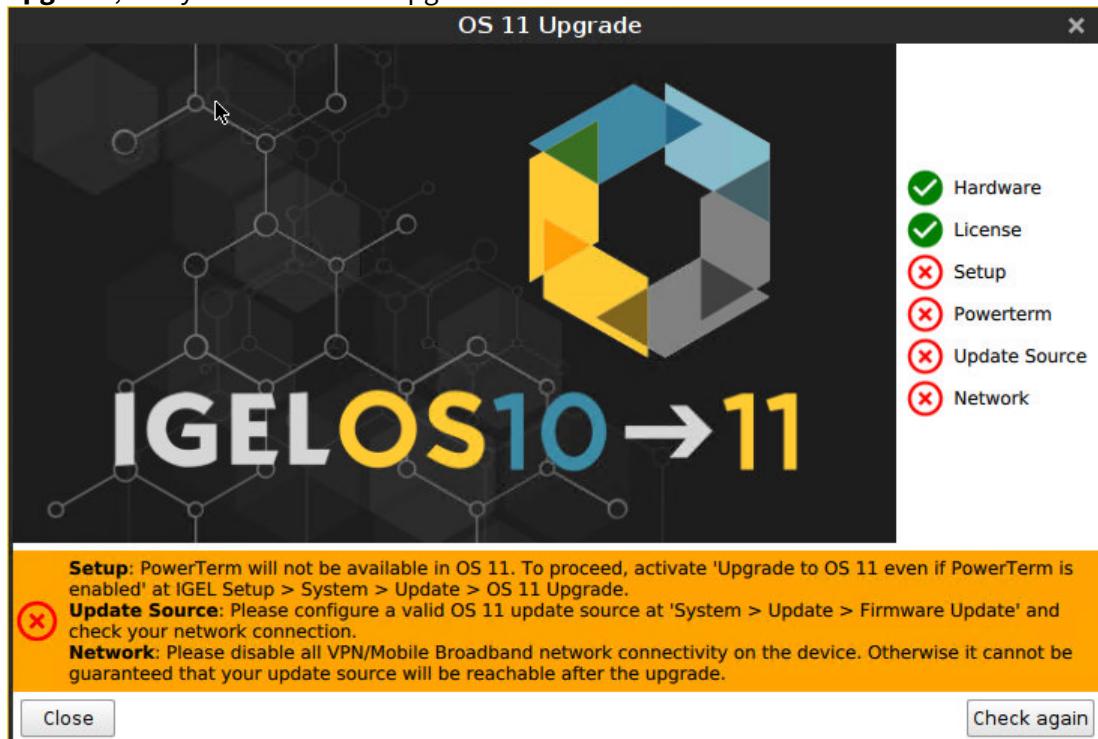
You can change the starting methods for the OS 11 Upgrade Tool in the Setup under **Accessories > OS11 Upgrade**.



2. Check the output of the OS 11 Upgrade Tool and continue appropriately:
  - If each requirement has an , click **OS Upgrade** to start the upgrade process.
  - If one or more requirements have an , check the messages and resolve the issues. Afterwards, click **Check again**. If all requirements are met, the button changes to **OS**

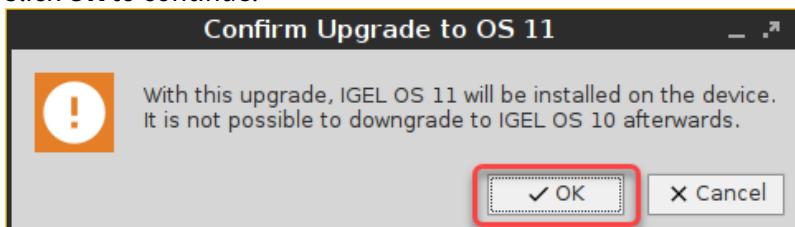


**Upgrade**, and you can start the upgrade.

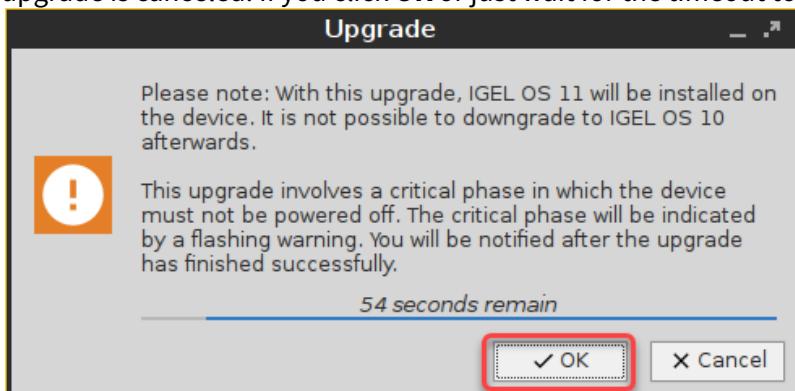


When you start the upgrade, a warning dialog is shown.

- Click **OK** to continue.



A warning dialog with a timeout is shown. If you click **Cancel** before the timeout expires, the upgrade is canceled. If you click **OK** or just wait for the timeout to expire, the upgrade is started



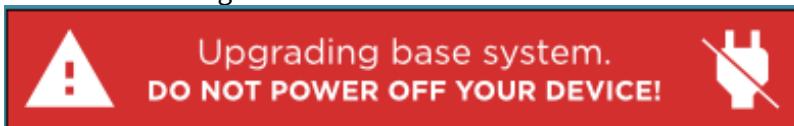
After the warning dialog has been confirmed or the timeout has expired, the device reboots into a special IGEL OS 10 environment, in which the system upgrade is executed. The **Upgrade** window



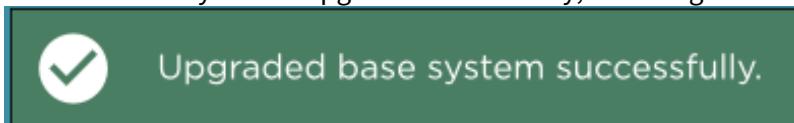
show the progress.



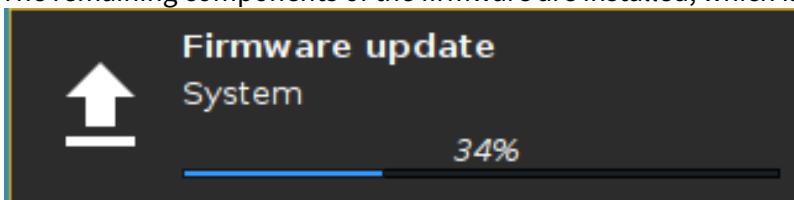
During the critical phase, the device must not be powered off. At this stage in the progress, an additional warning is shown.



When the base system is upgraded successfully, a message is shown.



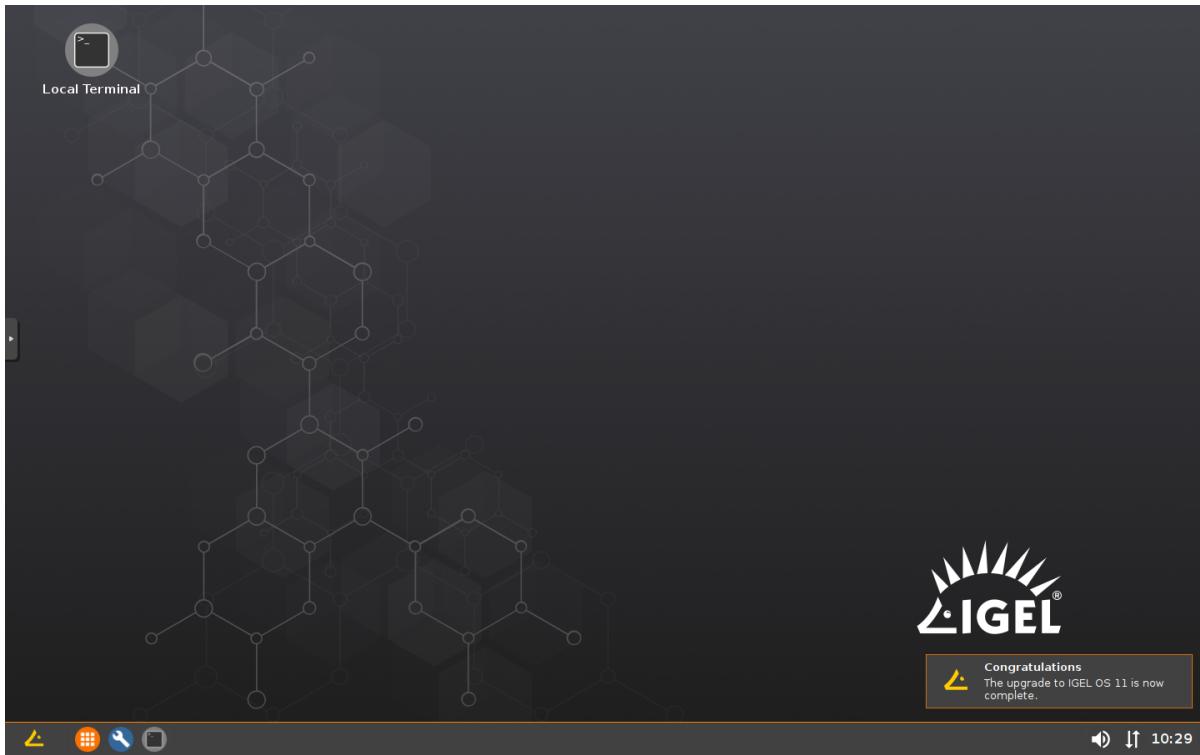
The remaining components of the firmware are installed, which is indicated by update messages.



When the installation is completed, the **Upgrade** window looks like this:



After a few seconds the device reboots into IGEL OS 11.



When the upgrade test has been successful, you are ready to set up the mass upgrade. Continue with [Checking the Requirements](#)(see page 154).

### Checking the Requirements

The following requirements must be met:

- The upgrade has been tested with characteristic devices.
- UMS 6.01.130 or higher is available.



- The firmware IGEL OS 10.05.800 (or higher) is known to the UMS. For this purpose, a device with this firmware version must be registered in the UMS. This is already the case if you tested the upgrade with the same UMS with which you are about to do the mass upgrade. If not, you must register a device with the appropriate firmware version now.
- All devices are connected to a regular LAN (not OpenVPN, OpenConnect, genucard, NCP VPN or mobile broadband).
- All devices are in a safe environment where the upgrade process cannot be disrupted, e.g. by powering off the devices.

When all requirements are met, continue with [Configuring Two Update Buddies](#)(see page 155).

### Configuring Two Update Buddies

For setting up buddy updates, see the how-to [Buddy Update](#)(see page 221).

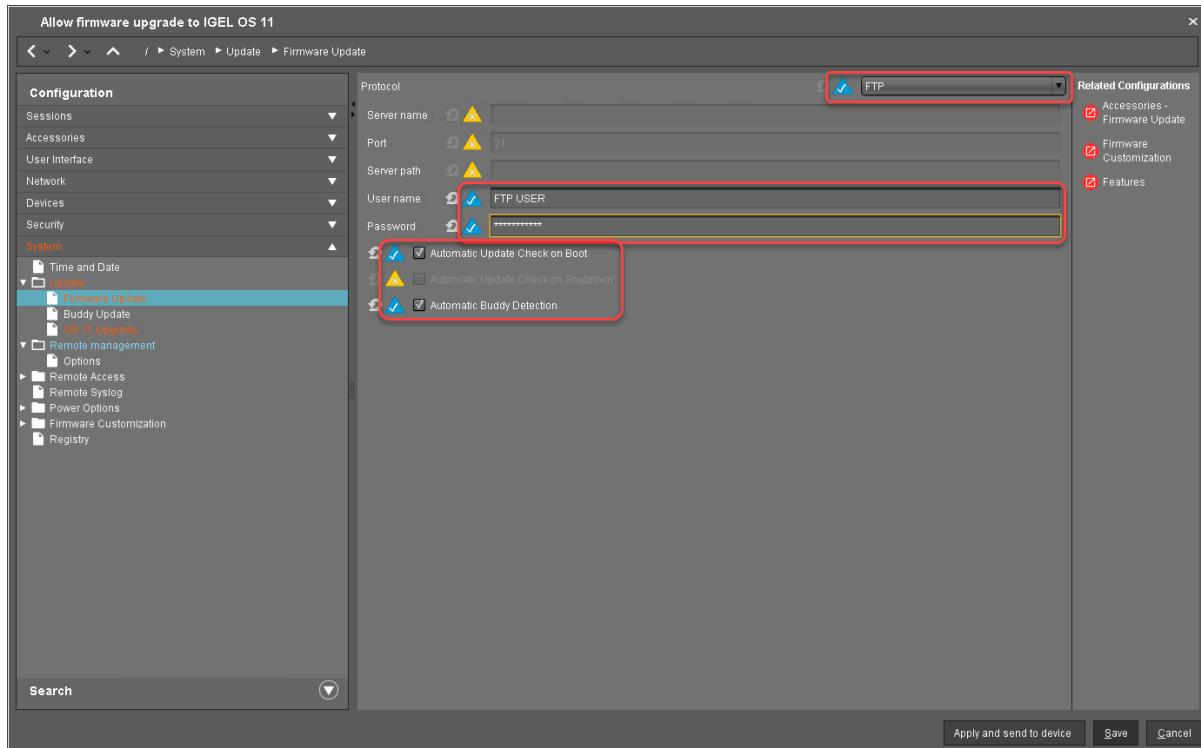
Ensure that the network contains only the update buddies and the devices that are to be updated. This prevents other devices from updating inadvertently.

1. Update one device to the appropriate IGEL OS 10 firmware (10.05.800 or higher) and configure it as an update buddy.
2. Upgrade another device to IGEL OS 11 and configure it as an update buddy. Make sure that the IGEL OS 11 update buddy has the same **User Name** and **Password** in **System > Update > Buddy Update** as the IGEL OS 10 update buddy.

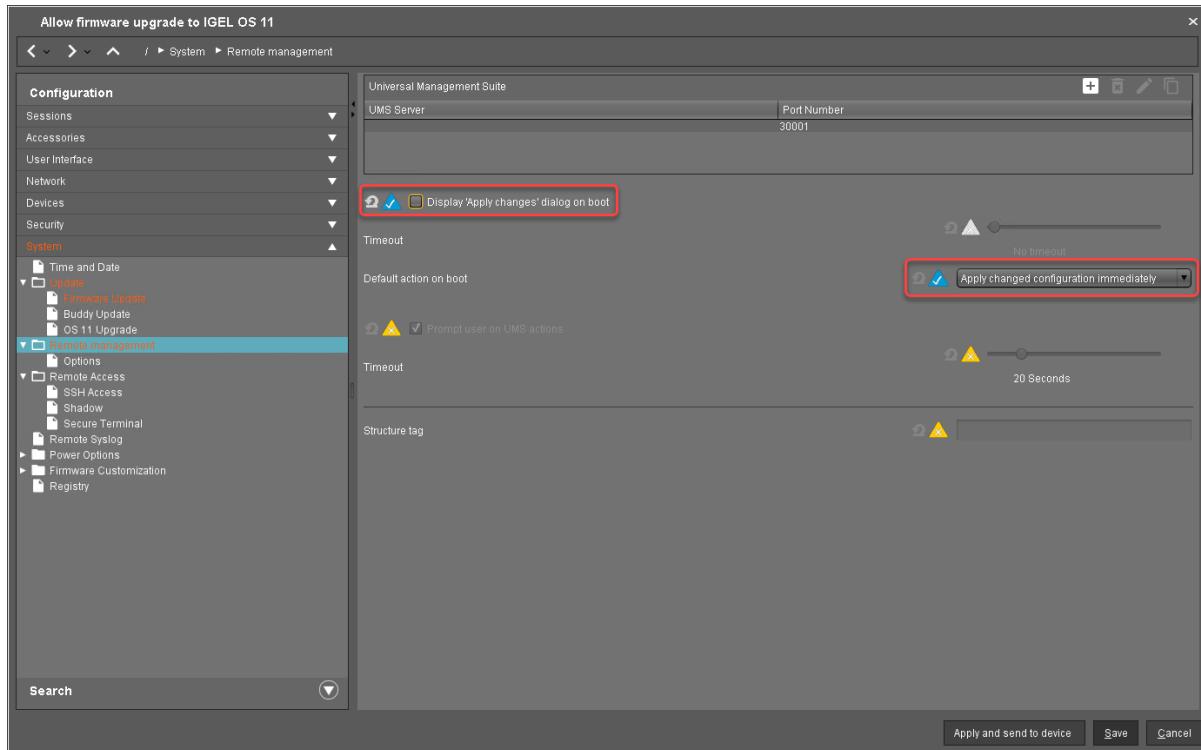
When the update buddies are configured, continue with [Creating a Profile](#)(see page 155).

### Creating a Profile

1. Create a profile that is based on the appropriate IGEL OS 10 version (10.05.800 or higher). Find a suitable name for the profile, e.g. "Firmware upgrade to IGEL OS 11".
2. In the profile's configuration dialog, go to **System > Update > Firmware Update** and change the settings as follows:
  - Select "FTP" as **Protocol**.
  - Enter **User Name** and **Password** according to the update buddy server.
  - Activate **Automatic Update Check on Boot**.
  - Ensure that **Automatic Update Check on Shutdown** is deactivated. Otherwise, the device will shut down when the upgrade to OS 10.05.800 is finished.
  - Activate **Automatic Buddy Detection**.



3. Go to **System > Update > OS 11 Upgrade** and change the following settings according to your successful upgrade test (for details, see [Adjusting the Setup\(see page 149\)](#)):
  - Activate **Upgrade to OS 11**.
  - Set **Upgrade to OS 11 even if PowerTerm is enabled** according to your needs.
  - Set **Require an Enterprise Management Pack license to upgrade to OS 11** according to your needs.
  - Set **Timeout waiting for OS 11 license to start automatic upgrade** to **10 Minutes**.
4. Go to **System > Remote Management** and change the settings as follows:
  - Deactivate **Display 'Apply changes' dialog on boot**.
  - Set **Default action on boot** to **Apply changed configuration immediately**.



## 5. Click **Save**.

When the profile is created, continue with [Deploying the Licenses](#)(see page 157).

## Deploying the Licenses

Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see [Setting up Automatic License Deployment \(ALD\)](#)<sup>71</sup>.
- Manual License Deployment: Licenses are created and deployed manually. For instructions, see [Manual License Deployment for IGEL OS](#)<sup>72</sup>.

When the license deployment is set up, continue with [Putting It All Together](#)(see page 157).

## Putting It All Together

1. Assign the profile to all devices that are to be upgraded. This can be done by assigning the profile to the directory that contains these devices.

Do not assign the profile to the update buddies.

2. In the context menu of the assignment, select **Now**.

---

<sup>71</sup> <https://kb.igel.com/pages/viewpage.action?pageId=10325058>

<sup>72</sup> <https://kb.igel.com/display/licensesmoreigelos11/Manual+License+Deployment+for+IGEL+OS>



3. For Automatic license deployment, a condition can be set to the directory. For more information, see [Configuring the Distribution Conditions](#)<sup>73</sup>, section "Distributing Licenses to Devices in a Specified Directory".

When everything is in place, continue with [Executing the Upgrade](#)(see page 158).

### Executing the Upgrade

1. In the UMS, select all devices that are to be upgraded and reboot them.

Alternatively, you can create a scheduled job for reboot or wake up and assign it to the devices or the directory containing these devices; for more information, see [Jobs](#)<sup>74</sup>.

On reboot or wake up, the devices choose the IGEL OS 10 buddy. They ignore the IGEL OS 11 buddy at this stage because this version is not known to them yet. The devices update to the appropriate IGEL OS 10 version (10.05.800 or higher). With this version, the **Upgrade to OS 11** parameter is recognized by the devices; also, the devices request IGEL OS 11 licenses from the UMS (Workspace Edition and, if required, Enterprise Management Pack).

If no IGEL OS 11 licenses have been deployed on the devices yet, the licenses are deployed within a few minutes. The upgrade will be started when the licenses are deployed. The maximum time period the device will wait for a license is configured by the parameter **Timeout waiting for OS 11 license to start automatic upgrade**; for details, see [Adjusting the Setup](#)(see page 149).

The parameters **Automatic update check on boot** and **Automatic buddy detection** cause the devices to look for a new firmware and wait for an IGEL OS 11 update buddy to reply. When an IGEL OS 11 update buddy is found, the devices start the upgrade process.

#### Update Can Be Canceled After Timeout

An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

2. When all devices have been upgraded successfully, remove the "Firmware upgrade to IGEL OS 11" profile.

The upgrade is completed.

### Mass Deployment Using a Scheduled Job

This scenario is appropriate if you already have a working environment with IGEL OS 10.05.800 (or higher) and want to update all devices to IGEL OS 11 at a defined time.

Read all the following chapters carefully and follow the instructions.

<sup>73</sup> <https://kb.igel.com/display/licensesmoreigelos11/Configuring+the+Distribution+Conditions>

<sup>74</sup> <https://kb.igel.com/display/endpointmgmt601/Jobs>



1. [Checking the Requirements](#)(see page 159)
2. [Creating a Profile](#)(see page 160)
3. [Deploying the Licenses](#)(see page 163)
4. [Assigning the Profile](#)(see page 164)
5. [Creating the Scheduled Job](#)(see page 166)

### Checking the Requirements

The following requirements must be met:

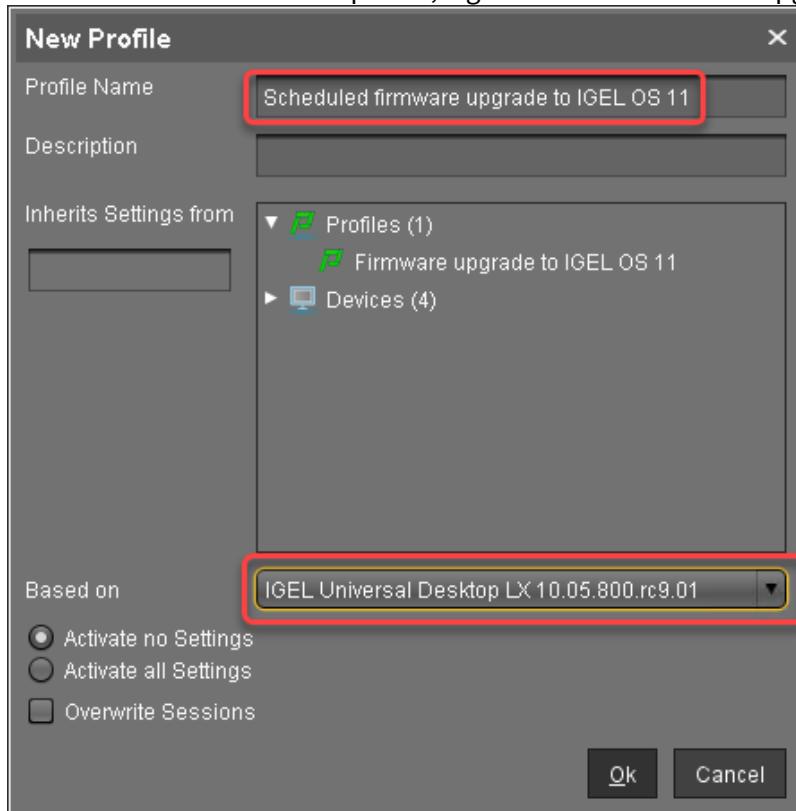
- The upgrade has been tested with characteristic devices.
- UMS 6.01.130 or higher is available.
- The firmware IGEL OS 10.05.800 (or higher) is known to the UMS. For this purpose, a device with this firmware version must be registered in the UMS. This is already the case if you tested the upgrade with the same UMS with which you are about to do the mass upgrade. If not, you must register a device with the appropriate firmware version now.
- All devices are connected to a regular LAN (not OpenVPN, OpenConnect, genucard, NCP VPN or mobile broadband).
- All devices are in a safe environment where the upgrade process cannot be disrupted, e.g. by powering off the devices.

When all requirements are met, continue with [Creating a Profile](#)(see page 160).



## Creating a Profile

1. Create a profile that is based on the appropriate IGEL OS 10 firmware version (10.05.800 or higher). Find a suitable name for the profile, e.g. "Scheduled firmware upgrade to IGEL OS 11".



2. In the profile's configuration dialog, go to **System > Update > Firmware Update** and change the settings according to your environment:

If you use [Universal Firmware Update](#)(see page 183) for OS 11, you do not need to configure the settings described in this step.

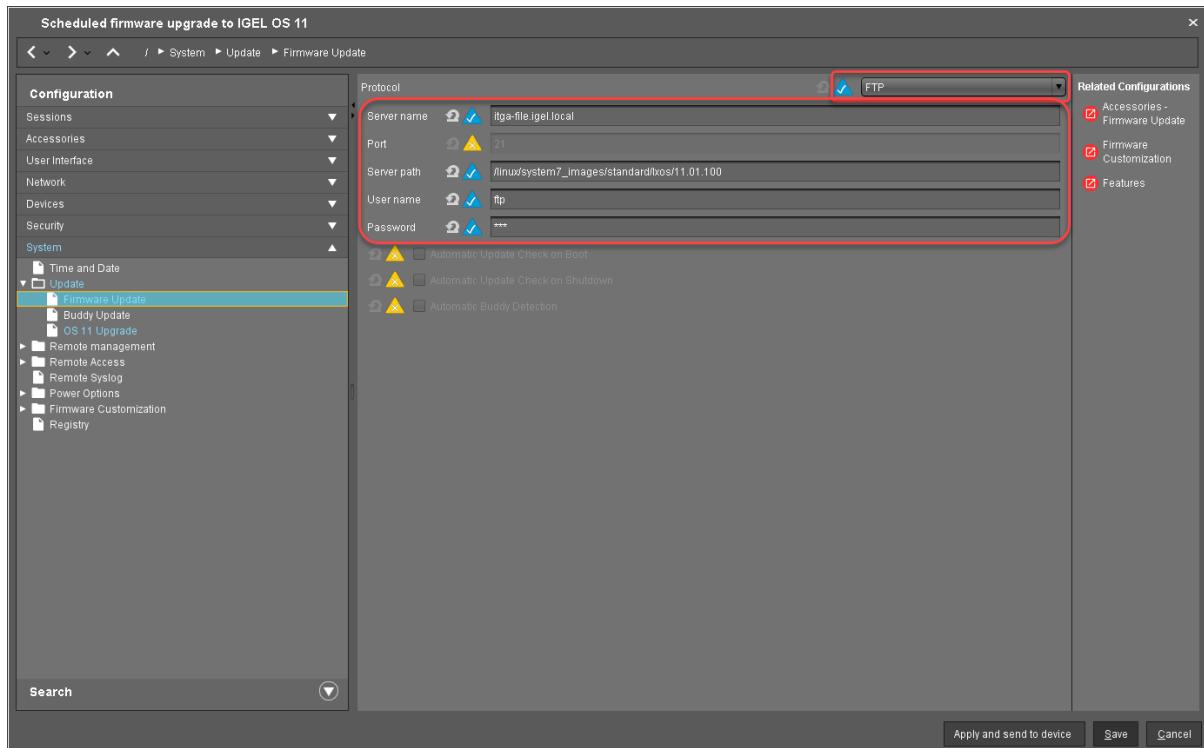
- Select an update source for IGEL OS 11. For further information, see [Firmware Update](#)(see page 1252).

If you use **FILE** as the protocol (local file or network drive), the device will show an error message and go through an additional reboot. Apart from that, the upgrade will work normally.

- Ensure that **Automatic Update Check on Boot** and **Automatic Update Check on Shutdown** are deactivated.

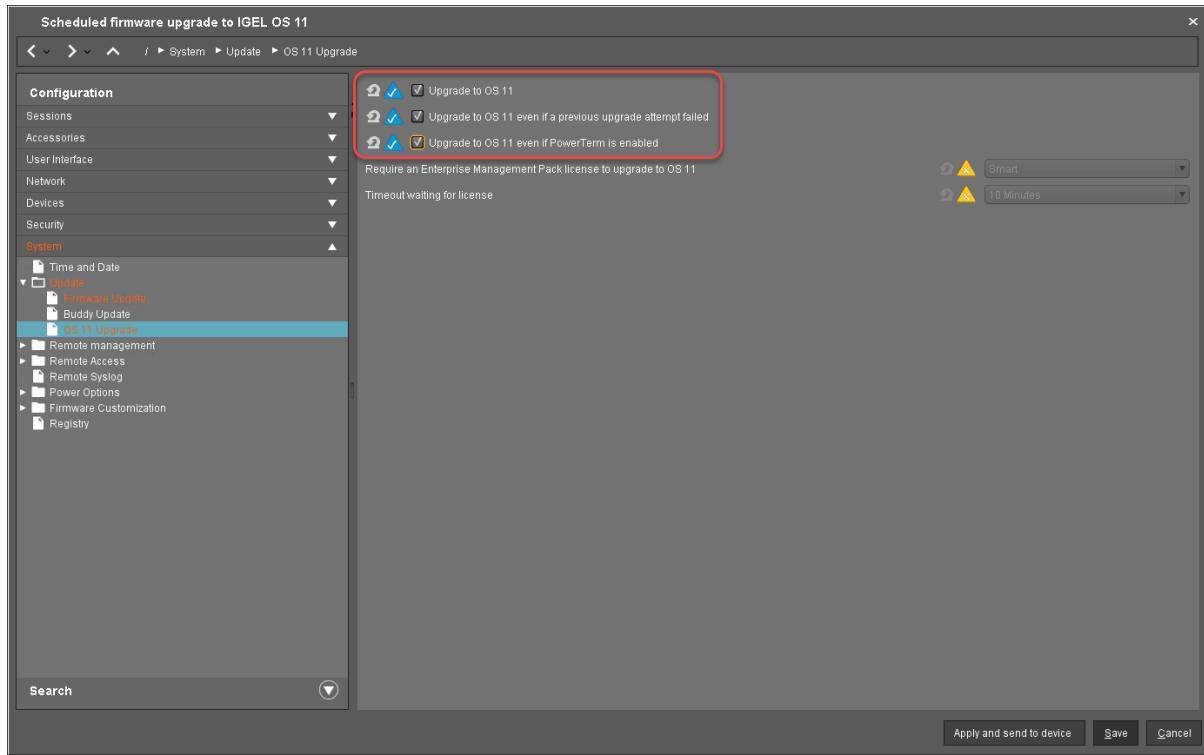


In the following screenshot, FTP is used as an example. The other protocols can be used as well.

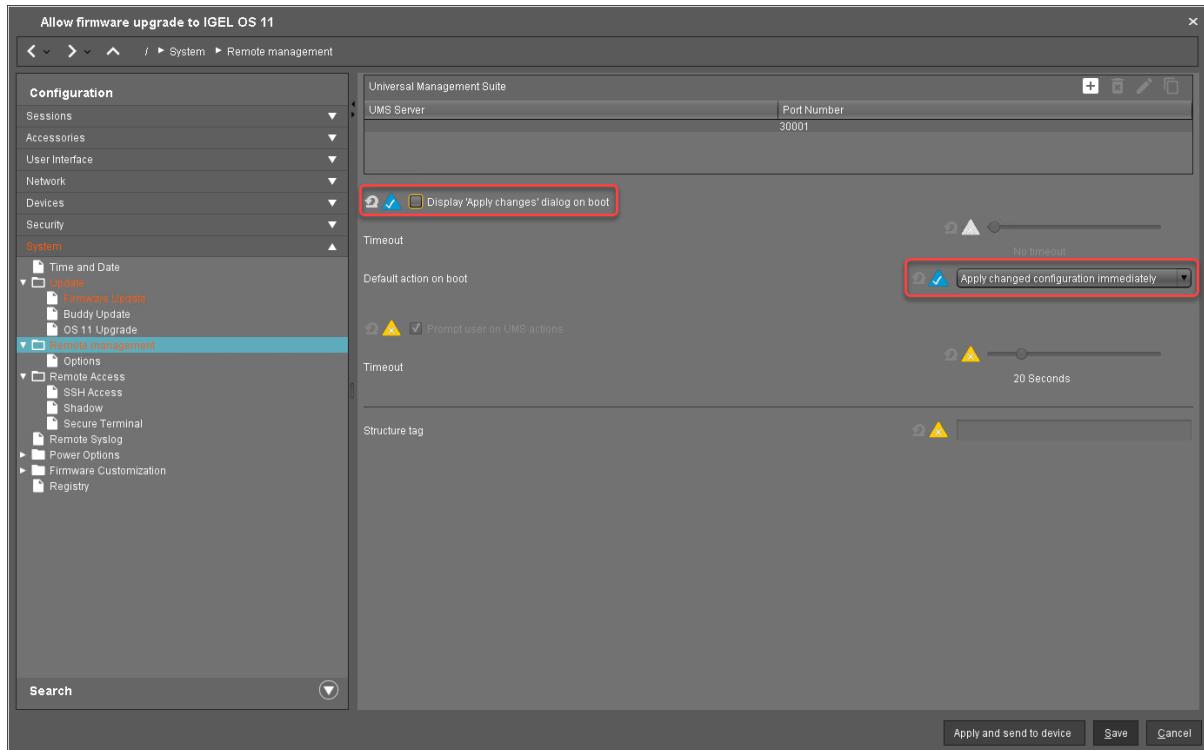


3. Go to **System > Update > OS 11 Upgrade** and change the following settings according to your successful upgrade test:

- Activate **Upgrade to OS 11**.
- Set **Upgrade to OS 11 even if PowerTerm is enabled** according to your needs.
- Set **Upgrade to OS 11 even if a previous upgrade attempt failed** according to your needs.
- Set **Require an Enterprise Management Pack license to upgrade to OS 11** according to your needs.
- Ensure that the **Timeout waiting for OS 11 license to start automatic upgrade** is set to **10 Minutes**.



4. Go to **System > Remote Management** and change the settings as follows:
  - Deactivate **Display 'Apply changes' dialog on boot**.
  - Set **Default action on boot** to **Apply changed configuration immediately**.



## 5. Click **Save**.

When the profile is created, continue with [Deploying the Licenses](#)(see page 137).

## Deploying the Licenses

Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see [Setting up Automatic License Deployment \(ALD\)](#)<sup>75</sup>.
- Manual License Deployment: Licenses are created and deployed manually. For instructions, see [Manual License Deployment for IGEL OS](#)<sup>76</sup>.

When the license deployment is set up, continue with [Assigning the Profile](#)(see page 164).

---

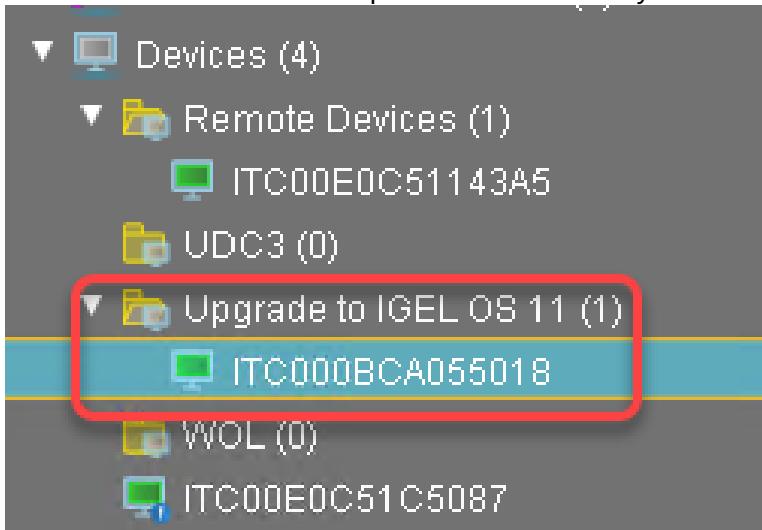
<sup>75</sup> <https://kb.igel.com/pages/viewpage.action?pageId=10325058>

<sup>76</sup> <https://kb.igel.com/display/licensesmoreigelos11/Manual+License+Deployment+for+IGEL+OS>

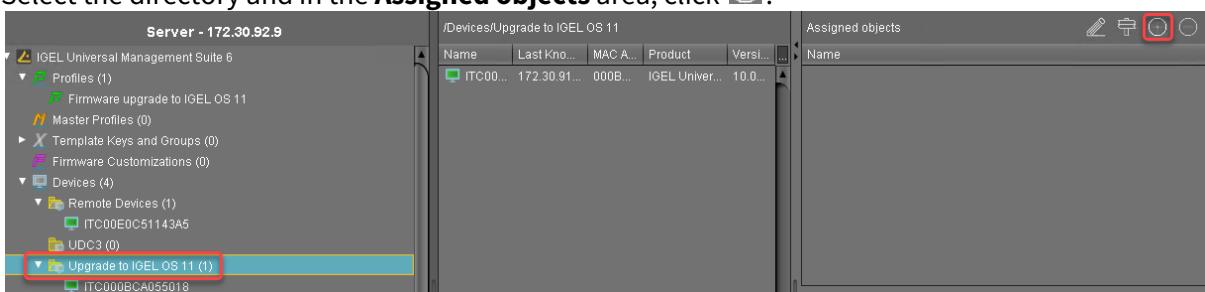


## Assigning the Profile

1. Put all devices that are to be updated into a directory.

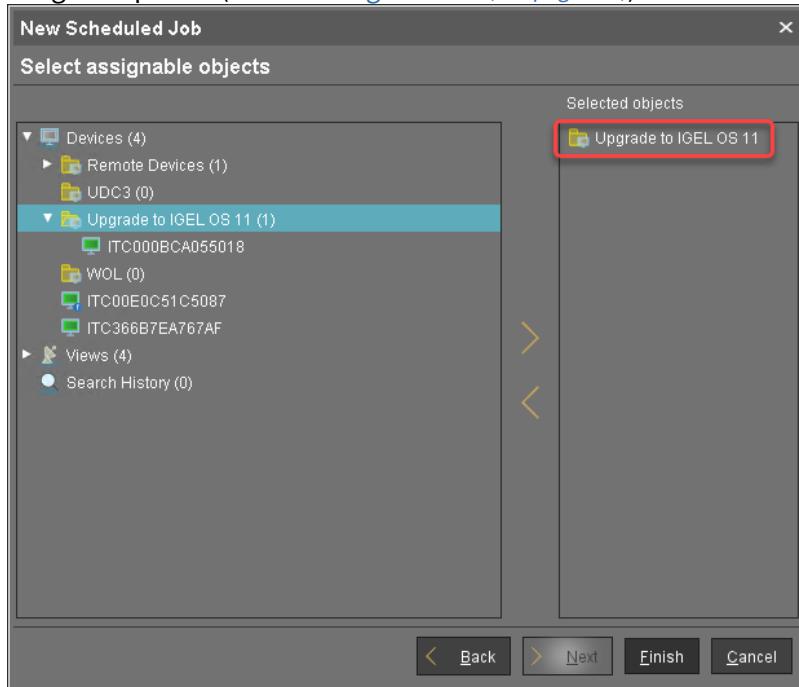


2. Select the directory and in the **Assigned objects** area, click .

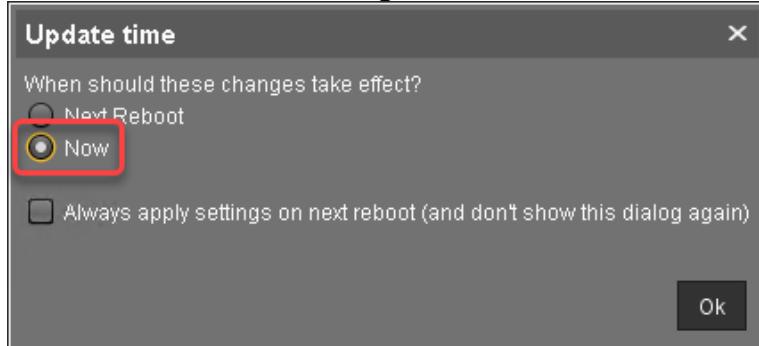




3. Assign the profile (see [Creating a Profile\(see page 160\)](#)) to the directory and click **Ok**.



4. In the context menu of the assignment, select **Now**.

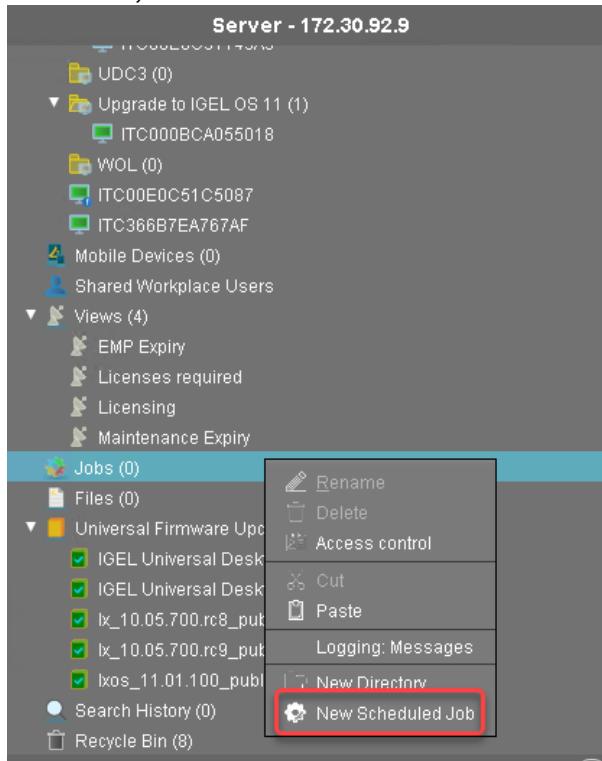


When the profile is assigned, continue with [Creating the Scheduled Job\(see page 166\)](#).



## Creating the Scheduled Job

1. In the UMS, select **Jobs > New Scheduled Job**.





2. Under **Name**, enter a suitable name for the job, e. g. "Upgrade to IGEL OS 11".

New Scheduled Job

**Details**

Name	Upgrade to IGEL OS 11
Command	OS 11 Upgrade
Execution time	11:53
Start date	2019-04-10
Comment	(empty)

**Options**

<input checked="" type="checkbox"/> Log results	<input type="checkbox"/> Retry next boot
Max. Threads	99
Delay	0
Seconds	(empty)
Timeout	30

**Job-Info**

Job ID	(empty)
Next Execution	Apr 10, 2019 11:53 AM
User	(empty)

Back Next Finish Cancel



3. Under **Command**, select **OS 11 Upgrade**.

New Scheduled Job

**Details**

Name	Upgrade to IGEL OS 11
Command	OS 11 Upgrade
Execution time	11:53
Start date	2019-04-10
Comment	(empty)

**Options**

<input checked="" type="checkbox"/> Log results	<input type="checkbox"/> Retry next boot
Max. Threads	99
Timeout	30

**Job-Info**

Job ID	
Next Execution	Apr 10, 2019 11:53 AM
User	

Back Next Finish Cancel



4. Under **Execution time** and **Start date**, set the time at which the upgrade should be executed, and click **Next**.

New Scheduled Job

Details

Name	Upgrade to IGEL OS 11
Command	OS 11 Upgrade
Execution time	11:53
Start date	2019-04-10
Comment	(empty)

Options

<input checked="" type="checkbox"/> Log results	<input type="checkbox"/> Retry next boot
Max. Threads	99
Timeout	30
Delay	0 Seconds

Job-Info

Job ID	(empty)
Next Execution	Apr 10, 2019 11:53 AM
User	(empty)

Buttons: Back, Next, Finish, Cancel



5. Review the execution time and click **Next**.

New Scheduled Job

Schedule

Execution time: 11:53 Start date: 2019-04-10  
 Expiration date: Time: 11:49

Repeat Job:

Never  
 Every: 0 day, 0 hour  
 Weekdays:  Mon,  Tue,  Wed,  Thu,  Fri,  Sat,  Sun  
 Exclude Public Holidays

Date Comment

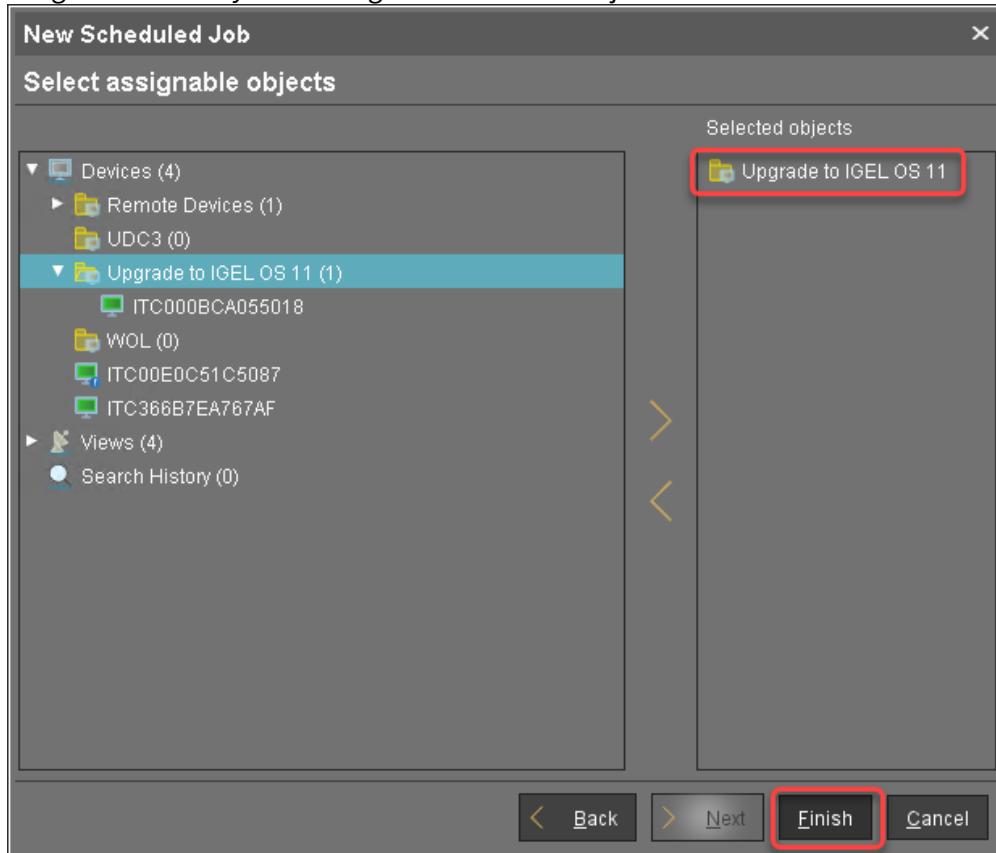
Cancel job execution:

Never  
 Time: 00:00  
 Max. duration: 00:00

[Back](#) [Next](#) [Finish](#) [Cancel](#)



6. Assign the directory containing the devices to the job and click **Finish**.



#### Update Can Be Canceled After Timeout

An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

The upgrade is completed.

#### Troubleshooting

This section describes possible error cases and solutions.

- [Regaining a Usable System](#)(see page 172)
- [Getting Error Messages](#)(see page 172)
- [Starting an New Upgrade Attempt](#)(see page 173)
- [Starting Another Upgrade Attempt after 5 Retries](#)(see page 173)



## Regaining a Usable System

Here you can find typical upgrade failures and the appropriate methods to regain a usable system.

Device Has Upgraded to Igel OS 11, but Does Not Boot Any More

To get a working IGEL OS 11 system:

- ▶ Use the IGEL OS Creator to recover the IGEL OS 11 system. For more information, see the [IGEL OS Creator Manual](#)(see page 1293).

IGEL OS 10 Rescue System Fails to Update Missing Partitions

If a severe error has occurred during the upgrade process, the device boots into a minimal IGEL OS 10 (10.05.800 or higher) rescue system. If unattended, the device tries to download and update the missing partitions and reboots on failure.

To regain a full IGEL OS 10 system, you have two possibilities:

- ▶ In the rescue system, start the Setup, go to **System > Update > Firmware Update** and set a valid update source for the appropriate IGEL OS 10 firmware (10.05.800 or higher).

Or:

- ▶ Configure a UMS profile that contains a valid update source for the appropriate IGEL OS 10 firmware (10.05.800 or higher) under **System > Update > Firmware Update** and assign it to the device.

## Getting Error Messages

- ▶ Open the OS 11 Upgrade Tool (default path: click System and then **Upgrade to OS 11**).

The OS 11 Upgrade Tool shows the error messages. The most important message is prefixed with **Retries**; see the example below:



- ▶ For more information, review the main migration log under `/wfs/migration.log`

You can use the system log viewer to review the migration log (see the chapter [System Log Viewer](#)(see page 1070) in the IGEL OS Manual) or save the log files in order to send them to the IGEL Support Team (see the chapter [Save Device Files for Support](#)<sup>77</sup> support).

#### Starting an New Upgrade Attempt

If you want the device to start multiple upgrade attempts (and the device is not already configured to do so):

1. In the UMS profile or in the Setup, go to **System > Update > OS 11 Upgrade** and activate **Upgrade to OS 11 even if a previous upgrade attempt failed**.
2. Reboot the device.

#### Starting Another Upgrade Attempt after 5 Retries

When the **Upgrade to OS 11 even if a previous upgrade attempt failed** option is set and the upgrade has failed each time, the system will stop trying after 5 attempts.

To reset the retry counter:

1. In the Setup or the UMS profile, go to **System > Update > OS 11 Upgrade** and deactivate **Upgrade to OS 11 even if a previous upgrade attempt failed**.

<sup>77</sup> <https://kb.igel.com/display/endpointmgmt601/Save+TC+Files+for+Support>



2. When the setting is effective on the devices, go to **System > Update > OS 11 Upgrade** again and activate **Upgrade to OS 11 even if a previous upgrade attempt failed..**

The retry counter is reset, and the devices will try upgrading another 5 times, if necessary.

## Upgrading IGEL Devices from IGEL OS 10 to IGEL OS 11

This document describes how to upgrade any number of IGEL Universal Desktop devices (UD) from IGEL OS 10 to IGEL OS 11.

IGEL OS 10.05.700 or higher is required for upgrading to IGEL OS 11. If you have an older version of IGEL OS 10, you need to update to version 10.05.700 or a higher version first.

The following methods of mass deployment are described here:

- [Zero-Touch Deployment Using Universal Firmware Update](#)(see page 174): Mass upgrade from any version of IGEL OS 10 to IGEL OS 11 in one step using Universal Firmware Update. This method can be started immediately or as a scheduled job (wake up or reboot).
- [Zero-Touch Deployment Using Buddy Update](#)(see page 197): Mass upgrade from any version of IGEL OS 10 to IGEL OS 11 in one step using two devices as update buddies. This method can be started immediately or as a scheduled job (wake up or reboot).
- [Mass Deployment Using a Scheduled Job](#)(see page 209): Upgrade devices that are already running IGEL OS 10.05.700 (or higher) using a specific scheduled job.

### Zero-Touch Deployment Using Universal Firmware Update

This method is the most convenient way to upgrade from IGEL OS 10 to IGEL OS 11. The method uses the Universal Firmware Update feature of the UMS (Universal Management Suite) and a profile.

Read all the following chapters carefully and follow the instructions.

1. [IGEL Devices That Can Be Upgraded to IGEL OS 11](#)(see page 174)
2. [Important! Consider This Before Upgrading](#)(see page 176)
3. [Preparing the Upgrade](#)(see page 177)
4. [Testing the Upgrade](#)(see page 179)
5. [Checking the Requirements](#)(see page 182)
6. [Creating the Universal Firmware Updates](#)(see page 183)
7. [Creating a Profile](#)(see page 188)
8. [Deploying the Licenses](#)(see page 192)
9. [Putting It All Together](#)(see page 193)
10. [Executing the Upgrade](#)(see page 195)

### IGEL Devices That Can Be Upgraded to IGEL OS 11

IGEL UD (Universal Desktop)

Product Line	Device Type	Hardware ID	64 Bit	Memory	Storage	HW Video Acceleration
UD2	D220	40	Yes	2 GB	4 GB	Yes
UD2	M250C	50	Yes	2 GB	4 GB	Yes
UD2	M250C	51/52	Yes	2 GB	8 GB	Yes



Product Line	Device Type	Hardware ID	64 Bit	Memory	Storage	HW Video Acceleration
UD3*(see page 175)	M340C	50	Yes	2 GB	4 GB	Yes
UD3	M340C	51	Yes	2 GB	4 GB	Yes
UD3	M350C	60	Yes	4 GB	8 GB	Yes
UD5	H830C	50	Yes	2 GB	4 GB	Yes
UD6	H830C	51	Yes	2 GB	4 GB	Yes
UD7	H850C	10	Yes	4 GB	4 GB	Yes
UD7***(see page 175)	H850C	11	Yes	4 GB	4 GB	Yes
UD7	H860C	20	Yes	8 GB	8 GB	Yes
UD9	TC215B	40 / 41 (Touch)	Yes	2 GB	4 GB	Yes

\* IGEL UD3-LX 50 is officially supported up to IGEL OS 11.05, incl. private builds.

\*\*As of December 2019, IGEL UD7 model H850C is equipped with the AMD Secure Processor<sup>78</sup>, for further information, see [UD7 Model H850C](#)<sup>79</sup>.

## IGEL Zero

### Note on IZ Devices

The IZ devices listed below can be upgraded to IGEL OS 11. To upgrade your IZ devices to IGEL OS 11, please contact your IGEL sales representative. See also <https://www.igel.com/tradeup/> and [The IGEL OS 11 Trade-Up](#)<sup>80</sup>.

Product Line	Device Type	Hardware ID	64 Bit	Memory	Storage	UEFI Secure Boot Support	HW Video Acceleration
IZ2	D220	40	Yes	2 GB	4 GB	Yes	Yes
IZ3	M340C	50	Yes	2 GB	4 GB	Yes	Yes
IZ3	M340C	51	Yes	2 GB	4 GB	Yes	Yes

When you have confirmed that your devices can be upgraded to IGEL OS 11, make sure to consider [Important! Consider This Before Upgrading](#)(see page 176).

<sup>78</sup> <https://kb.igel.com/display/securitysafety/AMD+Secure+Processor>

<sup>79</sup> <https://kb.igel.com/display/securitysafety/UD7+Model+H850C>

<sup>80</sup> <https://kb.igel.com/display/licensesmoreigelos11/The+IGEL+OS+11+Trade+up>



## Important! Consider This Before Upgrading

To make sure that your upgrade can be successful, check the following warnings and notes; a warning symbol indicates that irreversible damage can be done to your devices.

### No Downgrade

You cannot restore your IGEL OS 10 system once you have migrated to IGEL OS 11. The device storage is overwritten completely with a new partitioning scheme.

### Features (e.g. Clients)

IGEL OS 11 does not have the complete feature set of IGEL OS 10. Make sure that the current version of IGEL OS 11 meets your requirements. For details, refer to the appropriate release notes.

### Custom Partitions

The contents of custom partitions will be deleted by the upgrade. Make sure to back up the contents and restore them after the upgrade has finished. Besides becoming dysfunctional after the upgrade, applications and kernel drivers in a custom partition might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device. We recommend that you disable custom partitions when upgrading; you can enable them once the upgrade has been successfully completed.

### Custom Commands

The persistence of custom commands cannot be guaranteed. Besides becoming dysfunctional after the upgrade, custom commands might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device. In general, custom commands must be adapted for IGEL OS 11. We recommend that you disable custom commands when upgrading; you can enable them once the upgrade has been successfully completed.

### Network

All devices must be connected to a WLAN or LAN. LAN is the recommended option. The device will not be upgraded if connected to OpenVPN, OpenConnect, genucard, NCP VPN or mobile broadband.

### Hardware Support

Make sure that your devices support IGEL OS 11; please refer to [IGEL Devices Supported by IGEL OS 11<sup>81</sup>](#). This document describes upgrading methods for IGEL UD and IGEL IZ devices. Upgrading methods for IGEL UDC3 and UD Pocket are described under [Upgrading UDC3 Devices from IGEL OS 10 to IGEL OS 11<sup>82</sup>](#).

<sup>81</sup> <https://kb.igel.com/display/hardware/IGEL+Devices+Supported+by+IGEL+OS+11+1>

<sup>82</sup> <https://kb.igel.com/display/igelos1102/Upgrading+UDC3+Devices+from+IGEL+OS+10+to+IGEL+OS+11>



### License

- A valid license from an IGEL Workspace Edition (WE) Product Pack must be available for each device. For general information, see [IGEL Software License Overview<sup>83</sup>](#). For deploying licenses, see [Setting up Automatic License Deployment \(ALD\)<sup>84</sup>](#) or [Manual License Deployment for IGEL OS<sup>85</sup>](#).
- IZ devices are not allowed to upgrade to IGEL OS 11. Please contact your IGEL sales representative for a UD Upgrade License which allows you to upgrade your IZ devices.

### UMS Version

UMS version 6.01.130 or higher is required for upgrading from IGEL OS 10 to IGEL OS 11.

When you have considered everything that is relevant, continue with [Preparing the Upgrade\(see page 177\)](#).

### Preparing the Upgrade

This section describes the required preparations and tests before any productive devices can be updated. The testing should be done with at least one device that is characteristic of your environment. This device should have every custom partition and every custom command that may possibly exist in any of your devices.

First of all, you should check thoroughly if IGEL OS 11 has all features required for your purposes.

- Continue with [Preparing the UMS\(see page 177\)](#).

### Preparing the UMS

To upgrade your devices to IGEL OS 11, you need the appropriate version of the UMS. Also, the devices must be registered with the UMS to receive their licenses.

1. If you have not already done so, update your UMS to version 6.01.130 or higher. For instructions, see [Updating a UMS Installation<sup>86</sup>](#).
2. Make sure that your devices are registered with the UMS. For more information, see the chapter [Registering Devices on the UMS Server<sup>87</sup>](#) in the UMS Manual.

When the UMS is prepared, continue with [Adjusting the Setup\(see page 177\)](#).

### Adjusting the Setup

Depending on the features that are in use now or will be used in the future, a specific set of parameters must be set in the device's Setup.

1. In the Setup, go to **System > Update > OS 11 Upgrade**.
2. Make your settings as appropriate:
  - Activate **Upgrade to OS 11**.
  - If you want the device to retry the upgrade immediately after a failed attempt, activate **Upgrade to OS 11 even if a previous upgrade attempt failed**. The device will retry

<sup>83</sup> <https://kb.igel.com/display/licensesmoreigelos11/IGEL+Software+License+Overview>

<sup>84</sup> <https://kb.igel.com/pages/viewpage.action?pageId=10325058>

<sup>85</sup> <https://kb.igel.com/display/licensesmoreigelos11/Manual+License+Deployment+for+IGEL+OS>

<sup>86</sup> <https://kb.igel.com/display/endpointmgmt601/Updating+a+UMS+Installation>

<sup>87</sup> <https://kb.igel.com/display/endpointmgmt601/Registering+devices+on+the+UMS+Server>



the upgrade 5 times. When the 5th attempt has failed, a message will be shown in the upgrade tool window.

- If your device has a PowerTerm license, and you want to upgrade to IGEL OS 11 even though it does not support PowerTerm, you must activate **Upgrade to OS 11 even if PowerTerm is enabled**.
  - Under **Require an Enterprise Management Pack license to upgrade to OS 11**, select the appropriate option:
    - If you are using IGEL Cloud Gateway (ICG) or Shared Workplace (SWP) or a Custom Partition and want to make sure that the upgrade is performed only if these features can be used furthermore, select **Smart**. When this option is selected, and any of these features is activated, the upgrade is performed only if the device could fetch a license from an Enterprise Management Pack.
    - If you want to force the device to fetch a license from an Enterprise Management Pack and make sure that the upgrade is performed only if the license could be fetched, select **Always**.
    - If you want the device to upgrade to IGEL OS 11 without fetching an Enterprise Management Pack, disregarding the features that might be activated, select **Never**.
  - Under **Timeout waiting for OS 11 license to start automatic upgrade**, set the time period the device will wait for a license in a mass deployment scenario (see [Zero-Touch Deployment Using Universal Firmware Update](#)(see page 174), [Zero-Touch Deployment Using Buddy Update](#)(see page 197) and [Mass Deployment Using a Scheduled Job](#)(see page 209)). This setting prevents the device from starting the upgrade at an inappropriate time as a result of the license just being deployed. This way, the setting prevents unwanted interruptions at work. For a mass deployment scenario, the default value **10 Minutes** is recommended.
3. Click **Apply**.
  4. Continue with [Deploying a License](#)(see page 178).

#### Deploying a License

To upgrade from IGEL OS 10 to IGEL OS 11, you need an appropriate license. Depending on your requirements, one or more of these licenses will be needed for each device:

- One Workspace Edition license for basic functionality; see [Workspace Edition](#)<sup>88</sup>
- If one of the following features is used, one Enterprise Management Pack license is required (see [Enterprise Management Pack](#)<sup>89</sup>):
  - IGEL Cloud Gateway (ICG)
  - Shared Workplace (SWP)
  - Custom Partition - if IGEL OS 11.03.100 or lower is the target version; in IGEL OS 11.03.500 or higher, the Custom Partition feature is included in the Workspace Edition.

Proceed as follows:

- Deploy the licenses for IGEL OS 11 using the method that suits your needs:
- **Manual License Deployment:** Licenses are created and deployed manually. For instructions, see [Manual License Deployment for IGEL OS](#)<sup>90</sup>.

---

<sup>88</sup> <https://kb.igel.com/display/licensesmoreigelos11/Workspace+Edition>

<sup>89</sup> <https://kb.igel.com/display/licensesmoreigelos11/Enterprise+Management+Pack>

<sup>90</sup> <https://kb.igel.com/display/licensesmoreigelos11/Manual+License+Deployment+for+IGEL+OS>



- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see [Setting up Automatic License Deployment \(ALD\)](#)<sup>91</sup>.
- Download three demo licenses from <https://www.igel.com/download/>.

When the device has a license, continue with [Configuring the Update Source](#)(see page 179).

#### Configuring the Update Source

1. In the Setup, go to **System > Update > Firmware Update** and configure the update source for IGEL OS 11. For more information, see the [Firmware Update](#)(see page 1252) chapter in the IGEL OS Manual.
2. Click **Ok**.

When the correct update source is configured, continue with [Testing the Upgrade](#)(see page 179).

#### Testing the Upgrade

1. Click System and then **Upgrade to OS 11**. The OS 11 Upgrade Tool starts and indicates whether all requirements are met.

You can change the starting methods for the OS 11 Upgrade Tool in the Setup under **Accessories > OS11 Upgrade**.



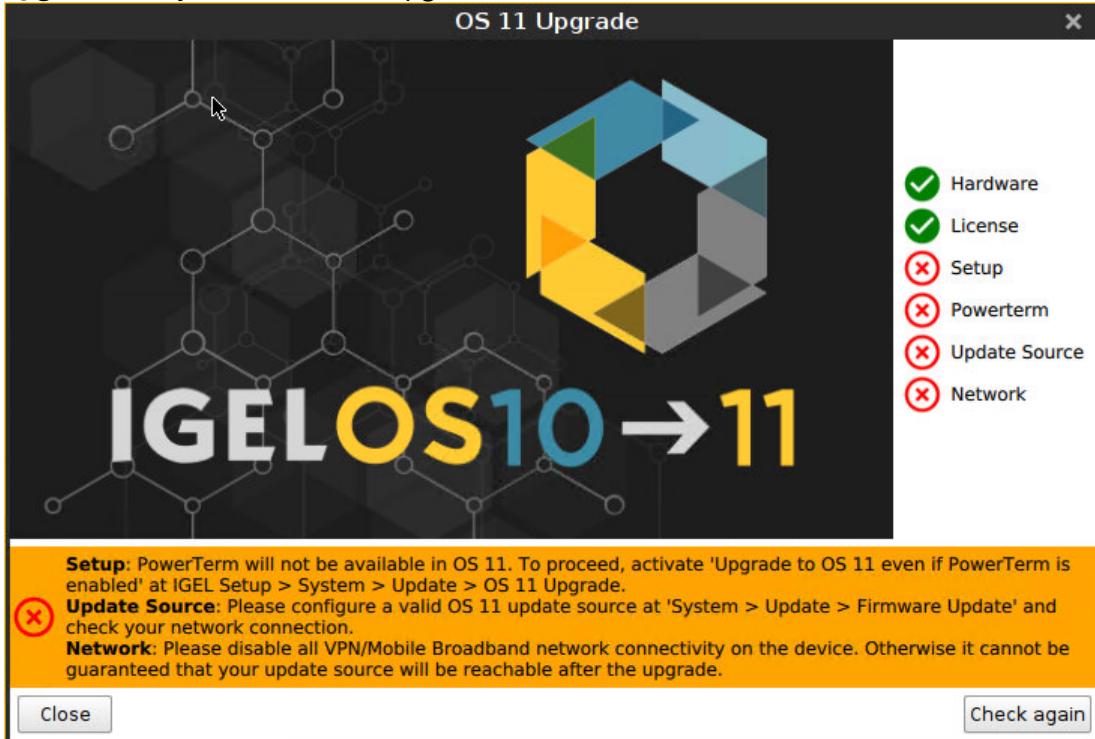
2. Check the output of the OS 11 Upgrade Tool and continue appropriately:

---

<sup>91</sup> <https://kb.igel.com/pages/viewpage.action?pageId=10325058>

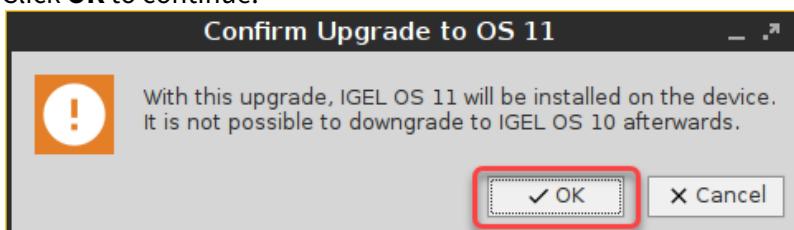


- If each requirement has an icon, click **OS Upgrade** to start the upgrade process.
- If one or more requirements have an icon, check the messages and resolve the issues. Afterwards, click **Check again**. If all requirements are met, the button changes to **OS Upgrade**, and you can start the upgrade.

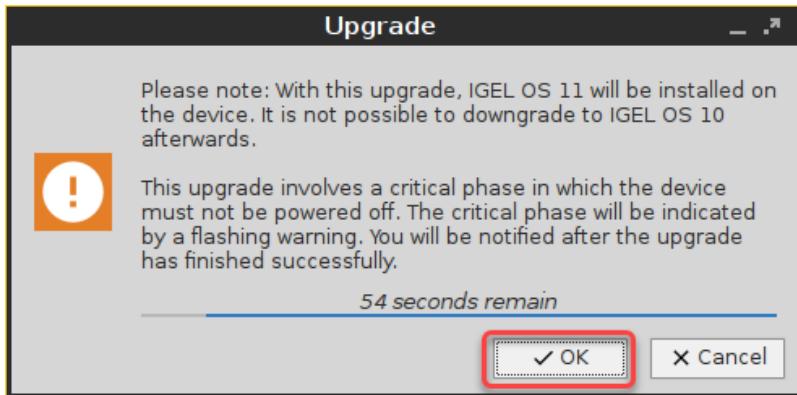


When you start the upgrade, a warning dialog is shown.

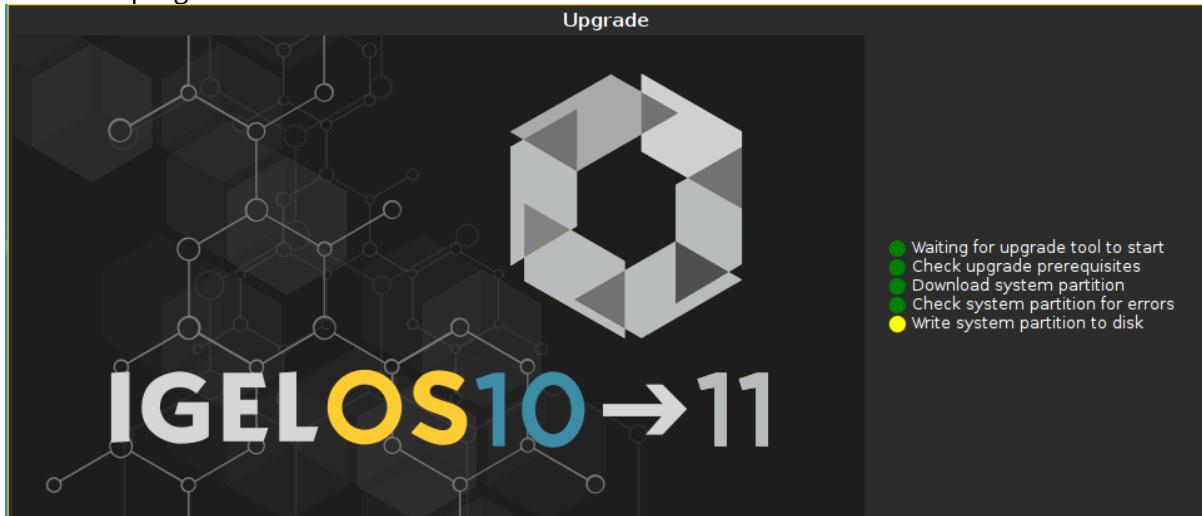
3. Click **OK** to continue.



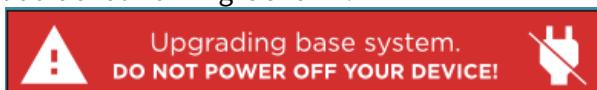
A warning dialog with a timeout is shown. If you click **Cancel** before the timeout expires, the upgrade is canceled. If you click **OK** or just wait for the timeout to expire, the upgrade is started



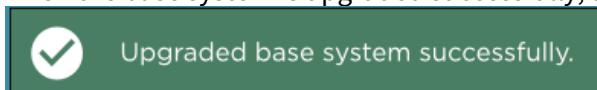
After the warning dialog has been confirmed or the timeout has expired, the device reboots into a special IGEL OS 10 environment, in which the system upgrade is executed. The **Upgrade** window shows the progress.



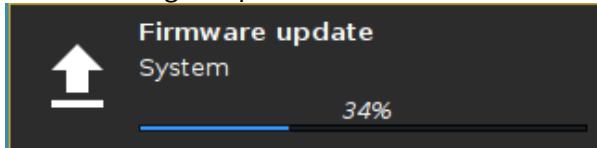
During the critical phase, the device must not be powered off. At this stage in the progress, an additional warning is shown.



When the base system is upgraded successfully, a message is shown.



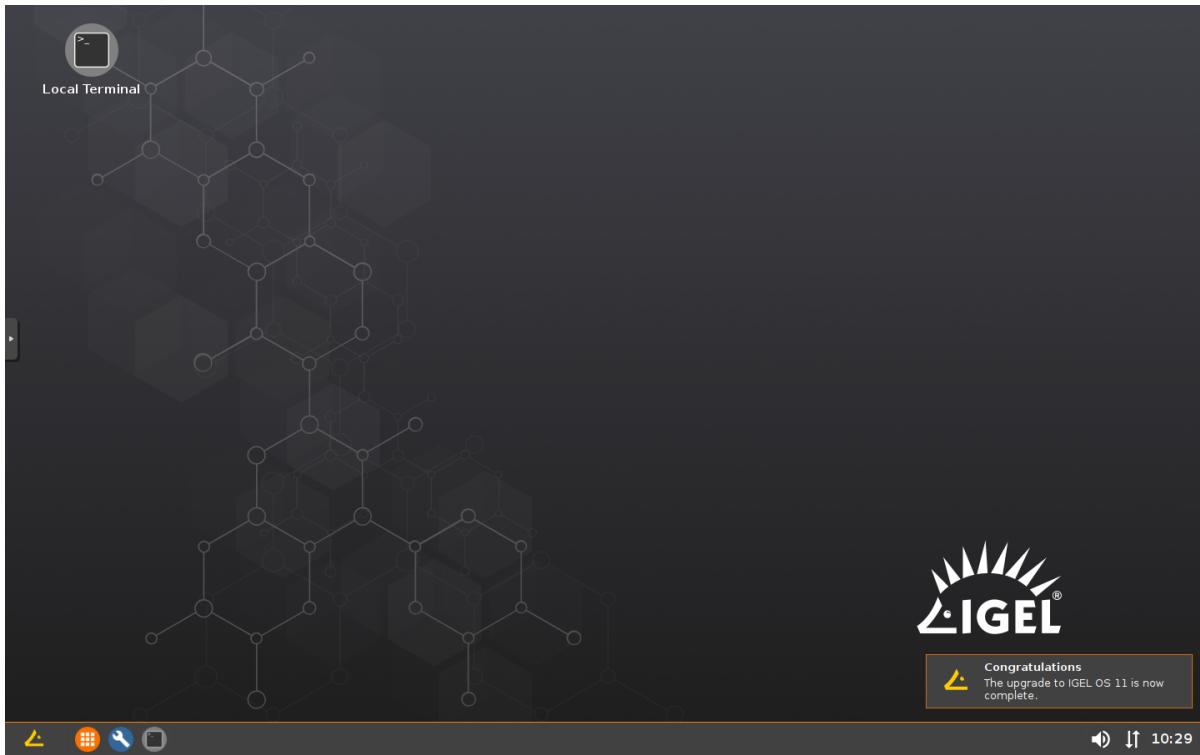
The remaining components of the firmware are installed, which is indicated by update messages.



When the installation is completed, the **Upgrade** window looks like this:



After a few seconds the device reboots into IGEL OS 11.



When the upgrade test has been successful, you are ready to set up the mass upgrade. Continue with [Checking the Requirements](#) (see page 182).

### Checking the Requirements

The following requirements must be met:

- The upgrade has been tested with characteristic devices.
- UMS 6.01.130 or higher is available.



- The appropriate IGEL OS 10 firmware version (10.05.700 or higher) is known to the UMS. For this purpose, a device with this firmware version must be registered in the UMS. This is already the case if you tested the upgrade with the same UMS with which you are about to do the mass upgrade. If not, you must register a device with the appropriate IGEL OS 10 firmware version now.
- All devices are connected to a regular LAN (not OpenVPN, OpenConnect, genucard or mobile broadband).
- All devices are in a safe environment where the upgrade process cannot be disrupted, e.g. by powering off the devices.

When all the requirements are met, continue with [Creating the Universal Firmware Updates\(see page 183\)](#).

#### Creating the Universal Firmware Updates

For detailed information, see the chapter [Universal Firmware Update<sup>92</sup>](#) in the UMS Manual.

If you use the [High Availability Extension<sup>93</sup>](#), note that Universal Firmware Updates are NOT synchronized, that is why you have to either download them to all HA nodes or configure an external (FTP) server.

1. Create a Universal Firmware Update for the appropriate IGEL OS 10 firmware (10.05.700 or higher).
2. After you have created the Universal Firmware Update for IGEL OS 10, create a Universal Firmware Update for IGEL OS 11.

The order of creation is crucial because the IGEL OS 11 firmware must have a higher ID in order to be chosen by the device. For details, see [Executing the Upgrade\(see page 195\)](#).

#### Configuring the Universal Firmware Update for ICG

If you are using IGEL Cloud Gateway (ICG), an FTP server that is accessible to all devices must be configured as the update source.

To configure an FTP server as update source:

1. In the UMS, go to **UMS Administration > Universal Firmware Update** and click [Edit...](#).

<sup>92</sup> <https://kb.igel.com/display/endpointmgmt601/Universal+Firmware+Update>

<sup>93</sup> <https://kb.igel.com/pages/viewpage.action?pageId=915787>



2. Enter the data required for accessing the FTP server and click **Save**.

**Edit FTP Server Configuration**

Universal update settings  
The IGEL Universal Firmware files are downloaded from: 'fwu.igel.com'.

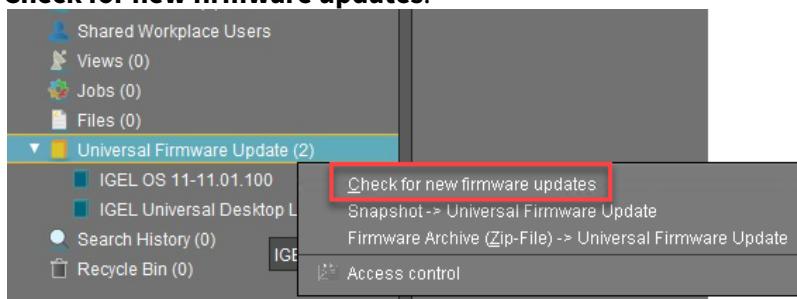
Proxy Server [ ]

The FTP server settings where the files are downloaded to (optionally).

Host	ftpServername
Port	21
User name	ftp
Password	***
Directory	directory/subdir

Save Cancel

3. Go to **Server - [UMS address] > Universal Firmware Update** and in the context menu, select **Check for new firmware updates**.



4. Select the entry for the appropriate IGEL OS firmware, click to select the FTP server selected in step 2 and select **Download**.

**Universal Firmware Updates**

Universal Firmware Updates

Include	Model	Version	Target directory	Release Notes	Release Notes
<input checked="" type="checkbox"/>	IGEL UD LX	10.05.700	ftp://ftpServername:21/ftpServerpath	<a href="#">HTML</a>	<a href="#">Text</a>
<input type="checkbox"/>	IGEL OS 11	11.01.100	ftp://ftpServername:21/ftpServerpath	<a href="#">HTML</a>	<a href="#">Text</a>

Show only latest firmware versions (hides already downloaded versions)

Download Cancel



5. The firmware is transferred to the FTP server.

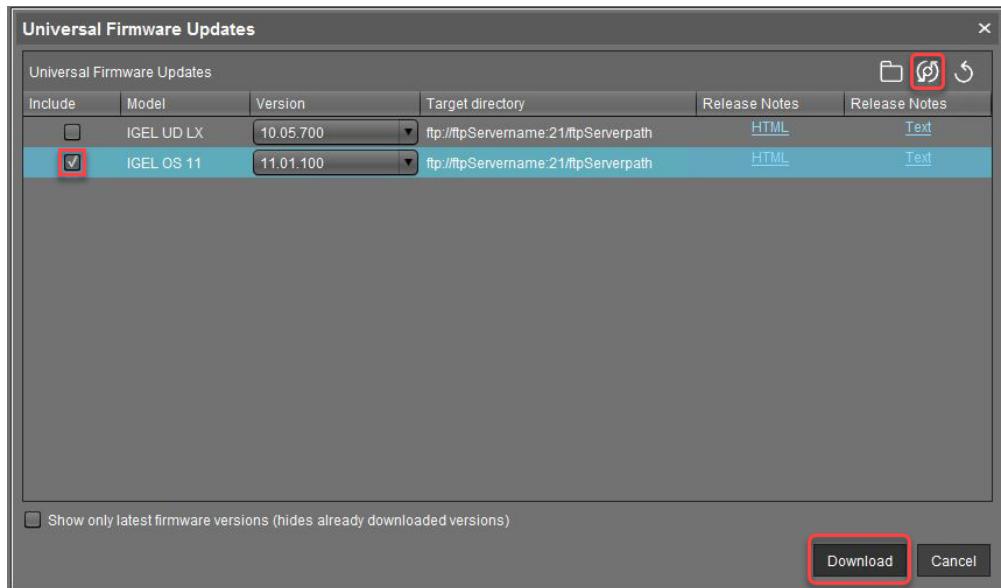
A screenshot of a web-based configuration interface for a Universal Firmware Update. At the top, it shows the path "/Universal Firmware Update/IGEL Universal Desktop LX-10.05.700". Below this, there are sections for Product (IGEL Universal Desktop LX), Version (10.05.700), and Release Notes (HTML Text). The "Firmware Update Settings" section contains fields for User (ftpUser), Password (redacted), Host (ftpServername), Port (21), Protocol (ftp), Target URL (/ftpServerpath/IGEL\_Universal/Desktop\_LX-10.05.700), and Snapshot file (empty). The "Download Status" section shows a progress bar labeled "Started" with the message "Download the firmware update..." and an empty "Error" field.

6. Under **Server - [UMS address] > Universal Firmware Update**, in the context menu, select **Check for new firmware updates** again.

A screenshot of the UMS (Universal Management System) interface. On the left, there's a sidebar with icons for Shared Workplace Users, Views (0), Jobs (0), Files (0), and a expanded "Universal Firmware Update (2)" folder. The "Universal Firmware Update" folder is highlighted with a teal background. A context menu is open over this folder, with the option "Check for new firmware updates" highlighted with a red box. Other options in the menu include "Snapshot -&gt; Universal Firmware Update", "Firmware Archive (.Zip-File) -&gt; Universal Firmware Update", and "Access control".



7. Select the entry for the IGEL OS 11 firmware, click to select the FTP server selected in step 2 and select **Download**.





#### 8. The firmware is transferred to the FTP server.

A screenshot of a web-based application titled "/Universal Firmware Update/IGEL OS 11-11.01.100". The interface includes sections for Product (IGEL OS 11), Version (11.01.100), Release Notes (HTML Text), Firmware Update Settings (User: ftpUser, Password: masked, Host: ftpServername, Port: 21, Protocol: ftp, Target URL: /ftpServerpath/IGEL\_OS\_11-11.01.100), and Snapshot file. The Download Status section shows a progress bar labeled "Started" with the message "Download the firmware update..." and an Error section below it.

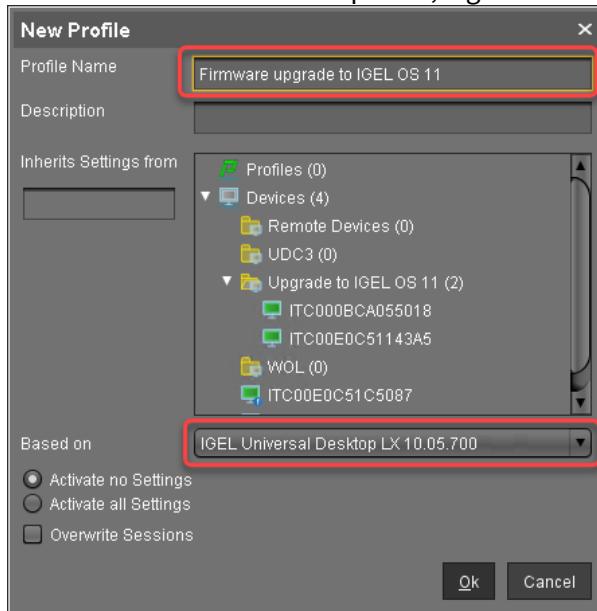
The devices can download the firmware from the FTP server.

When the Universal Firmware Update is ready, continue with [Creating a Profile](#)(see page 188).



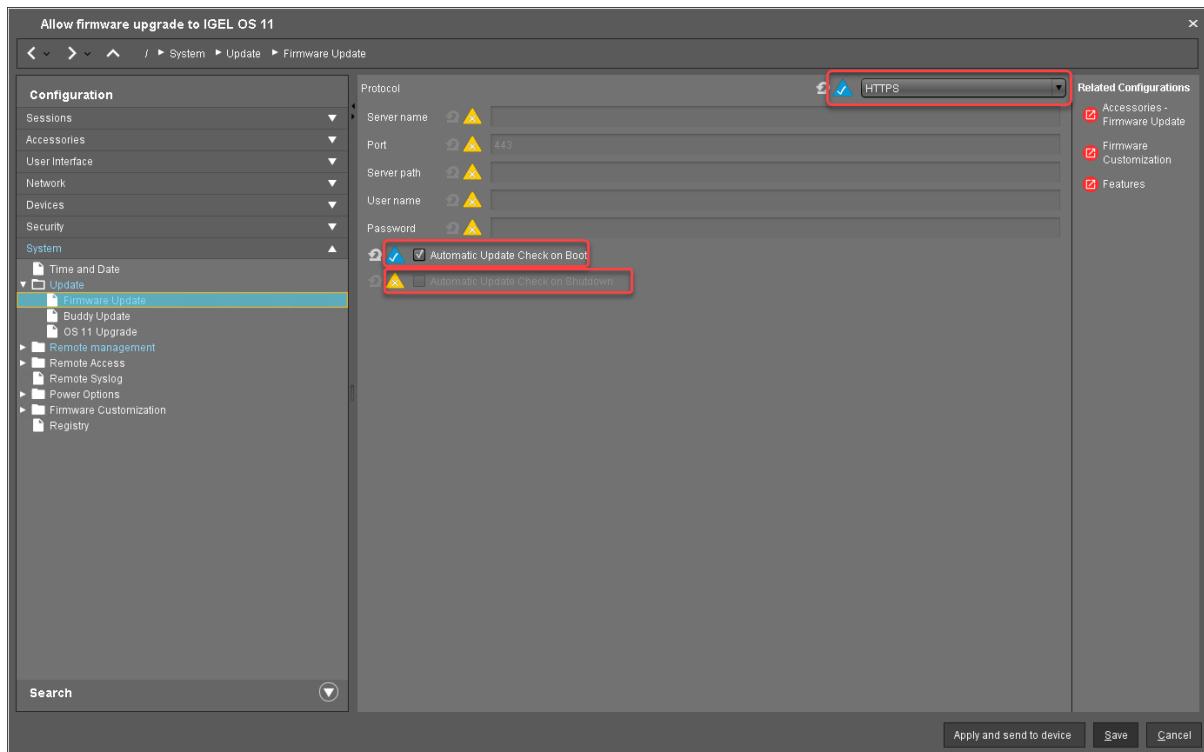
## Creating a Profile

1. Create a profile that is based on the appropriate IGEL OS 10 firmware version (10.05.700 or higher). Find a suitable name for the profile, e.g. "Firmware upgrade to IGEL OS 11".

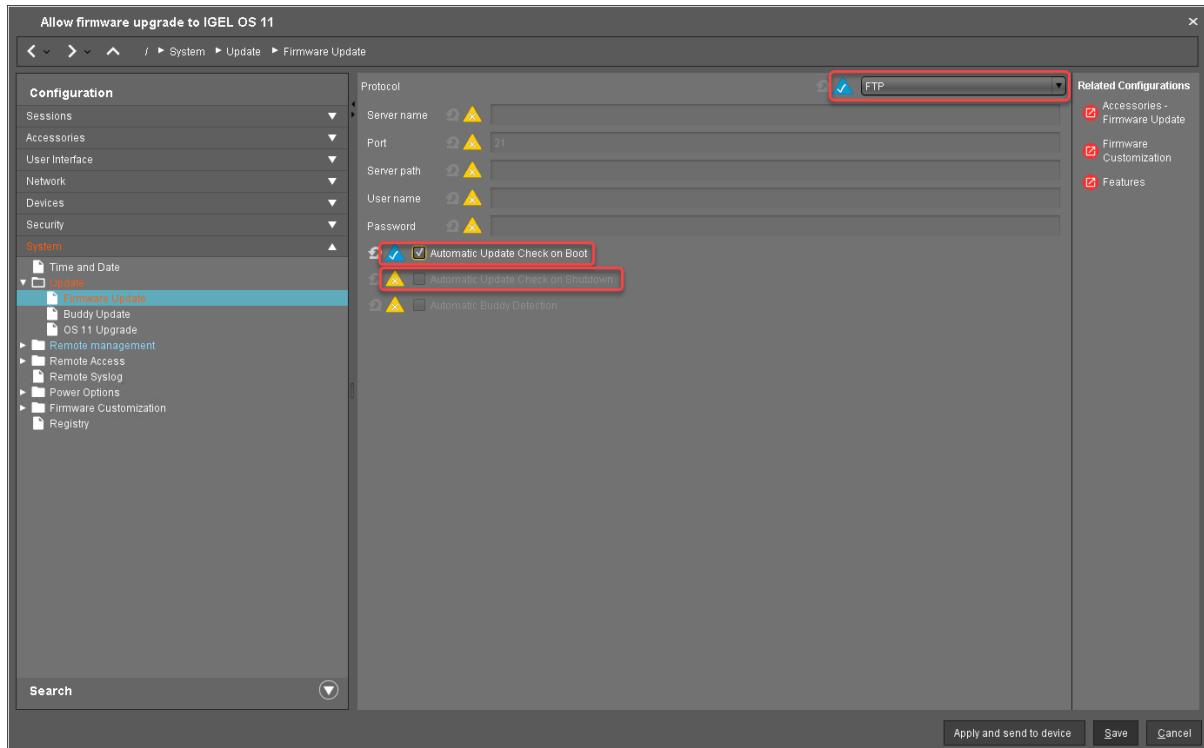


2. In the profile's configuration dialog, go to **System > Update > Firmware Update** and change the settings according to your environment:

- If the UMS and the devices are in one and the same network, and no IGEL Cloud Gateway (ICG) is used:
  - Select "HTTPS" as **Protocol**.
  - Activate **Automatic Update Check on Boot**.
  - Ensure that **Automatic Update Check on Shutdown** is deactivated. Otherwise, the device will shut down when the update is finished.

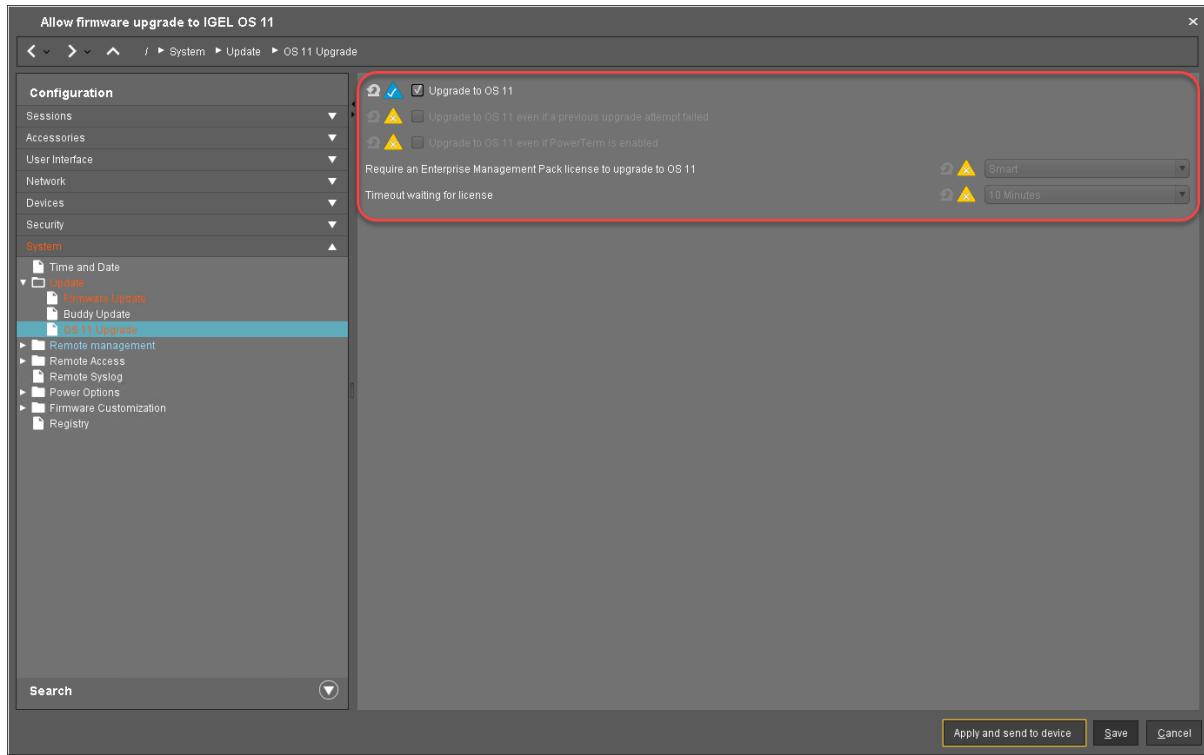


- If IGEL Cloud Gateway (ICG) is used:
  - Select "FTP" as **Protocol**.
  - Activate **Automatic Update Check on Boot**.
  - Ensure that **Automatic Update Check on Shutdown** is deactivated. Otherwise, the device will shut down when the update is finished.



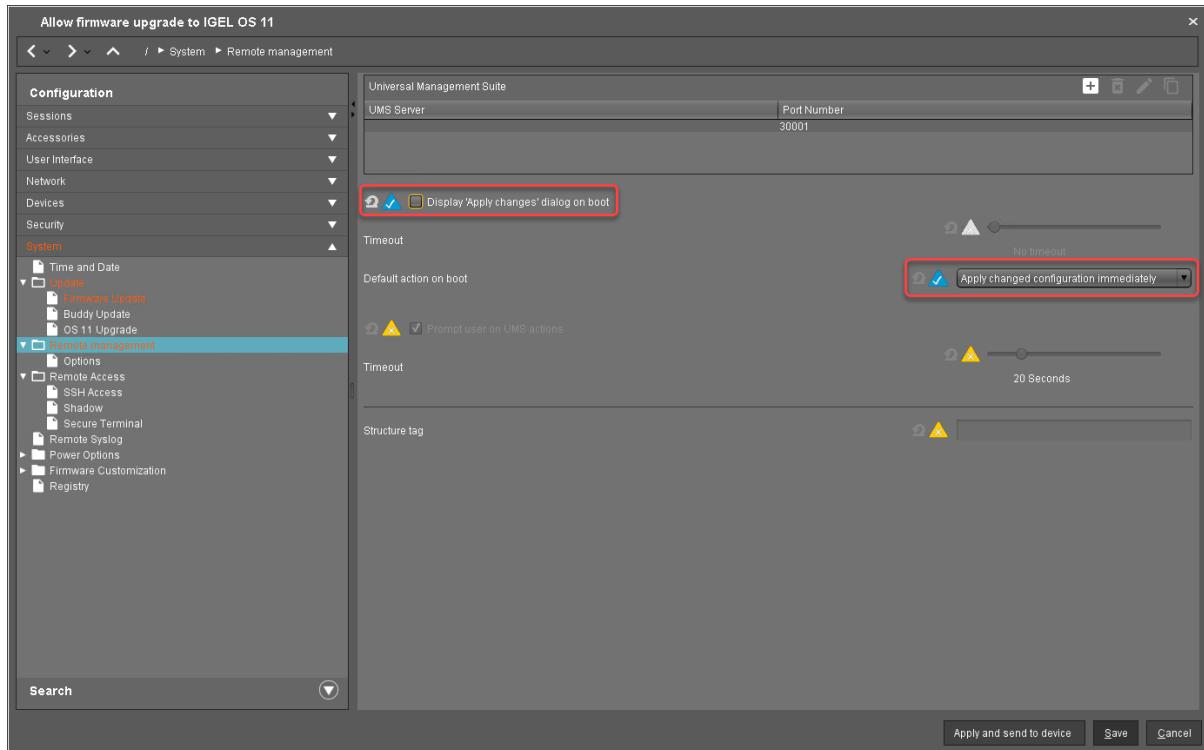
3. Go to **System > Update > OS 11 Upgrade** and change the following settings according to your successful upgrade test:

- Activate **Upgrade to OS 11**.
- Set **Upgrade to OS 11 even if PowerTerm is enabled** according to your needs.
- Set **Upgrade to OS 11 even if a previous upgrade attempt failed** according to your needs.
- Set **Require an Enterprise Management Pack license to upgrade to OS 11** according to your needs.
- Ensure that the **Timeout waiting for OS 11 license to start automatic upgrade** is set to **10 Minutes**.



4. Go to **System > Remote Management** and change the settings as follows:

- Deactivate **Display 'Apply changes' dialog on boot**.
- Set **Default action on boot** to **Apply changed configuration immediately**.



## 5. Click **Save**.

When the profile is created, continue with [Deploying the Licenses](#)(see page 192).

## Deploying the Licenses

Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see [Setting up Automatic License Deployment \(ALD\)](#)<sup>94</sup>.
- Manual License Deployment: Licenses are created and deployed manually. For instructions, see [Manual License Deployment for IGEL OS](#)<sup>95</sup>.

When the license deployment is setup up, continue with [Putting It All Together](#)(see page 193).

---

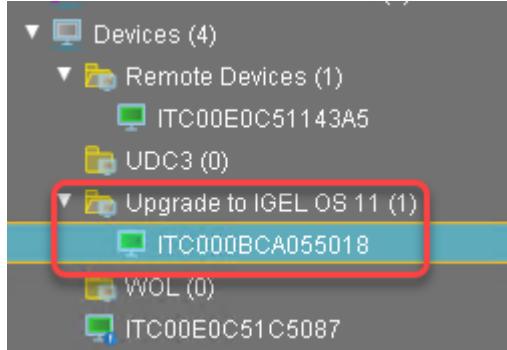
<sup>94</sup> <https://kb.igel.com/pages/viewpage.action?pageId=10325058>

<sup>95</sup> <https://kb.igel.com/display/licensesmoreigelos11/Manual+License+Deployment+for+IGEL+OS>

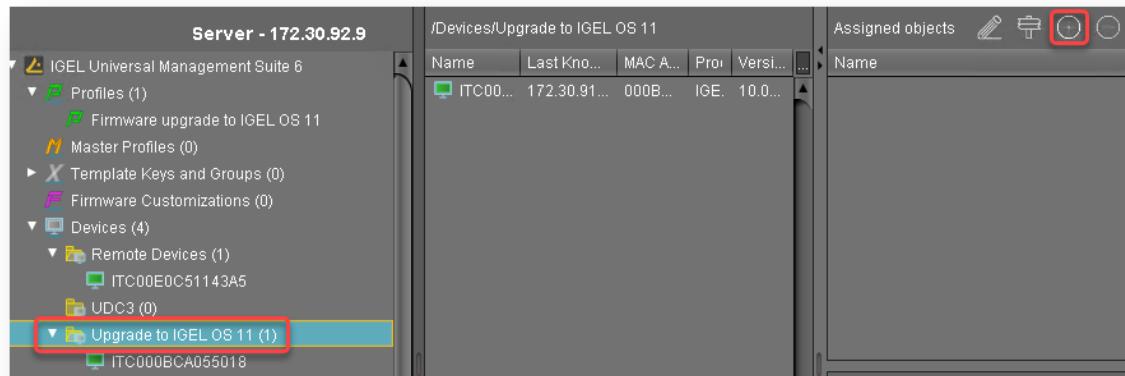


## Putting It All Together

1. Put all devices that are to be updated into a directory.

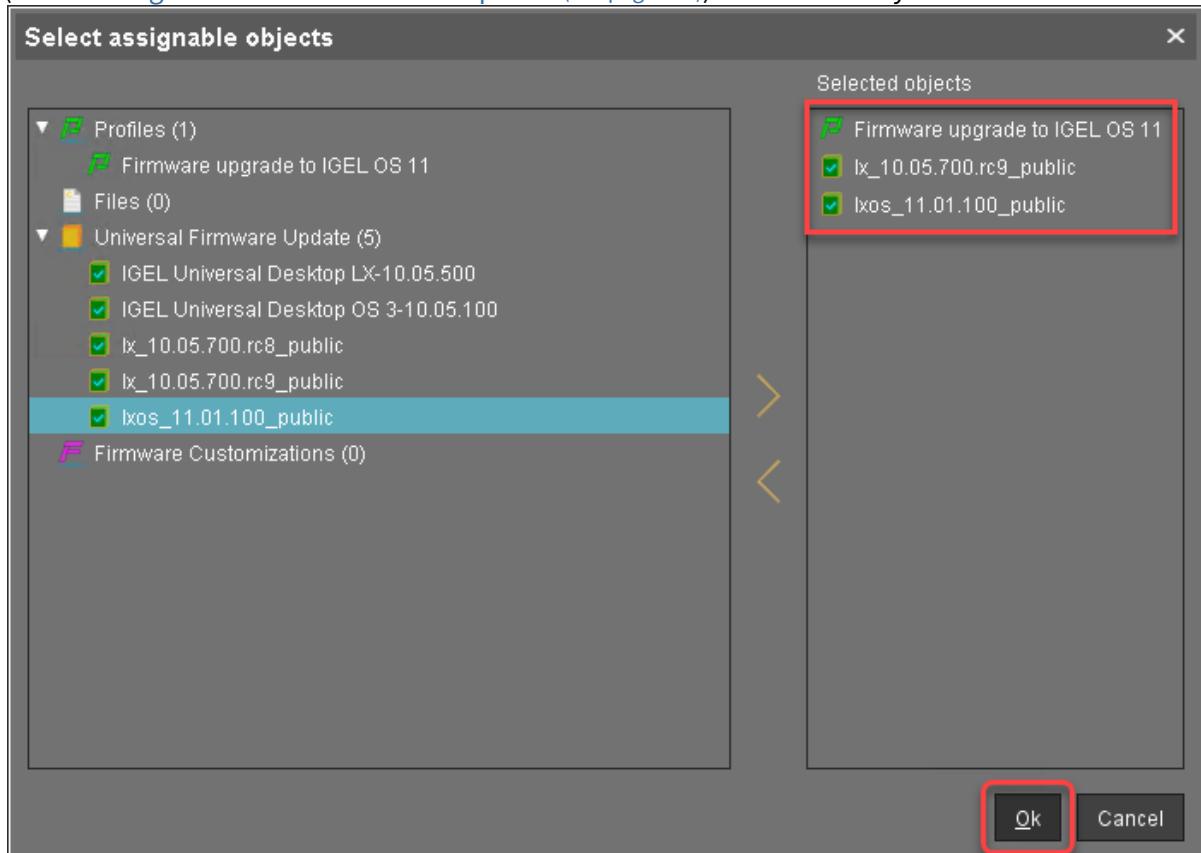


2. Select the directory and in the **Assigned objects** area, click **+**.

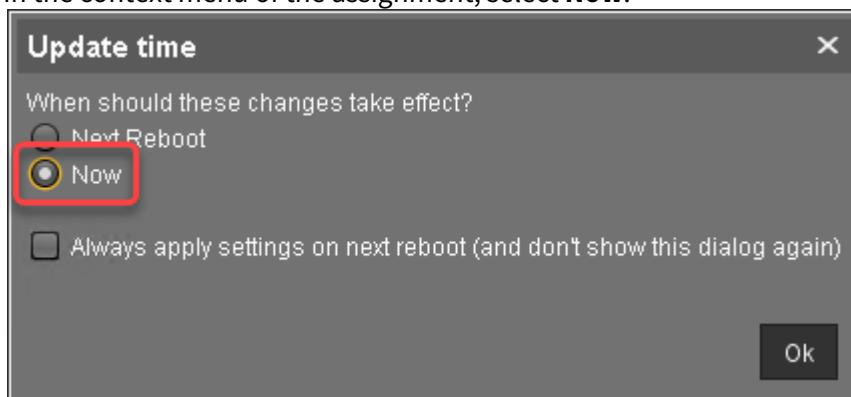




3. Assign the profile (see [Creating a Profile\(see page 188\)](#)) and the two Universal Firmware Updates (see [Creating the Universal Firmware Updates\(see page 183\)](#)) to the directory and click **Ok**.



4. In the context menu of the assignment, select **Now**.



In the **Assigned objects** area, the profile and the Universal Firmware Updates are shown:



Name	Last Known ...	MAC	Pro	Version
ITC000... 172.30.91.87	000E	IGE	11.01...	

5. If you are using Automatic License Deployment (ALD), it might be feasible to confine the distribution of licenses to the current directory. For more information, see [Configuring the Distribution Conditions<sup>96</sup>](#), section "Distributing Licenses to Devices in a Specified Directory".

When everything is in place, continue with [Executing the Upgrade](#)(see page 195).

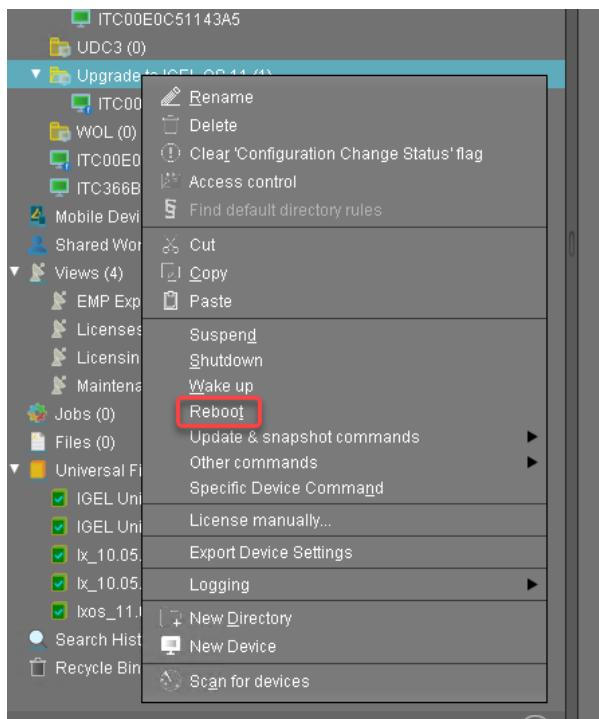
#### Executing the Upgrade

1. In the UMS, select the directory containing all devices that are to be upgraded and reboot them.

Alternatively, you can create a scheduled job for reboot or wake up and assign it to the devices or the directory containing these devices. For more information, see [Jobs<sup>97</sup>](#).

<sup>96</sup> <https://kb.igel.com/display/licensesmoreigelos11/Configuring+the+Distribution+Conditions>

<sup>97</sup> <https://kb.igel.com/endpointmgmt-5.08/en/jobs-910606.html>



On reboot or wake up, the devices update to the appropriate IGEL OS firmware version (10.05.700 or higher). With this version, the **Upgrade to OS 11** parameter is recognized by the devices; also, the devices request IGEL OS 11 licenses from the UMS (Workspace Edition and, if required, Enterprise Management Pack).

If no IGEL OS 11 licenses have been deployed on the devices yet, the licenses are deployed within a few minutes. The upgrade will be started when the licenses are deployed. The maximum time period the device will wait for a license is configured by the parameter **Timeout waiting for OS 11 license to start automatic upgrade**; for details, see [Adjusting the Setup](#)(see page 177).

The parameter **Automatic update check on boot** causes the devices to look for new firmware again. Although two Universal Firmware Updates are assigned to the devices, the UMS offers the IGEL OS 11 firmware, because the ID of the IGEL OS 11 firmware is higher than the ID of the IGEL OS 10 firmware.

## 2. Update Can Be Canceled After Timeout

An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.



3. When all devices have been upgraded successfully, remove the "Firmware upgrade to IGEL OS 11" profile and the two Universal Firmware Updates from the directory.

The screenshot shows a software interface for managing firmware profiles. At the top, there's a toolbar with icons for edit, delete, and other functions. The main area is titled 'Assigned objects' and lists a single profile: 'Firmware upgrade to IGEL OS 11'. Underneath this profile, two update files are listed with checkmarks: 'lxos\_11.01.100\_public' and 'lx\_10.05.700.rc9\_public'. The 'delete' icon in the toolbar is highlighted with a red box.

The upgrade is completed.

### Zero-Touch Deployment Using Buddy Update

This method uses the buddy update feature of IGEL OS. One or more devices that are configured as an update buddy access the main server and download the firmware. The other devices are configured to download their firmware from an update buddy.

Read all the following chapters carefully and follow the instructions.

1. [IGEL Devices That Can Be Upgraded to IGEL OS 11](#)(see page 197)
2. [Important! Consider This Before Upgrading](#)(see page 176)
3. [Preparing the Upgrade](#)(see page 177)
4. [Testing the Upgrade](#)(see page 179)
5. [Checking the Requirements](#)(see page 182)
6. [Configuring Two Update Buddies](#)(see page 205)
7. [Creating a Profile](#)(see page 206)
8. [Deploying the Licenses](#)(see page 207)
9. [Putting It All Together](#)(see page 208)
10. [Executing the Upgrade](#)(see page 208)

### IGEL Devices That Can Be Upgraded to IGEL OS 11

#### IGEL UD (Universal Desktop)

<b>Product Line</b>	<b>Device Type</b>	<b>Hardware ID</b>	<b>64 Bit</b>	<b>Memory</b>	<b>Storage</b>	<b>HW Video Acceleration</b>
UD2	D220	40	Yes	2 GB	4 GB	Yes
UD2	M250C	50	Yes	2 GB	4 GB	Yes
UD2	M250C	51/52	Yes	2 GB	8 GB	Yes
UD3*(see page 198)	M340C	50	Yes	2 GB	4 GB	Yes
UD3	M340C	51	Yes	2 GB	4 GB	Yes
UD3	M350C	60	Yes	4 GB	8 GB	Yes
UD5	H830C	50	Yes	2 GB	4 GB	Yes
UD6	H830C	51	Yes	2 GB	4 GB	Yes



Product Line	Device Type	Hardware ID	64 Bit	Memory	Storage	HW Video Acceleration
UD7	H850C	10	Yes	4 GB	4 GB	Yes
UD7** (see page 198)	H850C	11	Yes	4 GB	4 GB	Yes
UD7	H860C	20	Yes	8 GB	8 GB	Yes
UD9	TC215B	40 / 41 (Touch)	Yes	2 GB	4 GB	Yes

\* IGEL UD3-LX 50 is officially supported up to IGEL OS 11.05, incl. private builds.

\*\*As of December 2019, IGEL UD7 model H850C is equipped with the AMD Secure Processor<sup>98</sup>; for further information, see [UD7 Model H850C<sup>99</sup>](#).

## IGEL Zero

### Note on IZ Devices

The IZ devices listed below can be upgraded to IGEL OS 11. To upgrade your IZ devices to IGEL OS 11, please contact your IGEL sales representative. See also <https://www.igel.com/tradeup/> and [The IGEL OS 11 Trade-Up<sup>100</sup>](#).

Product Line	Device Type	Hardware ID	64 Bit	Memory	Storage	UEFI Secure Boot Support	HW Video Acceleration
IZ2	D220	40	Yes	2 GB	4 GB	Yes	Yes
IZ3	M340C	50	Yes	2 GB	4 GB	Yes	Yes
IZ3	M340C	51	Yes	2 GB	4 GB	Yes	Yes

When you have confirmed that your devices can be upgraded to IGEL OS 11, make sure to consider [Important! Consider This Before Upgrading](#)(see page 198).

### Important! Consider This Before Upgrading

To make sure that your upgrade can be successful, check the following warnings and notes; a warning symbol indicates that irreversible damage can be done to your devices.

### No Downgrade

You cannot restore your IGEL OS 10 system once you have migrated to IGEL OS 11. The device storage is overwritten completely with a new partitioning scheme.

<sup>98</sup> <https://kb.igel.com/display/securitysafety/AMD+Secure+Processor>

<sup>99</sup> <https://kb.igel.com/display/securitysafety/UD7+Model+H850C>

<sup>100</sup> <https://kb.igel.com/display/licensesmoreigelos11/The+IGEL+OS+11+Trade+up>



### Features (e.g. Clients)

IGEL OS 11 does not have the complete feature set of IGEL OS 10. Make sure that the current version of IGEL OS 11 meets your requirements. For details, refer to the appropriate release notes.

### Custom Partitions

The contents of custom partitions will be deleted by the upgrade. Make sure to back up the contents and restore them after the upgrade has finished. Besides becoming dysfunctional after the upgrade, applications and kernel drivers in a custom partition might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device. We recommend that you disable custom partitions when upgrading; you can enable them once the upgrade has been successfully completed.

### Custom Commands

The persistence of custom commands cannot be guaranteed. Besides becoming dysfunctional after the upgrade, custom commands might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device. In general, custom commands must be adapted for IGEL OS 11. We recommend that you disable custom commands when upgrading; you can enable them once the upgrade has been successfully completed.

### Network

All devices must be connected to a WLAN or LAN. LAN is the recommended option. The device will not be upgraded if connected to OpenVPN, OpenConnect, genucard, NCP VPN or mobile broadband.

### Hardware Support

Make sure that your devices support IGEL OS 11; please refer to [IGEL Devices Supported by IGEL OS 11<sup>101</sup>](#). This document describes upgrading methods for IGEL UD and IGEL IZ devices. Upgrading methods for IGEL UDC3 and UD Pocket are described under [Upgrading UDC3 Devices from IGEL OS 10 to IGEL OS 11<sup>102</sup>](#).

### License

- A valid license from an IGEL Workspace Edition (WE) Product Pack must be available for each device. For general information, see [IGEL Software License Overview<sup>103</sup>](#). For deploying licenses, see [Setting up Automatic License Deployment \(ALD\)<sup>104</sup>](#) or [Manual License Deployment for IGEL OS<sup>105</sup>](#).
- IZ devices are not allowed to upgrade to IGEL OS 11. Please contact your IGEL sales representative for a UD Upgrade License which allows you to upgrade your IZ devices.

<sup>101</sup> <https://kb.igel.com/display/hardware/IGEL+Devices+Supported+by+IGEL+OS+11+1>

<sup>102</sup> <https://kb.igel.com/display/igelos1102/Upgrading+UDC3+Devices+from+IGEL+OS+10+to+IGEL+OS+11>

<sup>103</sup> <https://kb.igel.com/display/licensesmoreigelos11/IGEL+Software+License+Overview>

<sup>104</sup> <https://kb.igel.com/pages/viewpage.action?pageId=10325058>

<sup>105</sup> <https://kb.igel.com/display/licensesmoreigelos11/Manual+License+Deployment+for+IGEL+OS>



### UMS Version

UMS version 6.01.130 or higher is required for upgrading from IGEL OS 10 to IGEL OS 11.

When you have considered everything that is relevant, continue with [Preparing the Upgrade](#)(see page 200).

### Preparing the Upgrade

This section describes the required preparations and tests before any productive devices can be updated. The testing should be done with at least one device that is characteristic of your environment. This device should have every custom partition and every custom command that may possibly exist in any of your devices.

To prepare the upgrade, perform the following steps:

1. [Preparing the UMS](#)(see page 200)
2. [Adjusting the Setup](#)(see page 200)
3. [Deploying a License](#)(see page 201)
4. [Configuring the Update Source](#)(see page 201)

### Preparing the UMS

To upgrade your devices to IGEL OS 11, you need the appropriate version of the UMS. Also, the devices must be registered with the UMS to receive their licenses.

1. If you have not already done so, update your UMS to version 6.01.130 or higher. For instructions, see [Updating a UMS Installation](#)<sup>106</sup>.
2. Make sure that your devices are registered with the UMS. For more information, see the chapter [Registering Devices on the UMS Server](#)<sup>107</sup> in the UMS Manual.

When the UMS is ready, continue with [Adjusting the Setup](#)(see page 200).

### Adjusting the Setup

Depending on the features that are in use now or will be used in the future, a specific set of parameters must be set in the device's Setup.

1. In the Setup, go to **System > Update > OS 11 Upgrade**.
2. Make your settings as appropriate:
  - Activate **Upgrade to OS 11**.
  - If you want the device to retry the upgrade immediately after a failed attempt, activate **Upgrade to OS 11 even if a previous upgrade attempt failed**. The device will retry the upgrade 5 times. When the 5th attempt has failed, a message will be shown in the upgrade tool window.
  - If your device has a PowerTerm license, and you want to upgrade to IGEL OS 11 even though it does not support PowerTerm, you must activate **Upgrade to OS 11 even if PowerTerm is enabled**.
  - Under **Require an Enterprise Management Pack license to upgrade to OS 11**, select the appropriate option:
    - If you are using IGEL Cloud Gateway (ICG) or Shared Workplace (SWP) or a Custom Partition and want to make sure that the upgrade is performed only if these features can be used furthermore, select **Smart**. When this option is selected, and any of these

<sup>106</sup> <https://kb.igel.com/display/endpointmgmt601/Updating+a+UMS+Installation>

<sup>107</sup> <https://kb.igel.com/display/endpointmgmt601/Registering+devices+on+the+UMS+Server>



features is activated, the upgrade is performed only if the device could fetch a license from an Enterprise Management Pack.

- If you want to force the device to fetch a license from an Enterprise Management Pack and make sure that the upgrade is performed only if the license could be fetched, select **Always**.
- If you want the device to upgrade to IGEL OS 11 without fetching an Enterprise Management Pack, disregarding the features that might be activated, select **Never**.
- Under **Timeout waiting for OS 11 license to start automatic upgrade**, set the time period the device will wait for a license in a mass deployment scenario (see [Zero-Touch Deployment Using Universal Firmware Update](#)(see page 174), [Zero-Touch Deployment Using Buddy Update](#)(see page 197) and [Mass Deployment Using a Scheduled Job](#)(see page 209)). This setting prevents the device from starting the upgrade at an inappropriate time as a result of the license just being deployed. This way, the setting prevents unwanted interruptions at work. For a mass deployment scenario, the default value **10 Minutes** is recommended.

### 3. Click **Apply**.

When the Setup is adjusted, continue with [Deploying a License](#)(see page 201).

#### Deploying a License

To upgrade from IGEL OS 10 to IGEL OS 11, you need an appropriate license. Depending on your requirements, one or more of these licenses will be needed for each device:

- One Workspace Edition license for basic functionality; see [Workspace Edition](#)<sup>108</sup>
- If one of the following features is used, one Enterprise Management Pack license is required (see [Enterprise Management Pack](#)<sup>109</sup>):
  - IGEL Cloud Gateway (ICG)
  - Shared Workplace (SWP)
  - Custom Partition - if IGEL OS 11.03.100 or lower is the target version; in IGEL OS 11.03.500 or higher, the Custom Partition feature is included in the Workspace Edition.

Proceed as follows:

► Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Manual License Deployment: Licenses are created and deployed manually. For instructions, see [Manual License Deployment for IGEL OS](#)<sup>110</sup>.
- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see [Setting up Automatic License Deployment \(ALD\)](#)<sup>111</sup>.
- Download three demo licenses from <https://www.igel.com/download/>.

When the device has a license, continue with [Configuring the Update Source](#)(see page 201).

#### Configuring the Update Source

1. In the Setup, go to **System > Update > Firmware Update** and configure the update source for IGEL OS 11. For more information, see the [Firmware Update](#)(see page 1252) chapter in the IGEL OS Manual.

---

<sup>108</sup> <https://kb.igel.com/display/licensesmoreigelos11/Workspace+Edition>

<sup>109</sup> <https://kb.igel.com/display/licensesmoreigelos11/Enterprise+Management+Pack>

<sup>110</sup> <https://kb.igel.com/display/licensesmoreigelos11/Manual+License+Deployment+for+IGEL+OS>

<sup>111</sup> <https://kb.igel.com/pages/viewpage.action?pageId=10325058>



## 2. Click **Ok**.

When the correct update source is configured, continue with [Testing the Upgrade](#)(see page 202).

### Testing the Upgrade

1. Click System and then **Upgrade to OS 11**. The OS 11 Upgrade Tool starts and indicates whether all requirements are met.

You can change the starting the starting methods for the OS 11 Upgrade Tool in the Setup under **Accessories > OS11 Upgrade**.

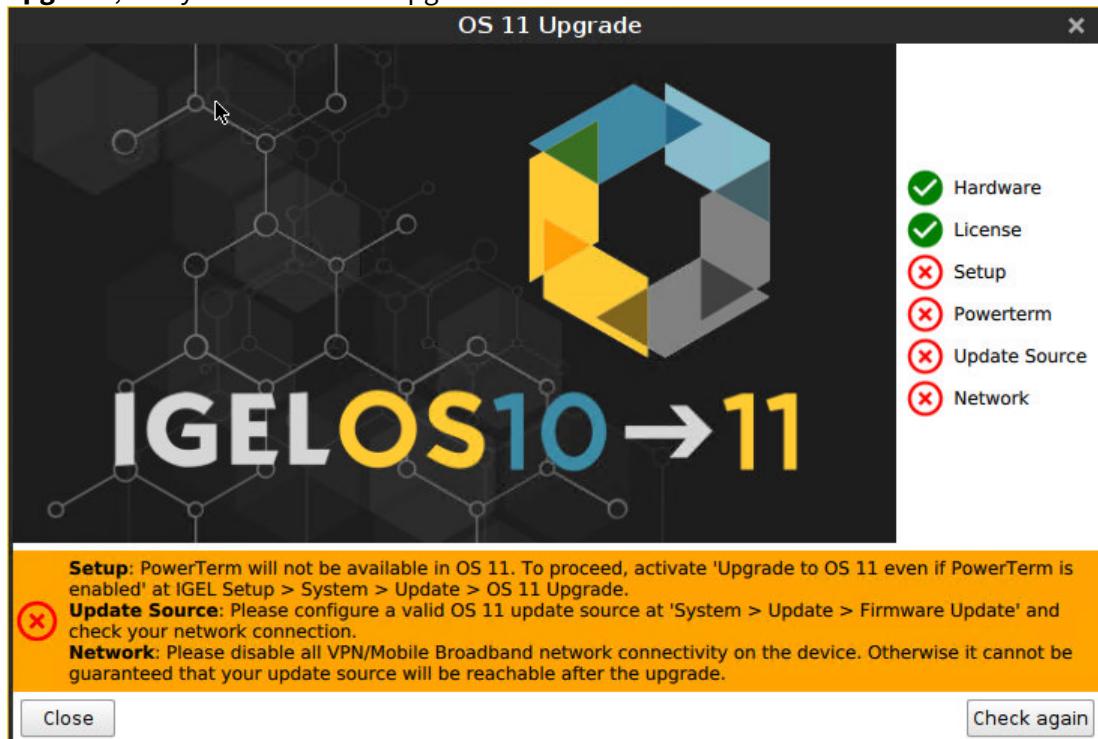


2. Check the output of the OS 11 Upgrade Tool and continue appropriately:

- If each requirement has an , click **OS Upgrade** to start the upgrade process.
- If one or more requirements have an , check the messages and resolve the issues. Afterwards, click **Check again**. If all requirements are met, the button changes to **OS**

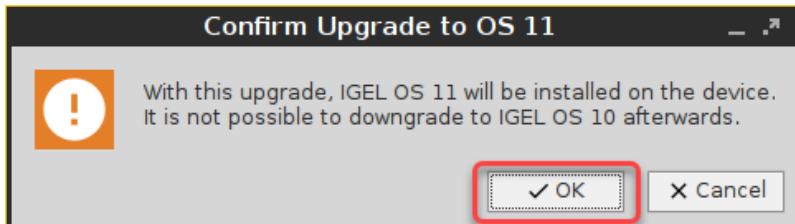


**Upgrade**, and you can start the upgrade.

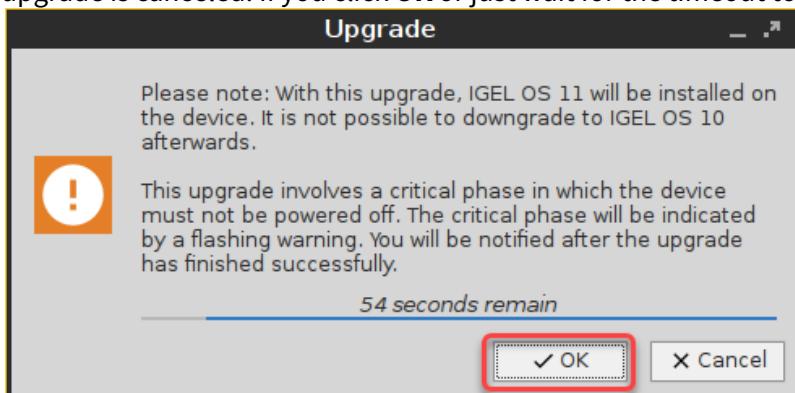


When you start the upgrade, a warning dialog is shown.

- Click **OK** to continue.



A warning dialog with a timeout is shown. If you click **Cancel** before the timeout expires, the upgrade is canceled. If you click **OK** or just wait for the timeout to expire, the upgrade is started



After the warning dialog has been confirmed or the timeout has expired, the device reboots into a special IGEL OS 10 environment, in which the system upgrade is executed. The **Upgrade** window



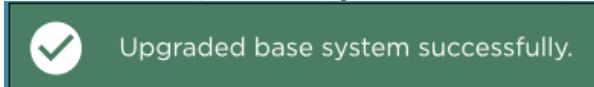
shows the progress.



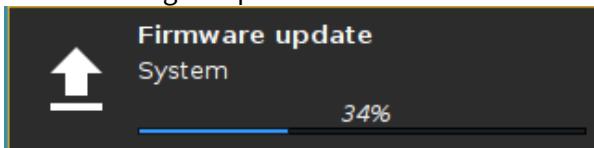
During the critical phase, the device must not be powered off. At this stage in the progress, an additional warning is shown.



When the base system is upgraded successfully, a message is shown.



The remaining components of the firmware are installed, which is indicated by update messages.

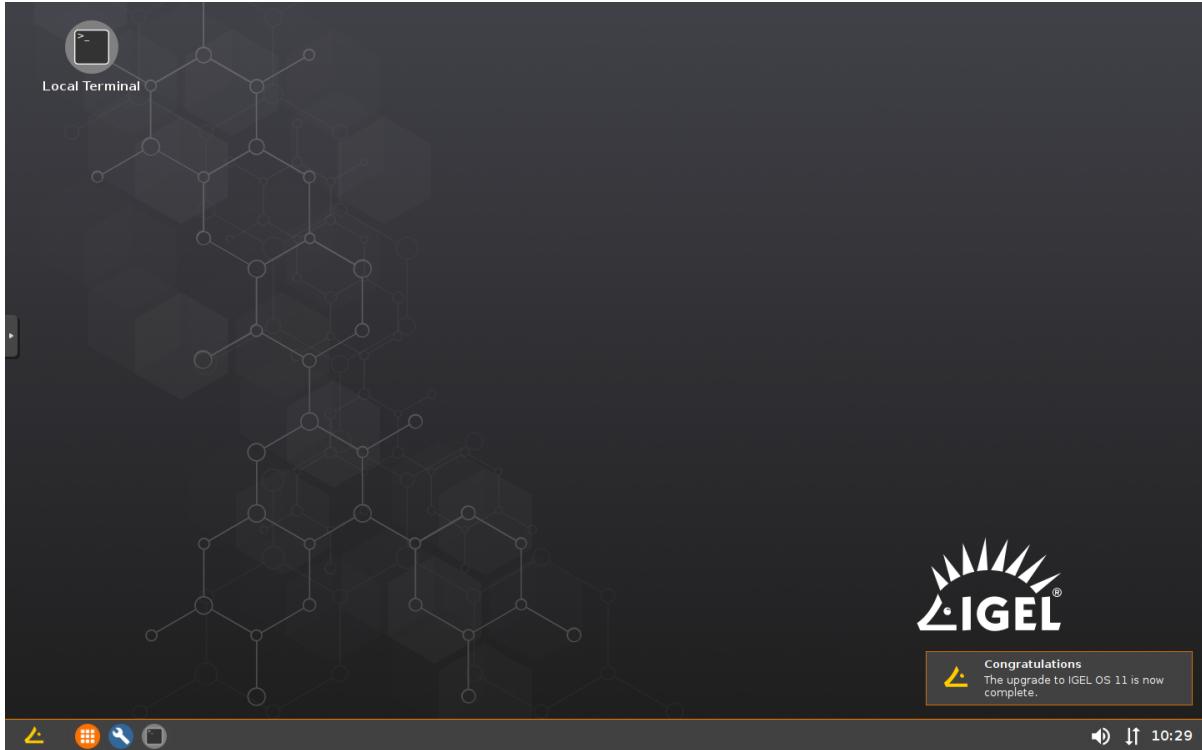


When the installation is completed, the **Upgrade** window looks like this:





After a few seconds the device reboots into IGEL OS 11.



When the upgrade test has been successful, you are ready to set up the mass upgrade. Continue with [Checking the Requirements](#)(see page 205).

### Checking the Requirements

The following requirements must be met:

- The upgrade has been tested with characteristic devices; see [Testing the Upgrade](#)(see page 179).
- UMS 6.01.130 or higher is available.
- The firmware IGEL OS 10.05.700 or 10.05.800 is known to the UMS. For this purpose, a device with OS 10.05.700 or 10.05.800 must be registered in the UMS. This is already the case if you tested the upgrade (see [Testing the Upgrade](#)(see page 179)) with the same UMS with which you are about to do the mass upgrade. If not, you must register a device with OS 10.05.700 or 10.05.800 now.
- All devices are connected to a regular LAN (not OpenVPN, OpenConnect, genocard, NCP VPN or mobile broadband).
- All devices are in a safe environment where the upgrade process cannot be disrupted, e.g. by powering off the devices.

### Configuring Two Update Buddies

For setting up buddy updates, see the [How-To Buddy Update](#)(see page 221).

Ensure that the network contains only the update buddies and the devices that are to be updated. This prevents other devices from updating inadvertently.

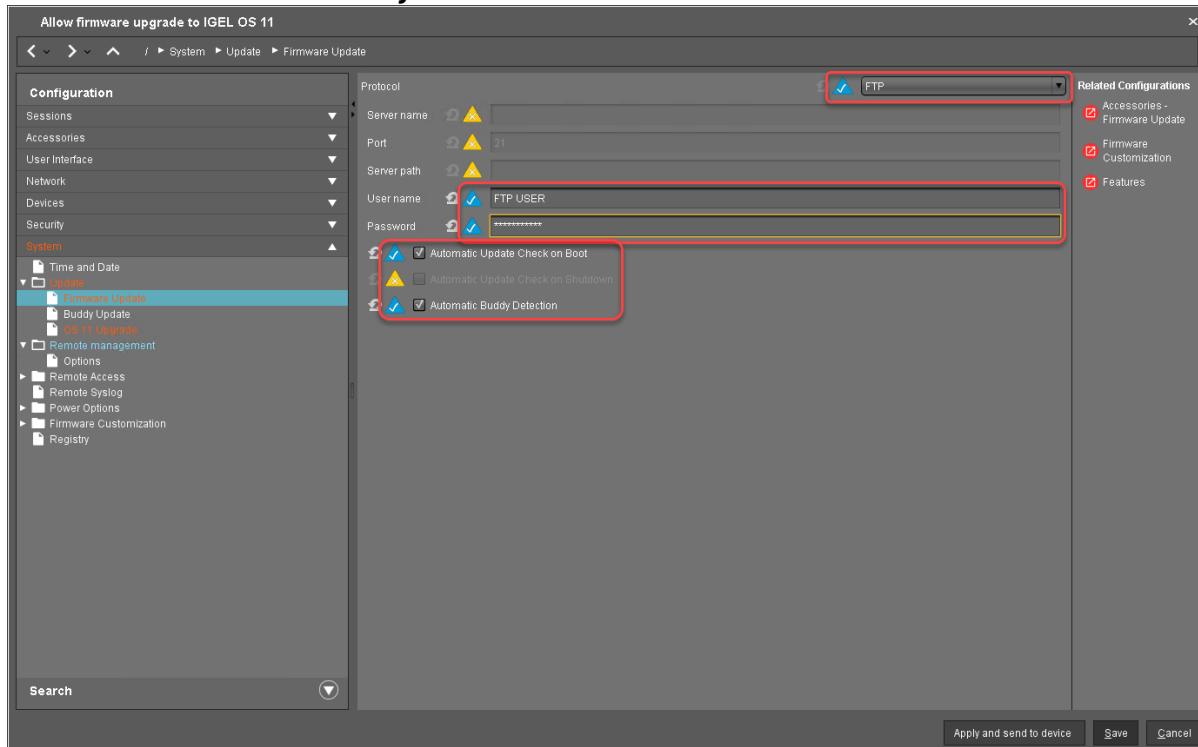


1. Update one device to the appropriate IGEL OS 10 firmware (10.05.700 or higher) and configure it as an update buddy.
2. Upgrade another device to IGEL OS 11 and configure it as an update buddy. Make sure that the IGEL OS 11 update buddy has the same **User Name** and **Password** in **System > Update > Buddy Update** as the IGEL OS 10 update buddy.

When the update buddies are configured, continue with [Creating a Profile](#)(see page 206).

### Creating a Profile

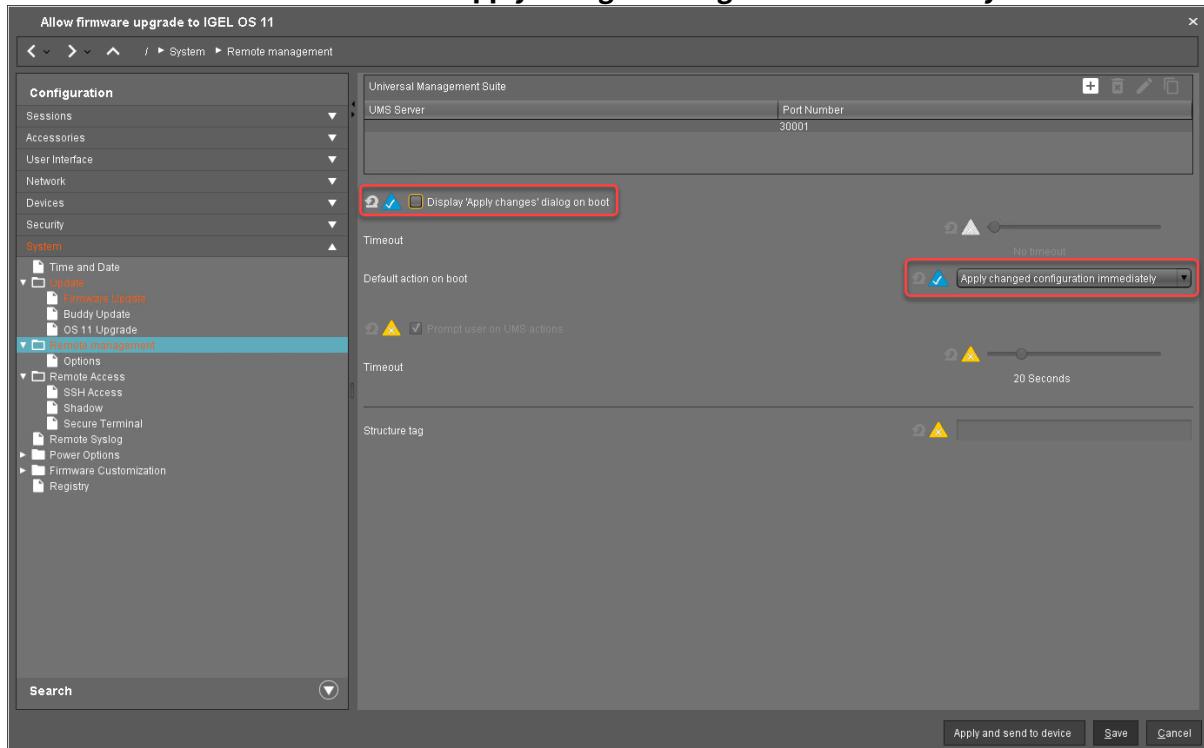
1. Create a profile which is based on the appropriate IGEL OS 10 firmware version (10.05.700 or higher). Find a suitable name for the profile, e.g. "Firmware upgrade to IGEL OS 11".
2. In the profile's configuration dialog, go to **System > Update > Firmware Update** and change the settings as follows:
  - Select "FTP" as **Protocol**.
  - Enter **User Name** and **Password** according the update buddy server.
  - Activate **Automatic Update Check on Boot**.
  - Ensure that **Automatic Update Check on Shutdown** is deactivated. Otherwise, the device will shut down when the update is finished.
  - Activate **Automatic Buddy Detection**.



3. Go to **System > Update > OS 11 Upgrade** and change the following settings according to your successful upgrade test:
  - Activate **Upgrade to OS 11**.
  - Set **Upgrade to OS 11 even if PowerTerm is enabled** according to your needs.



- Set **Require an Enterprise Management Pack license to upgrade to OS 11** according to your needs.
  - Set **Timeout waiting for OS 11 license to start automatic upgrade** to **10 Minutes**.
4. Go to **System > Remote Management** and change the settings as follows:
- Deactivate **Display 'Apply changes' dialog on boot**.
  - Set **Default action on boot** to **Apply changed configuration immediately**.



## 5. Click **Save**.

When the profile is created, continue with [Deploying the Licenses](#)(see page 207).

### Deploying the Licenses

Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see [Setting up Automatic License Deployment \(ALD\)](#)<sup>112</sup>.
- Manual License Deployment: Licenses are created and deployed manually. For instructions, see [Manual License Deployment for IGEL OS](#)<sup>113</sup>.

When the license deployment is set up, continue with [Putting It All Together](#)(see page 208).

<sup>112</sup> <https://kb.igel.com/pages/viewpage.action?pageId=10325058>

<sup>113</sup> <https://kb.igel.com/display/licensesmoreigelos11/Manual+License+Deployment+for+IGEL+OS>



## Putting It All Together

1. Assign the profile to all devices that are to be upgraded. This can be done by assigning the profile to the directory that contains these devices.

Do not assign the profile to the update buddies.

2. In the context menu of the assignment, select **Now**.
3. For Automatic license deployment, a condition can be set to the directory. For more information, see [Configuring the Distribution Conditions<sup>114</sup>](#), section "Distributing Licenses to Devices in a Specified Directory".

When everything is in place, continue with [Executing the Upgrade](#)(see page 208).

## Executing the Upgrade

1. In the UMS, select all devices that are to be upgraded and reboot them.

Alternatively you can create a scheduled job for reboot or wake up and assign it to the devices or the directory containing these devices; for more information, see [Jobs<sup>115</sup>](#).

On reboot or wake up, the devices choose the IGEL OS 10 buddy. They ignore the IGEL OS 11 buddy at this stage because this version is not known to them yet. The devices update to the appropriate version of IGEL OS 10 (10.05.700 or higher). With this version, the Upgrade to OS 11 parameter is recognized by the devices; also, the devices request IGEL OS 11 licenses from the UMS (Workspace Edition and, if required, Enterprise Management Pack).

If no IGEL OS 11 licenses have been deployed on the devices yet, the licenses are deployed within a few minutes. The upgrade will be started when the licenses are deployed. The maximum time period the device will wait for a license is configured by the parameter **Timeout waiting for OS 11 license to start automatic upgrade**; for details, see [Adjusting the Setup](#)(see page 177).

The parameters **Automatic update check on boot** and **Automatic buddy detection** cause the devices to look for a new firmware and wait for an IGEL OS 11 update buddy to reply. When an IGEL OS 11 update buddy is found, the devices start the upgrade process.

2. **Update Can Be Canceled After Timeout**

An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

<sup>114</sup> <https://kb.igel.com/display/licensesmoreigelos11/Configuring+the+Distribution+Conditions>

<sup>115</sup> <https://kb.igel.com/endpointmgmt-5.08/en/jobs-910606.html>



3. When all devices have been upgraded successfully, remove the "Firmware upgrade to IGEL OS 11" profile.

The upgrade is complete.

### Mass Deployment Using a Scheduled Job

This scenario is appropriate if you already have a working environment with IGEL OS 10.05.700 (or higher) and want to update all devices to IGEL OS 11 at a defined time.

Read all the following chapters carefully and follow the instructions.

1. [Checking the Requirements](#)(see page 209)
2. [Creating a Profile](#)(see page 210)
3. [Deploying the Licenses](#)(see page 213)
4. [Assigning the Profile](#)(see page 214)
5. [Executing the Upgrade](#)(see page 195)

### Checking the Requirements

The following requirements must be met:

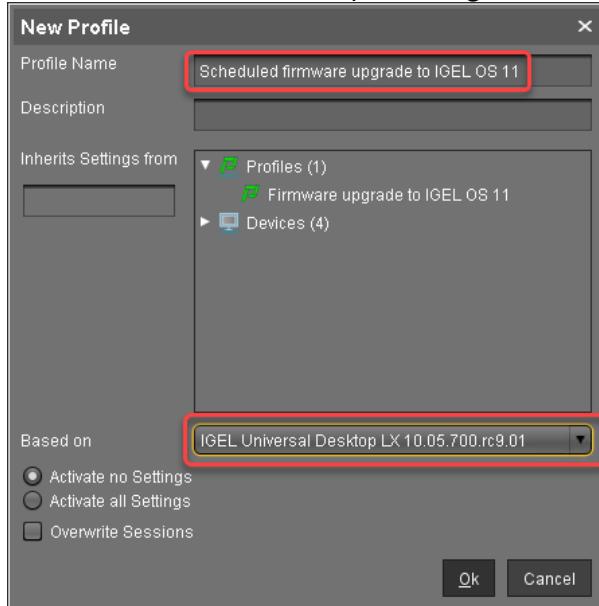
- The upgrade has been tested with characteristic devices.
- UMS 6.01.130 or higher is available.
- The appropriate IGEL OS 10 firmware version (10.05.700 or higher) is known to the UMS. For this purpose, a device with this firmware version must be registered in the UMS. This is already the case if you tested the upgrade with the same UMS with which you are about to do the mass upgrade. If not, you must register a device with the appropriate IGEL OS 10 firmware version now.
- All devices are connected to a regular LAN (not OpenVPN, OpenConnect, genucard or mobile broadband).
- All devices are in a safe environment where the upgrade process cannot be disrupted, e.g. by powering off the devices.

When all requirements are met, continue with [Creating a Profile](#)(see page 210).



## Creating a Profile

1. Create a profile that is based on the appropriate IGEL OS 10 firmware version (10.05.700 or higher). Find a suitable name for the profile, e.g. "Scheduled firmware upgrade to IGEL OS 11".



2. In the profile's configuration dialog, go to **System > Update > Firmware Update** and change the settings according to your environment:

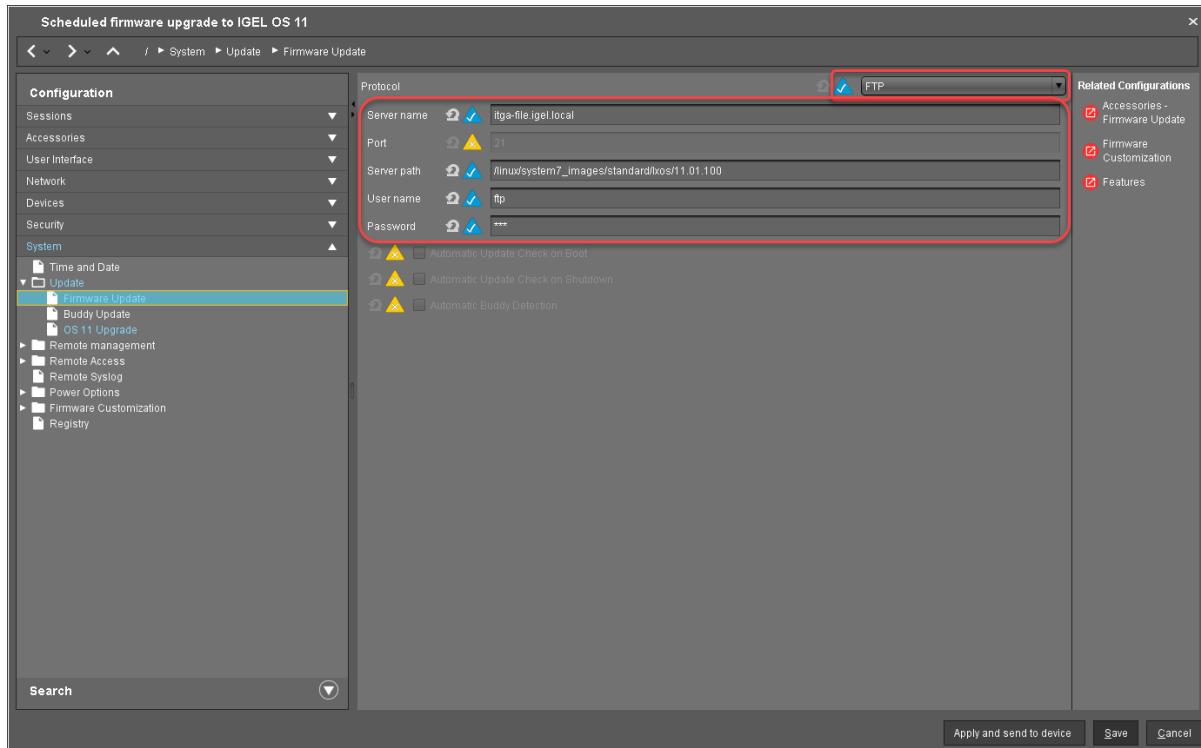
If you use [Universal Firmware Update](#)(see page 183) for OS 11, you do not need to configure the settings described in this step.

- Select an update source for IGEL OS 11. For further information, see [Firmware Update](#)(see page 1252).

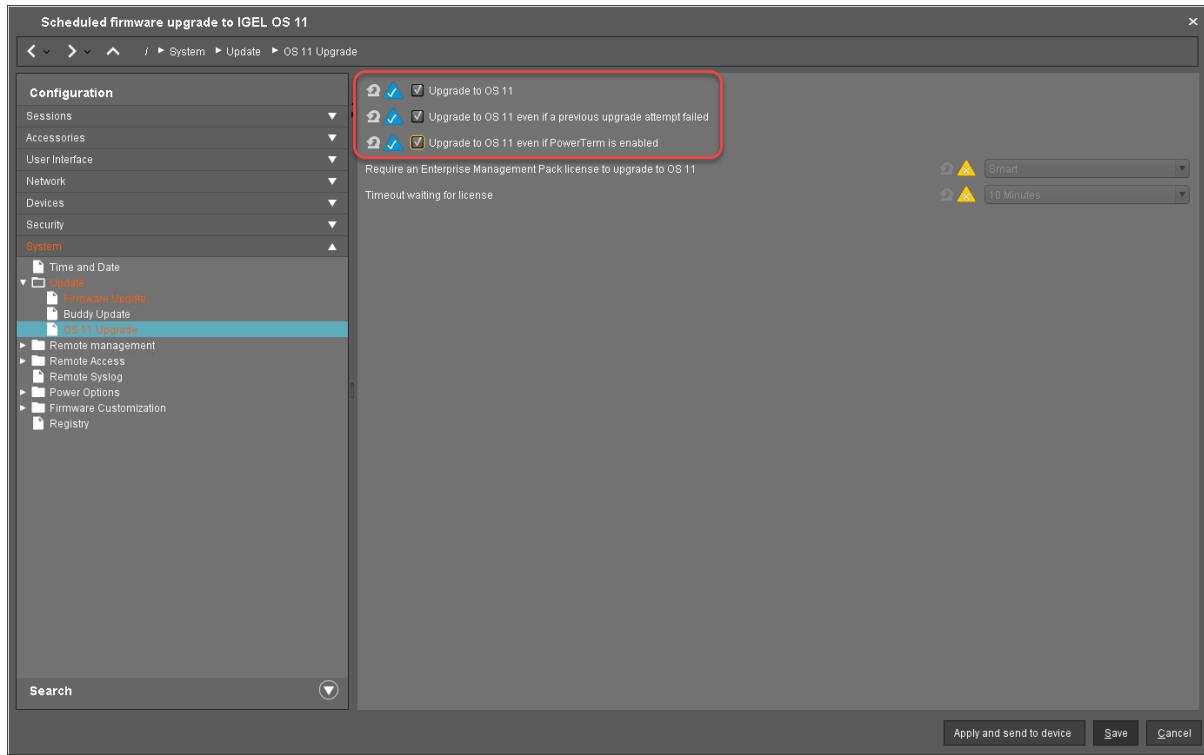
If you use **FILE** as the protocol (local file or network drive), the device will show an error message and go through an additional reboot. Apart from that, the upgrade will work normally.

- Ensure that **Automatic Update Check on Boot** and **Automatic Update Check on Shutdown** are deactivated.

In the following screenshot, FTP is used as an example. The other protocols can be used as well.

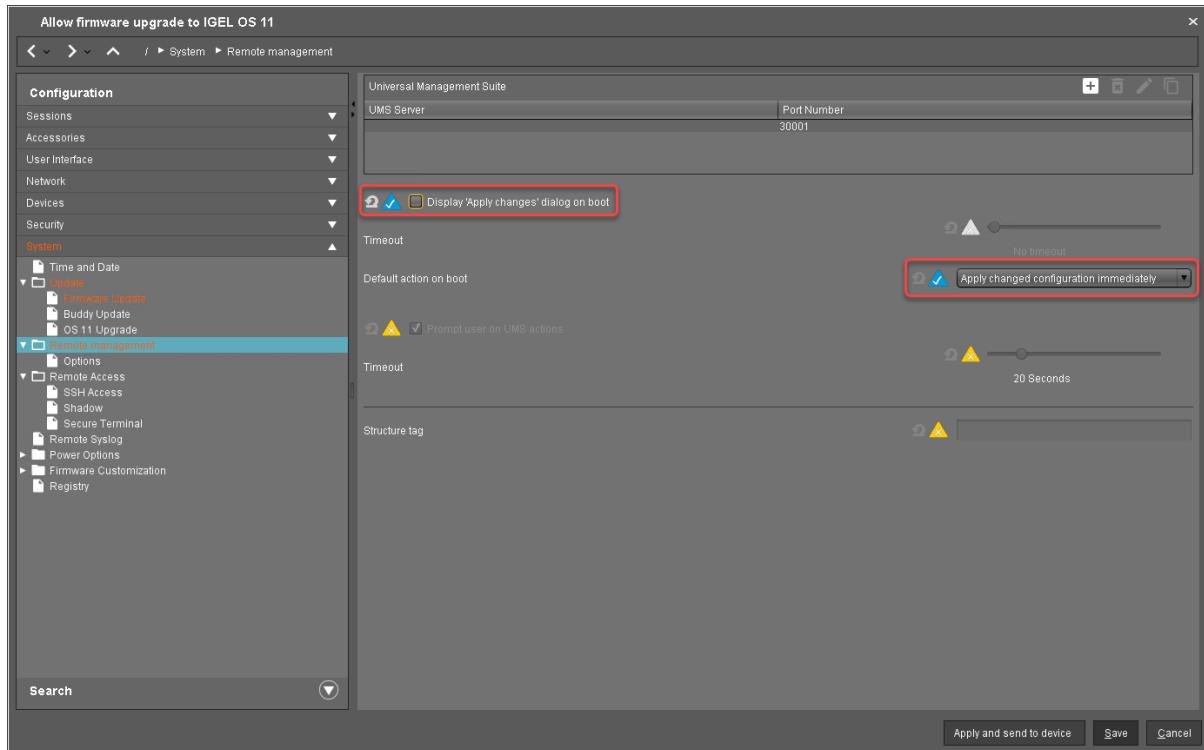


3. Go to **System > Update > OS 11 Upgrade** and change the following settings according to your successful upgrade test (for details of the settings, see [Adjusting the Setup](#)(see page 177)):
  - Activate **Upgrade to OS 11**.
  - Set **Upgrade to OS 11 even if PowerTerm is enabled** according to your needs.
  - Set **Upgrade to OS 11 even if a previous upgrade attempt failed** according to your needs.
  - Set **Require an Enterprise Management Pack license to upgrade to OS 11** according to your needs.
  - Ensure that the **Timeout waiting for OS 11 license to start automatic upgrade** is set to **10 Minutes**.



4. Go to **System > Remote Management** and change the settings as follows:

- Deactivate **Display 'Apply changes' dialog on boot**.
- Set **Default action on boot** to **Apply changed configuration immediately**.



## 5. Click **Save**.

When the profile is created, continue with [Deploying the Licenses](#)(see page 213).

## Deploying the Licenses

Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see [Setting up Automatic License Deployment \(ALD\)](#)<sup>116</sup>.
- Manual License Deployment: Licenses are created and deployed manually. For instructions, see [Manual License Deployment for IGEL OS](#)<sup>117</sup>.

When the license deployment is set up, continue with [Assigning the Profile](#)(see page 214).

---

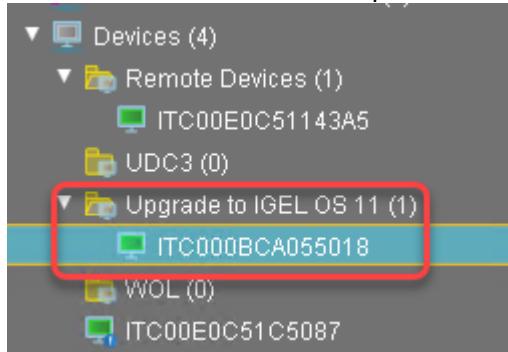
<sup>116</sup> <https://kb.igel.com/pages/viewpage.action?pageId=10325058>

<sup>117</sup> <https://kb.igel.com/display/licensesmoreigelos11/Manual+License+Deployment+for+IGEL+OS>



## Assigning the Profile

1. Put all devices that are to be updated into a directory.

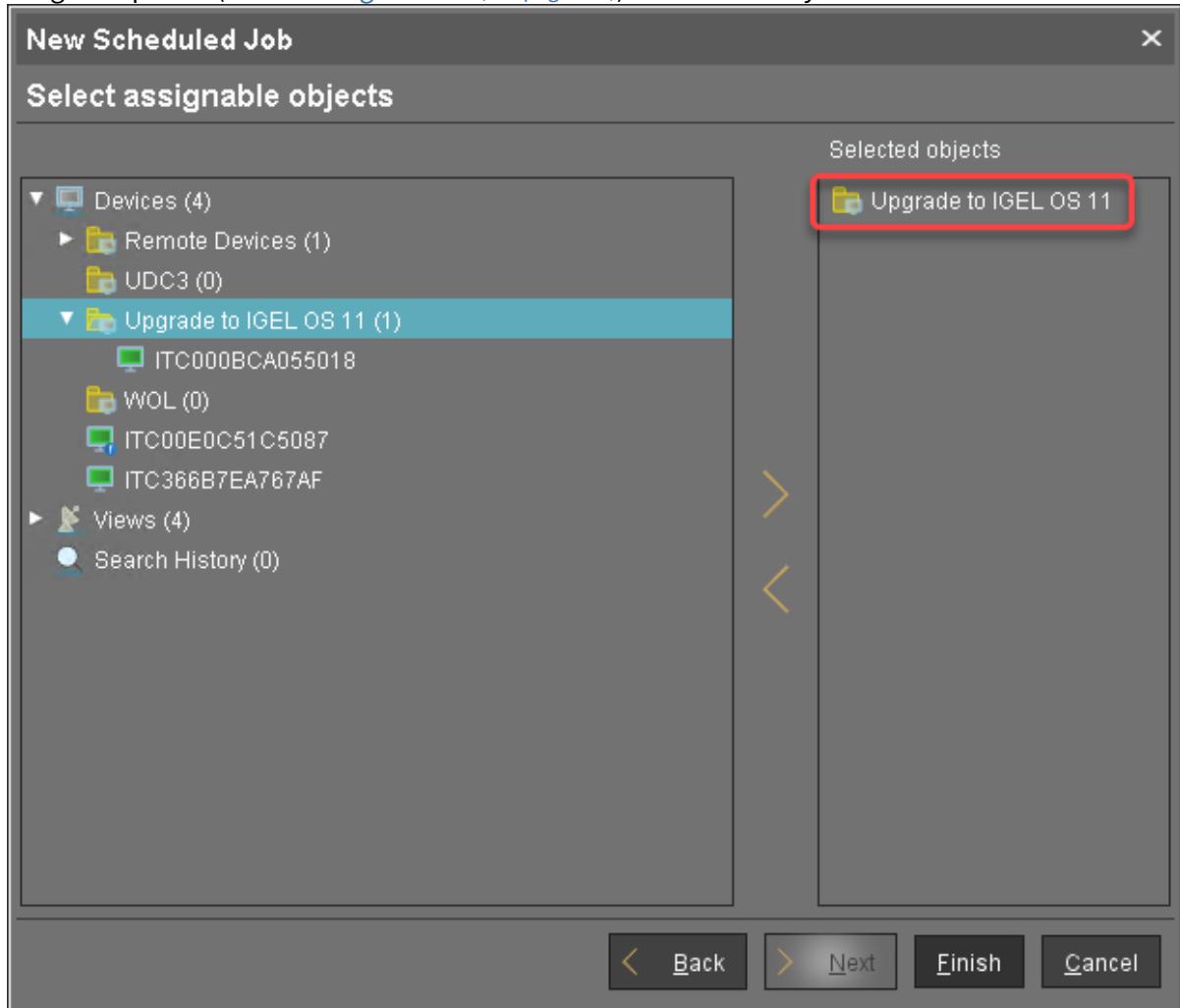


2. Select the directory and in the **Assigned objects** area, click .

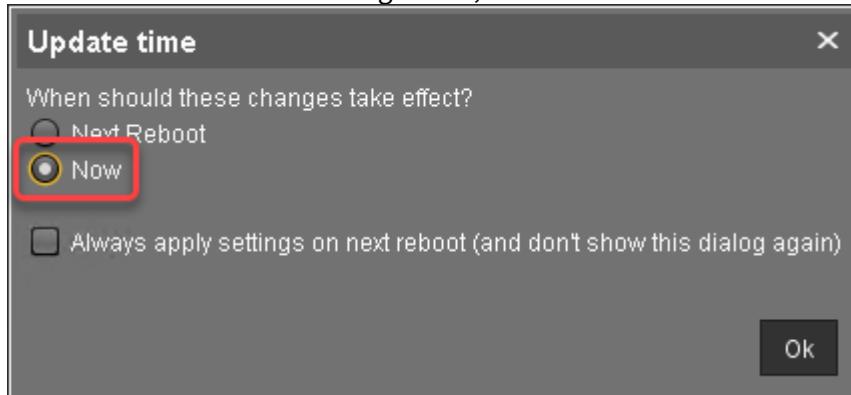




3. Assign the profile (see [Creating a Profile\(see page 210\)](#)) to the directory and click **Ok**.



4. In the context menu of the assignment, select **Now**.

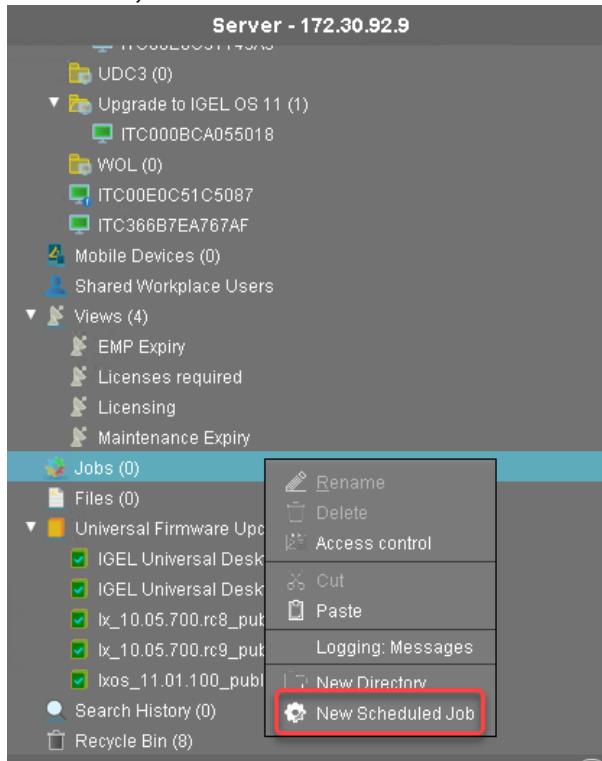


When the profile is assigned, continue with [Creating the Scheduled Job\(see page 216\)](#).



## Creating the Scheduled Job

1. In the UMS, select **Jobs > New Scheduled Job**.



2. Under **Name**, enter a suitable name for the job, e. g. "Upgrade to IGEL OS 11".

The 'New Scheduled Job' dialog box is displayed. The 'Details' tab is selected, showing the following configuration:

- Name:** Upgrade to IGEL OS 11 (highlighted with a red box)
- Command:** OS 11 Upgrade
- Execution time:** 11:53
- Start date:** 2019-04-10
- Enabled:** checked
- Comment:** (empty)
- Options:** Log results (checked), Retry next boot (unchecked)
- Max. Threads:** 99
- Delay:** 0 Seconds
- Timeout:** 30
- Job-Info:** Job ID: (empty), Next Execution: Apr 10, 2019 11:53 AM, User: (empty)

At the bottom of the dialog are buttons for Back, Next, Finish, and Cancel.



3. Under **Command**, select **OS 11 Upgrade**.

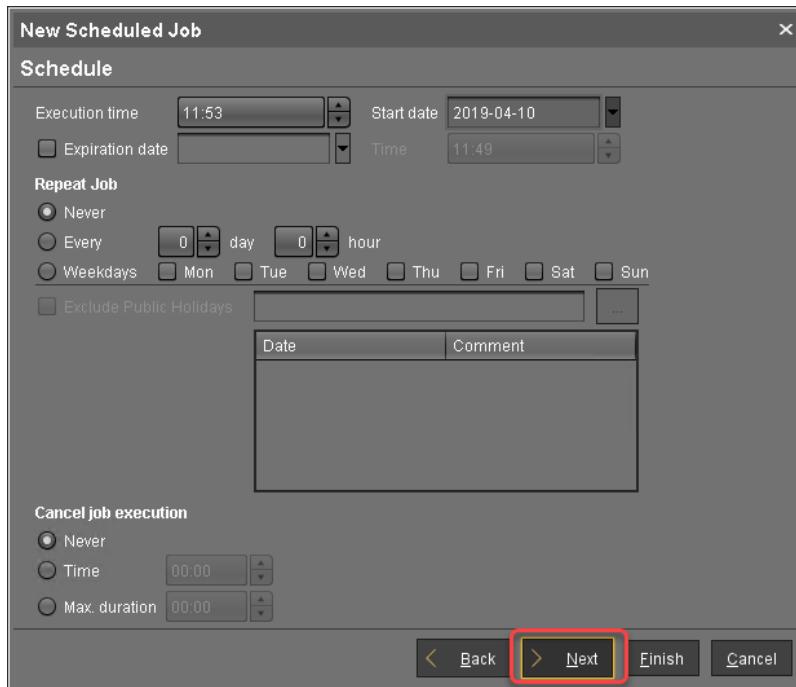
The screenshot shows the 'New Scheduled Job' dialog with the 'Details' tab selected. The 'Name' field contains 'Upgrade to IGEL OS 11'. The 'Command' dropdown is set to 'OS 11 Upgrade', also highlighted with a red box. The 'Execution time' is set to '11:53' and the 'Start date' is '2019-04-10'. The 'Enabled' checkbox is checked. In the 'Options' section, the 'Log results' checkbox is checked, while 'Retry next boot' is unchecked. The 'Max. Threads' is set to 99 and 'Timeout' is set to 30. The 'Job-Info' section shows 'Job ID' as empty, 'Next Execution' as 'Apr 10, 2019 11:53 AM', and 'User' as empty. At the bottom, there are 'Back', 'Next', 'Finish', and 'Cancel' buttons.

4. Under **Execution time** and **Start date**, set the time at which the upgrade should be executed, and click **Next**.

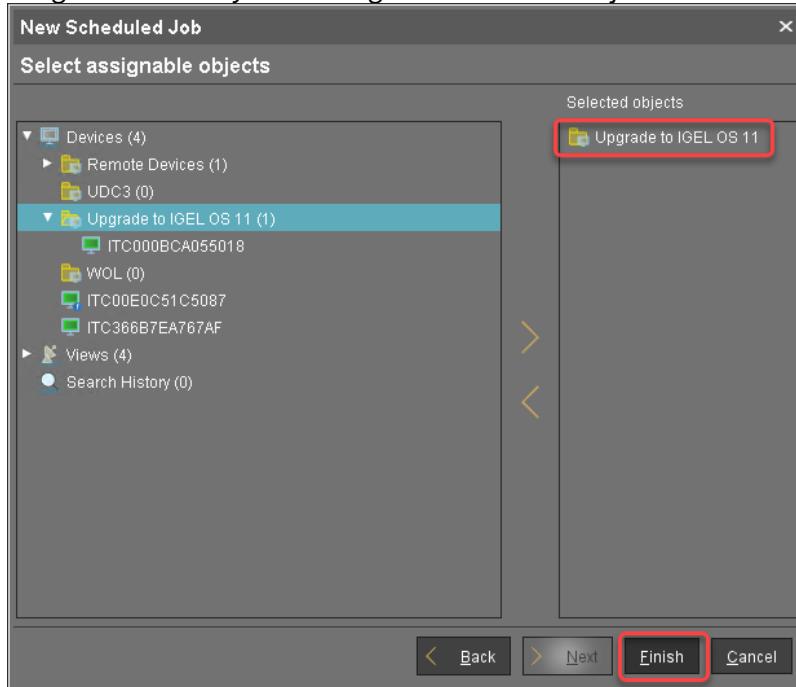
This screenshot shows the 'New Scheduled Job' dialog with the 'Details' tab selected. The 'Name' field is 'Upgrade to IGEL OS 11' and the 'Command' dropdown is 'OS 11 Upgrade'. The 'Execution time' is set to '11:02' and the 'Start date' is '2019-08-12', both highlighted with red boxes. The 'Enabled' checkbox is checked. The 'Options' section includes 'Log results' checked and 'Retry next boot' unchecked. The 'Max. Threads' is 99 and 'Timeout' is 30. The 'Job-Info' section is empty. At the bottom, the 'Next' button is highlighted with a red box, while 'Back', 'Finish', and 'Cancel' are standard grey buttons.



5. Review the execution time and click **Next**.



6. Assign the directory containing the devices to the job and click **Finish**.





### Update Can Be Canceled After Timeout

An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

## Troubleshooting

This section describes possible error cases and solutions.

- [Regaining a Usable System](#)(see page 219)
- [Getting Error Messages](#)(see page 219)
- [Starting a New Upgrade Attempt](#)(see page 220)
- [Starting Another Upgrade Attempt after 5 Retries](#)(see page 220)

### Regaining a Usable System

Here you can find typical upgrade failures and the appropriate methods to regain a usable system.

#### Device Has Upgraded to Igel OS 11, but Does Not Boot Any More

To get a working IGEL OS 11 system:

- Use the IGEL OS Creator to recover the IGEL OS 11 system. For more information, see the [IGEL OS Creator Manual](#)(see page 1293).

#### IGEL OS 10 Rescue System Fails to Update Missing Partitions

If a severe error has occurred during the upgrade process, the device boots into a minimal 10.05.700 (or higher) rescue system. If unattended, the device tries to download and update the missing partitions and reboots on failure.

To regain a full IGEL OS 10 system, you have two possibilities:

- In the rescue system, start the Setup, go to **System > Update > Firmware Update** and set a valid update source for the appropriate IGEL OS 10 firmware version (10.05.700 or higher).

Or:

- Configure a UMS profile that contains a valid update source for the appropriate IGEL OS 10 firmware version (10.05.700 or higher) under **System > Update > Firmware Update** and assign it to the device.

### Getting Error Messages

- Open the OS 11 Upgrade Tool (default path: click System and then **Upgrade to OS 11**).

The OS 11 Upgrade Tool shows the error messages. The most important message is prefixed with **Retries**; see the example below:



- ▶ For more information, review the main migration log under /wfs/migration.log

You can use the system log viewer to review the migration log (see the chapter [System Log Viewer](#)(see page 1070) in the IGEL OS Manual) or save the log files in order to send them to the IGEL Support Team (see the chapter [Save Device Files for Support](#)<sup>118</sup> support).

### Starting a New Upgrade Attempt

If you want the device to start multiple upgrade attempts (and the device is not already configured to do so):

1. In the UMS profile or in the Setup, go to **System > Update > OS 11 Upgrade** and activate **Upgrade to OS 11 even if a previous upgrade attempt failed**.
2. Reboot the device.

### Starting Another Upgrade Attempt after 5 Retries

When the **Upgrade to OS 11 even if a previous upgrade attempt failed** option is set and the upgrade has failed each time, the system will stop trying after 5 attempts.

To reset the retry counter:

1. In the Setup or the UMS profile, go to **System > Update > OS 11 Upgrade** and deactivate **Upgrade to OS 11 even if a previous upgrade attempt failed**.

---

<sup>118</sup> <https://kb.igel.com/display/endpointmgmt601/Save+TC+Files+for+Support>

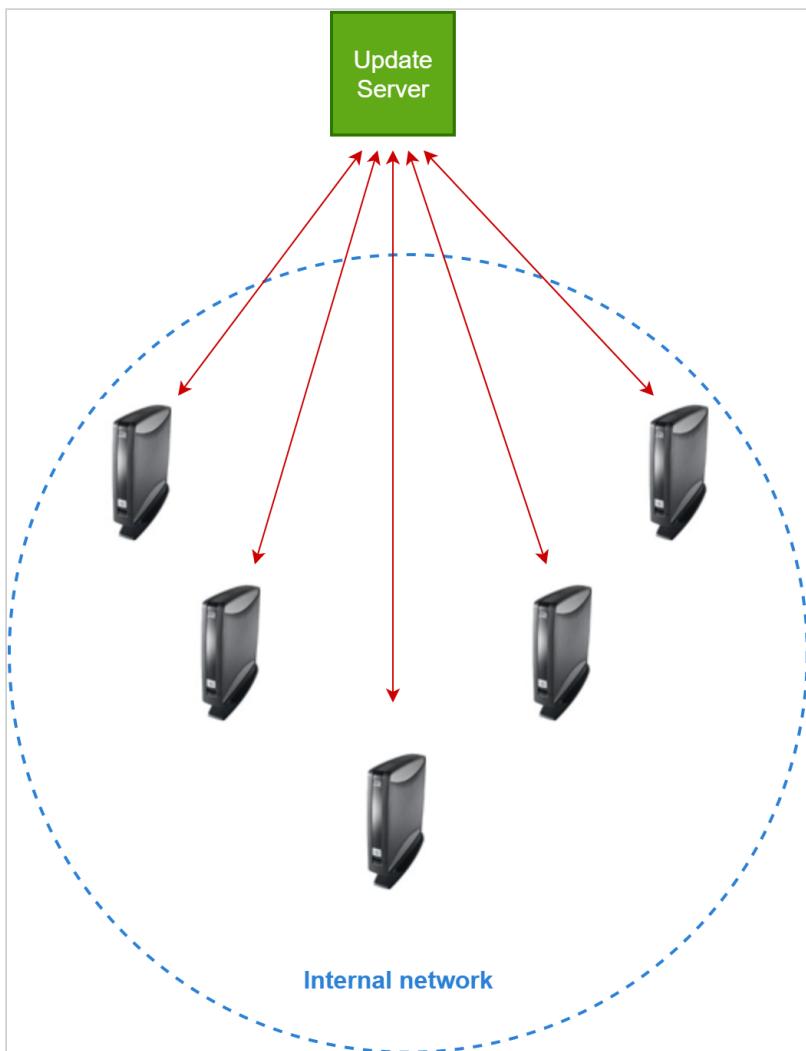


2. When the setting is effective on the devices, go to **System > Update > OS 11 Upgrade** again and activate **Upgrade to OS 11 even if a previous upgrade attempt failed..**

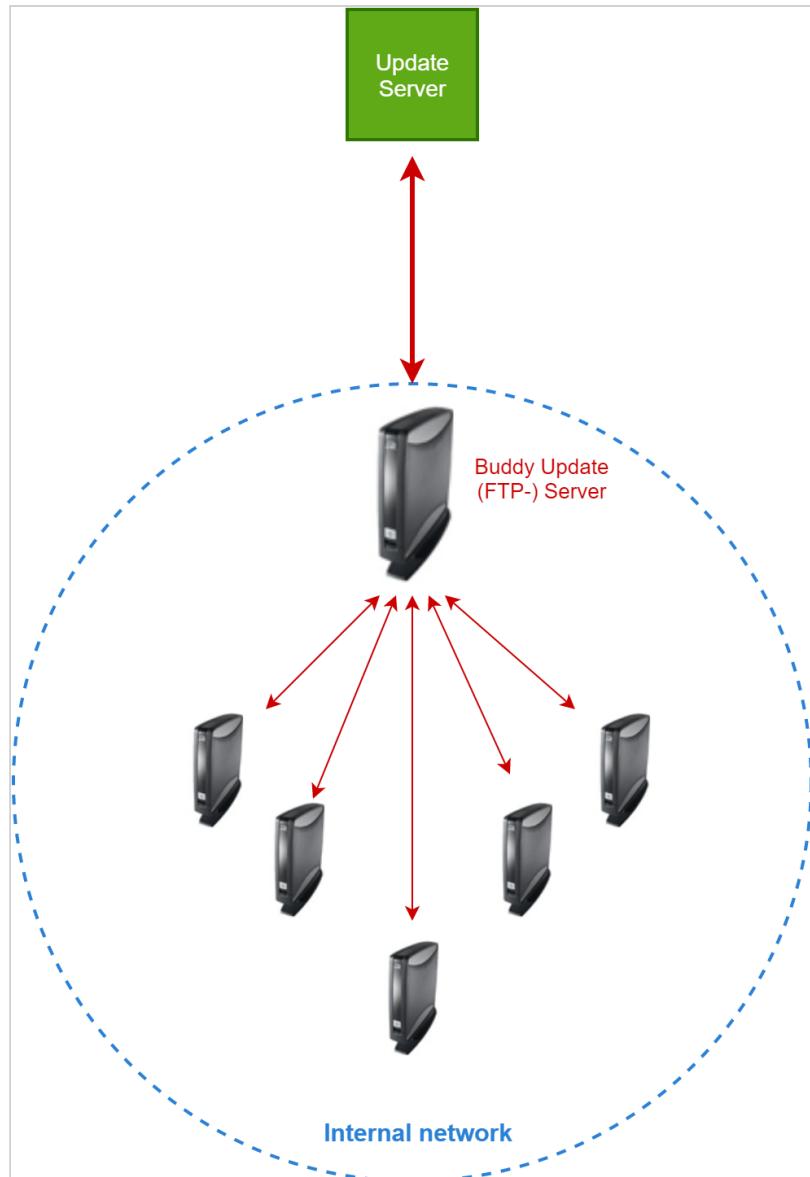
The retry counter is reset, and the devices will try upgrading another 5 times, if necessary.

## 2.2.4 Buddy Update

A certain number of devices that are running IGEL OS in your company regularly need to be updated. If every device accesses the main update server individually, maybe even over a great geographical distance, the update could take quite a long time and might overload the entire connection.



Set up one of your devices as a so-called buddy update server. In the future, only this client will access the main server to download the updates. All other clients access the local buddy update server from within the network and will no longer offload the network outside.



The buddy update server is always an FTP server.

For the configuration details, see:

- [Configuring the Buddy Update Server](#)(see page 223)
- [Configuring the Buddy Update Client](#)(see page 224)

TechChannel



Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:

<https://www.youtube.com/watch?v=IVUIFtOT5uE>

## Configuring the Buddy Update Server

### No Downgrade from IGEL OS 11.03

It is not possible to downgrade from IGEL OS 11.03 or higher to any version before IGEL OS 11.03, except IGEL OS 11.02.200. This is because, from IGEL OS 11.03 onwards, the system partitions are signed to guarantee their integrity; it is not possible to change from a system with signed partitions to a system with unsigned partitions. IGEL OS 11.02.200 is a special variant of IGEL OS 11.02 that has signed system partitions. IGEL OS 11.02.200 is only available from the IGEL Support Team.

### Basic Configuration

1. In the Setup, go to **System > Update > Buddy Update**.
2. Activate **Enable Update Server**.
3. Enter the credentials **User Name** and **Password**.
4. Specify the maximum number of **Concurrent Logins** allowed.
5. Click **Save** to confirm the changes.
6. Perform a complete firmware update on the server.
7. Reboot the server.

Whenever a buddy update server has received a firmware update, it needs to be rebooted before it can distribute the new firmware to other devices.

### Configuration for Different Firmware Versions

This feature is available for the following versions of IGEL OS:

- IGEL OS 10: 10.06.100 or higher
- IGEL OS 11: 11.02.100 or higher

If you have an environment which requires two or more different firmware versions running simultaneously, you can use the buddy update method to provide each buddy update client device with the appropriate firmware version. A typical use case might be two groups of employees, of which one requires an older version of the browser, or an older version of the Citrix receiver, whereas the other group should get the newest version of IGEL OS. This is achieved by dividing both the clients and the servers into groups. To each group, a specific firmware version is assigned by first installing that version on the group's update servers. As an example, you can assign group 1 to IGEL OS 10.07.100, and group 2 to IGEL OS 10.08.100.



In the following description, the local Setup is used for simplicity reasons; however, in a productive environment, it is recommended to use profiles. For further information, see [Profiles<sup>119</sup>](#).

To assign a server to a group:

1. Configure the server as described above ([Basic Configuration](#)(see page 223)), using the firmware that is to be assigned to this group.
2. In the Setup, go to **Registry > update > ftp > buddy\_group\_id**.
3. In the field **Buddy Group ID**, set the appropriate group id. Unsigned integers are allowed.
4. Click **Ok**.
5. Reboot the device.

The device will provide the firmware update for the group it is assigned to.

For client configuration, see [Configuring the Buddy Update Client](#)(see page 224), "Configuration for Different Firmware Versions".

## Configuring the Buddy Update Client

### Basic Configuration

1. In the Setup, go to **System > Update > Firmware Update**.
2. Set the following parameters:

**Server Name:** IP address of the buddy update server

**Port:** 21 (default with FTP protocol)

**Server Path:** -

**User Name:** User name of the buddy update server

**Password:** Password of the buddy update server

Ensure that all servers in the network use the same credentials. For security reasons, you have to enter them in the upper mask, even if you did not specify a server.

3. Activate **Automatic Update Check** if you want the client to check automatically during the boot process whether new updates are available on the server.
4. Activate **Automatic Buddy Detection** if you want the client to look for a buddy update server on its own.  
This is useful if you work with more than one buddy update server and do not wish to determine a specific one.  
In this case, you do not need to define the **Server Name**, **Port** and **Server Path**. If you enter a server name anyway, the system treats this server as a fall-back. Thus, you can be sure that the system accesses at least this one server if it cannot find any others.
5. Click **Ok**.
6. Continue with further configuration changes or reboot the device.

### Configuration for Different Firmware Versions

The feature is available for the following versions of IGEL OS:

---

<sup>119</sup> <https://kb.igel.com/display/endpointmgmt602/Profiles>



- IGEL OS 10: 10.06.100 or higher
- IGEL OS 11: 11.02.100 or higher

This feature is described under [Configuring the Buddy Update Server](#)(see page 223), "Configuration for Different Firmware Versions".

In the following description, the local Setup is used for simplicity reasons; however, in a productive environment, it is recommended to use profiles. For further information, see [Profiles](#)<sup>120</sup>.

To assign a client to a group:

1. In the Setup, go to **Registry > update > ftp > buddy\_group\_id**.
2. In the field **Buddy Group ID**, set the id of the group to which the desired firmware is assigned.
3. Click **Ok**.
4. Reboot the device.  
The device will use the firmware update for the group it is assigned to.

#### Balancing the Server Load

This feature is available for the following versions of IGEL OS:

- IGEL OS 10: 10.06.100 or higher
- IGEL OS 11: 11.02.100 or higher

It is possible to balance the load between several buddy update servers. If **System > Update > Firmware Update > Automatic Buddy Detection** is activated, the clients send a broadcast in their network to determine which buddy servers are available. Each server that responds within a fixed timeout is added to a list whose maximum length can be defined. When the list is complete, either because its maximum length is reached or because the timeout has expired, the client selects a random server from the list. This way, the load of the buddy servers is distributed evenly.

To configure a client for balancing the server load:

1. In the Setup, go to **Registry > update > ftp > buddy\_server\_candidates**.
2. In the field **Buddy Update Server Candidates**, enter the maximum number of servers the client should collect. If the number is 1, the server that responds first is selected.
3. Click **Ok**.
4. Reboot the device.

### 2.2.5 Firmware Update

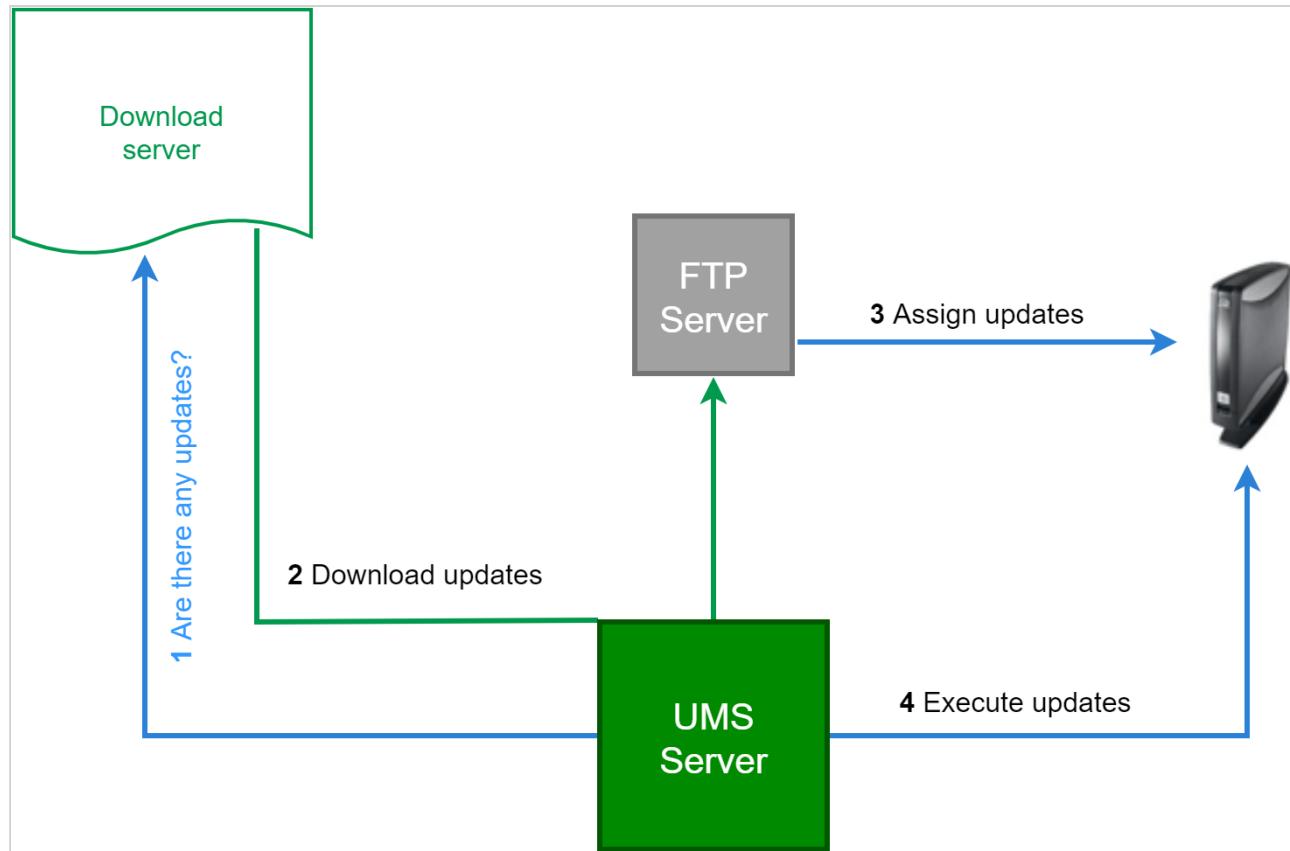
Here we show you the best practice of downloading a firmware update from our download server and distributing it to various devices in your company:

1. Check our [download server](#)<sup>121</sup> to see whether there are new updates which are relevant for your applications.
2. Download the relevant update files.
3. Install an update directory for them on the UMS server or on your FTP server.
4. Assign this update directory to your devices.
5. Start the update process manually or via a [Scheduled Job](#)(see page 227).

---

<sup>120</sup> <https://kb.igel.com/display/endpointmgmt602/Profiles>

<sup>121</sup> <https://www.igel.com/software-downloads/>



- [Downloading Updates and Storing them on an FTP Server](#)(see page 226)
- [Executing an Update Process](#)(see page 227)

### Downloading Updates and Storing them on an FTP Server

You can save the update files either directly on the UMS server or you can put them on your captive FTP server. If you have many devices to be updated, you should work with the FTP server because it makes it easier to distribute large amounts of data in the local network.

#### No Downgrade from IGEL OS 11.03

It is not possible to downgrade from IGEL OS 11.03 or higher to any version before IGEL OS 11.03, except IGEL OS 11.02.200. This is because, from IGEL OS 11.03 onwards, the system partitions are signed to guarantee their integrity; it is not possible to change from a system with signed partitions to a system with unsigned partitions. IGEL OS 11.02.200 is a special variant of IGEL OS 11.02 that has signed system partitions. IGEL OS 11.02.200 is only available from the IGEL Support Team.



### Important Notes on Downgrading from IGEL OS 11.06 or Higher

- If you have encrypted your IGEL OS 11.06 device, downgrading to IGEL OS 11.05 or lower will imply data loss on the following partitions, due to different partition schemes:
  - Browsing history of the browsers Firefox and Chromium
  - Custom Partitions
- The device settings and the UMS connection are preserved.
- The device encryption password must be entered by the user.

## Preparation

1. Click **Universal Firmware Update** in the UMS Administration area of *UMS console*.
2. Click **Edit....**
3. Enter your FTP server under **Host**, to save the update files in this location.
4. Add further details like storage path and access data for the server.
5. Save your settings and click **Test Server Connection**.

## Downloading updates

1. Right-click **Universal Firmware Update** on the UMS console tree.
2. Choose **Check for new firmware updates** from the context menu.  
A window opens with a list of all updates associated with the firmware versions registered in the UMS database.
3. Choose a **Version** in the drop-down-list.
4. Click **Information** to see the release notes of each update.
5. Activate the check box **Include** for downloading a certain update.
6. Click **Download** to start the process.  
The update will be added to the tree and the current processing status will be shown.  
The unpacked firmware files are finally in the target directory on the FTP server.

## Assigning updates to the thin clients

Assign the downloaded update by dragging and dropping to your device directory. Now, if you click this directory you can see the firmware update in the right window under **Assigned objects**. The devices will now know where to find the firmware update in the event of an update command.

## Executing an Update Process

1. Create one or more new **Views** to distinguish which thin clients will get the new update.
2. Create a new **Job**, called "firmware update" for example.
3. Specify on the **Schedule** tab when you want the update to be performed.

The **Repeat job** option should not be activated for **Update**, **Update on boot** or **Update on shutdown** commands.

4. Add one or more **Views** on the **Assignment tab**.



## 5. Save the job.

The update process will be performed according to the schedule specified in the job.

### **Update Can Be Canceled After Timeout**

An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

## 2.2.6 Updating the Firmware using a USB Storage Device

You can use a USB storage device to update the firmware locally. This method is particularly suitable if only one device or only a few devices are to be updated and it would not be worth installing an FTP or HTTP server purely for the update. Proceed as follows:

1. Download the update file (.zip) for your device from the [IGEL download server](#)<sup>122</sup>.
2. Unpack the update files and save them to a USB storage device.

You can find the officially supported file systems under [Storage Hotplug](#)(see page 1228).

3. In the local setup application select **Devices > Storage Devices > Storage Hotplug**.
4. Set **Client Drive Mapping to Static**
5. Enable **Private drive letter for each storage drive**.
6. Set **Number of drives** to at least 1.
7. **Apply** the changes so that they are effective for the device.

You can find more informations in the chapter [Storage Hotplug](#)(see page 1228).

8. Connect the USB storage device to the device and wait until the device has been detected.
9. Go to **System > Update > Firmware Update**.
10. Set **Protocol** to **FILE**.
11. Start the file chooser (**Server Path**) and navigate to /userhome/media/label of the file system/lxos.inf and click **Open**.
12. Click **Update Firmware** and confirm the warning message.

The device will reboot while updating the firmware. Do not remove the USB device until the update has finished.

Make sure you do not boot from the USB storage device. You might need to change the boot order in the BIOS/UEFI.

<sup>122</sup> <https://www.igel.com/software-downloads/workspace-edition/>



To update the device's firmware without having access to the local setup, follow FAQ [Updating the Firmware using the Linux Console](#)(see page 229).

## 2.2.7 Updating the Firmware using the Linux Console

### Issue

You have to update the device's firmware without *IGEL Universal Management Suite* or local *IGEL Setup* application.

### Solution

The device's firmware update can also be carried out directly on the Linux console itself without *IGEL Setup*:

1. Restart the device.
2. Press [ESC] key during booting to bring up the boot menu.
3. Select **Verbose Boot** from the boot menu.
4. When instructed, switch to the console by pressing [CTRL-ALT-F11] or [CTRL-ALT-F12].
5. Press [RETURN] key to log in.  
You may have to enter your password.

Carry out the update. The exact procedure varies according to the protocol which is to be used, that is, FILE, HTTP, or FTP; see the instructions below. You can check whether the correct parameter values have been passed using the `get` command, e.g. `get update.protocol`

#### HTTP

1. If necessary, set up a static IP address (DHCP is active by default)  
`setparam network.interfaces.ethernet.device0.usedhcp false`  
`setparam network.interfaces.ethernet.device0.manual true`  
`setparam network.interfaces.ethernet.device0.ipaddr`  
`setparam network.interfaces.ethernet.device0.netmask`
2. Configure the update server  
`setparam update.protocol http`  
`setparam update.http.server`  
`setparam update.http.port`

The default UMS port is 9080

- ```
setparam update.http.path
setparam update.http.user
setcryptparam update.http.crypt_password
3. Start the update process in the / directory using the command update
```



## FTP

1. If necessary, set up a static IP address (DHCP is active by default)  
`setparam network.interfaces.ethernet.device0.usedhcp false  
setparam network.interfaces.ethernet.device0.manual true  
setparam network.interfaces.ethernet.device0.ipaddr  
setparam network.interfaces.ethernet.device0.netmask`
2. Configure the update server  
`setparam update.protocol ftp  
setparam update.ftp.server  
setparam update.ftp.port`

The default port is 21

- ```
setparam update.ftp.path  
setparam update.ftp.user  
setcryptparam update.ftp.crypt_password
```
3. Start the update process in the / directory using the command update

## FILE

Requirement: The unpacked update files are available in the root directory of a USB storage device.

1. Configure at least one hotplug USB device:  
`setparam devices.hotplug.usb-storage.numdevices 1`
2. Apply your changes:  
`kill_postsetupd`
3. Connect the USB storage device to the device.
4. Wait for the USB storage device to be mounted automatically.
5. Determine the mount point:  
`ls /media/`
6. Configure the update parameters:  
`setparam update.protocol file  
setparam update.file.path /media/<name of USB storage device>`
7. Start the update process in the / directory using the command update



## 2.2.8 Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher

### Symptom

You have tried to update a device to IGEL OS 11.04.100 or higher, but the update fails with the error message "Not enough space on local drive".

### Problem

IGEL OS 11.04.100 or higher requires more than 2 GB storage; your device has less storage than required.

### Environment

This article is valid for the following environment:

- IGEL OS 11.04 or higher
- UMS 6.05 or higher (recommended)
- Endpoint device that is supported by IGEL OS 11.04.100 or higher but has a storage size lesser than the storage size required by the full feature set

### Solution

The recommended storage size for IGEL OS 11.04.100 or higher is 4 GB. However, you can update an endpoint device with lesser storage than required by a regular IGEL OS installation. This can be done by reducing the feature set. A modified INF file (`lxos-reduced.inf`) in the update source defines a reduced feature set that makes the firmware fit into your endpoint device's storage.

As an alternative to the preconfigured INF file, you can customize the INF file yourself to define your own reduced feature set.

#### **Reduced Feature Set Cannot Be Changed by Setup/UMS**

When you have reduced the firmware as described below, you cannot reactivate features via the Setup resp. the UMS configuration dialog. To recover the complete feature set, you must copy `lxos-full.inf` to `lxos.inf` and then start the firmware update.

#### **Buddy Update**

When you have downloaded a reduced firmware on a buddy update server by mistake, also the buddy server itself has the limited feature set. To recover the complete feature set on the buddy server, you must copy `lxos-full.inf` to `lxos.inf` in the update source and then update the buddy update server again.



## Using the Preconfigured INF File

- ▶ To find out which features are included in the reduced feature set, open the `readme[version].txt` in your update source directory and search for "Reduced Firmware". The table shows the features, the storage size they require, and whether they are included in the reduced feature set.

Replace the `lxos.inf` file as follows:

1. Go to the directory that contains the source files for the firmware update. If you use the WebDav capability of the UMS, this is `<UMS installation directory>\rmguiserver\webapps\ums_filetransfer\<firmware version>`; example: `C:\Program Files\IGEL\RemoteManager\rmguiserver\webapps\ums_filetransfer\IGEL_OS_11-11.04.100`
2. Delete `lxos.inf`

It is safe to delete `lxos.inf` because there is a backup file named `lxos-full.inf`
3. Copy `lxos-reduced.inf` to `lxos.inf`
4. Start the firmware update as usual.

## Customizing the INF File

- ▶ To get a list of all features and their storage requirement, go to [IGEL OS Release Notes](#)(see page 1422), look up your version of IGEL OS, go to "Component Versions [your version]", and find the "Services" section.

To customize the INF file:

1. Open `lxos.inf`
2. In the `[INFO]` section, add the following line:  
`custom="true"`
3. Delete the `[PART]` section of every partition you want to exclude, but do this ONLY IF the section has both of the following entries:  
`dispensable="true"`  
`type="squashfs-auto"`
4. Save `lxos.inf` and start the firmware update as usual.

## 2.2.9 Error: "legacy ICG Root (CA) certificate" When Updating to Igel OS 11.04 on Devices Connected via ICG

### Possible Problem

If you update to IGEL OS 11.04 or higher, devices might fail to connect to the ICG afterward because the CA root certificate does not have the CA flag (i.e. X509v3 BasicConstraint extension "is\_ca" is set to "false"). This is the case when the certificate has been created with UMS 5.07 or UMS 5.08.



## Environment

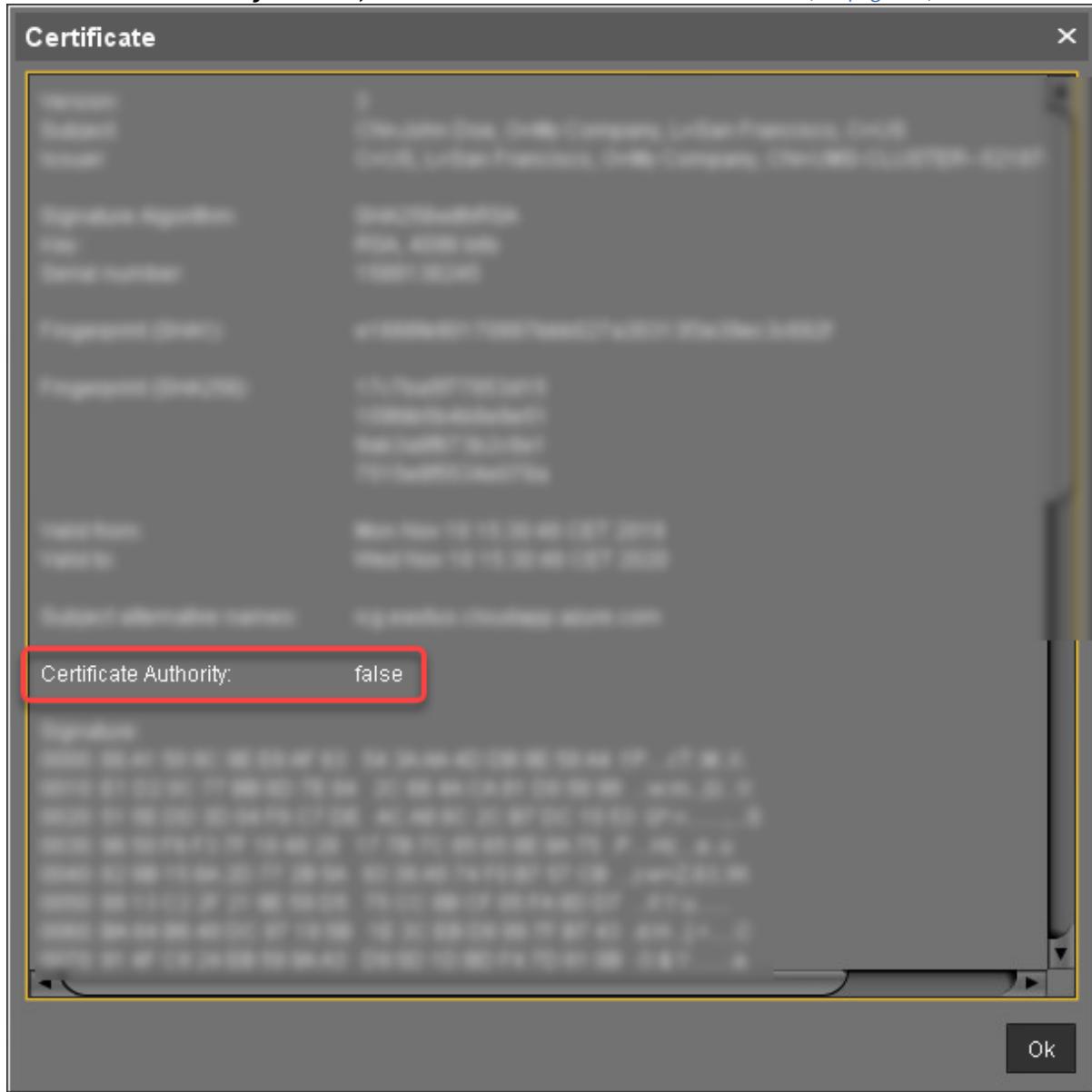
- UMS 5.07 or higher (update to UMS 6.06 or higher will be required if not already present)
- ICG with older root certificates that have been created with UMS 5.07 or UMS 5.08

## Diagnosis

1. Open the UMS Console, go to **UMS Administration > Global Configuration > Cloud Gateway Configuration** (UMS 5.07 to UMS 6.05) or **UMS Administration > Global Configuration > Certificate Management > Cloud Gateway** (UMS 6.06 or higher) and select your ICG root certificate.
2. Click to review the content of the certificate.



3. If **Certificate Authority:** is **false**, find further instructions under [Solution](#)(see page 234).



## Solution

1. Request IGEL OS 11.04.221DER from the IGEL Support team.
2. Update your devices to IGEL OS 11.04.221DER.
3. Update your UMS to version 6.06.100, if you have not already done so.
4. Exchange the root certificate for the ICG connection; see [Exchanging the Root Certificate for ICG](#)<sup>123</sup>.
5. Update your devices to IGEL OS 11.04.240 or higher.

---

<sup>123</sup> <https://kb.igel.com/display/igelicg202/Exchanging+the+Root+Certificate+for+ICG>



## 2.2.10 Device Does Not Connect to ICG after Update to IGEL OS 11.04 or Higher

### Symptom

After an update to IGEL OS 11.04 or higher, the device fails to connect to the UMS via ICG. The log journal shows a message similar to this:

```
igelrm_agent[9824]: [2020/11/11 17:56:16:0140] ERR: SSL error: invalid CA certificate  
(preverify_ok=0;err=24;depth=1)
```

### Environment

- UMS 5.07 or higher
- ICG with older root certificates that have been created with UMS 5.07 or UMS 5.08
- Devices that have just been updated to IGEL OS 11.04 or higher

### Problem/Possible Cause

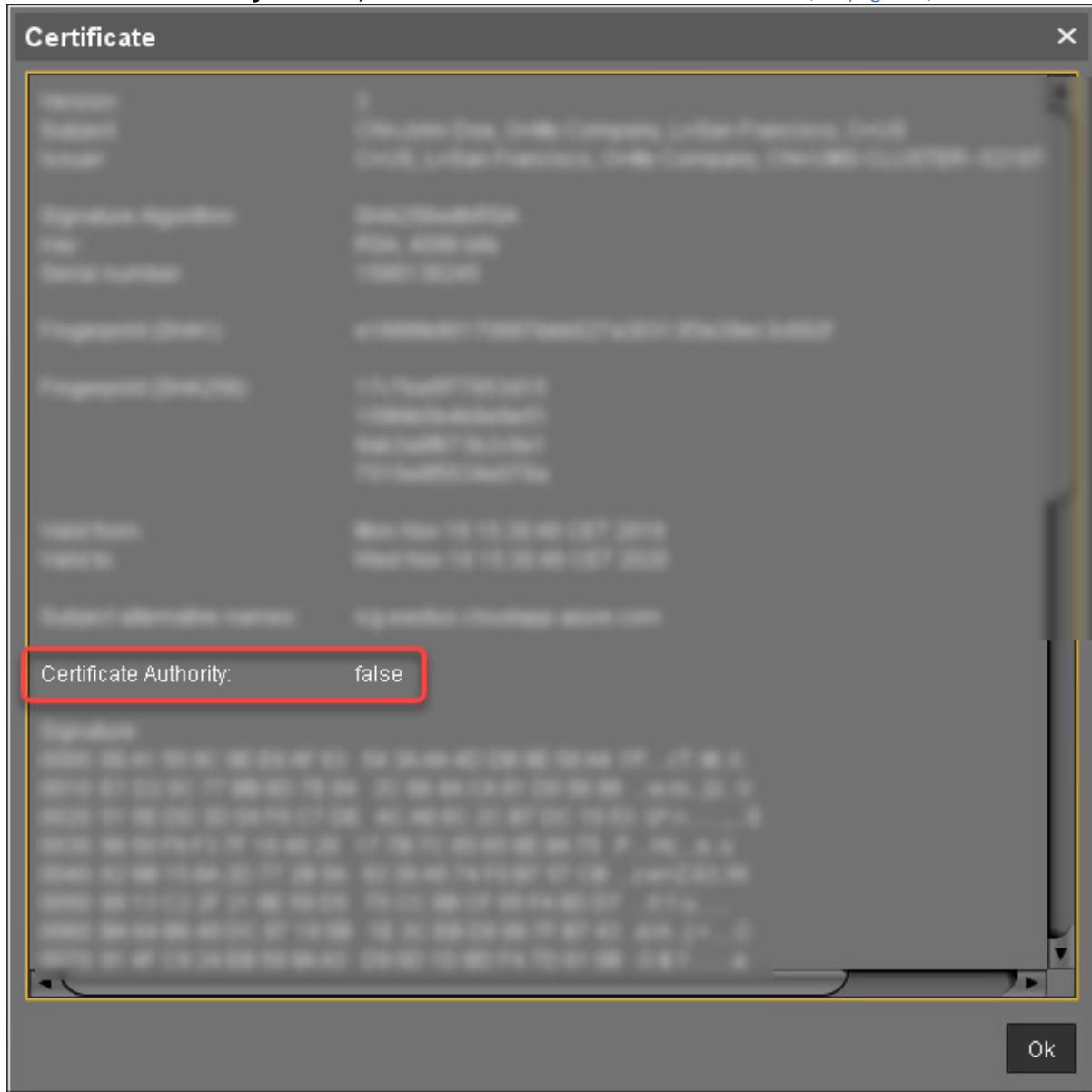
CA root certificates for ICG that have been created with UMS 5.07 or UMS 5.08 are not accepted by IGEL OS 11.04. This is because version 1.1 of the OpenSSL library does not accept certificates as CA certificates if they do not have the CA flag (i.e. X509v3 BasicConstraint extension "is\_ca" is set to "false"). As a consequence, IGEL OS 11.04 or higher refuses to use such a certificate.

### Diagnosis

1. Open the UMS Console, go to **UMS Administration > Global Configuration > Cloud Gateway Configuration** (UMS 5.07 to UMS 6.05) or **UMS Administration > Global Configuration > Certificate Management > Cloud Gateway** (UMS 6.06 or higher) and select your ICG root certificate.
2. Click to review the content of the certificate.



3. If **Certificate Authority:** is **false**, find further instructions under [Solution](#)(see page 236).



## Solution

1. Reinstall the ICG using an appropriate root certificate. For details, see the following articles:
  - [Providing the Certificates](#)<sup>124</sup>
  - [Installing the IGEL Cloud Gateway](#)<sup>125</sup>
2. Register the devices again. For details, see [Connecting the Devices](#)<sup>126</sup>.

<sup>124</sup> <https://kb.igel.com/display/igelicg202/Providing+the+Certificates>

<sup>125</sup> <https://kb.igel.com/display/igelicg202/Installing+the+IGEL+Cloud+Gateway>

<sup>126</sup> <https://kb.igel.com/display/igelicg202/Connecting+the+Devices>

## 2.2.11 IGEL OS Automatic Update Service for Device Evaluation

### Overview

The automatic update service checks for available firmware updates periodically; if a firmware update is available, the user is prompted to start the update. The firmware is provided by IGEL via a download server that is known by the automatic update service. Alternatively, you can use a download server of your own.

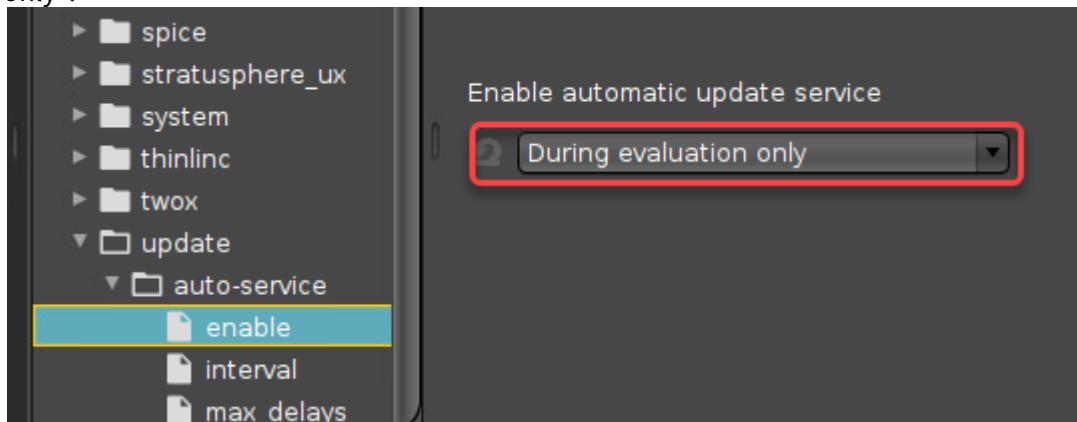
The automatic update service is only available for devices with an evaluation license; when the device receives a Workspace Edition license, the service is deactivated.

### Environment

- Endpoint device with IGEL OS 11.06.100 or higher

### Configuring the Automatic Update Service

1. In the UMS configuration dialog or the local Setup, go to **System > Registry > update > auto-service > enable** and ensure that **Enable automatic update service** is set to "During evaluation only".



2. Set the following parameters according to your requirements:
  - **interval:** Time interval in hours in which the device should check for firmware updates during runtime. When the value is 0, the device only checks on boot.
  - **max\_delays:** Maximal times the user can postpone an update. Example: When this value is set to 9, the user can postpone the update 9 times before the update will be forced. When the value is 0, the update will be forced immediately.
  - **randomized\_delay:** Delay time that is added to the interval to avoid an excessive amount of requests to the server at the same time.
  - **server:** If you want to use an update server of your own, enter its address here. If the field is empty, the public update server provided by IGEL will be used.
  - **user\_dialog\_timeout:** Timeout in seconds before the user dialog is closed and the update is started. When set to 0, the dialog remains open until the user closes it.



- **version:** The target version to which the device should be updated. If the field is left empty, the current version will be used. Example: "11.05.133"
3. Click **Apply** or **Ok** to confirm your settings.

## 2.3 Citrix

- [Performance](#)(see page 238)
- [Mouse](#)(see page 242)
- [How to Configure Citrix Native USB Redirection](#)(see page 247)
- [Citrix Fabulattech Scanner Redirection](#)(see page 248)
- [Mapping USB Storage Media into Citrix Sessions](#)(see page 249)
- [Auto-Hide Toolbar in Appliance Mode](#)(see page 251)
- [Create a Seamless, Transparent User Experience with Appliance Mode](#)(see page 252)
- [Connecting to a Citrix Farm](#)(see page 252)
- [Create a Self-Service Setup for the User with Quick Settings](#)(see page 255)
- [Login Failed because of the Expired AD Password](#)(see page 257)
- [Configuring Auto Logon for Citrix Virtual Desktops](#)(see page 258)
- [Force Citrix Logout Using Hotkey](#)(see page 262)
- [Citrix: Freeze at Logout](#)(see page 263)
- [Warning Message: \[Citrix Store\] Could Not Connect to the Citrix Server](#)(see page 264)
- [Setting up Citrix Sessions with Hardware-Accelerated H.264 Deep Compression Codec](#)(see page 265)
- [Using Font Smoothing \(ClearType\) in Citrix Sessions](#)(see page 266)
- [Highly Secured XenServer has Problems with LD\\_BIND\\_NOW Workaround](#)(see page 267)
- [Workaround for Citrix Receiver X Error](#)(see page 268)
- [Citrix HTML5 Receiver Issue](#)(see page 268)
- [Macbook Keyboard Layout inside Citrix Session](#)(see page 269)
- [Citrix Feature Matrix](#)(see page 269)
- [Using Lync / Skype for Business with Citrix HDX RealTime Optimization Pack](#)(see page 273)

### 2.3.1 Performance

- [Poor Performance: Black Blocks and Stripes in Citrix Sessions](#)(see page 238)
- [Poor Performance with Citrix XenDesktop 7.6 Deep Compression](#)(see page 239)
- [Citrix Receiver: Grey Blocks in Excel 2013](#)(see page 240)
- [Bar Code Scanning is Slow via Citrix](#)(see page 240)
- [Slow Performance of Citrix Session in a Cloud Environment](#)(see page 241)

#### Poor Performance: Black Blocks and Stripes in Citrix Sessions

##### Symptom

In the Citrix session, you sometimes experience a problem with black blocks, frames, or stripes.



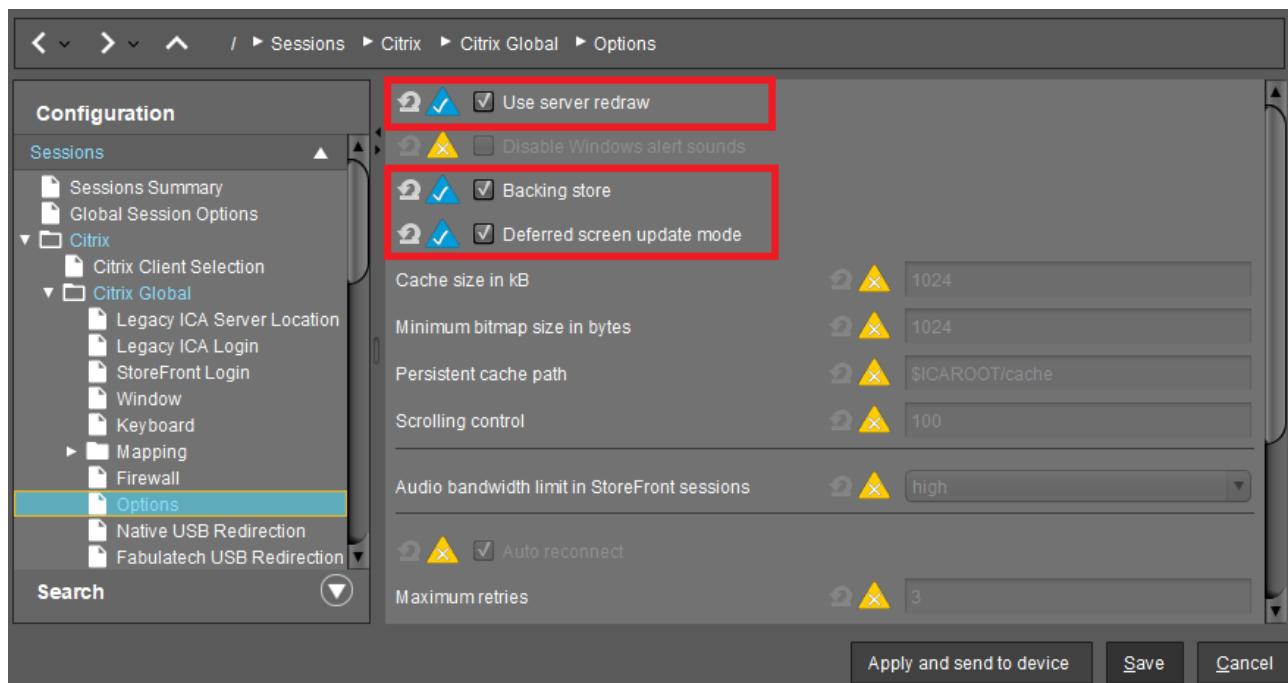
## Problem

Poor performance is often connected with the delayed or slow refreshing of the screen content.

## Solution

► In the IGEL Setup or the configuration dialog in the UMS, activate one of the following parameters or all of them under **Sessions > Citrix > Citrix Global > Options**:

- **Use server redraw**
- **Backing store**
- **Deferred screen update mode**



See also [Options](#)(see page 787) in the manual chapter for Citrix.

If this doesn't work, see also [Black Box Next to the Mouse Cursor](#)(see page 246).

## Poor Performance with Citrix XenDesktop 7.6 Deep Compression

### Symptom

When using XenDesktop 7.6 on Windows Server 2008R2 with Citrix Receiver 13.0.4, 13.1.4 or 13.2.1 with H.264 Deep Compression Codec, dragged Windows lag and the performance is generally poor.



## Problem

Server and/or client do not have enough computing power for the H.264 Deep Compression Codec.

## Solution

Enable the legacy graphics mode on the XenDesktop 7.6 server via a policy.

## Citrix Receiver: Grey Blocks in Excel 2013

### Symptom

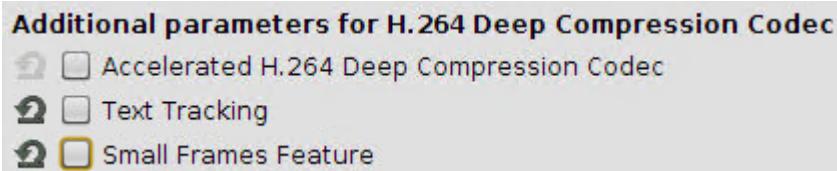
When using Microsoft Excel 2013 on XenDesktop 7.6 with Citrix Receiver 13.1.3, 13.1.4 or 13.2, grey blocks appear especially if you mark multiple cells.

### Problem

Codec parameters may not be optimal for this use case.

### Solution

1. In IGEL Setup, go to **Sessions > Citrix > Citrix Global > Codec**.
2. Disable **Text Tracking**.
3. Disable **Small Frames Feature**.



## Bar Code Scanning is Slow via Citrix

### Solution Based on Experience from the Field

This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

### Issue

Bar code scanning is slow via Citrix.

### Environment

- Firmware version: any



- UMS version: any

#### Description

USB attached bar code scanner is very slow via Citrix.

#### Solution

In order to pass the Bar Code scanner through correctly, you want it to be a HID so it passes through as a HID instead of using Native USB Redirection. A quick way to determine that would be to open a terminal in IGEL OS and simply scan something. If it populates data in the terminal, then it is configured as HID. Also, check the configuration guide for the particular scanner that you are using. The config guide is simply a bunch of barcodes that the device can scan. Once a code is scanned, the device beeps twice, and that changes the config on the scanner. On some devices, there is a setting for Alternate OS Linux/MACOS. The default setting for the scanner usually doesn't enable this. Once the setting was set, everything scanned very fast and that same speed was shown in Citrix.

### Slow Performance of Citrix Session in a Cloud Environment

#### Symptom

Your cloud-based Citrix session is very slow.

#### Environment

- IGEL OS 10.05 or higher, up to IGEL OS 11.05 (with IGEL OS 11.06 or higher, the default setting has changed)
- Citrix client is connected to a cloud server. NOT affected: On-premises and Netscaler environments

#### Problem

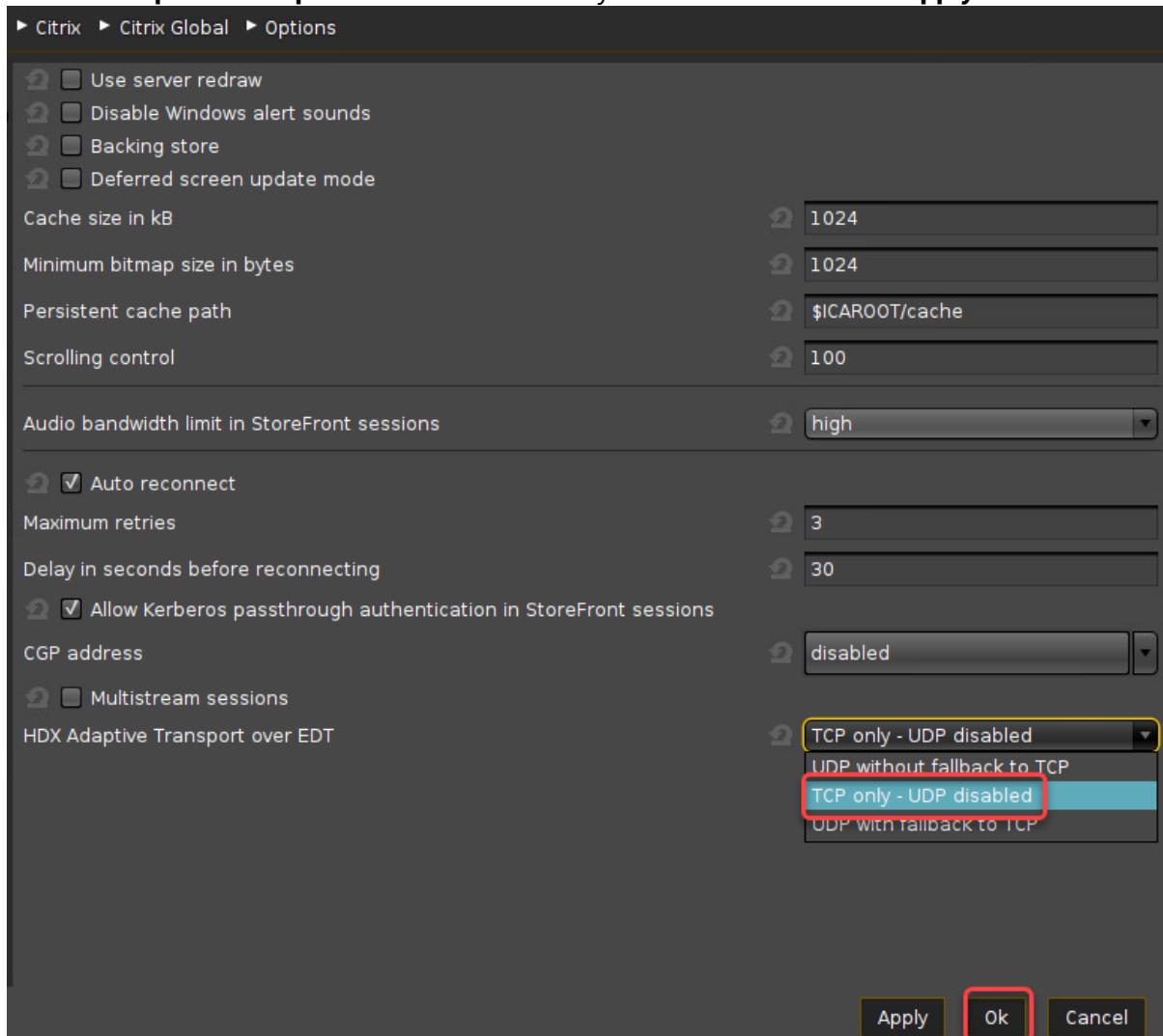
The HDX transport protocol is set to "UDP with fallback to TCP", which causes slow performance.

#### Solution

1. Open the UMS configuration dialog or the local Setup and go to **Citrix > Citrix Global > Options**.



2. Set **HDX Adaptive Transport over EFT** to "TCP only UDP disabled" and click **Apply** or **Ok**.



When the Citrix client is started again, the performance should be better.

### 2.3.2 Mouse

- [Changing Middle Mouse Button Function for Citrix Session and Local Firefox Browser\(see page 242\)](#)
- [How to Connect a SpaceMouse with a Citrix Session\(see page 243\)](#)
- [Solve SpaceMouse USB Reset Problem\(see page 245\)](#)
- [Wireless Mouse Keyboard Set Logitech k520 Freezes in Citrix Session\(see page 246\)](#)
- [Black Box Next to the Mouse Cursor\(see page 246\)](#)

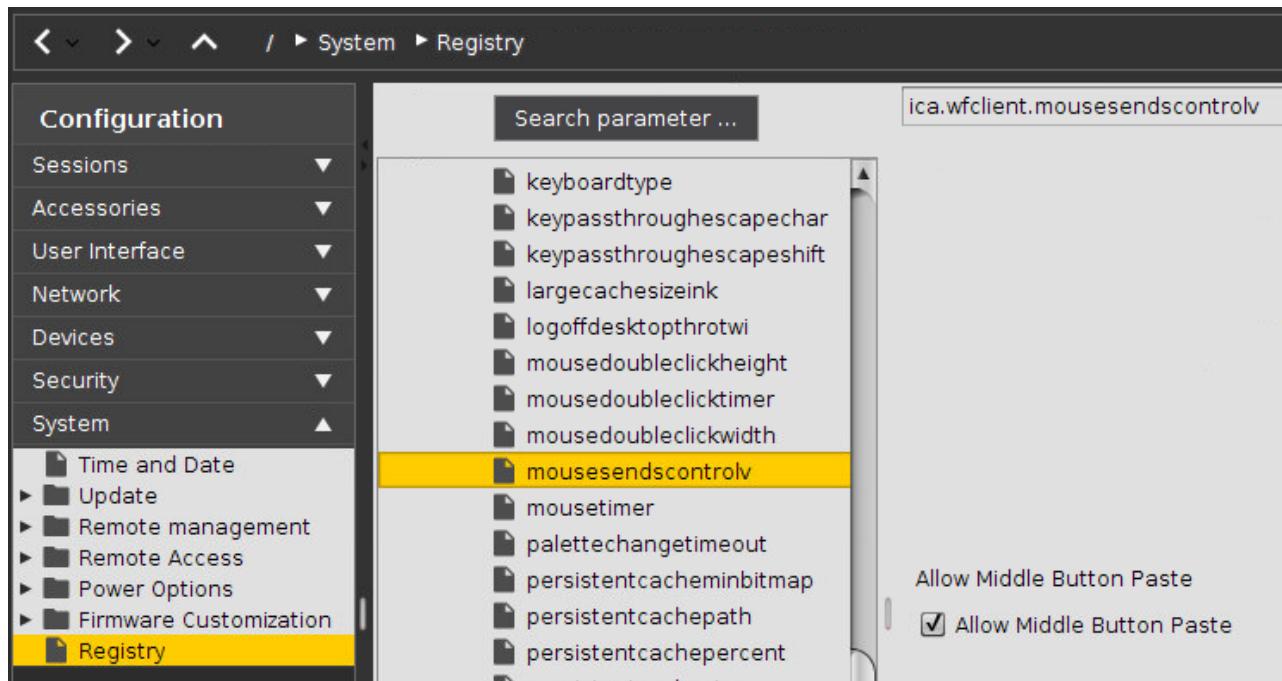
#### Changing Middle Mouse Button Function for Citrix Session and Local Firefox Browser

Middle mouse button cannot be used for smooth scrolling within applications like *Excel* or *Internet Explorer* within a Citrix session or with the local *Firefox* browser.



The default function of the middle mouse button is *copy and paste*.

- Open IGEL registry in local client setup or UMS.



- For Citrix sessions change:
  - **System > Registry > ica.wfclient.mousesendscontrolv**
- For local Firefox browser change:
  - **System > Registry > browerglobal.app.middlemouse\_contentloadurl**
  - **System > Registry > browerglobal.app.middlemouse\_paste**

More information on the Firefox parameters can be found at

<http://kb.mozilla.org/Middlemouse.contentLoadURL>

<http://kb.mozilla.org/Middlemouse.paste>

The changes will take effect after rebooting the thin client.

## How to Connect a SpaceMouse with a Citrix Session

This article describes how to use a 3Dconnexion SpaceMouse in a Citrix session.

Always use a SpaceMouse only as an additional, i.e. second, mouse.



From **version 10.06.100** or **11.02.100** on, the SpaceMouse does not interfere anymore with the local mouse pointer because of a registry key which is enabled by default.

This registry parameter ignores the SpaceMouse for the IGEL graphical user interface:

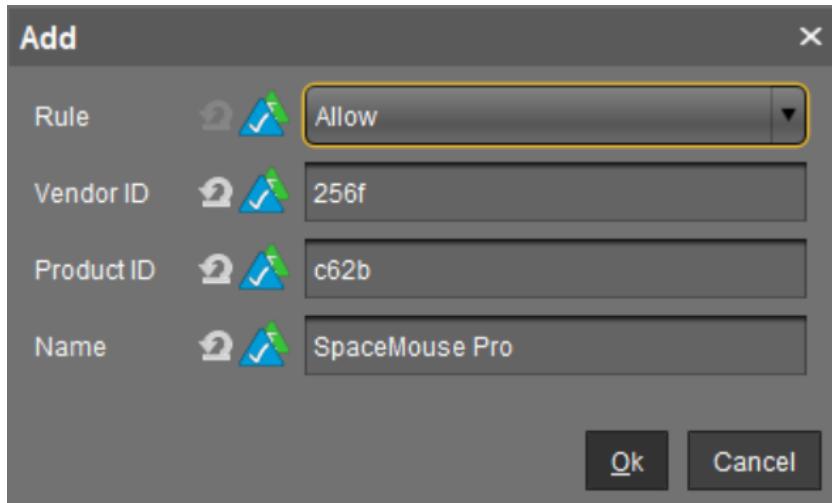
IGEL Setup	System > Registry
Parameter	Deactivates 3Dconnexion/Logitech SpaceMouse products as a standard mouse
Registry Key	userinterface.mouse.spacemouse.x11_ignore
Value	<u>enabled/disabled</u>
Info	"enabled" means that the SpaceMouse is passed through to the session and ignored by the local GUI. "disabled" means that the SpaceMouse is also used for the local GUI.

To configure the SpaceMouse for Citrix sessions:

1. In Setup, go to **Sessions > Citrix > Citrix Global > Native USB Redirection**.
2. Activate the checkbox **Native USB Redirection**.
3. Set the **Default rule** to **Deny**.
4. Add a device exception rule as in the following screenshot with the **Vendor ID** and **Product ID** of your specific SpaceMouse:

#### SpaceMouse products included (VID, PID, Vendor, Product)

- 0x046D; 0xC603; Logitech, Inc.; 3Dconnexion Spacemouse Plus XT
- 0x046D; 0xC605; Logitech, Inc.; 3Dconnexion CADman
- 0x046D; 0xC606; Logitech, Inc.; 3Dconnexion Spacemouse Classic
- 0x046D; 0xC621; Logitech, Inc.; 3Dconnexion Spaceball 5000
- 0x046D; 0xC623; Logitech, Inc.; 3Dconnexion Space Traveller 3D Mouse
- 0x046D; 0xC625; Logitech, Inc.; 3Dconnexion Space Pilot 3D Mouse
- 0x046D; 0xC626; Logitech, Inc.; 3Dconnexion Space Navigator 3D Mouse
- 0x046D; 0xC627; Logitech, Inc.; 3Dconnexion Space Explorer 3D Mouse
- 0x046D; 0xC628; Logitech, Inc.; 3Dconnexion Space Navigator for Notebooks
- 0x046D; 0xC629; Logitech, Inc.; 3Dconnexion SpacePilot Pro 3D Mouse
- 0x046D; 0xC62B; Logitech, Inc.; 3Dconnexion Space Mouse Pro
- 0x256F; \*; 3Dconnexion; SpaceMouse



## 5. Save the settings.

Now, the SpaceMouse is ready for use.

To achieve that the mouse behaves as usual in CAD programs, change the configuration as follows:

1. Go to **IGEL Setup > System > Registry > ica.wfclient.mousesendscontrolv**.
2. Set the parameter to **disable**.

If the SpaceMouse does not function properly after the previous Citrix session, the USB reset of the SpaceMouse must additionally be configured. Follow the instructions in [Solve 3Dconnexion SpaceMouse USB Reset Problem](#)(see page 245).

## Solve SpaceMouse USB Reset Problem

### Environment

Valid for IGEL hardware H850C, H830C, and M340C

### Problem

After a previous Citrix session, the SpaceMouse does not function properly (e.g. after the end of the Citrix session, the reset of the SpaceMouse does not take place; as a result, the display of the SpaceMouse always remains bright).

### Solution

Use a power cycle command to automatically turn all USB devices off and on again:

1. In IGEL Setup, go to **System > Firmware Customization > Custom Commands > Post Session**.
2. Under **Session type**, select **Citrix**.



3. Under **Post session command**, enter the following command: `/etc/igel/usb-power-reset/igel-usb-power-ctl -p cycle`

You do not need root permissions for this action.

As a result of the configured USB power cycle, after the end of the Citrix session, the display of the SpaceMouse should become dark for about 1 second and then bright again.

See also [How to Connect a SpaceMouse with a Citrix Session](#)(see page 243).

## Wireless Mouse Keyboard Set Logitech k520 Freezes in Citrix Session

### Solution Based on Experience from the Field

This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

#### Issue

Wireless Mouse Keyboard Set Logitech k520 freezes in Citrix XenDesktop session.

#### Environment

- IGEL OS 11
- UMS 6.01 and higher

#### Description

If the Wireless Mouse Keyboard's infrared signal is disturbed, it freezes.

#### Solution

This particular device uses infrared dongle. BT devices should work fine as a workaround and we suggest using those. Citrix discourages the use of the IR dongles.

## Black Box Next to the Mouse Cursor

#### Symptom

With certain programs (Adobe Reader, Visual Studio, ...) a black box is always displayed next to the cursor in XenDesktop VMs.



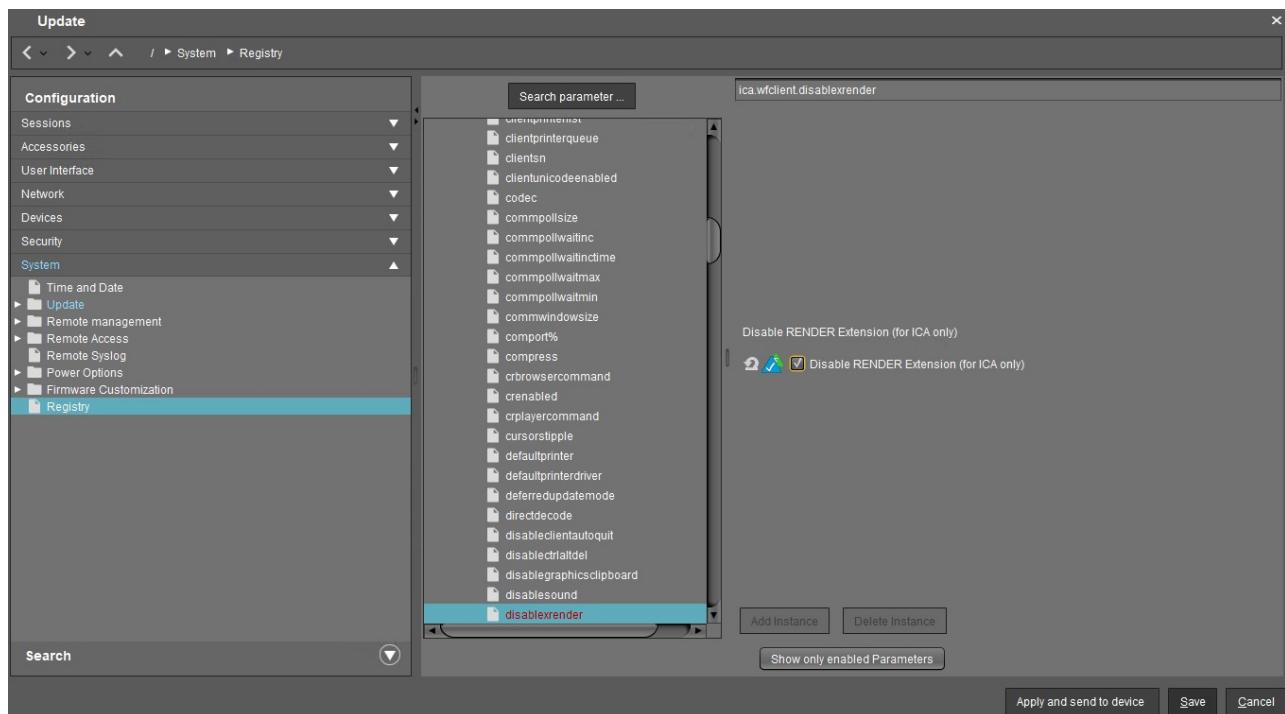
## Problem

This only happens when a connection is made to an IGEL device and disappears when a Windows device is connected. The box is only visible directly on the client (not via VNC).

The problem occurs on the UD7 as well as on Intel NUCs.

## Solution

- ▶ In the IGEL Setup disable the parameter **Disable RENDER Extension (for ICA only)** under **System > Registry > ica.wfclient.disablexrender**:



See also at Citrix: <https://support.citrix.com/article/CTX212013>

### 2.3.3 How to Configure Citrix Native USB Redirection

**Native USB Redirection** redirects most popular USB devices to the Citrix session. To use this feature, you must have at least **XenDesktop 7.6** installed. In addition, the guidelines for USB redirection must be defined. More information can be found on the following pages

- [Citrix Generic USB Redirection Configuration Guide](#)<sup>127</sup>
- [Generic USB redirection and client drive considerations](#)<sup>128</sup>

<sup>127</sup> <https://support.citrix.com/article/CTX137939>

<sup>128</sup> <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/general-content-redirection/usb.html>



The following types of USB device are **not** supported by default for use in a **Citrix Virtual Apps** and **Desktops** session:

- Bluetooth dongles
- Integrated NICs
- USB hubs

The following types of device are supported directly in a **Citrix Virtual Apps** and **Desktops** session, and so do not use USB support:

- Keyboards
- Mice
- Smart cards
- Headsets
- Webcams

In addition to the server policies, the USB redirection must also be activated at the client:

1. In Setup, go to **Sessions > Citrix > Citrix Global > Native USB Redirection**.
2. Enable **Native USB Redirection**.
3. Set the **Default rule** to **Deny** or **Allow**:
  - **Allow**: All devices that are allowed by default are redirected.
  - **Deny**: No device is redirected.

**Tip**

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

4. To customize the USB redirection, you can create classes or device rules to redirect e.g. Bloomberg keyboards or 3D Spacemouse.

To find out the **Vendor ID** and **Product ID** of the connected USB device, use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal. You can also use the **System Information** tool, see [Using “System Information” Function](#)(see page 1108).

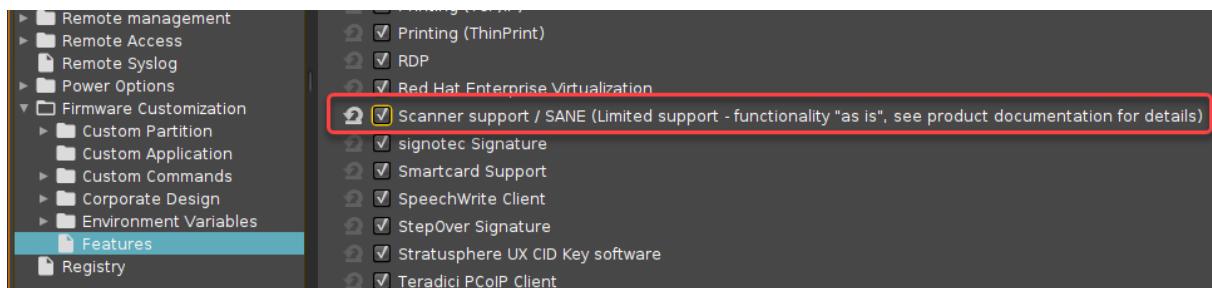
For a device exception rule, use the [SpaceMouse Guide](#)(see page 243).

For more information about USB redirection rules at the client, see the documentation of the respective receiver.

### 2.3.4 Citrix Fabulatech Scanner Redirection

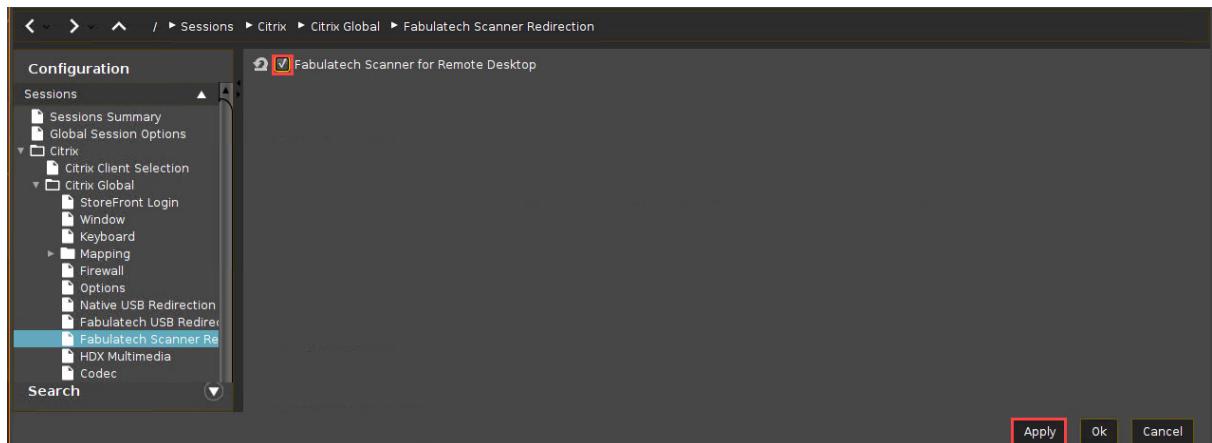
#### Enabling Fabulatech Scanner Redirection

1. In the IGEL Setup, go to **System > Firmware Customization > Features** and make sure that **Scanner support /SANE (Limited support - functionality "as is", see product documentation for details)** is activated.



- If the option is already activated, continue with step 2.
- If the option has not been activated before, the software component must be downloaded first. For this purpose, make sure that the source of the current firmware is set correctly:
  - If you are using Universal Firmware Update, make sure that the device is assigned to the current firmware. For details, see [Universal Firmware Update<sup>129</sup>](#) and [Assigning Updates<sup>130</sup>](#).
  - If you are not using Universal Firmware Update, make sure that **System > Update > Firmware Update** is set to the source of the current firmware. For details, see [Firmware Update](#)(see page 1252).
- After clicking **OK** to confirm your changes, you must reboot the system.

2. In the IGEL Setup, go to **Sessions > Citrix > Citrix Global > Fabulatech Scanner Redirection**.
3. Check **Fabulatech Scanner for Remote Desktop**.



4. Click **Apply** or **Ok** to confirm the settings.

### 2.3.5 Mapping USB Storage Media into Citrix Sessions

How to configure USB storage mapping so that users can access USB storage media attached to the IGEL OS device within Citrix sessions?

<sup>129</sup> <https://kb.igel.com/display/endpointmgmt607/Universal+Firmware+Update>

<sup>130</sup> <https://kb.igel.com/display/endpointmgmt607/Assigning+updates>



The mapping of USB storage devices is possible for "USB mass storage class" devices. The storage of smartphones and digital cameras is usually accessed via the MTP protocol. Mobile device access via MTP is available with IGEL Linux 10.04.100 or higher; for more information see the how-to [Using Mobile Device Access](#)(see page 692).

## Basic Configuration of the Client

Within the IGEL Setup or a UMS profile, you basically need to configure these parameters:

- ▶ Activate **Devices > Storage Devices > Storage Hotplug > Client drive mapping > Dynamic**. This option activates dynamic client drive mapping. It automatically recognizes new storage media as they are connected to the endpoint device. The endpoint device beeps and shows a notification while it mounts the new device. The storage devices automatically become usable on the endpoint and in Citrix ICA Sessions.

Mounted devices need to be unmounted before they are removed to ensure data integrity. This can be done via the [Disk Utility](#)(see page 1109), the [Disk Removal](#)(see page 1112) tool, or a tray icon.

## Additional Parameters to Check

- ▶ The following parameters are set by default, thus storage mapping will work, but maybe for some reason you have changed these and need to adjust them to allow the storage mapping:

**Sessions > Citrix > Citrix Global > Mapping > Drive mapping** (set checkmark)

**Sessions > Citrix > Citrix Global > Native USB Redirection > Native USB redirection** (remove checkmark)

**Sessions > Citrix > Citrix Global > Fabulatech USB Redirection > Fabulatech USB redirection** (remove checkmark)



**Devices > USB access control > Enable** (remove checkmark)

**Sessions > RDP > RDP Sessions > [session name] > USB Redirection > Enable Native USB Redirection** (set to **Global setting**)

**Sessions > RDP > RDP Sessions > [session name] > Mapping > Enable Drive Mapping** (set to **Global setting**)

### Assigning a Drive Letter within the Session (Optional)

- ▶ In case you not only want to see the drive in the session as e.g. "A on IGEL-123456789", but want to address the drive with a real drive letter within the session, you may run one of these commands:

subst T: \\tsclient\t

or

net use T: \\tsclient\t

In this example, "T on IGEL-123456789" is assigned to drive letter T: within the session. You may also assign the mapped drive to another drive letter than is used in its name.

### Configuration on the Server Side

On the server side, e.g. with Windows Server 2008R2, a user in the group "Users" with access to the terminal server will have the mapping default. This is true for a newly installed server. But the mapping can be prevented by changing the policies:

**Do not allow drive redirection** specifies whether to prevent the mapping of client drives in a Remote Desktop Services session (drive redirection). By default, an RD Session Host server maps client drives automatically upon connection. Mapped drives appear in the session folder tree in Windows Explorer or Computer in the format [driveletter] on [computername]. You can use this setting to override this behavior." Source: <https://technet.microsoft.com/de-de/library/ee791794%28v=ws.10%29.aspx>

## 2.3.6 Auto-Hide Toolbar in Appliance Mode

### Environment

IGEL Linux v5.x or newer

### Problem

In the appliance mode, the toolbar at the top of the screen is permanently displayed.

You want to configure the toolbar to hide automatically after it loses the focus of the mouse pointer.

### Solution

1. In IGEL Setup, go to **System > Registry > userinterface.igel\_toolbar.show\_always\_in\_appliance\_mode**.



2. Disable **Show toolbar always in appliance mode**.
3. Click **Ok** to save the changes.

For the changes to take effect, you need to restart active appliance mode sessions.

### 2.3.7 Create a Seamless, Transparent User Experience with Appliance Mode

With appliance mode, you can confine a device to a specific session. In appliance mode, the device itself fades in the background, and the session is presented to the user in the most straightforward way. The user will not have to deal with a Linux desktop, multiple login procedures, switching between windows, or device configuration.

Use the appliance mode to allow access only to one specific session. On device startup, the user is directed immediately to the login screen of the virtual desktop.

The appliance mode can be applied to the following session types:

- VMware Horizon
- Citrix Self-Service (for published desktops only, not for published applications)
- RHEV/Spice
- Imprivata
- RDP MultiPoint Server
- XDMCP for this display

To configure a session that runs in appliance mode:

1. Open the setup and go to **Sessions > Appliance mode**.
2. Choose the session type of the desired session using the drop-down menu **Appliance mode**.
3. Configure your appliance mode session as appropriate.

For further information, see the manual chapter [Appliance Mode](#)(see page 869).

### 2.3.8 Connecting to a Citrix Farm

By connecting a Citrix farm, your data and applications are kept centrally on a Citrix farm. Applications must now be delivered instantly to users anywhere on any device.

There are several ways of connecting to a Citrix farm and starting sessions. We describe three best practice variants below:

- [Citrix StoreFront](#)(see page 253): Integrates published applications into the IGEL GUI.
- [Citrix Self-Service](#)(see page 253): Users will be directed to a web interface where they will find pre-defined published applications and they will be able to add more published applications the server provides.
- [Appliance Mode](#)(see page 255): Shows only the web interface of the farm and hides the IGEL GUI completely.



## Citrix StoreFront

Prerequisites:

- Trust root certificate in directory /wfs/ca-certs (see [Deploying Trusted Root Certificates](#)(see page 470))

Connecting via **StoreFront**:

1. Click **Sessions** in the configuration tree of the IGEL setup.
2. Click **Citrix > Citrix StoreFront > Server**.
3. Click the **ADD** icon in the **Server location** window.  
The **ADD** mask opens.
4. Enter the names or IP addresses of the services sites.
5. Confirm with **OK**.
6. Click **Citrix StoreFront > Desktop Integration**.
7. Enter "Citrix Storefront" under **Login Session Name**.
8. Choose **Desktop** as the starting method.
9. Click **OK** to save the changes.  
Setup closes.
10. Doubleclick the Citrix icon on the desktop.  
The login window opens.
11. Enter the credentials of a user in the login window.  
The published applications of the Citrix farm will appear on the desktop.
12. Doubleclick an application icon on the desktop to start the program.

## Citrix Self-Service

Prerequisites:

- Trust root certificate in directory /wfs/ca-certs (see [Deploying Trusted Root Certificates](#)<sup>131</sup>)

Connecting via **StoreFront**:

1. Click **Sessions** in the configuration tree of the IGEL setup.
2. Click **Citrix > Citrix Self-Service > Server**.
3. Enter the **Server**, the **Path to Store** and the **Store name** of the services sites.
4. Confirm with **OK**.
5. Click **Citrix Self-Service > Desktop Integration**.
6. Enter "Citrix Self-Service" under **Login Session Name**.
7. Choose **Desktop** as the starting method.
8. Click **OK** to save the changes.  
Setup closes.
9. Doubleclick the Citrix icon on the desktop.  
The login window opens.

---

<sup>131</sup> <https://kb.igel.com/display/igelos1005/Deploying+Trusted+Root+Certificates>



10. Enter the credentials of a user in the login window.  
The published application icons of the Citrix farm will appear in the Self-Service UI.
11. Doubleclick an application icon to start the program.

#### Using Citrix Self-Service

1. Start **Citrix Self-Service** e.g. with desktop icon.
2. Log on to the server.
3. Add published applications to the list (+-button on the left).
4. Click a published application to start.
5. Use the search bar to find a published application.
6. Use the user's menu to change preferences, server etc.

The screenshot shows the Citrix Self-Service interface. At the top, there is a header bar with the IGEL logo, a Quality Assurance XenServer 7.15 LTSR badge, and navigation buttons for FAVORITEN, DESKTOPS, and APPS. Below the header, a search bar contains the text "Alle Apps durchsuchen". The main area is titled "Alle Apps" and displays a grid of nine published applications:

Icon	Name	Details
	Access 2013 - SRV1	<a href="#">Details</a>
	Calculator - SRV2	<a href="#">Details</a>
	Citrix HDX Monitor	<a href="#">Details</a>
	Excel 2013 - SRV1	<a href="#">Details</a>
	Internet Explorer 11 - SRV2	<a href="#">Details</a>
	Media Player - SRV2	<a href="#">Details</a>
	Notepad - SRV2	<a href="#">Details</a>
	Outlook 2013 - SRV1	<a href="#">Details</a>
	Paint - SRV2	<a href="#">Details</a>
	PowerPoint 2013 - SRV1	<a href="#">Details</a>
	Publisher 2013 - SRV1	<a href="#">Details</a>
	Skype for Business 2015	<a href="#">Details</a>

- [Configure Full-Screen Mode\(see page 255\)](#)



## Configure Full-Screen Mode

Use following parameter in your Custom Command script to activate the full-screen mode for *Citrix Self-Service*:

► \$ICADIR/storebrowse -c FullscreenMode=[0/1/2]

With following options:

- 0 = The window is not displayed full-screen
- 1 = The window is displayed full-screen
- 2 = The window is displayed maximized and undecorated, which does not mask the desktop environment's taskbar

## Appliance Mode

Connecting Citrix via Selfservice:

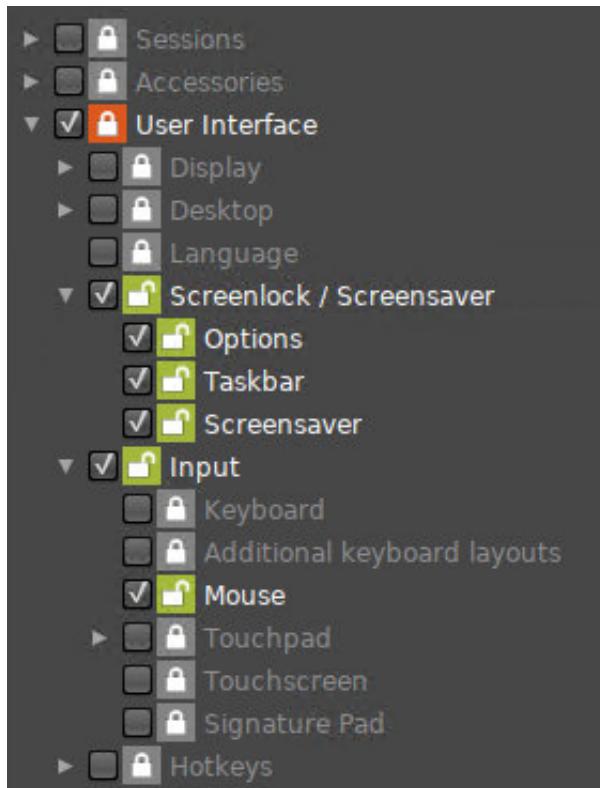
1. Click **Sessions > Appliance Mode** in the configuration tree of the IGEL setup.
2. Select **Citrix Self-Service** under **Appliance mode**.
3. Enter the **URL** of the delivery server.
4. Click **OK** to save the changes and close setup.
5. Follow the instructions on the screen.

### 2.3.9 Create a Self-Service Setup for the User with Quick Settings

Usually, the user should not have full access to the thin client's setup. However, it may prove useful to enable users to quickly change certain settings by themselves, without even needing a password. Typical examples are settings for keyboard, mouse, or screen. This can be done using the **Quick Settings**.

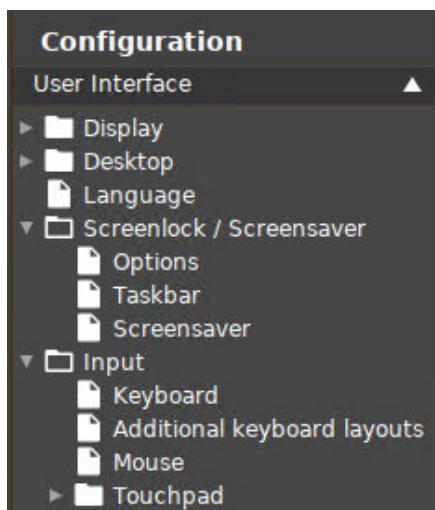
Here is how to select setup pages for quick setup:

1. Open the setup and go to **Accessories > Quick Settings > Setup User Permissions**.
2. Select the setup pages to which the user should have access, e. g. **User Interface > Input > Mouse**, or **Screenlock / Screensaver**.



3. Click **Apply** or **Ok**.

When the user starts **Quick Settings**, the previously selected options are presented.



Quick settings set permissions for setup screens. If you want to set permissions for individual parameters, you can use UMS profiles. For more information, see [Profiles<sup>132</sup>](#).

---

<sup>132</sup> <https://kb.igel.com/display/endpointmgmt604/Profiles>



## 2.3.10 Login Failed because of the Expired AD Password

### Problem

When you try to log in to a native **Citrix Storefront** session, you get the error message "Login Failed!" because your Active Directory password expired.

You are unable to change your password, because the local login does not provide an option for that.

Before you follow these instructions, check that the ports are open, maybe you can fix the problem by that:

- Login to Client -> Port: 88
- Change password -> Port: 464

Here you find an overview of ports of the domain controller: [Required Ports to Communicate with Domain Controller<sup>133</sup>](#)

### Solution

Enable **Active Directory/Kerberos** authentication for the **Storefront** session. The next time you try to log in to IGEL OS, you will be prompted to change your expired password.

### Changing an Expired Active Directory Password

When using sessions with passthrough authentication, it is essential that you lock your device's screen when leaving it unattended.

#### Enabling Active Directory/Kerberos Authentication for Storefront Sessions

1. In IGEL setup, go to **Security > Login > Active Directory/Kerberos**.
2. Enable **Login to Active Directory domain**.
3. Go to **Security > Active Directory/Kerberos**.
4. Activate **Enable**.
5. Fill in the **Default domain (fully qualified domain name)**.
6. Go to **Sessions > Citrix > Citrix Storefront > Login**.
7. Enable **Use passthrough authentication**.
8. Click **Apply** or **Ok**.

<sup>133</sup> <https://social.technet.microsoft.com/Forums/windows/en-US/1c6a59de-c1fe-4946-bb4e-1fe36fd40b08/required-ports-to-communicate-with-domain-controller?forum=winserverDS>



Please note that the client must now be locked locally and no longer in the session to prevent another person from entering the session via the passthrough without specifying the password.

## Enabling Screenlock

1. In the IGEL setup go to **User Interface > Screenlock / Screensaver**.
2. Enable **Use hotkey**.
3. Under **Modifiers** select Win.
4. Under **Hotkey** enter "L".
5. Go to **User Interface > Screenlock / Screensaver > Options**.
6. Enable **User password**.

So the "Win + L" hotkey locks the IGEL client instead of the session desktop.

The AD password must be entered to activate the IGEL clients.

### 2.3.11 Configuring Auto Logon for Citrix Virtual Desktops

This how-to describes how to configure Auto Logon for Citrix Virtual Desktops.

#### Steps

1. In IGEL Setup, go to **Sessions > Citrix > Citrix StoreFront > Server**.

Server location			
Protocol	Store address	Path to Store	Store name

2. Add your **Server Location**.



**Configuration**

Sessions

- Sessions Summary
- Global Session Options
- Citrix
  - Citrix Client Selection
  - Citrix Global
  - Citrix StoreFront
    - Server
    - Login
    - Appearance
    - Reconnect
    - Refresh
    - Logoff
    - Desktop Integration
  - Citrix Self-Service
- RDP

**Server location**

Protocol	Store address	Path to Store	Store name

**Add**

Citrix Store site address	: 443	Path to Store
https://		Citrix/Store
Store name		

**Ok**   **Cancel**

3. Add your Active Directory domain to **Domains**, making sure that you use its Fully Qualified Domain Name (FQDN).

**Configuration**

Sessions

- Sessions Summary
- Global Session Options
- Citrix
  - Citrix Client Selection
  - Citrix Global
  - Citrix StoreFront
    - Server
    - Login
    - Appearance
    - Reconnect
    - Refresh
    - Logoff
    - Desktop Integration
  - Citrix Self-Service
  - RDP
  - Horizon Client
  - Appliance Mode
  - Evidian AuthMgr
  - NoMachine NX Client
  - X Sessions
  - Parallels Client
  - IBM iAccess Client
  - ThinLinc
  - SSH
  - VNC Viewer

**Server location**

Protocol	Store address	Path to Store	Store name

**Domains**



Handling of domain in login window: normal



**Add**

Domain

**Ok** **Cancel**

4. Go to **Sessions > Citrix > Citrix StoreFront > Login**.

The screenshot shows the 'Configuration' interface with the following navigation path selected: Sessions > Citrix > Citrix StoreFront > Login. The 'Login' option is highlighted with a red box. On the right, the 'Authentication type' dropdown is set to 'Password authentication'. Other settings include 'User name', 'Password', 'Domain', and several checkboxes for 'Remember user name and domain', 'Synchronize Citrix password with screenlock', 'Relaunch Citrix login after logoff', and 'Start a single published application automatically'. A 'Start following applications automatically after server connection is established' section is also visible.

5. Set **Authentication type** to **Password authentication**.

This screenshot shows the 'Authentication type' configuration screen. The 'Password authentication' dropdown is highlighted with a red box. The 'Only for Citrix StoreFront' section contains options for 'Use passthrough authentication' and 'Auto login'. Below these are fields for 'User name', 'Password', and 'Domain'.

6. Activate **Auto Login**.



Authentication type: Password authentication

**Only for Citrix StoreFront**

Use passthrough authentication  
 Auto login

User name: [Redacted]

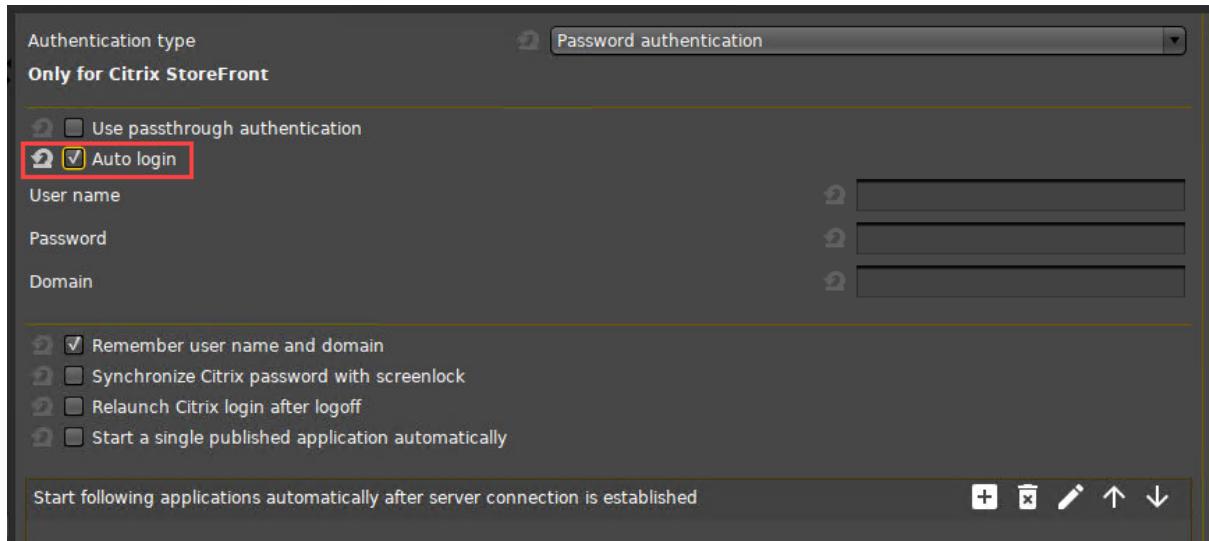
Password: [Redacted]

Domain: [Redacted]

Remember user name and domain  
 Synchronize Citrix password with screenlock  
 Relaunch Citrix login after logoff  
 Start a single published application automatically

Start following applications automatically after server connection is established

[+ X P ↑ ↓]



7. Set **User Name** to the Active Directory user name.

Authentication type: Password authentication

**Only for Citrix StoreFront**

Use passthrough authentication  
 Auto login

User name: [Redacted]

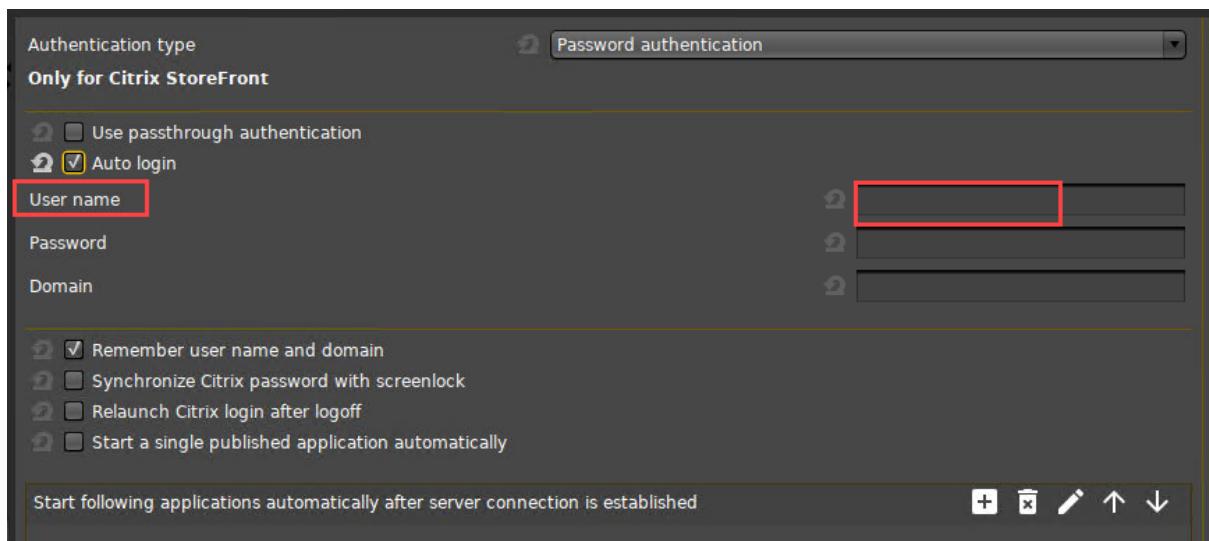
Password: [Redacted]

Domain: [Redacted]

Remember user name and domain  
 Synchronize Citrix password with screenlock  
 Relaunch Citrix login after logoff  
 Start a single published application automatically

Start following applications automatically after server connection is established

[+ X P ↑ ↓]



8. Set the **Password**.

A screenshot of a software interface for configuring Citrix authentication. At the top, it says "Authentication type: Password authentication". Below that, it says "Only for Citrix StoreFront". Under "User name", there is a "Password" field which is highlighted with a red box. Under "Domain", there is a "Domain" field which is also highlighted with a red box. There are several checkboxes for options like "Remember user name and domain", "Synchronize Citrix password with screenlock", "Relaunch Citrix login after logoff", and "Start a single published application automatically". At the bottom, there is a button bar with icons for adding, deleting, editing, and sorting.

9. Set **Domain** to your Active Directory domain's FQDN, the same as in step 3.

A screenshot of the same software interface as the previous one. The "Domain" field is highlighted with a red box. The rest of the interface is identical to the first screenshot, including the "Authentication type", "User name", "Password", and various checkboxes.

### 2.3.12 Force Citrix Logout Using Hotkey

You will find the instructions under [Citrix: Freeze at Logout](#)(see page 263).

This page is due for deletion. Please check the above link and use it in the future.



### 2.3.13 Citrix: Freeze at Logout

#### Symptom

A user tries to log out from a Citrix session but the session does not respond.

Example: Once you connect to a Citrix session, everything works. After having reconnected and disconnected several times, you log out. The window freezes while the logout screen is shown.

#### Solution

- ▶ Go to **Sessions > Citrix > Citrix Global > Options > HDX Adaptive Transport over EDT** and select **TCP only - UDP disabled**. (Default as of 11.06.100)

OR

- ▶ Try to use another Citrix Receiver version: **Sessions > Citrix > Citrix Client Selection > Citrix client version**.

OR

- ▶ Troubleshoot the issue with your Citrix infrastructure to discover why the session is not closing when the wfica process makes the call for disconnection.

#### Workaround

As a less recommended alternative, you can configure a hotkey to force a logout in such situations. Note, however, that this workaround can cause issues with hung sessions on the Citrix servers.

To configure a logout hotkey:

1. In IGEL Setup, go to **System > Firmware Customization > Custom Application**.
2. Click **[+]** to create a new **Custom Application** and name it e.g. "Kill Citrix Sessions".
3. Disable all **Starting Methods** for this session.
4. Enable **Hotkey**.
5. Choose e.g. Ctrl|Alt as **Modifiers** and define C (for "Citrix) as **Key**.
6. Go to **System > Firmware Customization > Custom Application > Kill Citrix Sessions > Settings**.
7. Enter an **Icon name**.
8. Enter /tmp/kill\_citrix as **Command**.
9. Go to **System > Firmware Customization > Custom Commands > Desktop**.
10. In the field **Desktop initialization** enter following command in one line:  
`echo -e "#! /bin/bash\n\nps -eo comm,pid | grep ^wfica | while read c p\ntail; do echo \$p; done | xargs -r kill -TERM" >/tmp/kill_citrix; chmod 755 /tmp/kill_citrix`
11. Click **Apply** and reboot the device.



To configure the hotkey for a group of devices, you can alternatively create a profile or use this one: [profile\\_KillCitrixSessionsViaHotkey.xml](#)<sup>134</sup>.

Here you can learn how to import a profile: [Importing a Profile and Firmware](#)<sup>135</sup>.

### 2.3.14 Warning Message: [Citrix Store] Could Not Connect to the Citrix Server

#### Environment

- You are using Citrix Receiver 13.0.x or newer.
- You have a session of the type Citrix StoreFront configured.

#### Symptom

- When establishing the connection, a warning message appears:  
Warning: [Citrix Store] Could not connect to the Citrix server.

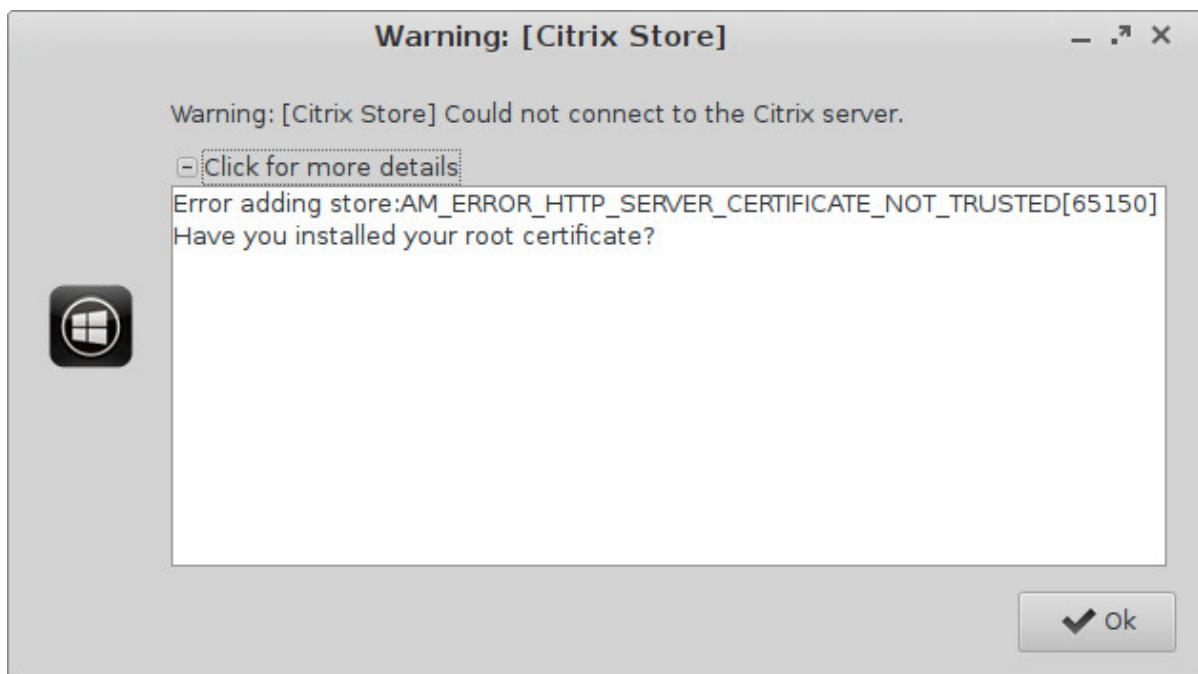


or

---

<sup>134</sup>[https://kb.igel.com/download/attachments/49587129/profile\\_KillCitrixSessionsViaHotkey.xml?  
api=v2&modificationDate=1557987932486&version=1](https://kb.igel.com/download/attachments/49587129/profile_KillCitrixSessionsViaHotkey.xml?api=v2&modificationDate=1557987932486&version=1)

<sup>135</sup><https://kb.igel.com/display/endpointmgmt604/Importing+a+Profile+and+Firmware>



## Problem

Citrix Receiver 13.0.x or newer on Linux only supports connections via HTTPS, and you have to make sure the device has a valid root certificate of the Certificate Authority (CA) available. If the root certificate is missing, the connection will fail.

## Solution

Install an appropriate root certificate on the device to allow HTTPS connections to your Citrix Server.

For information on how to distribute the certificate, see [Deploying Trusted Root Certificates](#)(see page 470).

### 2.3.15 Setting up Citrix Sessions with Hardware-Accelerated H.264 Deep Compression Codec

This document describes how to activate a hardware-accelerated H.264 deep compression codec for Citrix sessions.

#### Prerequisites

- Licensed IGEL Multimedia Codec Pack
- IGEL UD device offering hardware video acceleration, see the FAQ [Hardware Video Acceleration on IGEL OS](#)<sup>136</sup>.
- Citrix XenApp / XenDesktop server with active H.264 display mode  
See <http://support.citrix.com/article/CTX200370> to learn how to determine the display mode.

<sup>136</sup> <https://kb.igel.com/display/igelos/Hardware+Video+Acceleration+on+IGEL+OS>



## Activating the Codec

1. In Setup, go to **System > Firmware Customization > Features**.
2. Enable **Hardware Video Acceleration**.
3. Go to **Sessions > Citrix > Citrix Client Selection**.
4. Select the **Citrix Client Version**.
5. Go to **Sessions > Citrix > Citrix Global > Codec**.
6. Set **Graphical Codec** to **H.264 Deep Compression Codec**.
7. Enable **Accelerated H.264 Deep Compression Codec**.

Known issues on VIA-based IGEL devices UD3-LX 40/41/42 and UD10-LX:

- Hardware-accelerated HDX only works with 256 MB video memory or more. Video memory must be adjusted in the system BIOS. The default is 128 MB.
- Seamless window mode is not supported.
- Desktop sessions spanning 2 monitors are not supported.
- Desktop sessions on rotated screens may flicker (depending on the screen resolution).

If you use the **Citrix Receiver 13.5** or older in combination with a **Citrix Server 7.15**, the **Always Lossless** option for the **Visual Quality** policy will not work under Linux.

With IGEL Linux version 10.05.100 the **Build to Lossless** option for the **Visual Quality** policy will work on the condition that you are using **Citrix Receiver 13.6** or younger and the **Use Video Codec** policy is set to **For actively changing regions**.

### 2.3.16 Using Font Smoothing (ClearType) in Citrix Sessions

#### Symptom

- You have set **Font Smoothing** to *ClearType* in  
**IGEL Setup > Sessions > Citrix > Citrix Global > Window > Font smoothing (Off / Standard / ClearType)**
- *ClearType* does not work for *Citrix PNAgent / Webinterface* sessions.

#### Problem

*ClearType* is not supported in *PNAgent / Webinterface* sessions because *Citrix Receiver* uses *Windows* settings which are not present on the Linux client.

#### Solution

All *Citrix Receivers* up to version 12.x do not use *wfclient.ini* to configure **Font Smoothing**. To force *Webinterface, PNAgent/XenApp* to enable **Font Smoothing** proceed as follows:



*PNAgent / XenApp:*

1. On the Citrix server open C:\inetpub\wwwroot\citrix\pnagent\config\default.ica .
2. Go to section **Application** .
3. Add new line FontSmoothingType=3 .
4. Save and close the file.

*Webinterface:*

1. On the Citrix server open C:\inetpub\wwwroot\citrix\xenapp\config\default.ica .
2. Go to section **Application** .
3. Add new line FontSmoothingType=3 .
4. Save and close the file.

If you installed the *Webinterface* site to a different location, please change the path accordingly.

**FontSmoothingType** parameter options:

- 0 = No smoothing
- 1 = No smoothing
- 2 = Standard smoothing
- 3 = *ClearType* (horizontal sub-pixel) smoothing (default)

#### Legal Note

IGEL's [Terms & Conditions](#)<sup>137</sup> apply.

### 2.3.17 Highly Secured XenServer has Problems with LD\_BIND\_NOW Workaround

#### Problem

You want to launch multiple desktop sessions with RTME and H.264 acceleration, but it doesn't work.

#### Solution

1. In **IGEL Setup**, go to **System > Registry > ica > workaround-dual-rtme** (Search parameter: **ica.workaround-dual-rtme**)
2. Enable **Activate workaround for dual RTME sessions and H264 acceleration**.
3. Click **Apply** or **Ok** to save the changes.

---

<sup>137</sup> <https://www.igel.com/terms-conditions/>



This registry key should not be used if "Enable Secure ICA" is active for the specific delivery group. You have to decide if you want to use the registry key or to reduce security.

### 2.3.18 Workaround for Citrix Receiver X Error

#### Problem

When starting Citrix XenApp you get the following Citrix Receiver errors on your IGEL OS devices:

The X Request 55.0 caused error: "9: BadDrawable (invalid Pixmap or Window parameter)"

The X Request 60.0 caused error: "13: BadGC (invalid GC parameter)".

#### Environment

- Citrix XenApp 7.15
- Citrix Receiver e.g. 13.2, 13.3, 13.7, 13.8

#### Solution

Two parameters have to be activated in IGEL Setup:

1. Go to **System > Registry > ica > forceignoreerrors**.
2. Activate **Suppress X error message boxes**.
3. Go to **System > Registry > ica > wfclient > ignoreerrors**.
4. Activate **IgnoreXErrors** and pass the parameters: **55.0/9, 60.0/13**

See also the corresponding entry in the [Citrix forum](#)<sup>138</sup>.

### 2.3.19 Citrix HTML5 Receiver Issue

#### Affected Versions

- IGEL OS 10.05.100 or higher
- IGEL OS 11.01.100 or higher

#### Issue

Due to the abolition of plugin technology in Firefox 60+, the Workspace app installed under Linux is no longer automatically recognized.

---

<sup>138</sup> <https://discussions.citrix.com/topic/393872-possible-workaround-citrix-receiver-x-error-on-linux-thin-clients/>



## Solution

1. If your device has IGEL OS 10.05, update to IGEL OS 10.06; if applicable, you can also upgrade to IGEL OS 11.02. If your device has IGEL OS 11.01, update to IGEL OS 11.02.  
IGEL OS 10.06 and IGEL OS 11.02 have been adapted for a workaround that requires server-side modifications.
2. Change the server-side settings according to the instructions under <https://support.citrix.com/article/CTX237727>.

### 2.3.20 Macbook Keyboard Layout inside Citrix Session

To get the Macbook keyboard layout working correctly inside Citrix sessions, proceed as follows:

1. Under **Sessions > Citrix > Citrix Global > Keyboard > Keyboard mapping file**, select "Linux".
2. Under **User Interface > Input > Keyboard > Keyboard type**, select "Macbook".  
All other keyboard layout settings can be left unchanged, i.e. as set by default.

In order to type special characters like € and #, use the right-hand Alt/Option key, not the left-hand key.

### 2.3.21 Citrix Feature Matrix

According to the details provided by the vendor, the following Citrix Client features are supported with Citrix Workspace App 2009:

For details on the Citrix Clients that are built into your version of IGEL OS, see [IGEL OS Release Notes\(see page 1422\)](#) > Notes for Release [your version] > Component Versions [your version].

See also the original document at [https://www.citrix.com/content/dam/citrix/en\\_us/documents/data-sheet/citrix-workspace-app-feature-matrix.pdf](https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-workspace-app-feature-matrix.pdf).

Category	Feature	Supported
Citrix Workspace	Citrix Virtual Apps	yes
	Citrix Virtual Desktops	yes
	Citrix Content Collaboration (Citrix Files)	no
	Citrix Access Control Service	no
	Citrix Workspace Browser	no
	SaaS/Webapps with SSO	yes



Category	Feature	Supported
	Citrix Mobile Apps	no
	Intelligent Workspace features	no
Endpoint Management	Auto configure using DNS for Email Discovery	no
	Centralized Management Settings	yes
	App Store Updates / Citrix Auto updates	no
UI	Desktop Viewer/Toolbar	yes
	Multi-tasking	yes
	Follow Me Sessions (Workspace Control)	yes
HDX Host Core	Adaptive transport	yes
	SDWAN support	yes
	Session reliability	yes
	Auto-client Reconnect	yes
	Bi-directional Content redirection	no
	URL redirection	yes
	File open in Citrix Workspace app	yes
	Browser content redirection	yes
	Multiport ICA	yes
HDX IO / Devices / Printing	Local Printing	yes
	Generic USB Redirection	yes
	Client drive mapping / File Transfer****	yes



Category	Feature	Supported
HDX Integration	Local App Access	no
	Multi-touch	no
	Mobility Pack	no
	HDX Insight	yes
	HDX Insight with NSAP VC	yes
	EUEM Experience Matrix	yes
	Session Sharing	yes
HDX Multi-media	Audio Playback	yes
	Bi-directional Audio (VoIP)	yes
	Web-cam redirection	yes
	Video playback	yes
	Flash redirection	yes
	Microsoft Teams Optimization	yes
	Skype for business Optimization pack	yes
	Cisco Jabber Unified Communications Optimization	yes
	Windows Multimedia redirection	yes
	UDP Audio	yes (not with NSG)
Security	TLS 1.2	yes
	TLS 1.0/1.1	yes
	DTLS 1.0	yes



Category	Feature	Supported
	DTLS 1.2	no
	SHA2 Cert	yes
	Smart Access	yes
	Remote Access via Citrix Gateway	yes
	Workspace for Web Access	yes
	IPV6	yes
HDX Graphics	H.264-enhanced SuperCodec	yes
	Client hardware acceleration	yes
	3DPro Graphics	yes
	External Monitor Support	yes
	Desktop Composition redirection	no
	True Multi Monitor	yes
	Location Based Services (Location available via API-description)	no
Authentication	Federated Authentication (SAML/Azure AD)	yes
	NetScaler Full VPN	yes
	RSA Soft Token	no
	Challenge Response SMS (Radius)	no
	User Cert Auth via NetScaler Gateway (via Browser Only)	no
	Smart Card (CAC,PIV Etc.)	yes
	Proximity/Contactless Card	yes
	Credential insertion (E.g.. Fast Connect, Storebrowse)	yes
	Pass Through Authentication	no
	Save credentials *(on prem and only SF)	no
	NetScaler nFactor Authentication	yes



Category	Feature	Supported
	Netscaler Native OTP	yes
	Biometric Authentication (Touch ID, Face ID..)	no
	Single Sign-On to Citrix Files App	no
	Single Sign on to Citrix Mobile apps	no
	Anonymous Store Access	yes
Keyboard Enhancements	Dynamic Keyboard Layout Synchronization with Windows VDA  Note: Dynamic keyboard layout sync for non-Windows receivers requires enablement of the Unicode Keyboard Layout Mapping feature on the Windows VDA.	yes
	Unicode Keyboard Layout Mapping with Windows VDA	yes
	Client IME Enhancements with Windows VDA	no
	Language Bar Show/Hide with Windows VDA Applications	no
	Option Key mapping for server-side IME input mode on	no
	Windows VDA	
	Dynamic Keyboard Layout Synchronization with Linux VDA	
	Client IME Enhancements with Linux VDA	no
	Language Bar support for Linux VDA Applications	yes

### 2.3.22 Using Lync / Skype for Business with Citrix HDX RealTime Optimization Pack

#### Issue

You want to use Microsoft Lync or Skype for Business via a Citrix session with IGEL OS devices.

#### Solution

IGEL OS comes with Citrix HDX RealTime Media Engine (RTME) preinstalled: Setup > **Sessions > Citrix > Citrix Global > Unified Communications > Skype for Business**. See also [HDX Multimedia](#)(see page 792).



- IGEL OS 11.04.100 contains RTME 2.9 (activated by default).
  - IGEL OS 11.02.100 and higher contains RTME 2.8 (activated by default).
  - IGEL OS 11.01.100 contains RTME 2.7 (disabled by default).
- 
- IGEL OS 10.06.100 contains RTME 2.8 (disabled by default).
  - IGEL OS 10.05.500 contains RTME 2.6 (disabled by default).
  - IGEL OS 10.05.100 contains RTME 2.6 (disabled by default).

For further information, see [Citrix HDX RealTime Optimization Pack<sup>139</sup>](#).

## 2.4 RDP

- [Mapping USB Storage Media into RDP Sessions](#)(see page 274)
- [What Is the String for Token-Based Load Balancing?](#)(see page 276)
- [RDP Fabulatech Scanner Redirection](#)(see page 277)
- [RDP RemoteApp Parameter Settings](#)(see page 278)
- [RDP Performance Enhancements](#)(see page 279)
- [RDP Session playing Sound: Error RDPSND\\_NEGOTIATE](#)(see page 280)
- [Crackling and Audio Dropouts in RDP Sessions](#)(see page 281)
- [Login Failed Because of Expired AD Password](#)(see page 282)
- [User Has to Provide Credentials Twice for RDP Logon](#)(see page 283)

### 2.4.1 Mapping USB Storage Media into RDP Sessions

How to configure USB Storage mapping so that users can access USB storage media attached to the IGEL LX Client within RDP sessions?

Solution:

The mapping of USB storage devices is possible for "usb mass storage class" devices. The storage of smartphones and digital cameras is usually accessed via the MTP protocol. Mobile device access via MTP is available with IGEL Linux 10.04.100 or higher; for more information see the how-to [Using Mobile Device Access<sup>140</sup>](#).

<sup>139</sup> <https://docs.citrix.com/en-us/hdx-optimization/>

<sup>140</sup> <https://kb.igel.com/display/igelos1005/Using+Mobile+Device+Access>



## Basic Configuration of the Client

Within the IGEL Setup or an UMS profile you basically need to configure these parameters:

- ▶ Activate **Devices > Storage Devices > Storage Hotplug > Client drive mapping > Dynamic**. This option activates dynamic client drive mapping. It automatically recognizes new storage media as they are connected to the thin client. The thin client beeps and shows a notification while it mounts the new device. The storage devices automatically become usable on the thin client and in Citrix ICA Sessions.

Mounted devices need to be unmounted before they are removed to ensure data integrity. This can be done via the **Disk Utility**, the new **Safely Remove Hardware** Tool or a tray icon.

## Additional Parameters to Check

- ▶ The following parameters are set by default, thus storage mapping will work, but maybe for some reason you have changed these and need to adjust them to allow the storage mapping:

**Sessions > RDP > RDP Global > Mapping > Drive Mapping > Enable Drive mapping (set checkmark)**

**Sessions > RDP > RDP Global > Native USB Redirection > Enable Native USB redirection (remove checkmark)**

**Sessions > RDP > RDP Global > Fabulatech USB Redirection > Enable Fabulatech USB redirection (remove checkmark)**

**Devices > USB access control > Enable (remove checkmark)**



**Sessions > RDP > RDP Sessions > [session name] > USB Redirection > Enable Native USB Redirection (global setting)**

**Sessions > RDP > RDP Sessions > [session name] > Mapping > Enable Drive Mapping (global setting)**

Assigning a Drive Letter within the Session (Optional)

- ▶ In case you not only want to see the drive in the session as e.g. "A on IGEL-123456789", but want to address the drive with a real drive letter within the session, you may run one of these commands:

subst T: \\tsclient\t

or

net use T: \\tsclient\t

In this example "T on IGEL-123456789" is assigned to drive letter T: within the session. You may also assign the mapped drive to another drive letter than is used in its name.

## Configuration on the Server Side

On the server side, e.g. with Windows Server 2008R2, a user in the group "Users" with access to the terminal server will have the mapping default. This is true for a newly installed server. But the mapping can be prevented by changing the policies:

**Do not allow drive redirection** Specifies whether to prevent the mapping of client drives in a Remote Desktop Services session (drive redirection). By default, an RD Session Host server maps client drives automatically upon connection. Mapped drives appear in the session folder tree in Windows Explorer or Computer in the format [driveletter] on [computername]. You can use this setting to override this behavior." Source: <https://technet.microsoft.com/de-de/library/ee791794%28v=ws.10%29.aspx>

### 2.4.2 What Is the String for Token-Based Load Balancing?

#### Environment

A token-based mechanism is used as a load balancing method. This document does not apply to other load balancing methods.

#### Question

What string should be entered in **Sessions > RDP > RDP Sessions > [Session name] > Options** to make token-based load balancing work?



## Answer

IGEL OS 10.05.700 or Higher, IGEL OS 11.01.110 or Higher

- Under **Sessions > RDP > RDP Sessions > [Session name] > Options > Collection**, simply enter the name of your RDS collection. The collection name has been defined by the server administrator.

IGEL OS 10.01 to 10.05.500, 11.01.100

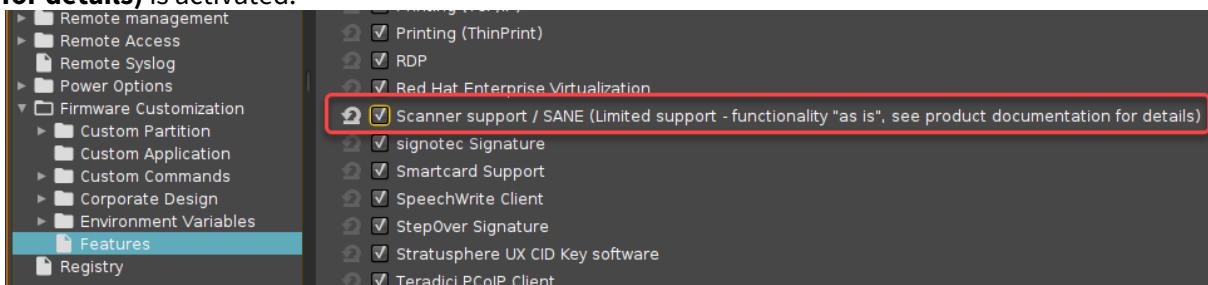
- Under **Sessions > RDP > RDP Sessions > [Session name] > Options > Load balancing routing token**, enter `tsv://MS Terminal Services Plugin.1.[collection name]`, where

- `tsv://MS Terminal Services Plugin.1.` is the routing token and
- `[collection name]` is the name of the RDS collection, defined by the server administrator.

### 2.4.3 RDP Fabulatech Scanner Redirection

#### Enabling Fabulatech Scanner Redirection

1. In the IGEL Setup, go to **System > Firmware Customization > Features** and make sure that **Scanner support /SANE (Limited support - functionality "as is", see product documentation for details)** is activated.



- If the option is already activated, continue with step 2.
- If the option has not been activated before, the software component must be downloaded first. For this purpose, make sure that the source of the current firmware is set correctly:
  - If you are using Universal Firmware Update, make sure that the device is assigned to the current firmware. For details, see [Universal Firmware Update<sup>141</sup>](#) and [Assigning Updates<sup>142</sup>](#).
  - If you are not using Universal Firmware Update, make sure that **System > Update > Firmware Update** is set to the source of the current firmware. For details, see [Firmware Update](#)(see page 1252).
- After clicking **OK** to confirm your changes, you must reboot the system.

2. In the IGEL Setup, go to **Sessions > RDP > RDP Global > Fabulatech Scanner Redirection**.

<sup>141</sup> <https://kb.igel.com/display/endpointmgmt607/Universal+Firmware+Update>

<sup>142</sup> <https://kb.igel.com/display/endpointmgmt607/Assigning+updates>



### 3. Check **Fabulatech Scanner for Remote Desktop**.



### 4. Click **Apply** or **Ok** to confirm the settings.

#### 2.4.4 RDP RemoteApp Parameter Settings

##### Symptom

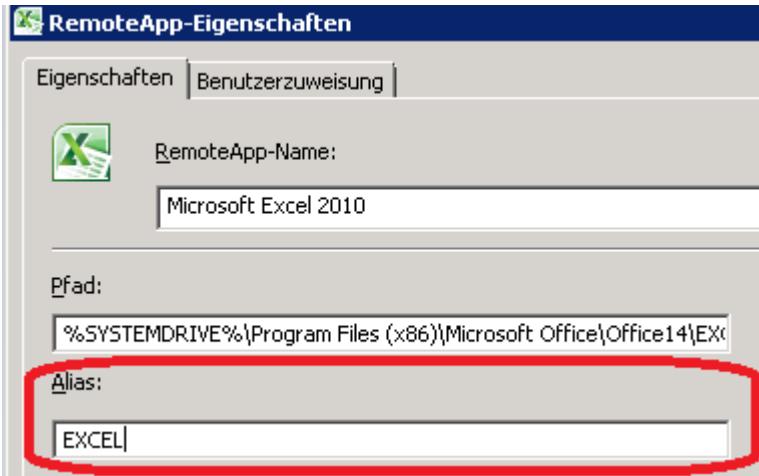
RemoteApp is not starting or closes immediately after login.

##### Problem

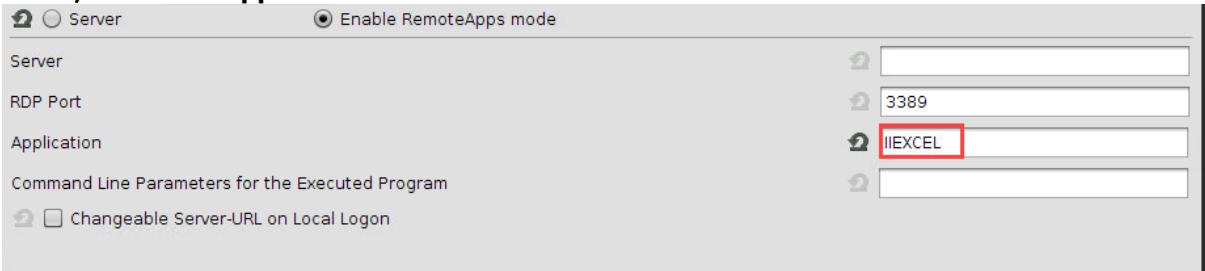
Missing or incomplete session settings on server or device

##### Solution

1. Set an ALIAS for the RemoteApp with the **RemoteApp Management Console** on the Terminalserver.



2. Use that ALIAS value in the device's setting in **Setup > Sessions > RDP > RDP Sessions > (Session Name) > Server > Application.**



Add two pipe-characters ( || ) at the beginning of the ALIAS value.

## 2.4.5 RDP Performance Enhancements

### Symptom

RDP users have performance issues (bad user experience).

For example:

- Mouse is lagging
- Screen is building up very slow
- Session uses high bandwidth
- Several other performance issues

### Problem

There are many different causes that can result in bad performance.



## Solution

The following settings can be used as a single option and also in combination.

### Basics

- The color depth should be the same on the server, the device, and in the session (best: 32 bit).
- In the BIOS, set the VGA shared memory to 64 MB or more.

### Optimizations for a LAN Environment

- Under **Sessions > RDP > RDP Global > Performance**, edit the settings as follows:
  - Disable **Compression**. (Increases performance, generates about 30% more traffic)
  - If RemoteFX 8 is available, activate **Enable RemoteFX**.
  - If RemoteFX 8 is available, set **RemoteFX codec mode** to "Optimized for LAN".
- If Windows Server 2012 R2 or lower or Windows 8.1 or lower is used: Under **Sessions > RDP > RDP Global > Multimedia**, activate **Enable Video Redirection**.

### Optimization for a WAN Environment

- Under **Sessions > RDP > RDP Global > Performance**, edit the settings as follows:
  - Enable **Compression**. (Generates about 30% less traffic, consumes more local resources)
  - If RemoteFX 8 is available, activate **Enable RemoteFX**.
  - If RemoteFX 8 is available, set **RemoteFX codec mode** to "Optimized for WAN".

## 2.4.6 RDP Session playing Sound: Error RDPSND\_NEGOTIATE

### Symptom

If the user plays some sound within the RDP session the connection terminates on some devices with error message:

```
ERROR: RDPSND: Extra RDPSND_NEGOTIATE in the middle of a session
ERROR: TCP Connection: Cannot receive data (Keep alive timeout)
```

 ERROR: RDPSND: Extra RDPSND\_NEGOTIATE in the middle of a session  
 ERROR: TCP Connection: Cannot receive data (Keep alive timeout)

### Problem

This may happen if during data transmission the connection fails.



## Solution

Try a different sound driver for RDP session:

1. Go to **System > Registry > rdp.winconnect.sound-driver**
2. Choose **OSS** or **ALSA**

### 2.4.7 Crackling and Audio Dropouts in RDP Sessions

#### Symptom

The user experience with RDP sessions is disturbed by crackling noises and glitches.

#### Environment

- Device with a sound card that has a small buffer, e. g. IGEL UD3 (M340C)
- Required for the solution: IGEL OS 11.03.500 or higher

#### Problem

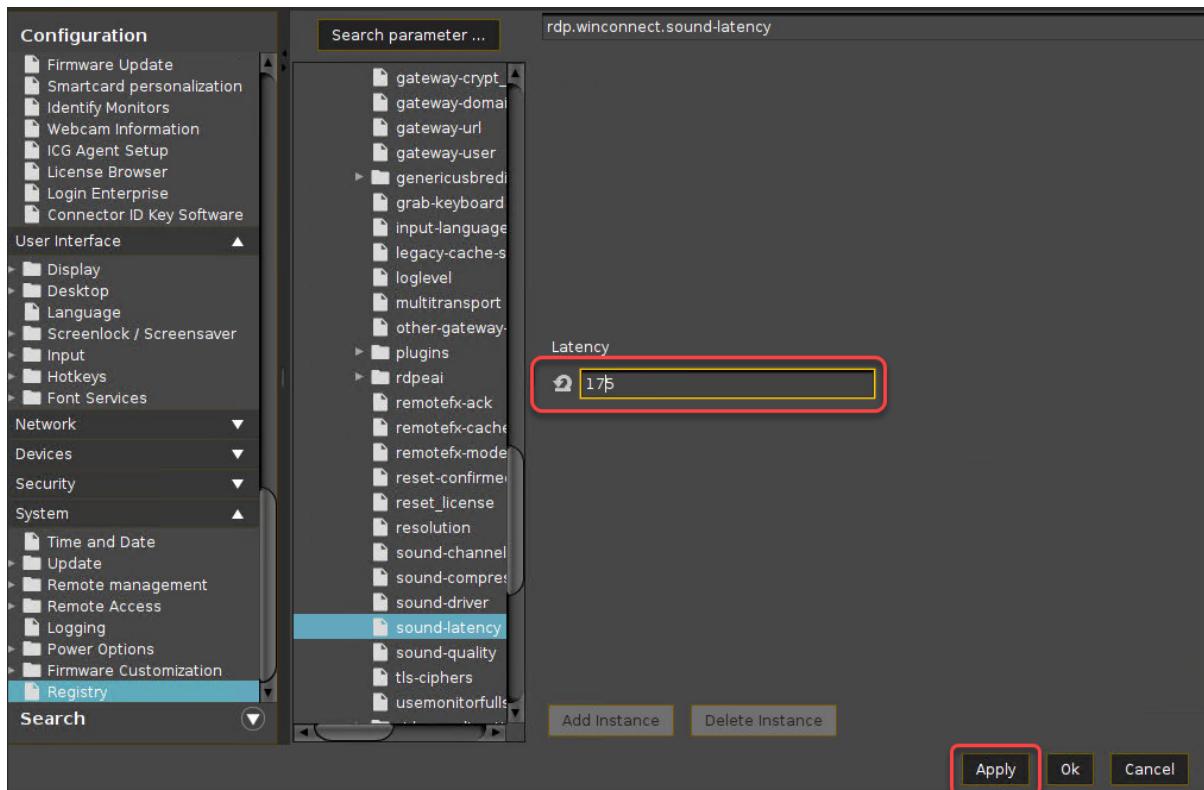
The crackling noises, or audio glitches, result from buffer underruns. This occurs when new audio data are not delivered fast enough and the sound card buffer has no more audio data left to play. Thus, it is not possible to bridge the replay gap. This is more likely to happen with sound cards that have a relatively small buffer.

#### Solution

To enable the device to bridge bigger gaps, buffer capacity must be added. This can be done by increasing the buffer of the RDP client, which implies increasing the latency. However, high latency can lead to a problem with interactive applications, such as calls or video conferences. Thus, the latency should be increased in small steps.

To increase the latency of the RDP client:

1. Open the Setup and go to **System > Registry > rdp > winconnect > sound-latency** (registry key: `rdp.winconnect.sound-latency`).
2. Increase the **Latency** by about 50 milliseconds (recommended) and click **Apply**.



3. Restart the RDP session and test the audio playback.
4. If the audio quality is good, click **Ok** to close the Setup. If there are still crackling noises, repeat steps 2 and 3 until the audio quality is acceptable.

## 2.4.8 Login Failed Because of Expired AD Password

### Issue

When you try to log in to a **RDP** session, you get the error message "Login Failed!" because your Active Directory password expired.

You are unable to change your password because the local logon does not provide an option for that.

Before following these instructions, check the ports:

- Login to Client -> Port 88
- Change password -> Port 464

Here you find an overview of ports of the Domain Controller: [Required Ports to Communicate with Domain Controller](#)<sup>143</sup>

<sup>143</sup> <https://social.technet.microsoft.com/Forums/windows/en-US/1c6a59de-c1fe-4946-bb4e-1fe36fd40b08/required-ports-to-communicate-with-domain-controller?forum=winserverDS>



## Solution

Enable **Active Directory/Kerberos** authentication for the **RDP** session. The next time you try to log in to IGEL OS, you will be prompted to change your expired password.

### Changing an Expired Active Directory Password

When using sessions with passthrough authentication, it is essential that you lock your device's screen when leaving it unattended.

#### Enabling Active Directory/Kerberos Authentication for RDP Sessions

1. In IGEL setup, go to **Security > Logon > Active Directory/Kerberos**.
2. Enable **Login to Active Directory Domain**.
3. Go to **Security > Active Directory/Kerberos**.
4. Activate **enable**.
5. Fill in the **Default Domain (Fully Qualified Domain Name)**.
6. Go to **Sessions > RDP > RDP sessions > [RDP session] > Logon**.
7. Enable **Use passthrough authentication for this session**.
8. Click **Apply** or **Ok**.

Please note that the client must now be locked locally and no longer in the session to prevent another person from entering the session via the passthrough without specifying the password.

#### Enabling Screen Lock

1. In the IGEL setup go to **User Interface > Screenlock / Screensaver**.
2. Enable **Use Hotkey**.
3. Under **Modifiers** select Win.
4. Under **Hotkey** enter "I".
5. Go to **User Interface > Screenlock / Screensaver > Options**.
6. Enable **User Password**.

So the "Win + L" hotkey locks the IGEL client instead of the session desktop.

The AD password must be entered to activate the IGEL clients.

### 2.4.9 User Has to Provide Credentials Twice for RDP Logon

#### Issue

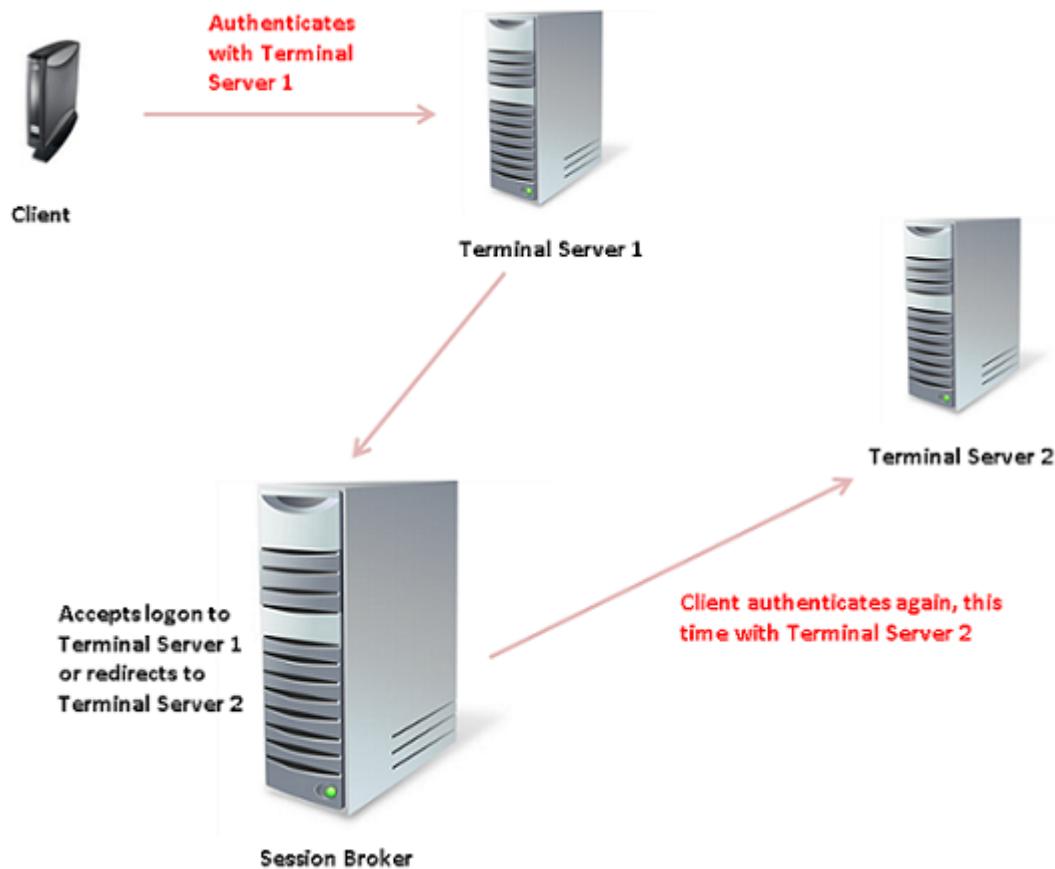
When you connect to a Windows terminal server, you are asked to provide your credentials twice.

## Cause

This behavior is caused by the way RDS load balancing works. The crucial point to understand is that the terminal server does not communicate with the session broker directly.

Instead, the scenario is the following:

1. The client connects to terminal server 1 and authenticates with terminal server 1. This is the first time the user is asked for their credentials.
2. Since we have a load balancing setup, terminal server 1 will talk to the session broker and ask if the client can use terminal server 1 or if it should be redirected to a different terminal server.
3. If redirection occurs, the client will also have to authenticate with the terminal server the client was redirected to (terminal server 2 in the figure below). This is the second time the user is asked for their credentials.





## Solution

The issue can be resolved by activating Kerberos/Active Directory authentication. For further information, see [Active Directory/Kerberos](#)(see page 1242).

## 2.5 VMware Horizon

- [Setting up VMware Blast Sessions](#)(see page 285)
- [Use NLA \(Network Layer Authentication\) for Logon with Horizon Client Sessions](#)(see page 285)
- [Workaround for Hotkeys in Horizon Sessions](#)(see page 286)
- [Multimedia Acceleration with VMware Horizon View in VESA Mode](#)(see page 286)
- [Horizon Feature Matrix](#)(see page 287)
- [Troubleshooting the Horizon Client](#)(see page 291)

### 2.5.1 Setting up VMware Blast Sessions

#### Prerequisites

- Device offering hardware video acceleration, see the FAQ [Hardware Video Acceleration on IGEL OS](#)<sup>144</sup>.
- VMware Horizon 7 Server  
For further information about the server configuration, refer to VMware's documents at <http://pubs.vmware.com/horizon-7-view/index.jsp>

#### Activating VMware Blast

1. In Setup, go to **System > Firmware Customization > Features**.
2. Enable **Hardware Video Acceleration**.
3. Go to **Sessions > Horizon Client > Horizon Client Global > Server Options**.
4. Set **Preferred desktop protocol** to **VMware Blast**.
5. Click **Apply** or **Ok**.

### 2.5.2 Use NLA (Network Layer Authentication) for Logon with Horizon Client Sessions

Starting a session, even just presenting a logon screen, has quite an impact on resources. Each time a user tries to logon, processes are started on the remote machine, no matter whether the user's credentials are valid or not. You can save resources and prevent Denial of Service (DoS) attacks by using Network Layer Authentication (NLA). NLA checks whether a user is the right person before any logon processes is started.

For more information about NLA, see <https://technet.microsoft.com/en-us/magazine/hh750380.aspx>.

NLA for *Horizon Client* Sessions is available from *IGEL* Linux version 5.08.100 upwards.

---

<sup>144</sup> <https://kb.igel.com/display/igelos/Hardware+Video+Acceleration+on+IGEL+OS>



To use NLA for a *Horizon Client* session:

1. Open the setup and go to **Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Options**.
2. Activate **Network Level Authentication**.

### 2.5.3 Workaround for Hotkeys in Horizon Sessions

#### Issue

You want to switch from the VMware Horizon session to the IGEL desktop with the key combination [Ctrl] + [Windows] + [D]. While the key combination [Ctrl] + [Windows] + [D] can be realized with IGEL OS 11.01.100 or lower (Horizon Client 4.x), this is not possible for IGEL OS 11.01.110 or higher (Horizon Client 5.x).

#### Solution

1. Press [Ctrl] + [Alt] and release the keys.  
The focus is switched from the VMware Horizon session to the local system.
2. Use [Ctrl] + [Windows] + [D] to switch to the IGEL desktop.
3. To switch the focus back to the VMware Horizon session, click into the VMWare Horizon session window.

### 2.5.4 Multimedia Acceleration with VMware Horizon View in VESA Mode

#### Symptom

You did install IGEL Universal Desktop OS 2 on not fully supported hardware using IGEL Universal Desktop Converter 2. Multimedia acceleration is not working within a VMware Horizon View session.

#### Problem

The graphics chip of your hardware is not supported and as a fallback the VESA mode is used.

#### Solution

There is no other solution to the problem than using fully supported hardware. Information on supported hardware can be found [in the UDC2 manual](#).<sup>145</sup>

You can also access [IGEL's 3rd party hardware support database](#)<sup>146</sup> to find fully supported graphic chips.

---

<sup>145</sup> <http://edocs.igel.com/index.htm#11873.htm>

<sup>146</sup> <https://www.igel.com/linux-3rd-party-hardware-database/>



## 2.5.5 Horizon Feature Matrix

According to the details provided by the vendor, the following Horizon Client features are supported with Horizon Client 5.4:

For details on the Horizon Clients that are built into your version of IGEL OS, see [IGEL OS Release Notes \(see page 1422\)](#) > Notes for Release [your version] > Component Versions [your version].

See also the original document at <https://kb.vmware.com/s/article/78810>.

Category	Feature	Supported
Client Appearance and Workflow	Customer branding	no
	Kiosk mode	yes
	English localization	yes
	Language localization	yes
Broker Connectivity	XML-API version	15
	SSL	yes
	SSL certificate verification	yes
	Disclaimer dialog	yes
	Security Server compatibility	yes
	UAG compatibility	yes
	Multi-broker/Multi-site redirection - DaaS	yes
	Client info	yes
	Phonehome	yes
Broker Authentication	Password authentication	yes
	Password change	yes
	Certificate authentication	no
	RSA authentication	yes
	Radius	yes
	Integrated RSA SecurID token generator	no
	Single Sign On	yes
	Log in as current user	no
	Nested log in as current user	no
	Biometric authentication	no
	Unauthentication access	yes
Smartcard	x.509 certificate authentication (Smart Card)	yes
	CAC support	no
	.Net support	yes
	PIV support	yes
	Java support	no



Category	Feature	Supported
	Purebred derived credentials	no
Desktop Operations	Reset	only supported with VDI
	Restart	only supported with VDI
	Log off	yes
Session Management (Blast Extreme & PCoIP)	Switch desktops	yes
	Multiple Connections	yes
	App Launch on Multiple end points	yes
	Auto-Retry	yes
	Auto-Retry 5+ minutes	yes
	Fullscreen mode	yes
	Fullscreen toolbar	yes
	Windowed mode	yes
	Time Zone Synchronization	yes
	Jumplist integration (Windows 7-Windows 10)	no
Client Customization	Command Line Options	yes
	URI Schema	yes
	Preference File	yes
	Non Interactive Mode	yes
	GPO-based customization	no
Protocols supported	Blast Extreme	yes
	H.264 - HW decode	yes
	H.265 - HW decode	no
	Blast Codec	yes
	JPEG / PNG	yes
	Switch Encoder	yes
	BENIT	yes
	Blast Extreme Adaptive Transportation	yes
	RDP 8.x, 10.x	yes
	PCoIP	yes
Protocol Enhancements	RDP-VC Bridge	yes
	Session Enhancement SDK	yes
Monitors / Displays	Dynamic Display Resizing	yes
	Multiple Monitor Support	yes
	External Monitor Support	yes
	Display Pivot	yes
	Multiple Aspect Ratio support	yes
	Number of displays supported	4
	Maximum Resolution	3840x2160
	Video out	yes



Category	Feature	Supported
	High DPI scaling	only supported with VDI
	DPI Sync	yes
	Exclusive Mode	no
	Multiple Monitor Selection	yes
Input Device (Keyboard / Mouse)	Relative mouse	yes
	External Mouse Support	yes
	Local buffer text input box	no
	Keyboard Mapping	yes
	Unicode Keyboard Support	no
	International Keyboard Support	yes
	Input Method local/remote switching	no
	IME Sync	yes
Clipboard Services	Clipboard Text	yes
	Clipboard Graphics	no
	Clipboard memory size configuration	yes
	Drag and Drop text	no
	Drag and Drop images	no
Client Caching	View Agent to Client-side caching	yes
Connection Management	Blast network recovery	yes
	IPv6 translation with UAG	no
	IPv6 only network support	no
	PCoIP IP roaming	yes
High-Level Device Redirection	Serial (COM) Port Redirection	yes
	Client Drive Redirection/File Transfer	yes
	Scanner (TWAIN/WIA) Redirection	yes
	x.509 Certificate (Smart Card)	yes
	Gyro Sensor Redirection	no
Real-Time Audio-Video	Analog in (input)	yes
	Real-Time Audio-Video	yes
	Multiple webcams	no
USB Redirection	Generic USB / HID	yes
	Policy: ConnectUSBOnInsert	only supported with VDI
	Policy: ConnectUSBOnStartup	only supported with VDI
	Connect/Disconnect UI	yes
	USB device filtering (client side)	yes
	Isochronous Device Support	only supported with VDI
	Split device support	yes
	Bloomberg Keyboard compatibility	only supported with VDI
	Smartphone sync	only supported with VDI



<b>Category</b>	<b>Feature</b>	<b>Supported</b>
Unified Communications	USB 3.0	yes
	USB Redirection USB storage devices	yes
	Cisco UC Jabber	only supported with VDI
	Avaya UC One-X Desktop	only supported with VDI
	Mitel UCA	no
	Microsoft Lync 2013	no
Multimedia Support	Skype for business	yes
	Microsoft Teams RTAV	yes
	Multimedia Redirection (MMR)	yes
	Flash URL Redirection (Unicast/Multicast)	only supported with VDI
	Flash Redirection	no
	HTML5 Redirection	yes
Graphics	Directshow Redirection	no
	vDGA	only supported with VDI
	vSGA	only supported with VDI
	NVIDIA GRID VGPU	yes
	Intel vDGA	only supported with VDI
Mobile Support	AMD vGPU	only supported with VDI
	Client-side soft keyboard	no
	Client-side soft touchpad	no
	Full Screen Trackpad	no
	Gesture Support	no
	Multi-touch Redirection	no
	Presentation Mode	no
Printing	Unity Touch	no
	Printer Redirection	yes
	VMware Integrated Printing	yes
	Location Based Printing	yes
Security	Native Driver Support	yes
	FIPS-140-2 Mode Support	yes
	Imprivata Integration	no
	Opswat agent	yes
	Opswat on-demand agent	no
	TLS 1.1	yes
	TLS 1.2	yes
Session Collaboration	Session Collaboration	yes
	Read-only Collaboration	yes
Update	Update notifications	no
	App Store update	no



Category	Feature	Supported
Other	Smart Policies	yes
	File Type Association	no
	URL content redirection	yes
	Browser content redirection	no
	Remember credentials	no
	Access to Linux Desktop - Blast Protocol Only	only supported with VDI
	Audio Playback	yes
	Seamless Window	yes
	Launching multiple client instances using URI	yes
	Parameter pass-through to RDSH apps	yes
	Performance Tracker	only supported with VDI
	Shortcuts from server	no
	Pre-install shortcuts from server	no
	Workspace ONE mode	yes

## 2.5.6 Troubleshooting the Horizon Client

### Solution Based on Experience from the Field

This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

### Symptom

There are some issues with the performance of the Horizon client.

### Environment

- IGEL OS 10 or higher

### Problem

You don't know how to collect the log files and send them to the IGEL Support team.

### Solution

- In the Setup, go to **System > Registry > sessions > vdmclient% > options > debug** and activate **Save debug information** (registry parameter: sessions.vdm\_client%.options.debug).



2. Go to **System > Registry > vmware > USB > log** and set **Set VMware Horizon USB debug level** to "debug" (registry parameter: `vmware.view.usb.log`).
3. Go to **System > Registry > vmwarevdmapp > debug** and activate **Save debug informations** (registry parameter: `vmwarevdmapp.debug`).  
The log files are created in the `/tmp` directory and can be found using the following patterns:  
`/tmp/vvdm*`  
`/tmp/vmware-*`
4. Change to `/tmp` and put the log files into a compressed tar file: `tar -czf vmware-logs.tar.gz [logfiles]`
5. In the structure tree of the UMS Console, go to the device and select **Device File->UMS** the context menu.
6. Under **Devices file location**, enter `"/tmp/vmware-logs.tar.gz"`.
7. Under **Target URL**, select the location on the UMS Server where the file is to be stored.
8. Click **Device->UMS**.

## 2.6 Microsoft Azure Virtual Desktop (AVD)

- Importance of Keeping IGEL OS Firmware Up-to-Date for Microsoft AVD and Windows 365 CloudPC(see page 292)

### 2.6.1 Importance of Keeping IGEL OS Firmware Up-to-Date for Microsoft AVD and Windows 365 CloudPC

If you are running the Microsoft Azure Virtual Desktop (AVD) client on an IGEL OS-powered endpoint (PC, laptop, or client), it is important to ensure that the client version is up-to-date.

#### Why Is It Important to Keep Your Igel OS Firmware Updated?

If the client version is not up-to-date, changes on the Microsoft AVD's server-side could lead to functionality issues. The latest IGEL OS firmware version is, in most cases, the current official build. To find the latest version, see <https://www.igel.com/software-downloads/workspace-edition/> > click **OS 11** to expand the relevant section.

However, an IGEL OS private build may be released to adapt for server-side changes that have been introduced between IGEL OS releases. This way, we maintain existing functionality and support new features/functionality. Therefore, please refer to [www.igel.com/avd](http://www.igel.com/avd)<sup>147</sup> for the latest Microsoft AVD / Windows 365 CloudPC specific IGEL OS releases.

#### IGEL Environment

- Endpoints with IGEL OS 11
- IGEL AVD client is used for Azure Virtual Desktop (AVD) and Windows 365 CloudPC by Microsoft
- Universal Management Suite (UMS) 6.08 or higher

---

<sup>147</sup> <http://www.igel.com/avd>



## How to Check for the Latest IGEL OS Firmware Version

1. Open the web browser and go to [www.igel.com/avd](http://www.igel.com/avd)<sup>148</sup>.
2. Fill in the form to register for AVD client access and submit it.

 A screenshot of a web-based registration form for AVD client access. The form is set against a black background with white and light gray input fields. It includes sections for personal information, company details, location, and management tools usage. A reCAPTCHA verification section and a prominent yellow "SEND" button are also present.
 

The form fields include:

- First Name: Ike (Required field)
- Last Name: (Required field)
- Email Address: @igel.com (Please supply your email address)
- Phone Number: (Required field)
- Company: IGEL Technology (Required field)
- Country: Germany (Required field)
- State/Region: (DE) Bayern
- Employee Count: <500 (Required field)
- Role: Yes (Required field)
- Management Tools: Citrix, VMware, Microsoft (Required field)
- Other: Other
- Subscription: Subscribe to IGEL communications (checkbox checked)
- reCAPTCHA: I'm not a robot (checkbox checked)
- SEND button: A large yellow button at the bottom.

After a few minutes, you will receive a confirmation mail from IGEL.

<sup>148</sup> <http://www.igel.com/avd>



3. In the confirmation mail, click **Update for current IGEL OS 11 installations.**

[Click here](#) to view this message in a browser window.



**Thank you for your registration!**

Please see below the first version of the RD Core integration within the IGEL OS.

For further information, please see the current [Feature Matrix and the Quick Start Guide](#).

Demo License can be fetched via the IGEL Setup Assistant ([Read more](#)).

[IGEL OS 11 Readme Notes](#)

Click the links below to download and install the software:

[Initial IGEL OS 11 deployment](#)

[Update for current IGEL OS 11 installations](#)

[IGEL Universal Management Suite](#)

Copyright © 2021 IGEL Technology GmbH  
Our address is Hermann-Ritter-Str. 110, 28197 Bremen, Germany

If you do not wish to receive future email, [click here](#).  
(You can also send your request to **Customer Care** at the street address above.)

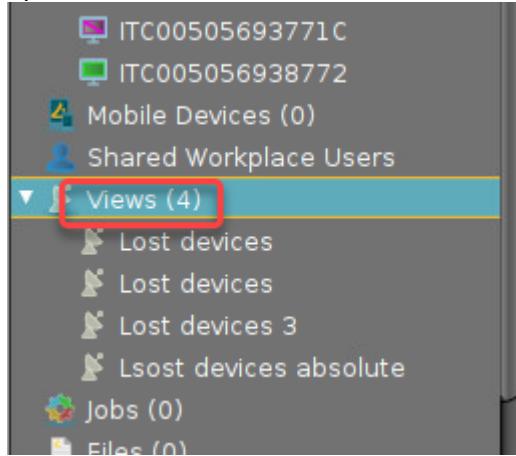
The IGEL OS firmware with the latest AVD client is downloaded (official or private build).

4. Note the version number that can be derived from the file name.  
Example: When the file name is `lxos_11.06.100_public.zip`, the version is 11.06.100.

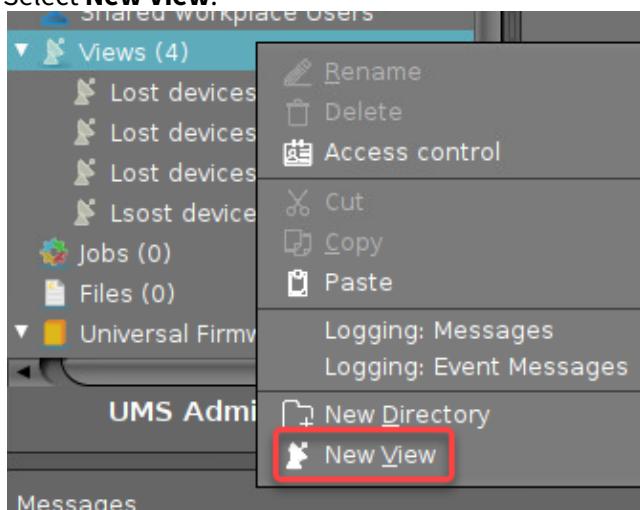
## How to Check If the IGEL OS Version Is Out-of-Date

We will create a view to find out which endpoint devices are running a firmware version lower than the one with the latest AVD client.

1. Open the UMS console and in the structure tree, go to **Views**.



2. Select **New View**.





3. Enter an appropriate **Name** and click **Next**.

Create new view

View name

Name **AVD client outdated**

Description

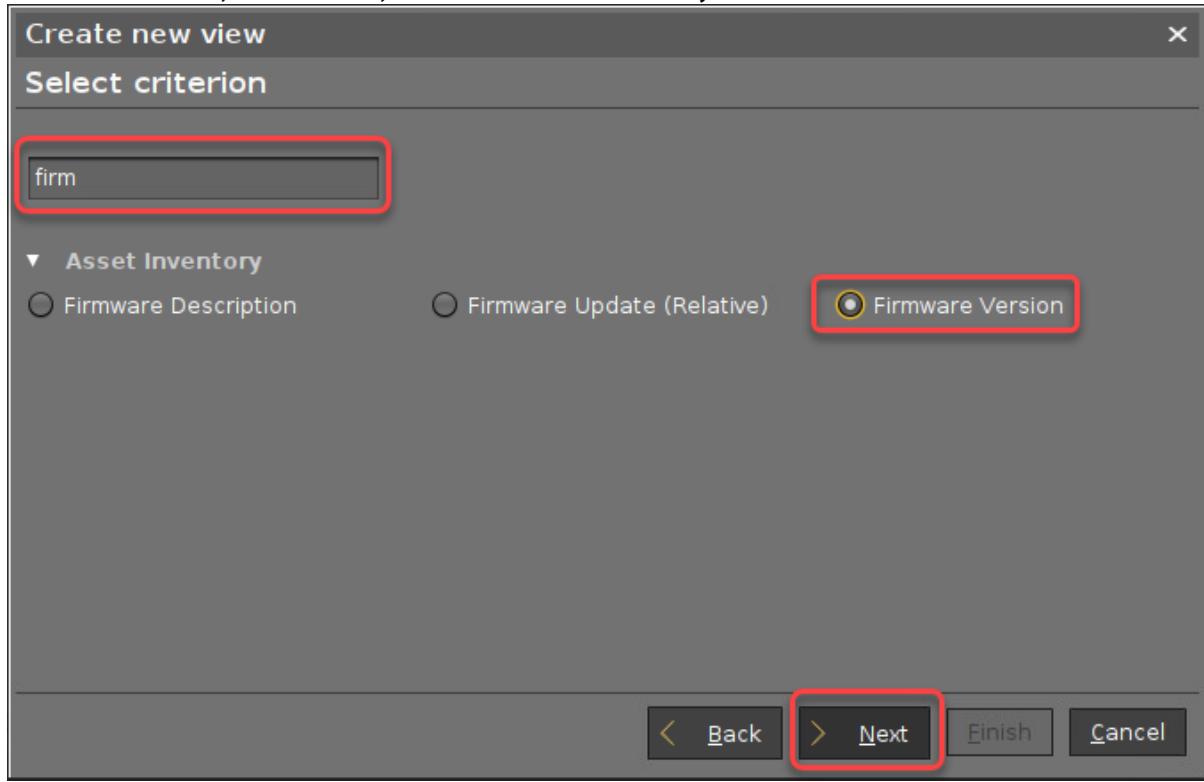
Expert mode

Back Next Finish Cancel

A screenshot of a software window titled 'Create new view'. Inside, there's a section labeled 'View name' with a 'Name' field containing the text 'AVD client outdated'. Below it is a 'Description' field which is empty. In the bottom right corner of the window, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'. The 'Next' button is highlighted with a red rectangular box around it. To the right of the 'Next' button, there is a small 'Expert mode' checkbox. The overall background of the window is dark grey.



4. In the search field, enter "firm", select **Firmware version**, and click **Next**.



5. Select **below**, enter the version number of the firmware you have downloaded beforehand, and click **Next**.



Create new view

### Version search

Version number  exact  above  below  Not like

Use regular expression

[Back](#) [Next](#) [Finish](#) [Cancel](#)

6. Click **Finish**.

The matching endpoint devices are shown.

Name	AVD client outdated			
Description				
Rule	Firmware version is less than 11.6.100			
Result list was last updated at 11:41 AM. <a href="#">Refresh</a>				
<a href="#">Settings</a>				
Matching devices (4 devices)				
Name	Last known IP address	MAC address	Product	Version
ITC001558CDD1C0	192.168.2.127	001558CDD1C0	IGEL OS 11	11.05.120.01
ITC005056930285	192.168.30.107	005056930285	IGEL OS 11	11.05.120.01
ITC005056930CAD	192.168.30.106	005056930CAD	IGEL OS 11	11.04.240.01
ITC00505693771C	192.168.30.104	00505693771C	IGEL OS 11	11.05.120.01

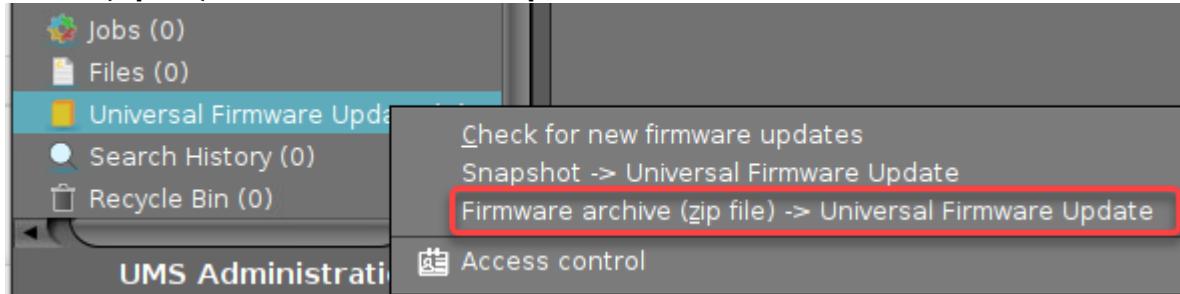
## How to Update IGEL OS Endpoint Devices to the Latest Firmware Version

In the following instructions, we will use the Universal Firmware Update feature of the UMS. For alternative methods, see [Firmware Update](#)(see page 225), [Buddy Update](#)(see page 221), [Updating the Firmware using a USB Storage Device](#)(see page 228), and [Updating the Firmware using the Linux Console](#)(see page 229).

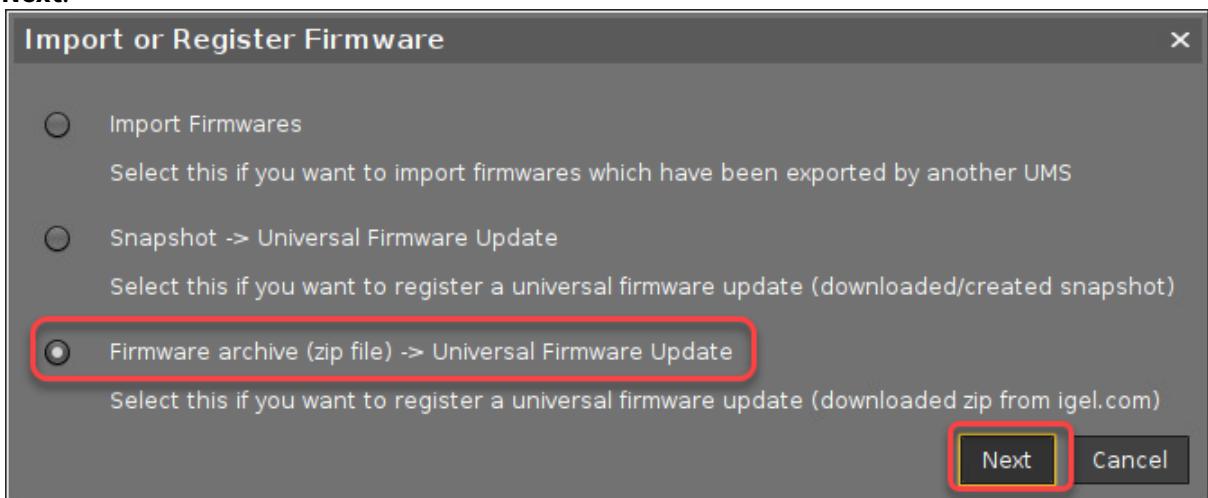
1. Make sure that the firmware file (in our example: `lxos_11.06.100_public.zip`) can be accessed from the machine that hosts the UMS Console (via local file or network drive).



2. In the structure tree of the UMS Console, go to **Universal Firmware Update** and select **Firmware archive (zip file) -> Universal Firmware Update**.

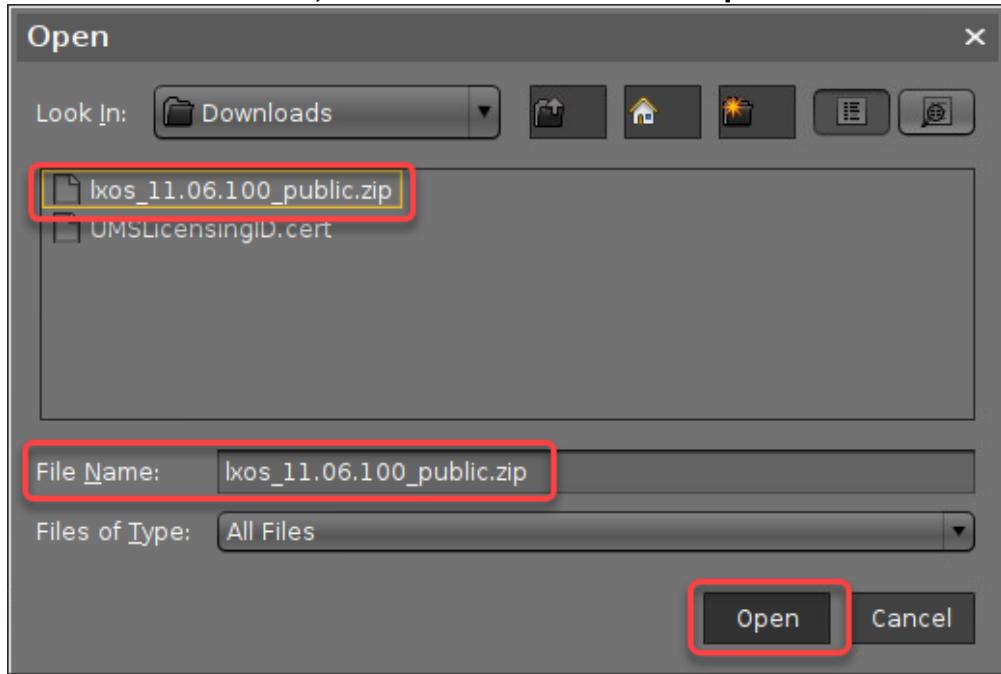


3. Make sure that **Firmware archive (zip file) -> Universal Firmware Update** is selected and click **Next**.

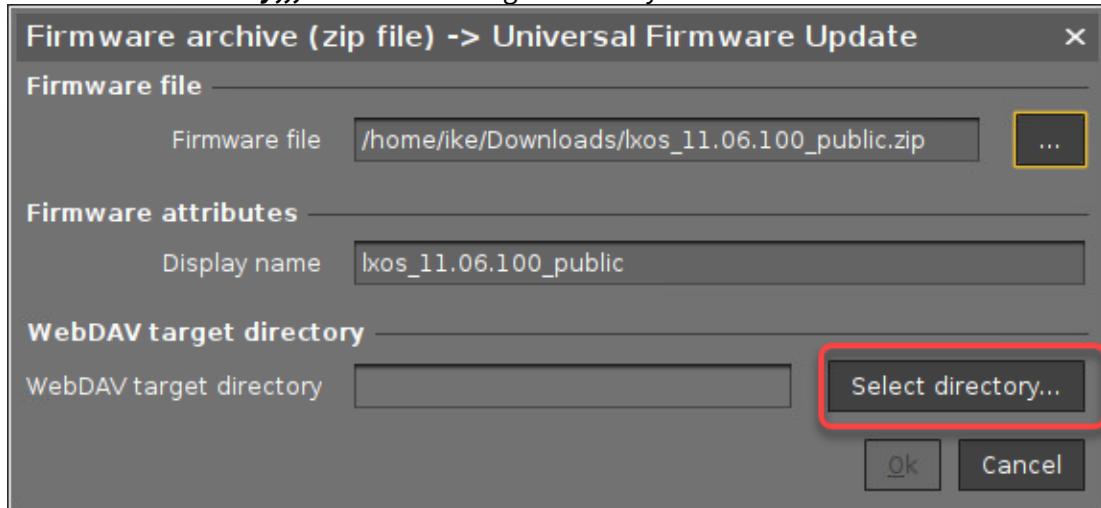




4. Click the file chooser icon, find the firmware file and click **Open**.

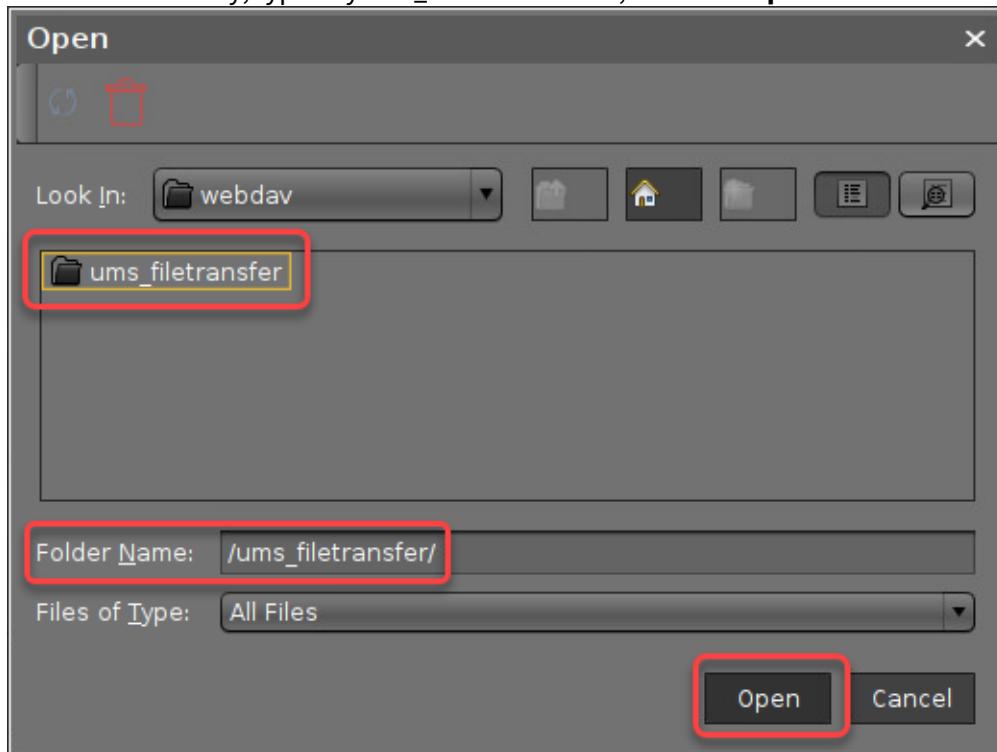


5. Click **Select directory,,,**, to define the target directory at the UMS Server.

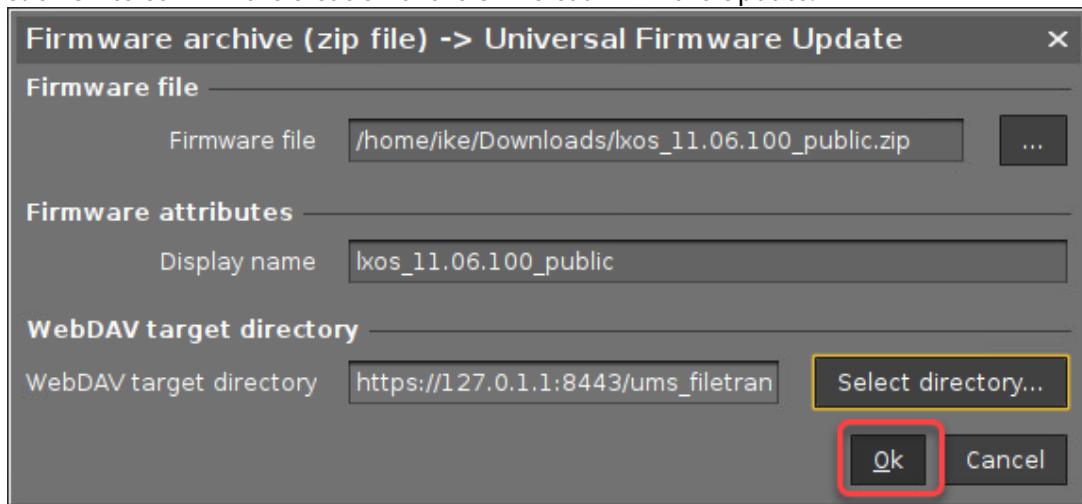




6. Select the directory, typically `ums_filetransfer`, and click **Open**.



7. Click **Ok** to confirm the creation of the Universal Firmware Update.



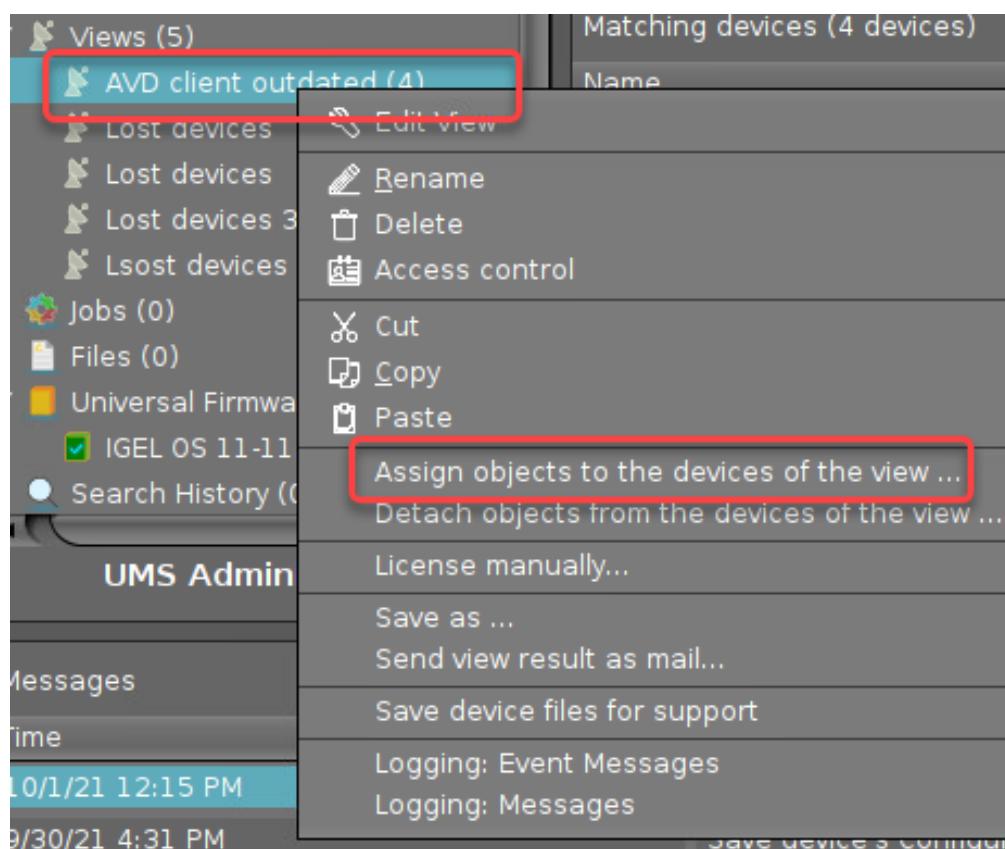
If everything went well, the new Universal Firmware Update is displayed.



/Universal Firmware Update/xos\_11.06.100\_public

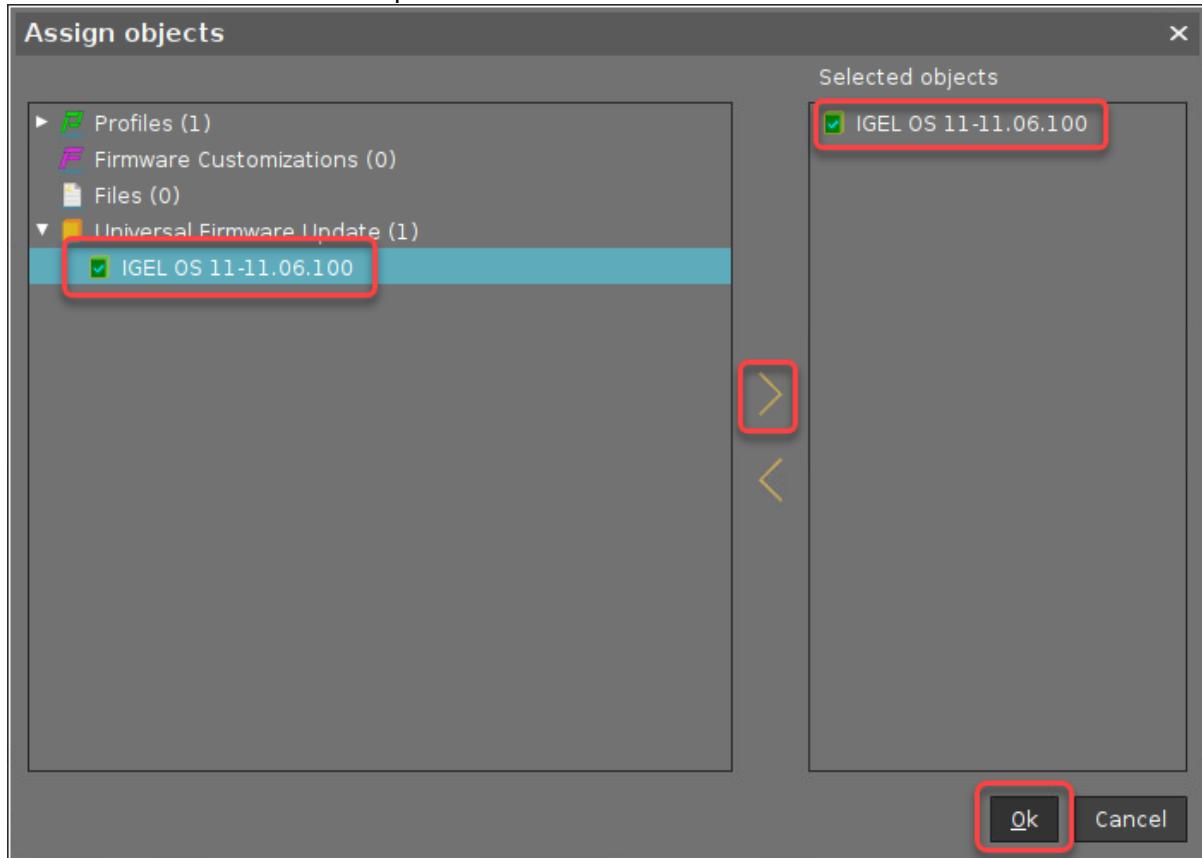
Product	IGEL OS 11
Version	11.06.100
Release Notes	<a href="#">HTML</a> <a href="#">Text</a>
<b>Firmware Update Settings</b>	
Host	<PUBLIC_ADDRESS/HOST>
Protocol	HTTPS (UMS WebDAV)
Port	<PUBLIC_WEB_PORT>/WEB_PORT>
Target URL	/ums_filetransfer/xos_11.06.100_public-1633084175258
Snapshot file	
User	IGEL_INTERNAL_FIRMWAREUPDATE_USER
Password	*****
<b>Download Status</b>	
Status	OK
	Finished
Error	

8. Go to the view you have created beforehand, open the context menu, and select **Assign objects to the devices of the view....**

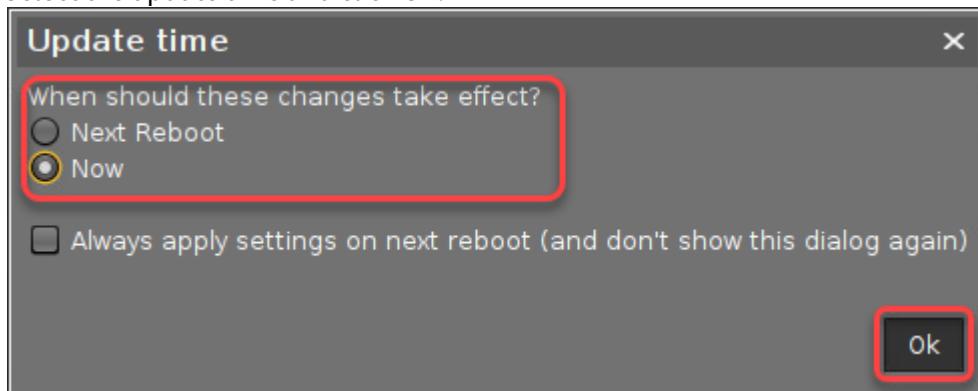




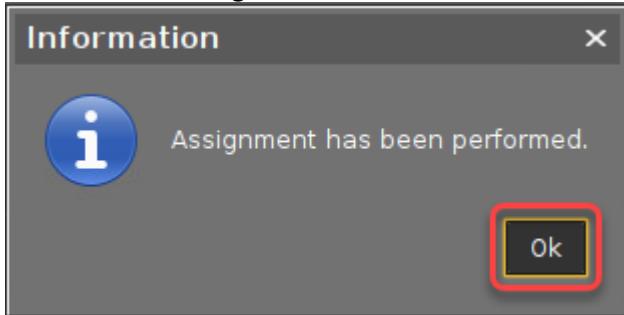
9. Select the Universal Firmware Update and click **Ok**.



10. Select the update time and click **Ok**.



11. Confirm the message window.



On the next reboot, the endpoint devices will update their firmware.

Whether you are implementing classic VDI, virtual apps, DaaS, or in this case AVD, it is always a good practice to make sure you are running the very latest version of IGEL OS to take advantage of the latest features.

## 2.7 Evidian

- [Authenticating with Evidian Authentication Manager\(see page 305\)](#)

### 2.7.1 Authenticating with Evidian Authentication Manager

You can connect to Citrix, RDP and VMware Horizon roaming sessions using RFID badges with Evidian Authentication Manager (AuthMgr). Custom commands are supported as well.

#### Prerequisites

- IGEL Universal Desktop Linux 5.06.100 or newer on the device.
- An installed and running Evidian SSO Controller, version 10.0 or higher
- When using HTTPS (IGEL Linux 5.07.100 or newer), the User Access Server's CA root certificate saved locally on the device.
- The device and the server(s) have to be part of the same Active Directory domain.
- A supported RFID reader (e.g. OMNIKEY 5022 CL, OMNIKEY 5421), connected to the device.
- RFID badges that are already enrolled.

#### Configuring an Evidian Authentication Manager Session

1. In IGEL Setup, go to **Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions**.
2. Add a new session.
3. Go to **Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions > [Session Name] > Connection**.
4. Choose the **Protocol** used for the user access service (e.g. HTTP).
5. Enter the IP address or DNS name used for the user access service under **Server**.
6. Choose the **Port** for the user access service (e.g. 9764).
7. Under **Path to service**, enter the path for the user access service (e.g. /soap).



8. Under **CA certificate**, enter the path to the CA certificate, including its name, or path of the certification authority (e.g. /wfs/ca-certs/ca.crt). The certificate is required for HTTPS connections.
9. Enter the secret for the **Roaming session secret**.
10. When using HTTPS, select **CA certificate** as the user access server's CA root certificate on the device.
11. Under **Evidian AuthMgr > Evidian AuthMgr Sessions > [Session Name] > Options**, select the desired **Session type**.

This will make Evidian Authentication Manager use the first configured session of its type, e.g. RDP. Make sure that a session is configured.

If you choose the user-defined session type, you need to supply the custom commands; see [Custom Commands](#)(see page 307). For further options, see [Options](#)(see page 883) in the IGEL OS Reference Manual.

12. Start the new session by clicking on its icon in the **Start Menu**. Alternatively, reboot the device. In the default autostart setting the Evidian Authentication Manager for your session will start automatically and wait for an RFID badge to be placed on the reader.

You can only start a single instance of an Evidian Authentication Manager session.

## Configuring Citrix/RDP/VMware Horizon Sessions

- ▶ Configure the session that you want to use with Evidian Authentication Manager as the first session of its kind. The shortcuts to the session settings are provided in the Setup section **Related Configurations**:

The screenshot shows the 'Configuration' menu on the left with 'Evidian AuthMgr Session' selected. The main window displays session configuration options: 'Session Type' (dropdown), 'Custom start command', 'Custom stop command', 'Language selection' (dropdown set to 'Automatic'), 'Custom catalog of messages', and 'Availability Message'. A 'Related Configurations' panel on the right lists 'Citrix Server Type', 'Horizon Client Sessions', and 'RDP Sessions'.

## Using a Custom Configuration File

Instead of using the settings provided by IGEL Setup, you can enable a custom configuration file under **Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions > [Session Name] > Options > Use configuration file**. Then all the other session settings will be ignored. You find a commented template for the configuration file at `/etc/rsUserAuth/rsUserAuth.ini`.

## Logging in with Evidian Authentication Manager

1. Place your RFID badge on the RFID reader (or tap the reader with it if you configured **Tapping Mode**)



2. Your Citrix/RDP/VMware Horizon session will open if an active roaming session for your user already exists. If it does not, you will be presented with a password prompt for the user's Active Directory password.
3. Remove your RFID badge (or tap the reader again) to disconnect from the session.

## Custom Commands

The following simple shell scripts illustrate how to write custom commands that receive username and domain as parameters from *Evidian Authentication Manager*.

In order to use them

1. Save the scripts in `/wfs/`.
2. Make them executable with `chmod a+x [filename]`.
3. Enter their full path (e.g. `/wfs/start.sh`) in **Sessions > Evidian > [Session name] > Options**.

### Start Script

```
#!/bin/sh
# Sample start script
if [ $# -eq 3 ] ; then
    # Start "session"
    gtkmessage -t "Evidian Authentication Manager Login" -m "Login as user '$1' with
domain '$3'.""
else
    exit 1
fi
exit 0
```

### Stop Script

```
#!/bin/sh
# Sample stop script
# Close running "session"
pkill gtkmessage
gtkmessage -t "Evidian Authentication Manager Logout" -s 5 -S -m "Logout user '$1'.""
exit 0
```

## Debugging and Troubleshooting

### Debugging

1. Enable **Debug mode** in **Sessions > Evidian > [Session Name] > Options** in **Setup** and set the level of detail.
2. Kill the *Evidian Authentication Manager* process (see Further Troubleshooting).
3. Start the desired Evidian session from the **Start Menu**.



4. Watch the output with `tail -F /var/log/user/rsuserauth[Session Number].debug` in **Local Terminal**. Alternatively, add the file to **System Log Viewer**.

The session number starts with 0, not 1. To watch the output of the first configured session, use thus `tail -F /var/log/user/rsuserauth0.debug`

## Further Troubleshooting

1. Open **Local Terminal**
2. Enter `ps fax | grep rsuserauth | grep -v grep` to look for *Evidian Authentication Manager* processes.
3. Use the **Evidian AuthMgr Restart** session to restart all Evidian sessions if necessary  
OR kill unwanted processes by entering `kill [process ID]` in the terminal, start desired processes via the Evidian entries in the **Start Menu**.

## 2.8 IBM iAccess

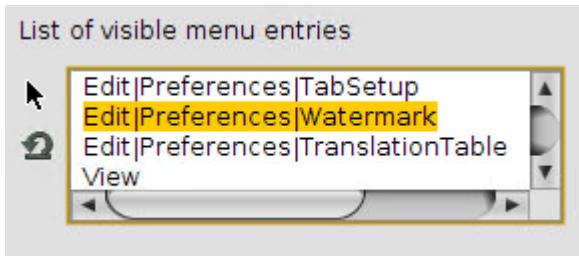
- [Editing the List of Visible Menu Entries for IBM iAccess](#)(see page 308)
- [Key Mapping for IBM iAccess Client](#)(see page 309)

### 2.8.1 Editing the List of Visible Menu Entries for IBM iAccess

You can simplify the menu of an IBM iAccess client session by removing items from the menu tree. You also can restore the original menu.

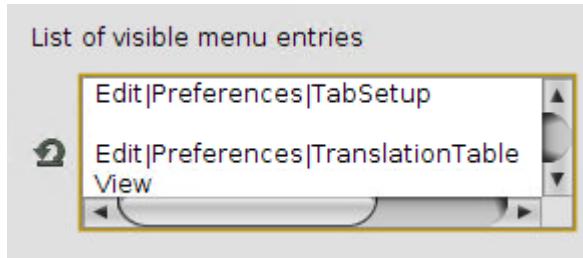
#### Removing Menu Items

1. In the IGEL Setup, go to **System > Registry > sessions > iaccess[NUMBER] > options > deletemenus** (Registry key: `sessions.iaccess[NUMBER].options.deletemenus`). [NUMBER] is the instance number of the session you want to configure; 0, for instance, stands for the first session, 1 for the second session, etc.
2. In the **List of visible menu entries**, using the mouse, mark the line with the entry you want to delete:



3. Press the backspace [←] or delete [Del] key.

The menu item is deleted:

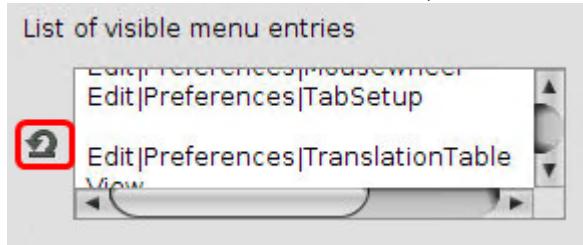


If you delete a menu item that has subitems, the subitems will be invisible, too.

4. To remove further menu items, repeat steps 2 and 3.
5. Click **Apply** or **Ok**.
6. Start or restart the IBM iAccess client to check your changes.

#### Restoring the Original Menu

1. In the IGEL Setup, go to **System > Registry > sessions > iaccess[NUMBER] > options > deletemenus** (Registry key: sessions.iaccess[NUMBER].options.deletemenus). [NUMBER] is the instance number of the session whose menu you want to restore; 0, for instance, stands for the first session, 1 for the second session, etc.
2. In the **List of visible menu entries**, click the following symbol:



The original menu is restored.

3. Click **Apply** or **Ok**.

### 2.8.2 Key Mapping for IBM iAccess Client

#### Problem

When you change the key mapping in the IBM iAccess client, the changes are not retained when the client is restarted.

Applying the changes via IGEL Setup is not possible.

#### Environment/Prerequisites

- IGEL OS 10.05.100 or higher
- UMS 5.09.110 or higher



- IBM iAccess Client session is set up

## Solution

Save the settings made in the IBM iAccess client in a file and distribute that file via the UMS.

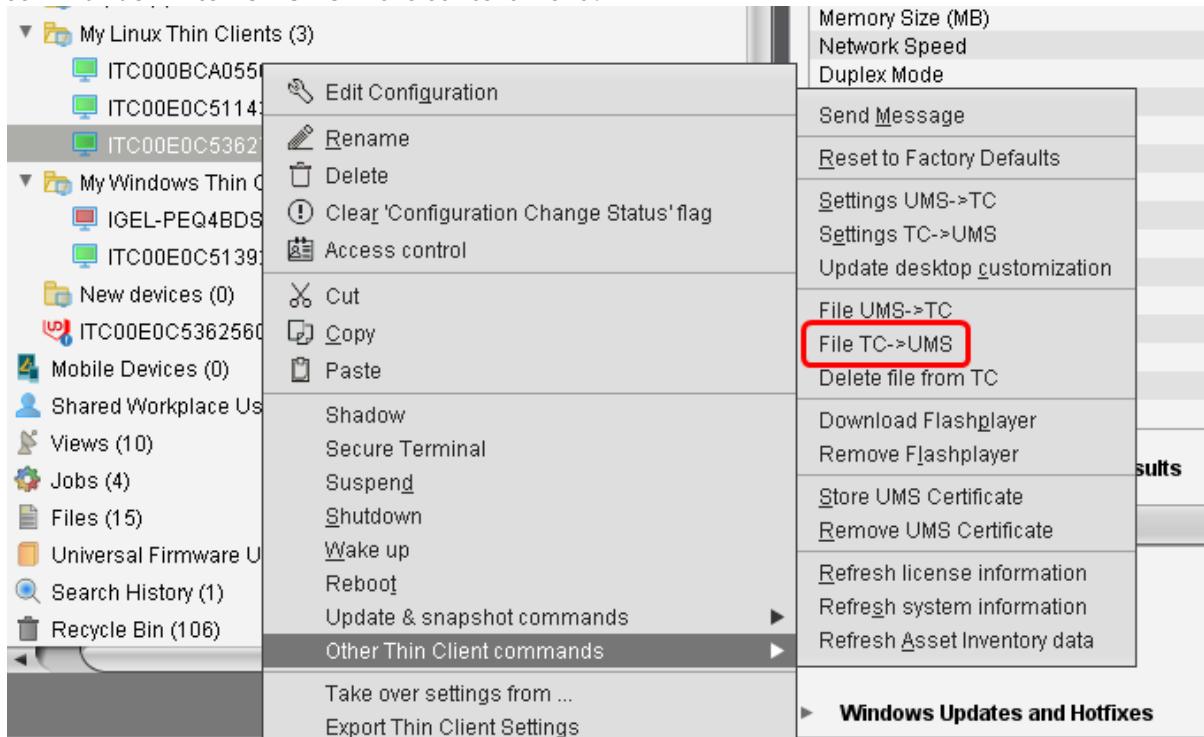
### Editing the Key Mappings

1. Open the IBM iAccess session and log on to your remote environment.
2. In the IBM iAccess client, go to **Edit > Preferences > Keyboard**.
3. On the **Key Assignment** tab, create the desired key bindings.
4. When you are finished creating key bindings, click **Save as....**
5. In the save dialog, choose **File** and edit the file path as follows: /userhome/IBM/iAccessClient/Emulator/IBMi.kmp
6. Click **OK**.

The IBM iAccess client will recognize the file **IBMi.kmp** as the default key.

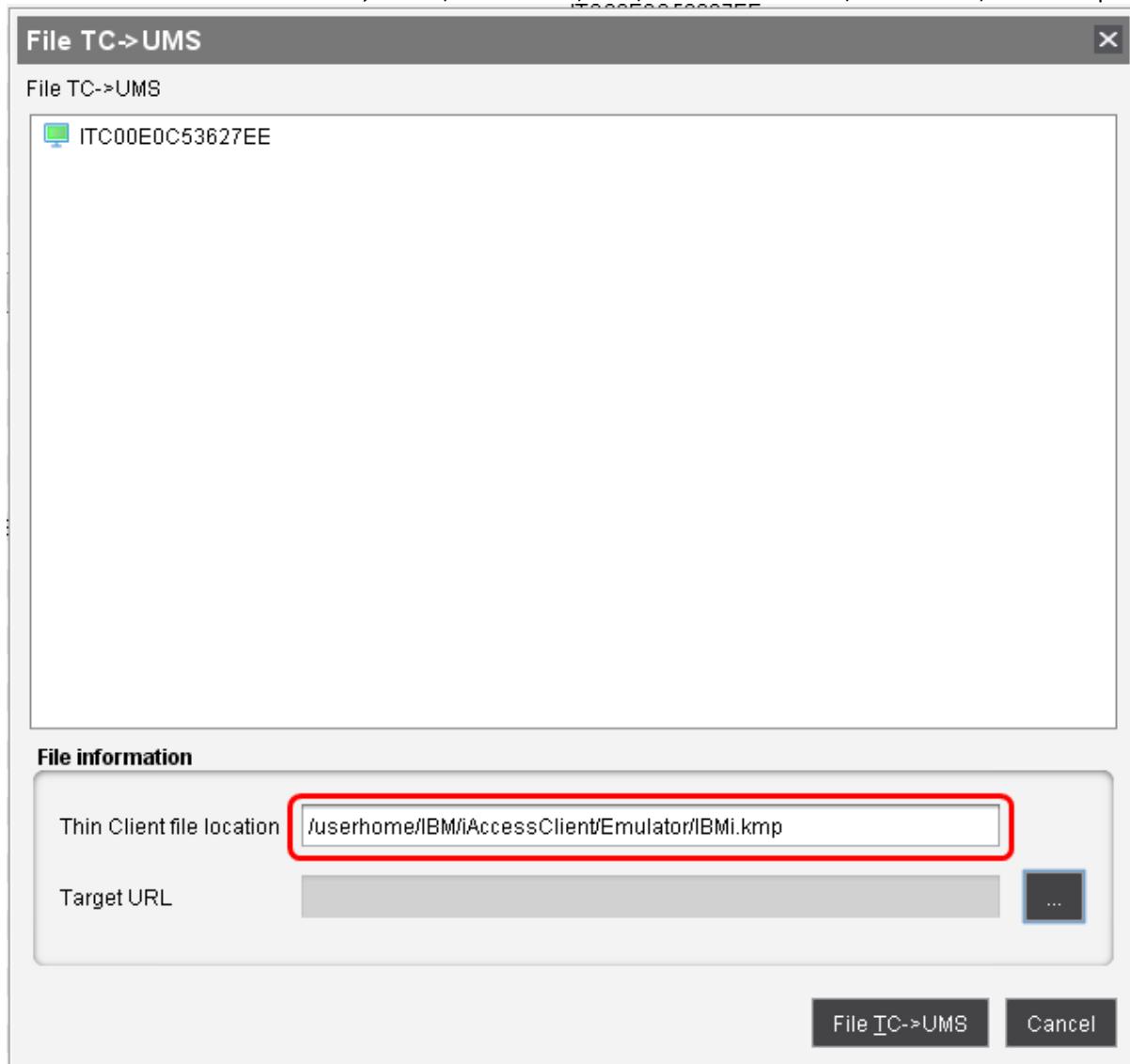
### Importing the Configuration File to the UMS

1. Open the UMS.
2. In the navigation tree, find the thin client with the **IBMi.kmp** file and select **Other Thin Client commands > File TC->UMS** in the context menu.



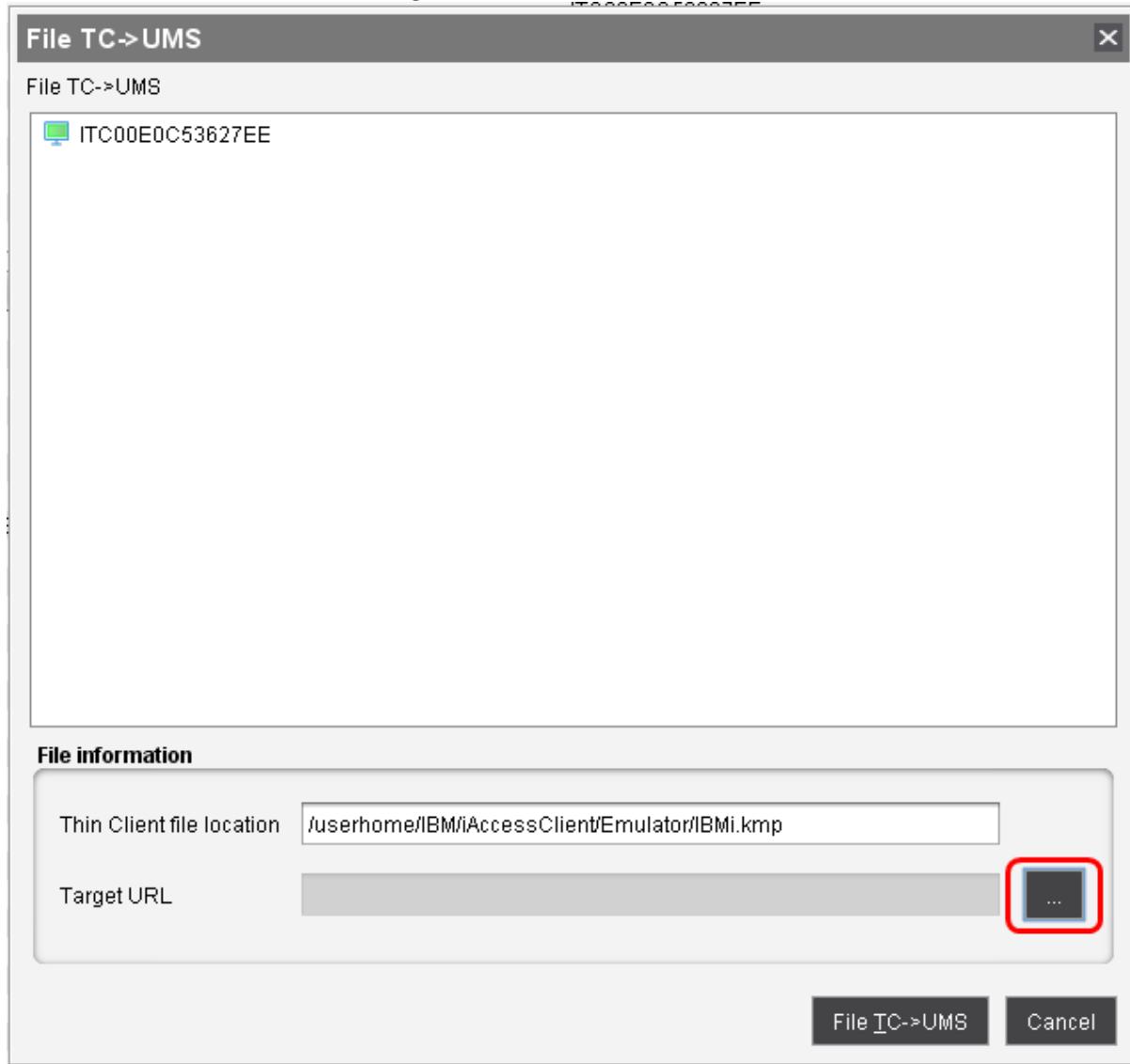


3. Under **Thin Client file location**, enter `/userhome/IBM/iAccessClient/Emulator/IBMi.kmp`

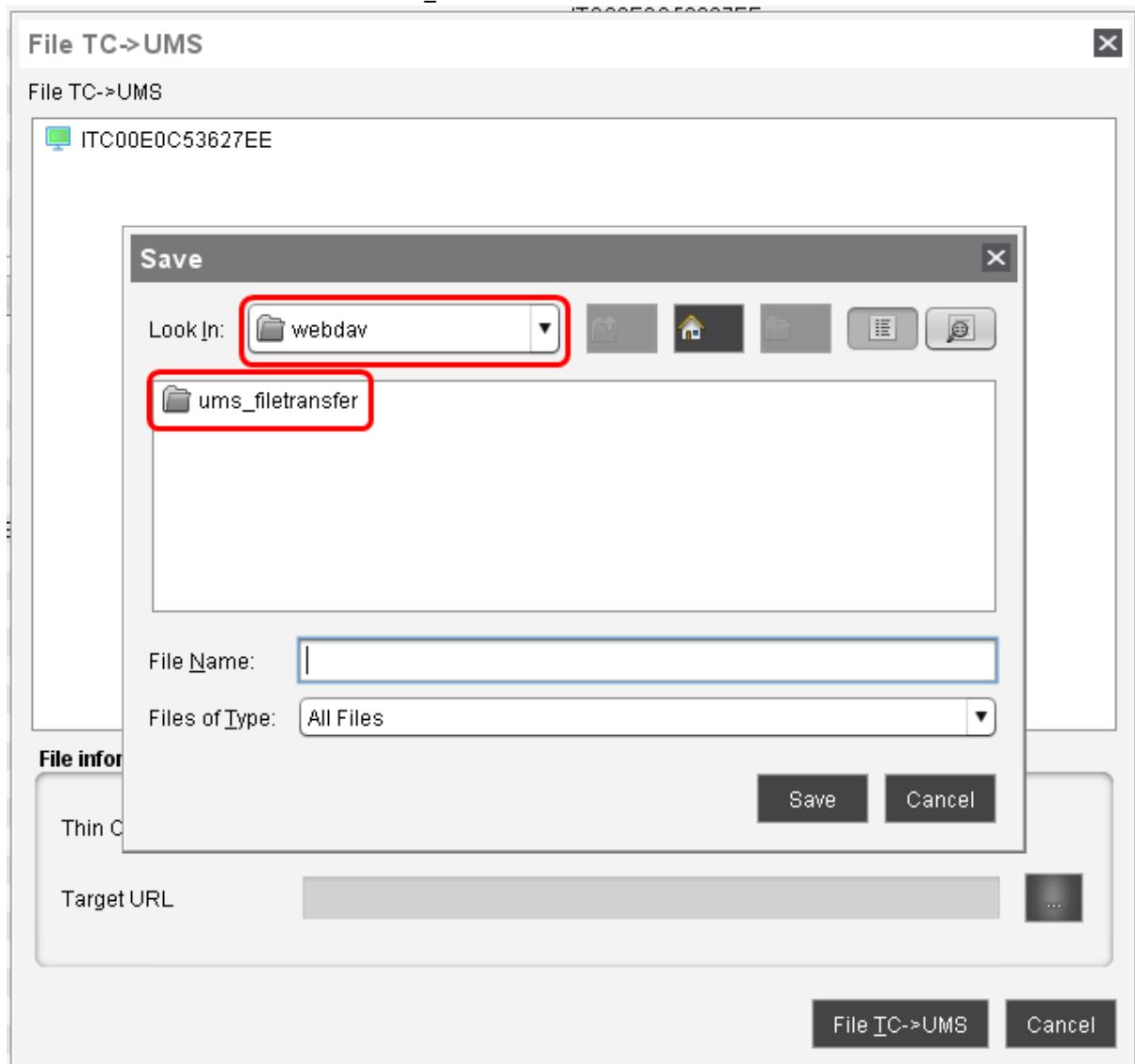




4. Click  to open the **Save** dialog.

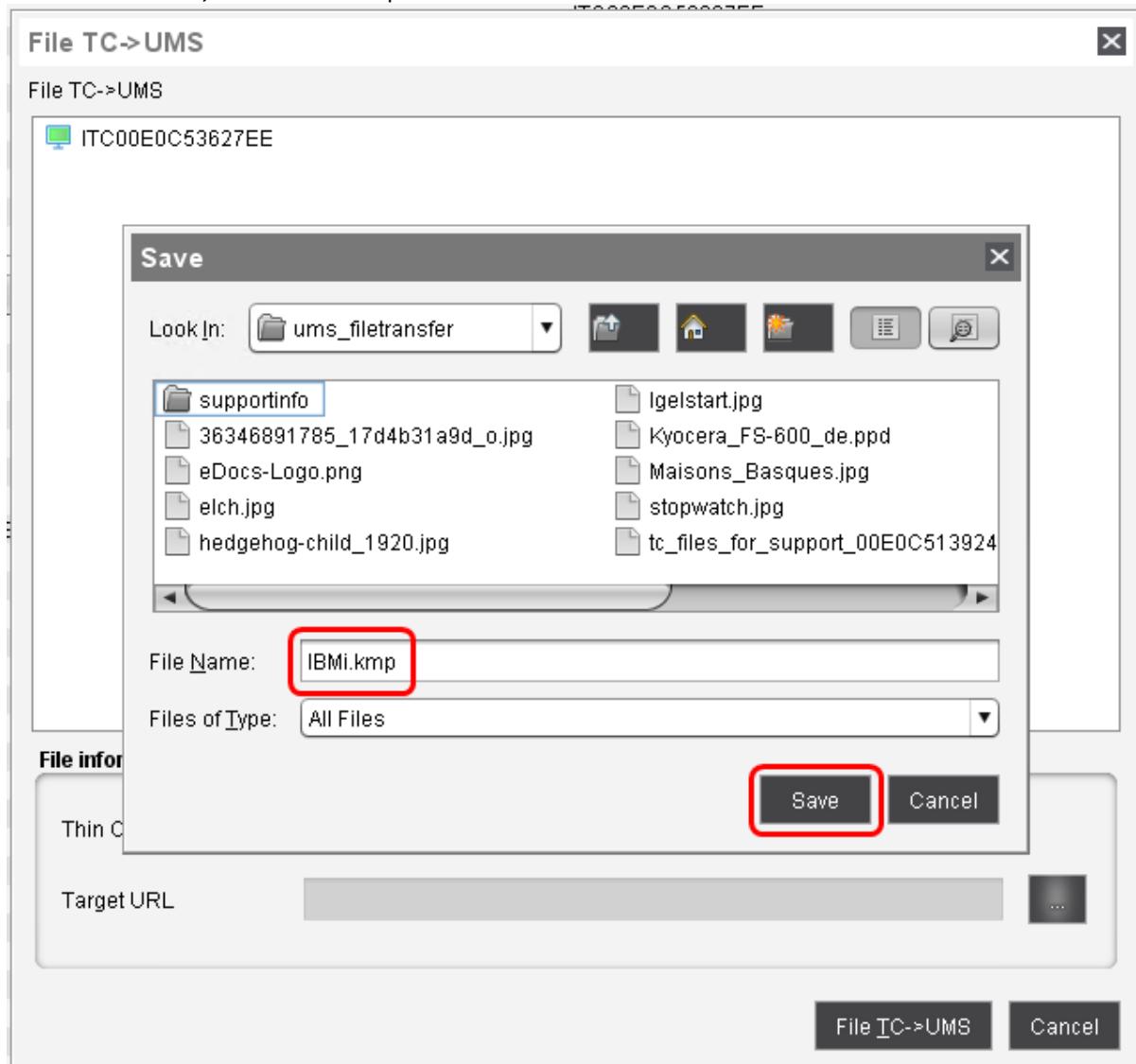


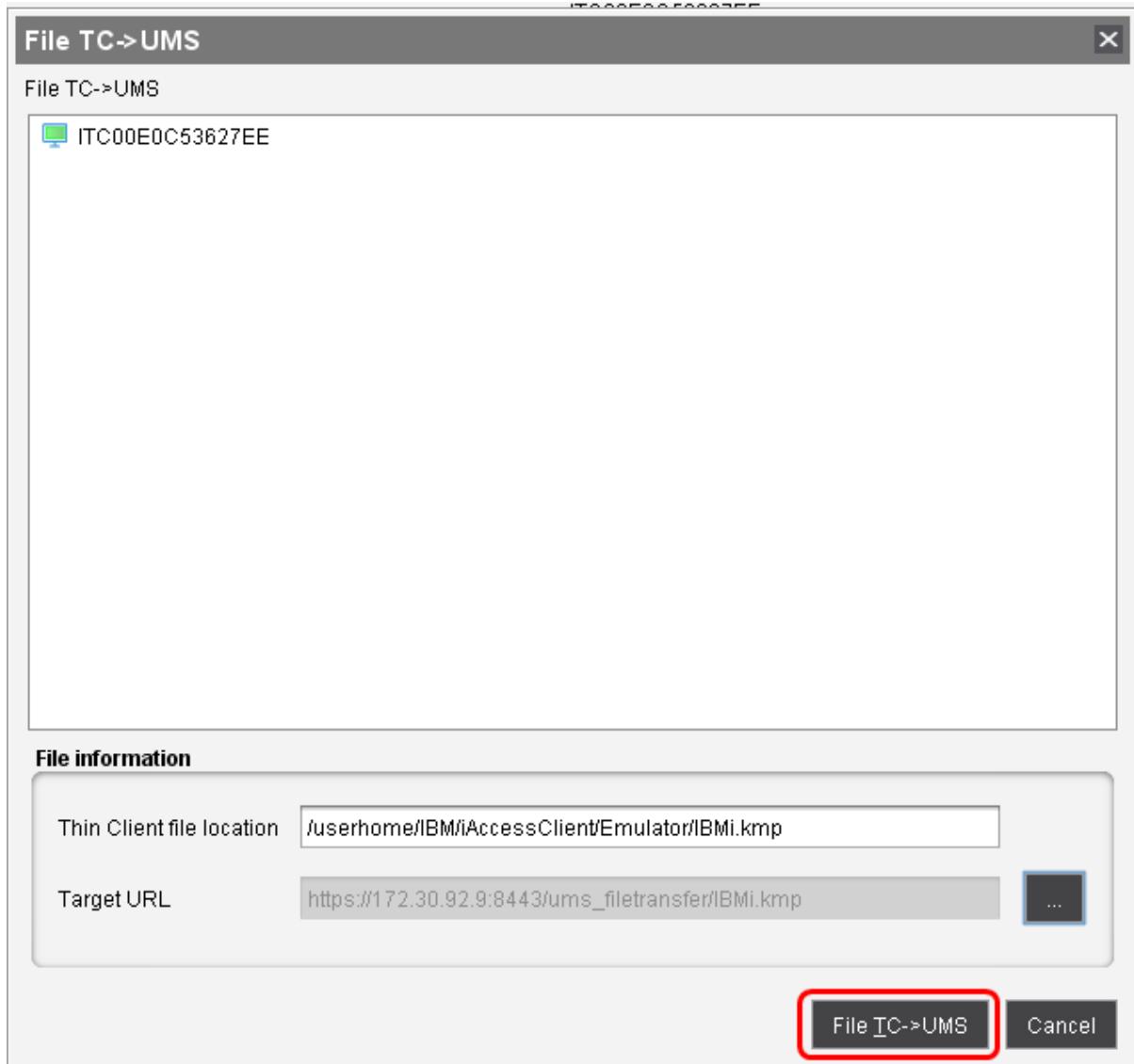
5. Choose a file location within the ums\_filetransfer folder.





6. Under **File Name**, enter IBMi.kmp and click **Save**.



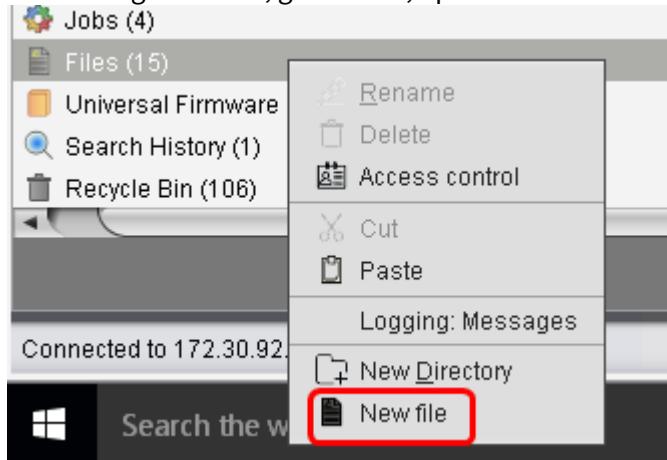
7. Click **TC->UMS**.

The file is stored within the UMS. Next, we will make it available as an object.

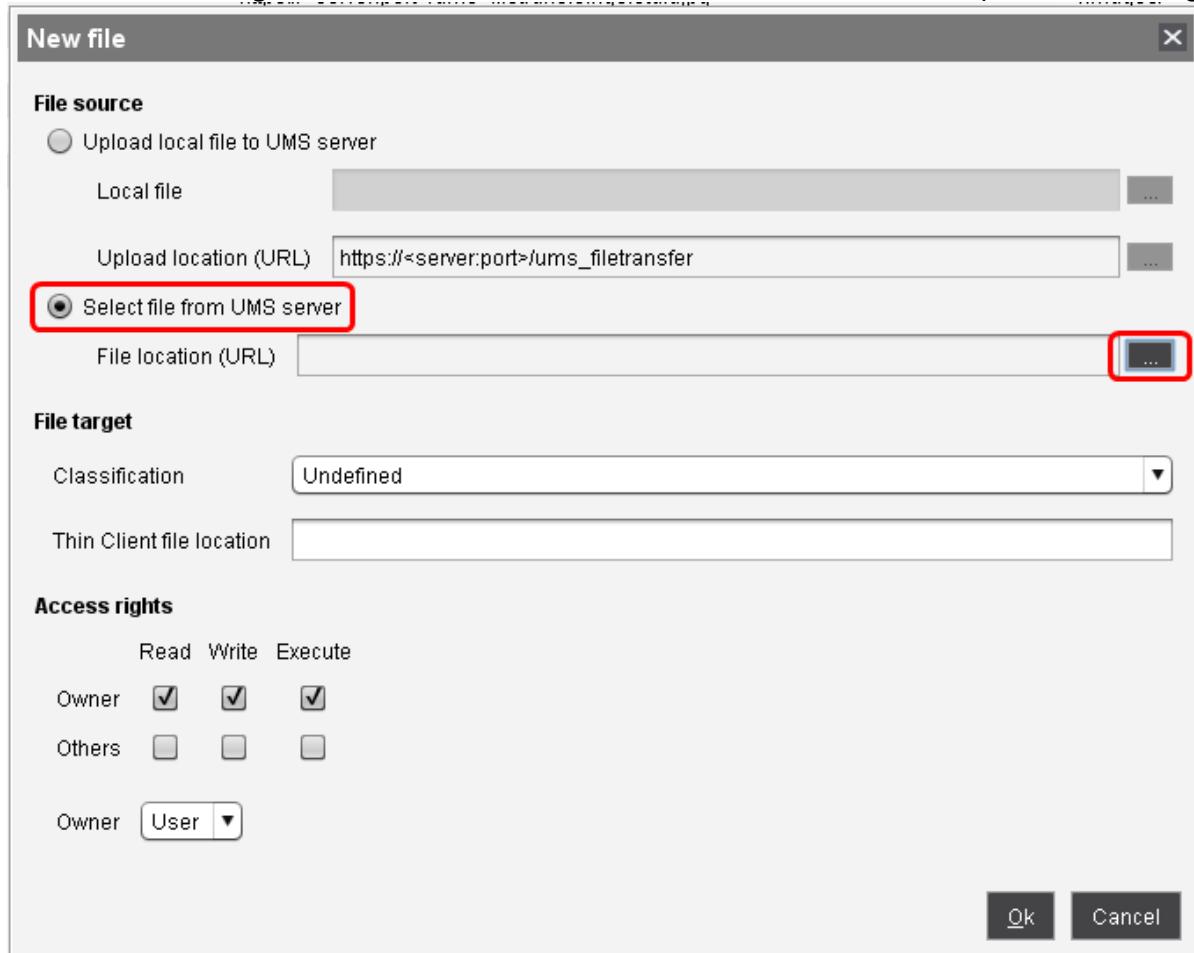


## Creating the File Object in the UMS

1. In the navigation tree, go to **Files**, open the context menu and choose **New file**.

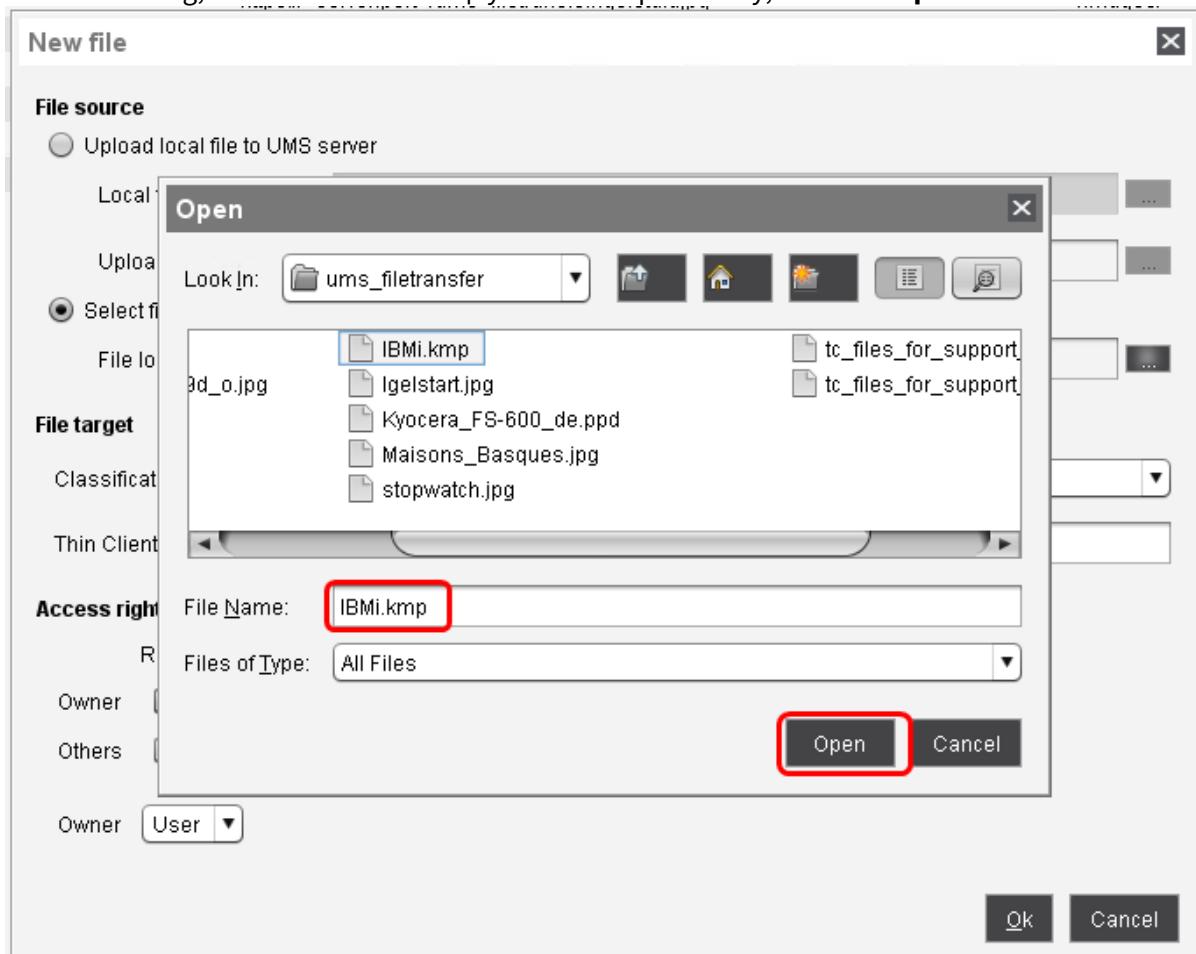


2. In the **New file** dialog, choose **Select file from UMS server** and click to open the file dialog.



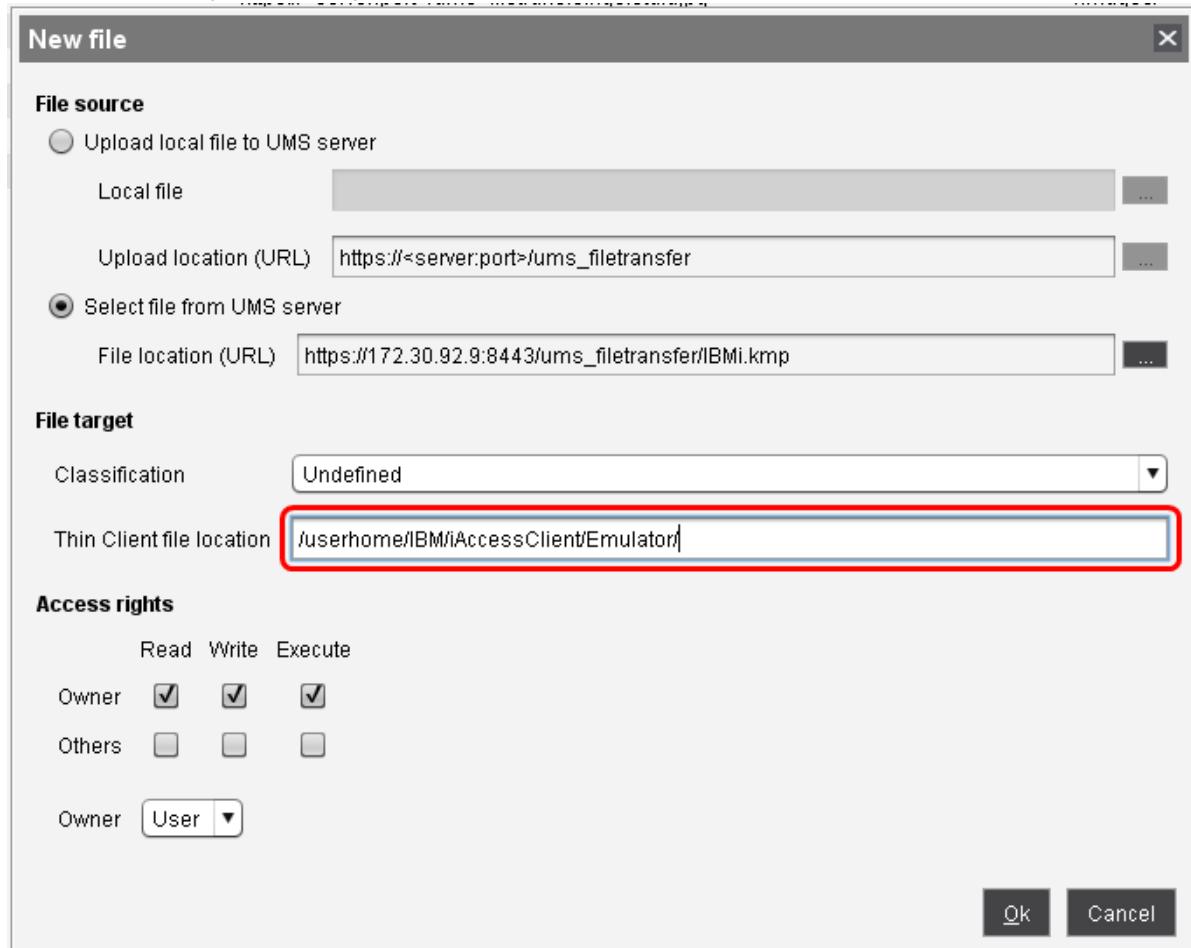


3. In the file dialog, find the file IBMi.kmp you created previously, and click **Open**.





4. Back in the **New file** dialog, enter the **Thin Client file location** as follows: /userhome/IBM/iAccessClient/Emulator/



5. Ensure that the **Access rights** and **Owner** are set as follows:

- **Owner** rights: **Read, Write, Execute**
- **Owner**: "User"



New file

**File source**

Upload local file to UMS server  
Local file

Select file from UMS server  
File location (URL)

**File target**

Classification

Thin Client file location

**Access rights**

	Read	Write	Execute
Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Others	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Owner



6. Click **Ok**.

The screenshot shows the 'New file' dialog box with the following configuration:

- File source:**
  - Upload local file to UMS server (radio button)
  - Local file: [Browse button]
  - Upload location (URL): `https://<server:port>/ums_filetransfer`
- Select file from UMS server (radio button)**
- File location (URL):** `https://172.30.92.9:8443/ums_filetransfer/IBMi.kmp`
- File target:**
  - Classification: `Undefined`
  - Thin Client file location: `/userhome/IBM/iAccessClient/Emulator/`
- Access rights:**

	Read	Write	Execute
Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Others	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Owner: User ▾
- Buttons:** Ok (highlighted with a red box) and Cancel

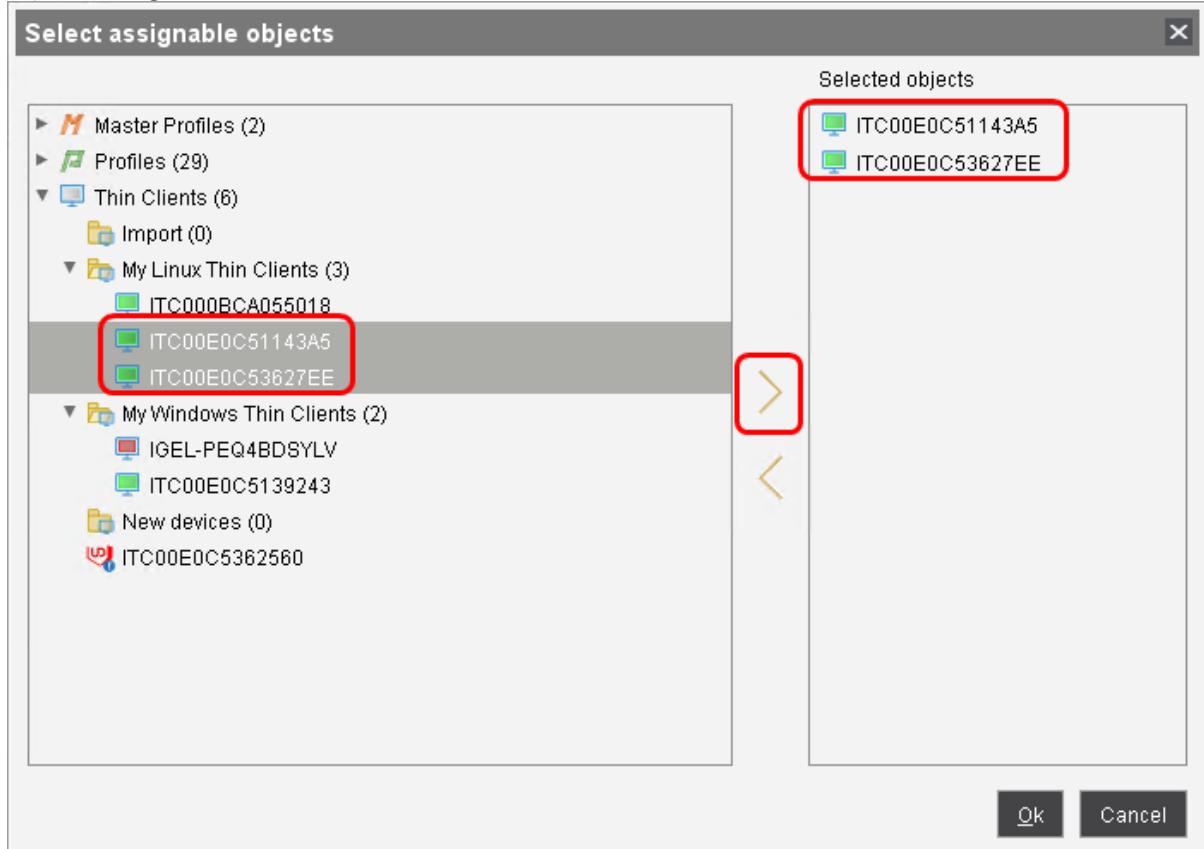
The file object "IBMi.kmp" is created.

#### Assigning the File Object to Thin Clients

1. In the navigation tree, select the file object "IBMi.kmp" and click  in the **Assigned objects** area (upper right).



2. In the **Select assignable objects** dialog, select the thin clients to which you want to assign the new key mapping and add them to the **Selected objects** area.

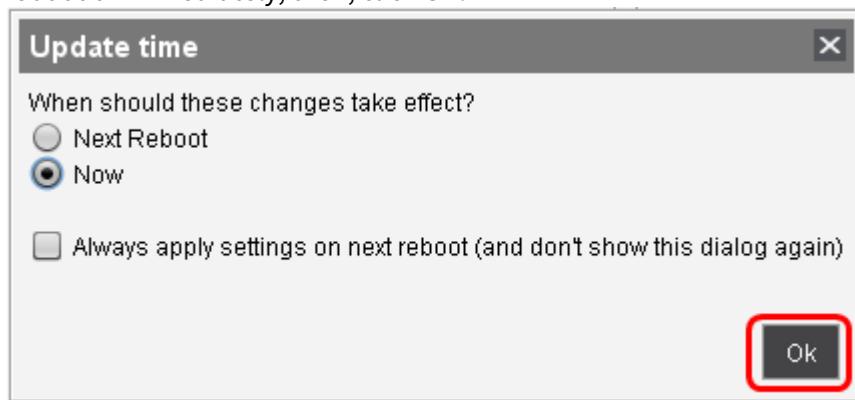




3. Click **Ok**.



4. In the **Update time** dialog, choose whether the file should be assigned to the thin clients at next reboot or immediately; then, click **Ok**.



The file is transferred to the thin clients.

## 2.9 Imprivata

- [Imprivata: Clear the Imprivata Data Partition](#)(see page 323)
- [Imprivata: Session Customization](#)(see page 323)



## 2.9.1 Imprivata: Clear the Imprivata Data Partition

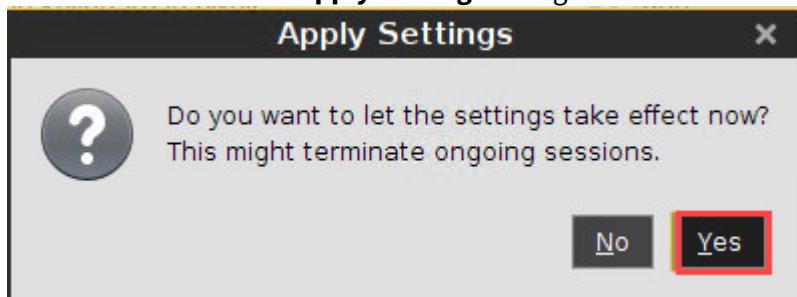
The function that explicitly clears the Imprivata data partition has been removed. However, you can simply emulate this feature by disabling and re-enabling the Imprivata appliance mode.

If you already have a valid appliance running and want to delete the Imprivata data partition, take the following steps:

1. In the IGEL Setup, go to **Sessions > Appliance Mode**.
2. Set **Appliance mode** to "Disabled".

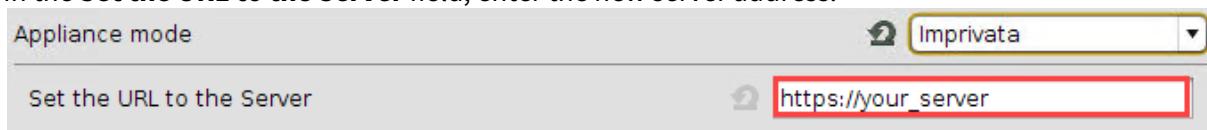


3. Click **Ok** to save the setting.
4. Click **Yes** to confirm the **Apply Settings** dialog.



Normal desktop mode is active. The Imprivata data partition is void now.

5. In the IGEL Setup, go to **Sessions > Appliance Mode**.
6. Set **Appliance Mode** to "Imprivata".
7. In the **Set the URL to the Server** field, enter the new server address.



8. Click **Ok** and confirm the **Apply Settings** dialog.
- Now you have a fresh Imprivata appliance mode without any outdated data.

## 2.9.2 Imprivata: Session Customization

You can make the same settings in the **IMPRIVATA\_RDP** (**IGEL Setup > RDP > RDP Sessions > IMPRIVATA\_RDP**) and **IMPRIVATA\_VMware** (**IGEL Setup > Horizon Client > Horizon Client Sessions > IMPRIVATA\_VMware**) sessions as in the standard sessions (see the description for [RDP Session](#)(see page 828) and [Horizon Client Session](#)(see page 860)).



**IMPRIVATA\_RDP** and **IMPRIVATA\_VMware** will be shown in the IGEL Setup when **Imprivata** is selected under **Setup > Sessions > Appliance Mode**, see [Imprivata](#)(see page 872).

However, the changes under the following subsections will be ignored:

### Imprivata\_Vmware Session

- **Connection Settings**

You can also ignore the VMware protocol selected by the Imprivata appliance by activating the registry key **imprivata.ignore\_horizon\_protocol** under **System > Registry**. Instead, the local selection under **Horizon Client > Horizon Client Global > Server Options > Preferred desktop protocol** will be used.

### Imprivata\_RDP Session

- **Server**
- **Logon**

## 2.10 Azure Virtual Desktop

This IGEL release is a build of IGEL OS which includes the AVD client as a configurable method for connecting to Azure Virtual Desktops.

- [Feature Matrix: AVD \(RDP3\) for IGEL OS 11](#)(see page 324)
- [How to Connect IGEL OS to Azure Virtual Desktop](#)(see page 327)

### 2.10.1 Feature Matrix: AVD (RDP3) for IGEL OS 11

The following matrix shows a selection of features and their state of implementation.

Feature	Linux RD Core SDK by Microsof t	IGEL OS RDP3 Client	Notes
AzureAD authentication	not applicable	yes	
Azure Resource Manager v2 Feed support	yes	yes	



Feature	Linux RD Core SDK by Microsof t	IGEL OS RDP3 Client	Notes
Folder redirection	yes	yes	Folder redirection is bound to the /media folder, so that locally mounted storage devices, including USB sticks, will be forwarded to the remote session.
Dynamic folder redirection	no	no	User may select specific drives/folders to redirect at run time.
Smartcard redirection	no	no	Smartcard redirection is implemented but not working. The problem exists in the RD Core SDK.
Clipboard redirection (text and images)	yes	yes	
Clipboard redirection (files)	no	no	
Microphone redirection	yes	yes	
Speaker redirection	yes	yes	
Webcam redirection	not applicabl e	yes	<a href="#">Fabulatech webcam redirection</a> (see page 1015) is implemented.
Printer redirection	no	yes	<a href="#">ezeep cloud printing</a> (see page 1024) is implemented. It is directly related to the ThinPrint configuration. <a href="#">CUPS printer redirection</a> (see page 1023) is implemented.
USB redirection	not applicabl e	yes	<a href="#">Fabulatech USB redirection</a> (see page 1015) is implemented.
Scanner redirection	not applicabl e	yes	<a href="#">Fabulatech scanner redirection</a> (see page 1015) is implemented.
Mouse input	yes	yes	
Keyboard input (scancodes)	yes	yes	
Keyboard input (Unicode)	yes	yes	



Feature	Linux RD Core SDK by Microsof t	IGEL OS RDP3 Client	Notes
Keyboard input mapping of dead/special keys	not applicable	yes	
Teams conferencing redirection	no	no	Teams redirection will be added as soon as it is available in the RD Core SDK.
Zoom conferencing redirection	not applicable	yes	<a href="#">Zoom redirection</a> (see page 1024) cannot be activated globally, but only for a specific session.
Multitouch redirection	no	no	No multitouch API present in the Linux RD Core SDK by Microsoft.
AVC Codec support (hardware acceleration)	yes	work in progress	
Dynamic display change	yes	yes	
Monitor DPI sync	yes	yes	
Monitor Layout Sync (multimon)	yes	yes	
Restrict full-screen sessions to single display	not applicable	yes	
On-premises services	not applicable	work in progress	
RemoteApps	yes	limited	Current user interface for RemoteApps control is to be further improved.
Seamless apps	work in progress	no	
Session auto reconnect	yes	yes	
Proxy support	yes	yes	
Local hostname in a session	yes	yes	



Feature	Linux RD Core SDK by Microsoft	IGEL OS RDP3 Client	Notes
Launch a single resource session/application	not applicable	yes	A resource is launched if only one resource is returned.
Dynamic virtual channel support	yes	work in progress	
UDP network support	work in progress	no	
User-definable hotkeys	not applicable	yes	Session chooser, session switcher, minimize to taskbar
Realtime user experience indicator	work in progress	no	
Configurable AVD Resource Feed	yes	yes	

## 2.10.2 How to Connect IGEL OS to Azure Virtual Desktop

### Quick Start Guide

This section describes how to set up an Azure Virtual Desktop (AVD) session (formerly Windows Virtual Desktop, WVD) with IGEL's AVD client based on Microsoft's RD Core SDK for Linux which can be used to connect to an AVD deployment.

### Requirements

- Device with IGEL OS 11.03.261 or higher; download the latest version at [igel.com/avd](https://www.igel.com/igel-solution-family/windows-virtual-desktop/)<sup>149</sup>
- Azure Virtual Desktop deployment

### Instructions

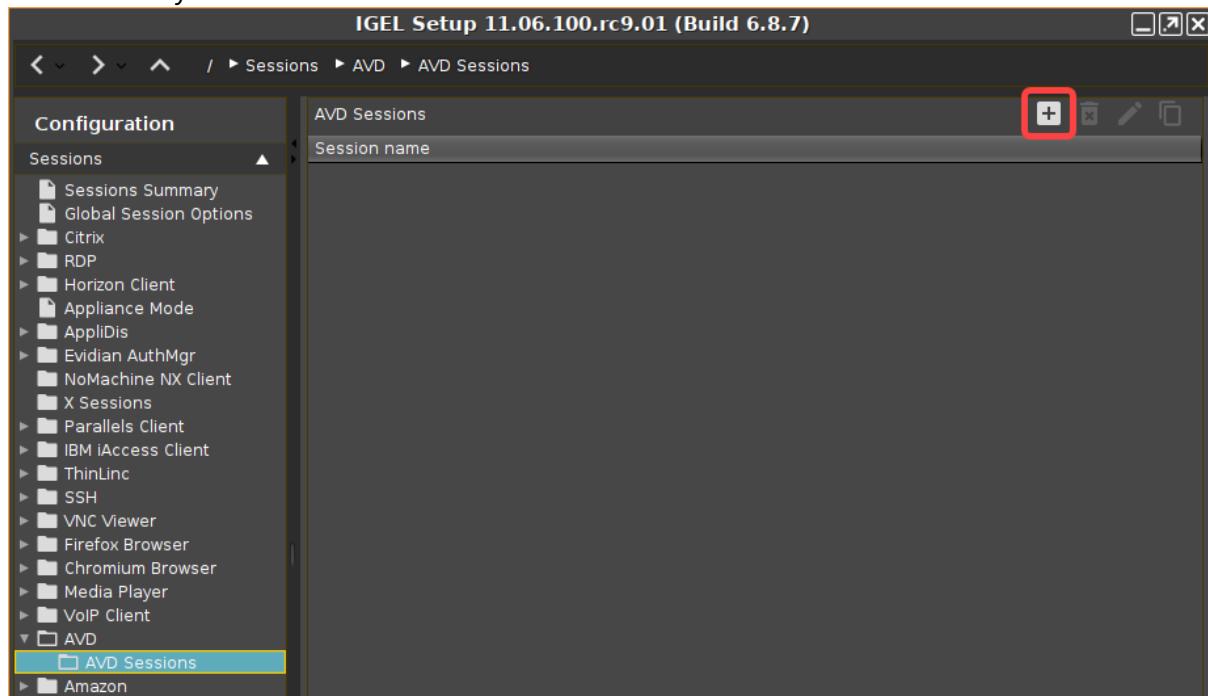
1. Open the Setup or the configuration dialog in the UMS and go to **Sessions > AVD > AVD Sessions**.

---

<sup>149</sup> <https://www.igel.com/igel-solution-family/windows-virtual-desktop/>



2. Click the **+** symbol to create a new AVD session instance.





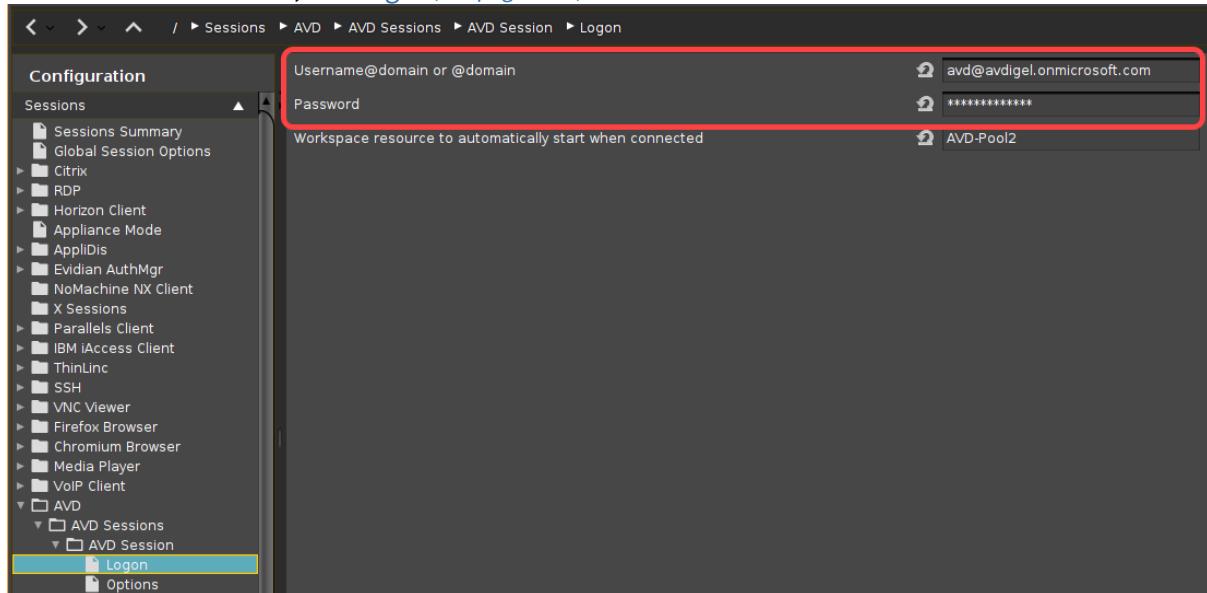
3. Enter a **Session name** and configure the starting methods according to your needs.

A screenshot of the IGEL OS Configuration software. The left sidebar shows a tree view of session types: Sessions, Citrix, RDP, Horizon Client, Appliance Mode, AppliDis, Evidian AuthMgr, NoMachine NX Client, X Sessions, Parallels Client, IBM iAccess Client, ThinLinc, SSH, VNC Viewer, Firefox Browser, Chromium Browser, Media Player, VoIP Client, and AVD. Under AVD, AVD Sessions is expanded, and AVD Session is selected. The main panel is titled "Session name" and contains "AVD Session". It includes sections for "Starting Methods for Session" (with checkboxes for Start Menu, Application Launcher, Desktop, Quick Start Panel, and three others), "Menu folder", "Application Launcher folder", "Desktop folder", "Password Protection" (set to None), "Hotkey" (disabled), "Modifiers" (set to None), "Key" (disabled), and "Autostart" (checkboxes for Autostart, Restart, and Autostart Delay set to 0). At the bottom are "Apply", "Ok", and "Cancel" buttons.

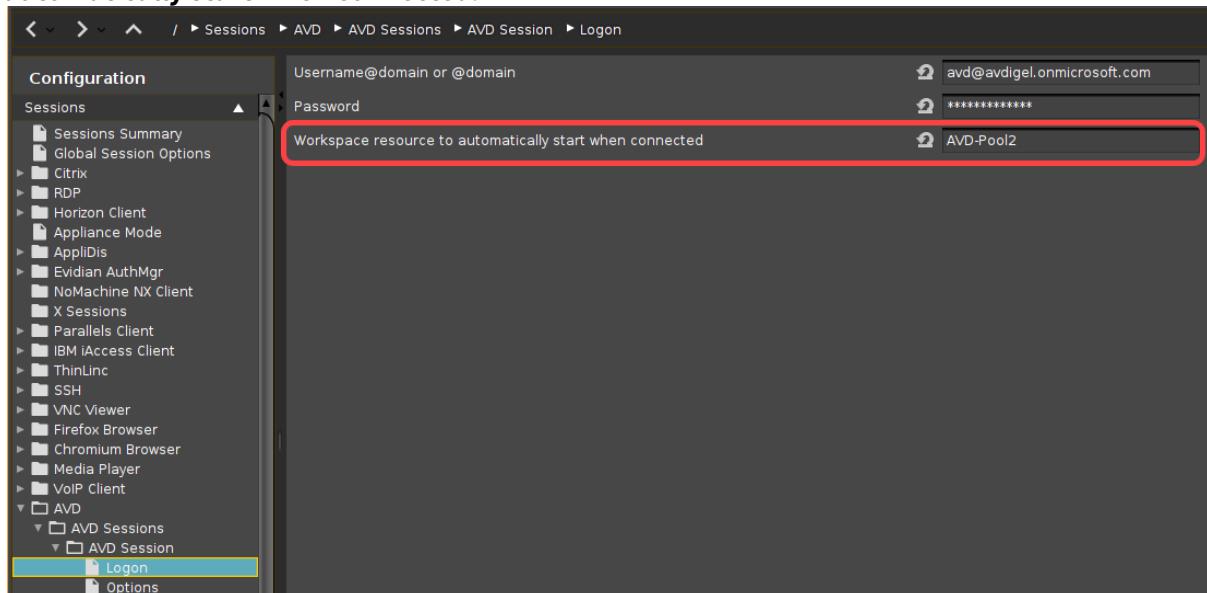
4. If the login is to be started automatically on session startup, go to **Sessions > AVD > AVD Sessions** > **[Session name]** > **Logon** and enter your credentials under **Username@domain or @domain** an



d **Password.** For details, see [Logon](#)(see page 1020).

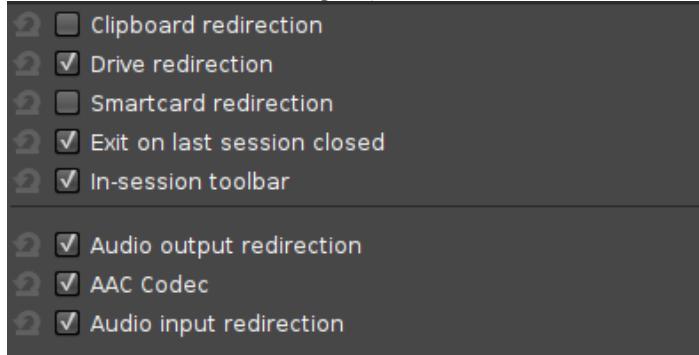


5. If a specific resource is to be started automatically, enter its name under **Workspace resource to automatically start when connected**.

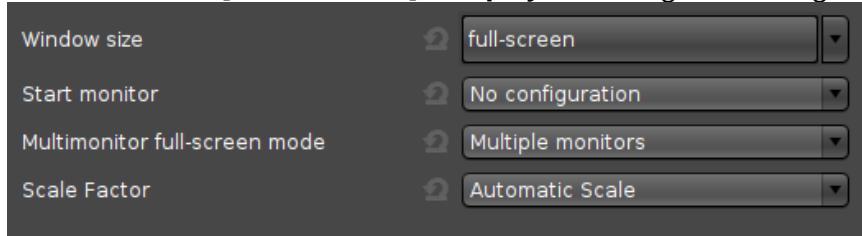




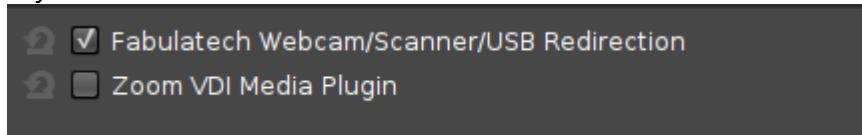
6. Go to **Sessions > AVD > AVD Sessions > [Session name] > Options** and enable or disable features and redirections according to your needs.



7. If you do not want to run the AVD client on all available screens in fullscreen, go to **Sessions > AVD > AVD Sessions > [Session name] > Display** and change the settings according to your needs.



8. Go to **Sessions > AVD > AVD Sessions > [Session name] > Plugins** and enable features according to your needs.



9. Click **Apply** or **OK**.

The AVD session is configured and can be started with the starting methods you have configured in step 3.

If you want to configure further AVD sessions, start again from step 2.

See also the reference manual chapter [AVD Session](#)(see page 1018).

## 2.11 SSH

- [Enable Weaker Algorithms in the Built-in OpenSSH Server](#)(see page 332)
- [Enable Weaker Algorithms in the SSH Client](#)(see page 332)
- [SSH: Deprecation of Weak Algorithms as of IGEL Linux 10.04.100](#)(see page 333)



## 2.11.1 Enable Weaker Algorithms in the Built-in OpenSSH Server

### Problem

You are trying to connect to the built-in OpenSSH server of IGEL OS with an SSH client which does not support the strong algorithms of the server.

### Solution

To enable weaker encryption algorithms, proceed as follows:

1. In Setup, go to **System > Registry > network > ssh\_server**.
2. Change the settings according to your requirements:
  - **disable\_weak\_encryption**: Disable this option to enable weaker encryption.
  - **disable\_weak\_hostkey\_algos**: Disable this option to enable weaker host key algorithms.
  - **disable\_weak\_kexalgorithms**: Disable this option to enable weaker key exchange algorithms.
  - **disable\_weak\_macs**: Disable this option to enable weaker MACs.
  - **minimal\_encryption\_level**: The minimal level of encryption

## 2.11.2 Enable Weaker Algorithms in the SSH Client

### Environment

IGEL Linux 10.04.100 or higher

### Problem

You are trying to connect to an SSH server which does not support the strong algorithms enabled by default in the SSH client.

### Solution

To enable weaker encryption algorithms, proceed as follows:

1. In Setup, go to **System > Registry > network > ssh\_client**.
2. Change the settings according to your requirements:
  - **disable\_weak\_encryption**: Disable this option to enable weaker encryption.
  - **disable\_weak\_hostkey\_algos**: Disable this option to enable weaker host key algorithms.
  - **disable\_weak\_kexalgorithms**: Disable this option to enable weaker key exchange algorithms.
  - **disable\_weak\_macs**: Disable this option to enable weaker MACs.
  - **minimal\_encryption\_level**: The minimal level of encryption



### 2.11.3 SSH: Deprecation of Weak Algorithms as of IGEL Linux 10.04.100

As of IGEL Linux 10.04.100, certain older, less secure algorithms are deprecated in both the SSH client and server.

The following table shows the algorithms enabled by default as of IGEL Linux version 10.04.100.

Key exchange algorithms	<ul style="list-style-type: none"> <li>• curve25519-sha256@libssh.org</li> <li>• ecdh-sha2-nistp521</li> <li>• ecdh-sha2-nistp384</li> <li>• ecdh-sha2-nistp256</li> <li>• diffie-hellman-group-exchange-sha256</li> </ul>
Message authentication codes (MACs)	<ul style="list-style-type: none"> <li>• hmac-sha2-512-etm@openssh.com</li> <li>• hmac-sha2-256-etm@openssh.com</li> <li>• umac-128-etm@openssh.com</li> <li>• hmac-sha2-512</li> <li>• hmac-sha2-256</li> <li>• umac-128@openssh.com</li> </ul>
Host keys	<ul style="list-style-type: none"> <li>• ssh-ed25519-cert-v01@openssh.com</li> <li>• ssh-rsa-cert-v01@openssh.com</li> <li>• ssh-ed25519</li> <li>• ssh-rsa</li> <li>• ecdsa-sha2-nistp521-cert-v01@openssh.com</li> <li>• ecdsa-sha2-nistp384-cert-v01@openssh.com</li> <li>• ecdsa-sha2-nistp256-cert-v01@openssh.com</li> <li>• ecdsa-sha2-nistp521</li> <li>• ecdsa-sha2-nistp384</li> <li>• ecdsa-sha2-nistp256</li> </ul>

If you need to enable weaker algorithms, see [Enable Weaker Algorithms in the SSH client](#)(see page 332) and/or [Enable Weaker Algorithms in the Built-in OpenSSH Server](#)(see page 332).

## 2.12 Amazon WorkSpaces – Teradici PCoIP Sessions

As of IGEL OS 11.06, you can configure an Amazon WorkSpaces session under **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces Session**, see [Amazon WorkSpaces](#)(see page 1026).

Alternatively, you can use Amazon WorkSpaces via [Teradici PCoIP](#)(see page 1011). The articles below will show you how you can do that.

- [Connecting IGEL OS Devices with Amazon WorkSpaces via PCoIP](#)(see page 334)
- [Use IGEL Setup for Configuration – Connecting with AWS via PCoIP](#)(see page 337)
- [Broker Types – Amazon WorkSpaces](#)(see page 338)
- [How Can I Use H.264 Acceleration in a Teradici PCoIP Session?](#)(see page 339)



## 2.12.1 Connecting IGEL OS Devices with Amazon WorkSpaces via PCoIP

You can set up and use IGEL OS devices via PCoIP with Amazon WorkSpaces.

### Set Up the Device Connection

Before you connect the device to the Amazon WorkSpaces for the first time, you might need to change some settings. Your Amazon WorkSpaces administrator can provide you with additional setup instructions that are needed for your particular environment.

#### Session Connection

To set the session connection:

1. In the IGEL Setup, go to **Sessions > Teradici PCoIP Client > PCoIP Sessions**.
2. Click to create a new session.
3. Go to **Connection Settings**.
4. Set **Server certificate verification mode** to "Warn but allow".



If you do not enable **Use IGEL Setup for configuration**, you have to enter the host address or code in the Teradici PCoIP Client login window. See the screenshot under "Connecting to Amazon WorkSpaces".

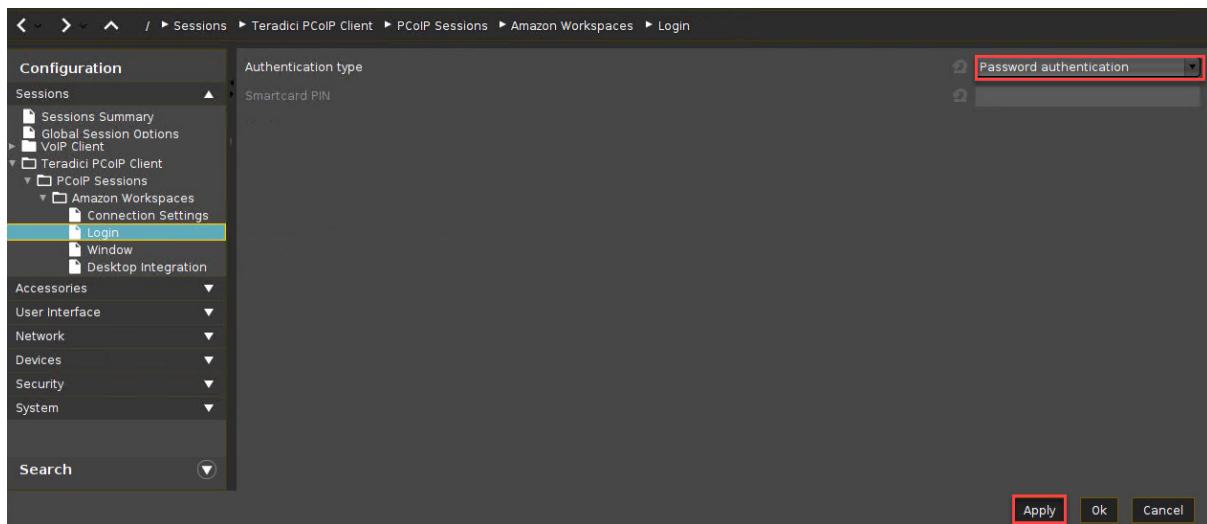
If you activate **Use IGEL Setup for configuration**, see [Use IGEL Setup for Configuration – Connecting with AWS via PCoIP](#)(see page 337).

For more information about the connection with the **Broker type** "PCoIP broker" or "Hardhost", see [Broker Types – Amazon WorkSpaces](#)(see page 338).

5. Click **Apply**.



6. Go to **Login** and set **Authentication type** to "Password authentication". Afterward, click **Apply**.



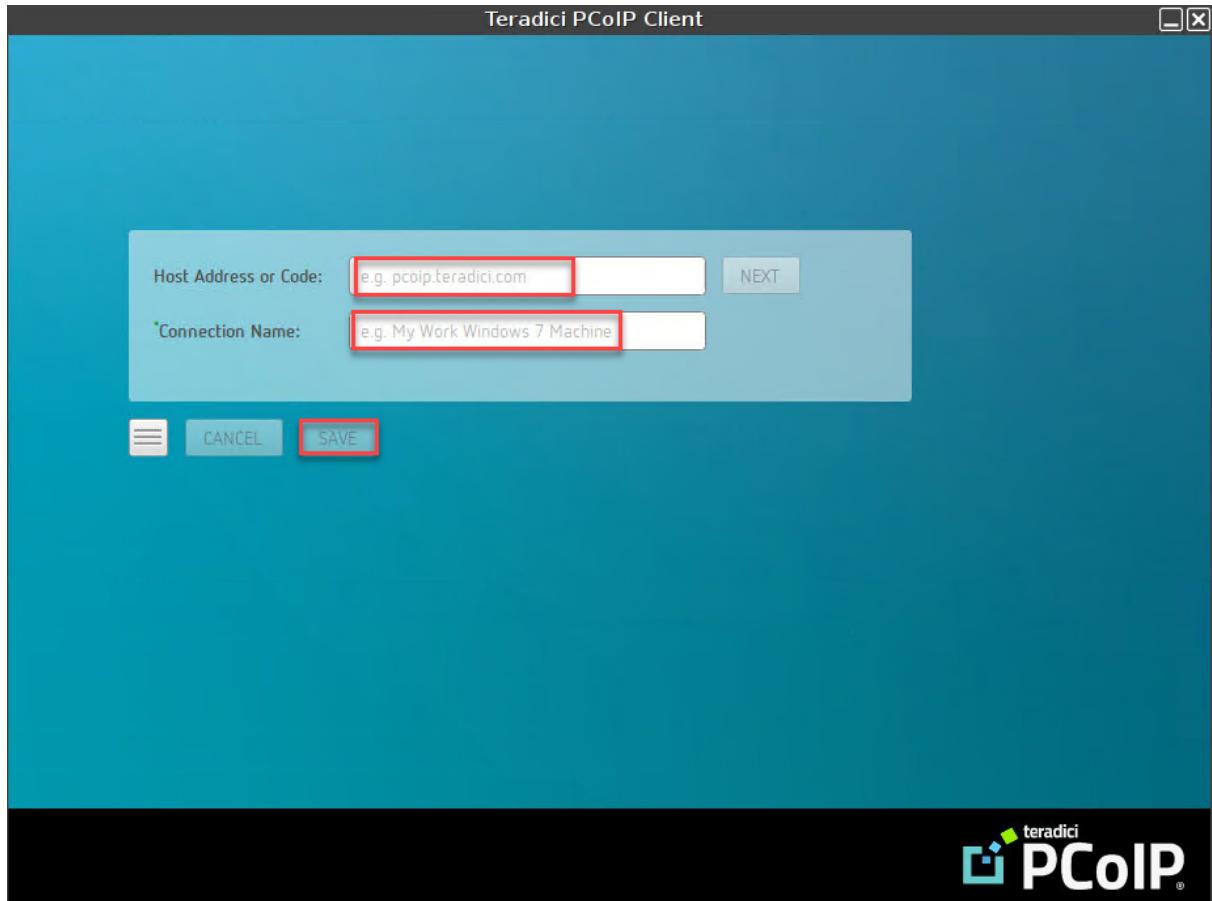
## Connecting to Amazon WorkSpaces

1. Double-click on the **AWS WorkSpaces** icon on your desktop.



The **Teradici PCoIP Client** dialog opens.

2. Enter the **Host Address or Code** that has been sent to you in the welcome e-mail from Amazon WorkSpaces.
3. Enter the **Connection Name** and click **SAVE**.



4. Enter your Amazon WorkSpaces credentials.
5. Enter the **Multi-Factor Authentication (MFA) Token**.

Multi-factor authentication is a proof of user identity which combines two different components (factors) that are independent from one another.

If you do not use multi-factor authentication, you still need to enter something in the MFA field, even when it is just a number or "1234".

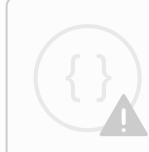
Otherwise, no connection to Amazon WorkSpaces can be established.

6. Click **Ok**.

The Amazon WorkSpaces desktop is shown.



See also our video description on youtube:



Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:

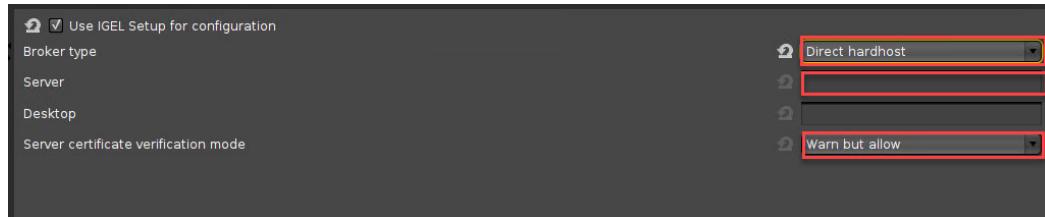
<https://www.youtube.com/watch?v=NDQxTEKLPZE>

## 2.12.2 Use IGEL Setup for Configuration – Connecting with AWS via PCoIP

### Configuring in the IGEL Setup

If you want to use the IGEL Setup for the configuration, proceed as follows:

1. Enable **Use IGEL Setup for Configuration**.
2. Select the **Broker type** you want to connect to Amazon WorkSpace.
  - a. Broker type: **Direct hardhost**
    - Enter the AWS WorkSpace's Registration Code as **Server**.
    - Set **Server certificate verification mode** to "Warn but allow".



- b. Broker type: **PCoIP broker**
  - Enter the server from the PCoIP broker as **Server**.
  - Set **Server certificate verification mode** to "Warn but allow".

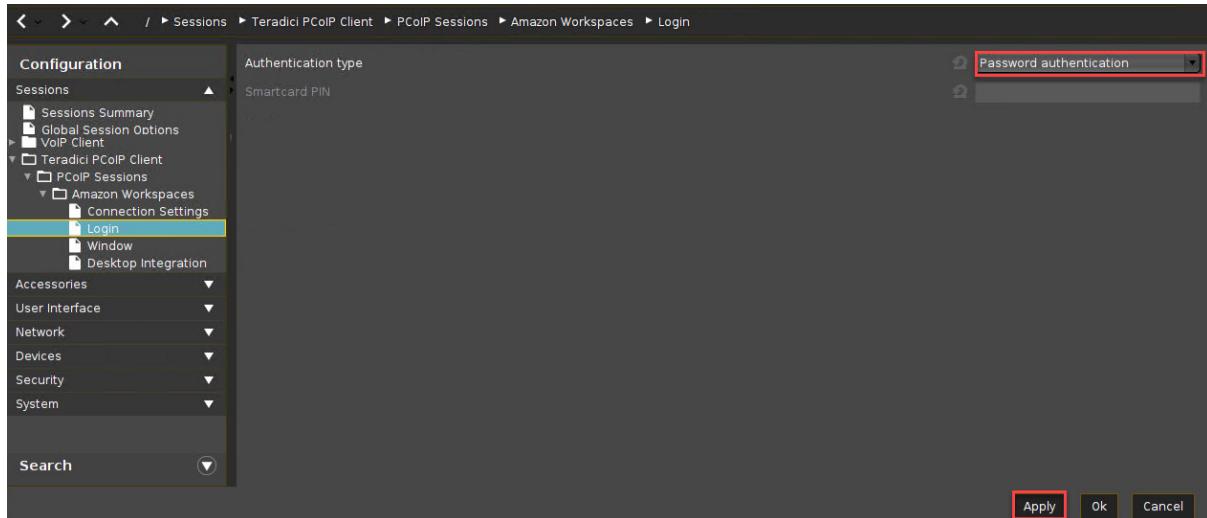


For more information about the broker types, see [Broker Types – Amazon WorkSpaces](#)(see page 338).

3. Click **Apply**.



4. Go to **Login** and set **Authentication type** to "Password authentication".
5. Click **Apply**.



### Connecting to Amazon WorkSpaces

1. Double-click on the **AWS WorkSpaces** icon on your desktop.



2. The Teradici PCoIP Client mask takes over the information you entered in the IGEL Setup.
3. Click **SAVE**.
4. Now enter your Amazon WorkSpace credentials.

For the rest of the procedure, see [aws.amazon.com](https://aws.amazon.com)<sup>150</sup>.

### 2.12.3 Broker Types – Amazon WorkSpaces

You can choose between two broker types with which you connect to Amazon WorkSpaces.

#### PCoIP Broker

PCoIP broker is a resource manager that dynamically assigns host PCs to zero clients based on the identity of the user establishing from the zero client. Connection brokers are also used to allocate a pool of hosts to a group of

---

<sup>150</sup> [https://aws.amazon.com/de/?nc2=h\\_lg](https://aws.amazon.com/de/?nc2=h_lg)



zero clients in a PCoIP deployment are configured to always connect to the same host (i.e., a static one-to-one pairing), then a connection broker is not required.



## Direct Hardhost

A direct hardhost is a direct connection between a zero client and a remote workstation containing a PCoIP Remote Workstation Card. You can specify a host's DNS name or IP address, or you can configure clients to use Service Location Protocol (SLP) to discover a host. You can also configure clients to automatically reconnect to a host when a session is lost.



## 2.12.4 How Can I Use H.264 Acceleration in a Teradici PCoIP Session?

### Question

How must I configure the client and the server to get H.264 acceleration in a Teradici PCoIP Session?

### Environment

This article is valid for the following environment:

- IGEL OS 11.04 or higher
- UMS 6.04 or higher
- Teradici PCoIP Graphics Agent for Windows 20.04

### Answer

#### Server-side

1. Open the Group Policy Editor (gpedit.msc).
2. Go to **Local Computer Policy > Administrative Templates > PCoIP Session Variables > Overridable Administrator Defaults**.
3. Edit the settings as follows:



- Set **Configure PCoIP image quality levels** to "Enabled".
- Set **Configure PCoIP image quality levels > YUV chroma subsampling** to "4:2:0".
- Set **Enable PCoIP Ultra GPU optimization** to "Enabled".

Client-side

1. Open the Setup or the UMS configuration dialog.
2. Go to **System > Registry > pcoip > codec\_h264** and activate **H.264 codec** (registry parameter: `pcoip.codec_h264`).
3. Save your settings.

## 2.13 Login Enterprise Configuration

With Login Enterprise Launcher (former Login PI), you can test changes that affect the performance of desktop and application logins, as well as the current processing of both applications and specific tasks inside of a given application before you implement them on real devices.

- [Login Enterprise Launcher in IGEL OS](#)(see page 340)
- [Getting the Secret for Login Enterprise Launcher](#)(see page 344)
- [Using the Login Enterprise Launcher within a VMware Horizon Session](#)(see page 347)

### 2.13.1 Login Enterprise Launcher in IGEL OS

#### Requirements

- IGEL OS 11.03.100 or higher

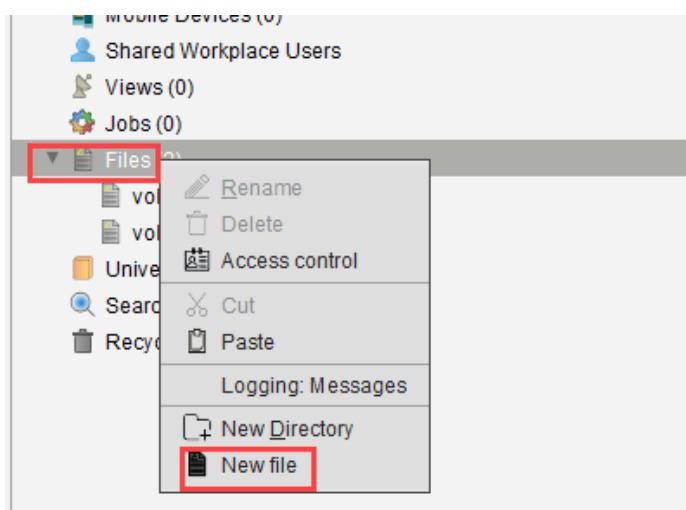
#### Uploading the SSL Certificate

In order to use Login Enterprise Launcher (former Login PI), you need first to download the SSL certificate from your Login Enterprise server: <https://yourServerURL/contentDelivery/content/CA.crt>. Click **Go on to the webpage**. Download the certificate.

You have to rename the file name from CA.crt to LoginPI.crt.



1. Open the **UMS Console**.
2. Select **New File** in the **Files** context menu.

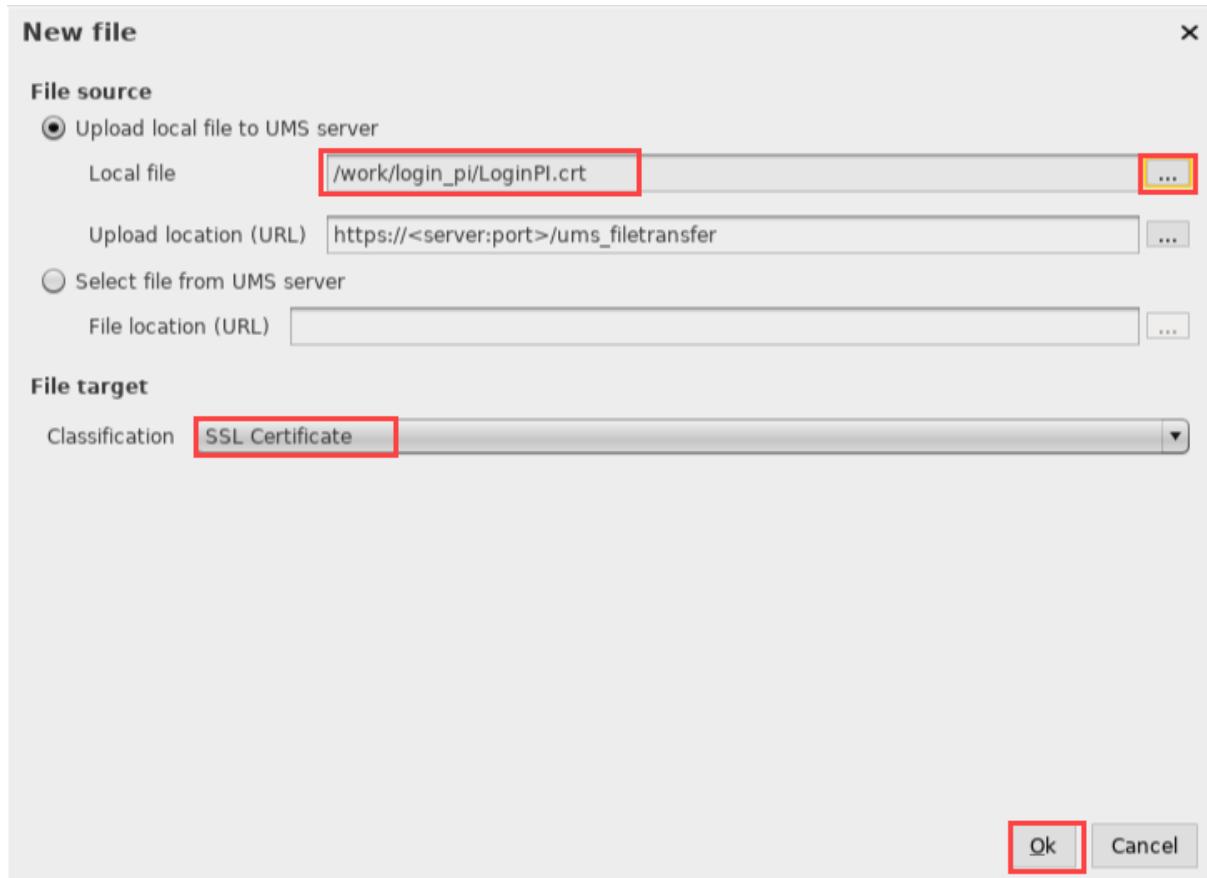


The window **New file** opens.

3. Select the **Local file** under **Upload local file to UMS server**.

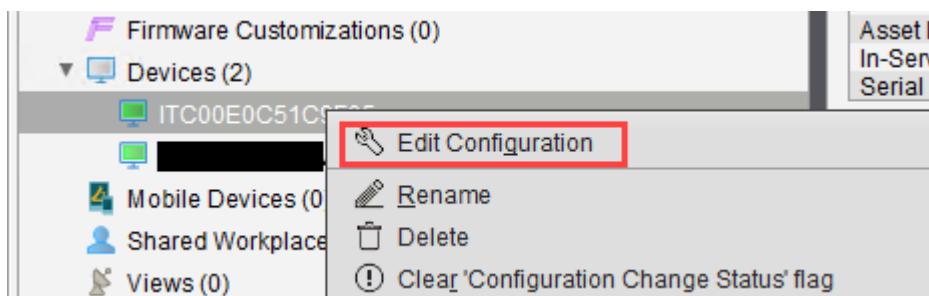


4. Choose **SSL Certificate** under **Classification** and click **Ok**.



## Configuration of Login Enterprise Launcher

- Under **Devices** in the UMS structure tree, choose the device and click **Edit Configuration** in its context menu. Or you can create a new profile with the required settings under **Profiles** and assign it to the device, see [Creating Profiles<sup>151</sup>](#).



- Go to **Accessories > Login Enterprise**.

<sup>151</sup> <https://kb.igel.com/display/endpointmgmt608/Creating+Profiles>



3. Enter the **Server URL** of your Login Enterprise server.
4. Enter the **Secret**, see [Getting the Secret for Login Enterprise Launcher\(see page 344\)](#).

The screenshot shows the 'Configuration' section of the IGEL software. On the left, there's a tree view with 'Configuration' expanded, showing various tools like Screenshot Tool, On-screen keyboard, Monitor Calibration, etc., and 'Login Enterprise' selected. The main pane displays the 'Login Enterprise-Launcher' configuration. It includes a detailed description of what the launcher does and two input fields: 'Server URL' containing 'https://loginpi.igel.example' and 'Secret' containing a redacted password.

5. Save the settings.

If you want to use the Login Enterprise Launcher within a VMware session, see [Using the Login Enterprise Launcher within a VMware Horizon Session\(see page 347\)](#).

## Starting the Login Enterprise Launcher from the UMS

After the Login Enterprise server has been set up, you can create a job in the UMS for the automatic start of your Login Enterprise Launcher at a defined time.

1. Select **Jobs** in the UMS structure tree and choose **New Scheduled Job** in the context menu.

The screenshot shows the UMS (User Management System) interface. The left sidebar shows a tree view with 'Mobile Devices (0)', 'Shared Workplace Users', 'Views (0)', and 'Jobs (4)' selected. A context menu is open over the 'Jobs' folder, listing options: Rename, Delete, Access control, Cut, Paste, Logging: Messages, New Directory, and New Scheduled Job. The 'New Scheduled Job' option is highlighted with a mouse cursor. A callout box labeled 'New Scheduled Job' points to the menu item.

The **New Scheduled Job** window opens.



2. Under **Name**, enter the name for the job, e.g. "Login Enterprise".
3. Choose **Start Login Enterprise Launcher** under **Command**.

**New Scheduled Job**

**Details**

Name	Login Enterprise
Command	Start Login Enterprise launcher
Execution time	15:24
Start date	2020-03-12
Comment	

**Options**

<input checked="" type="checkbox"/> Log results	<input type="checkbox"/> Retry next boot
Max. Threads	99
Delay	0 Seconds
Timeout	30

**Job-Info**

Job ID	
Next Execution	
User	

[Back](#)  [Next](#) [Finish](#) [Cancel](#)

4. Select the **Execution time** and **Start date**.
5. Click **Next** and assign the devices.
6. Click **Finish** to save the job.

To learn more about using Login Enterprise with IGEL, see <https://www.loginvsi.com/igel/> and the following webinar:



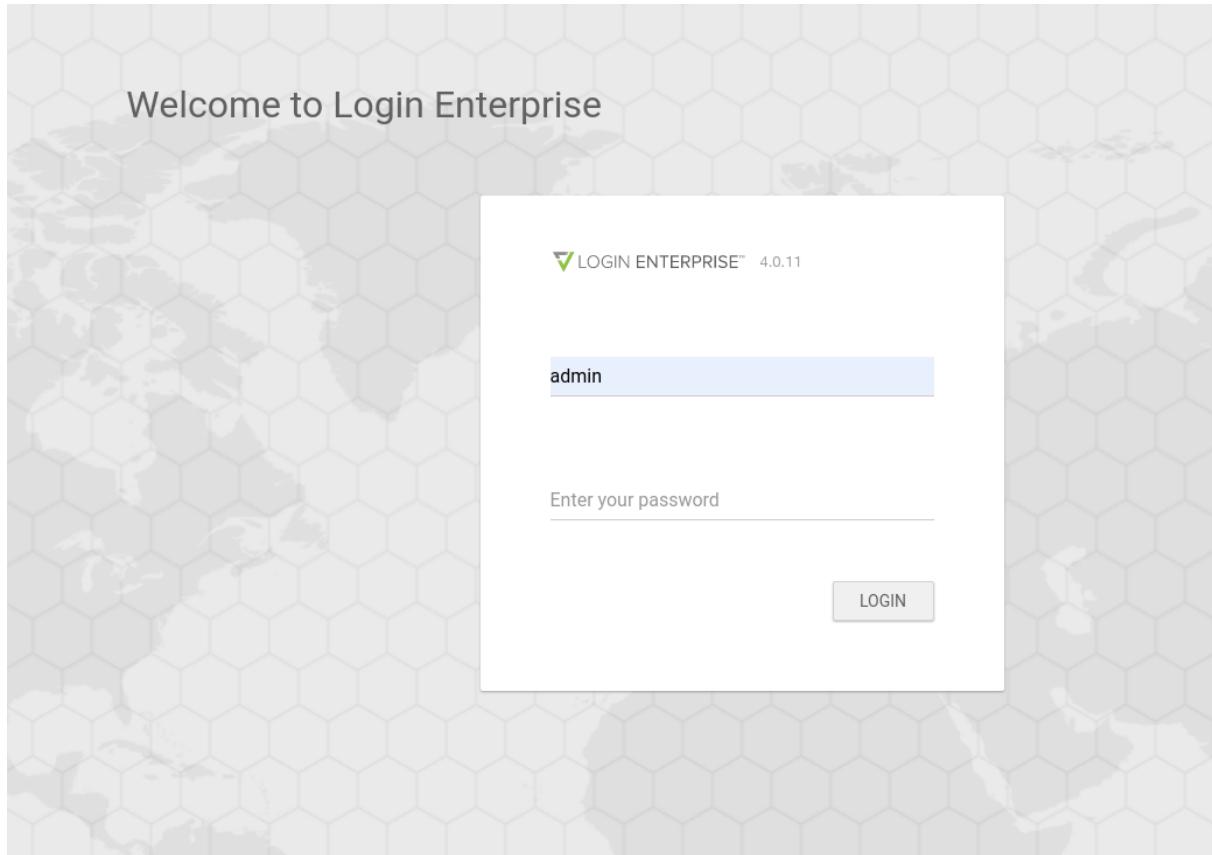
Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:  
<https://www.youtube.com/watch?v=N2L6z4nk8zQ>

## 2.13.2 Getting the Secret for Login Enterprise Launcher

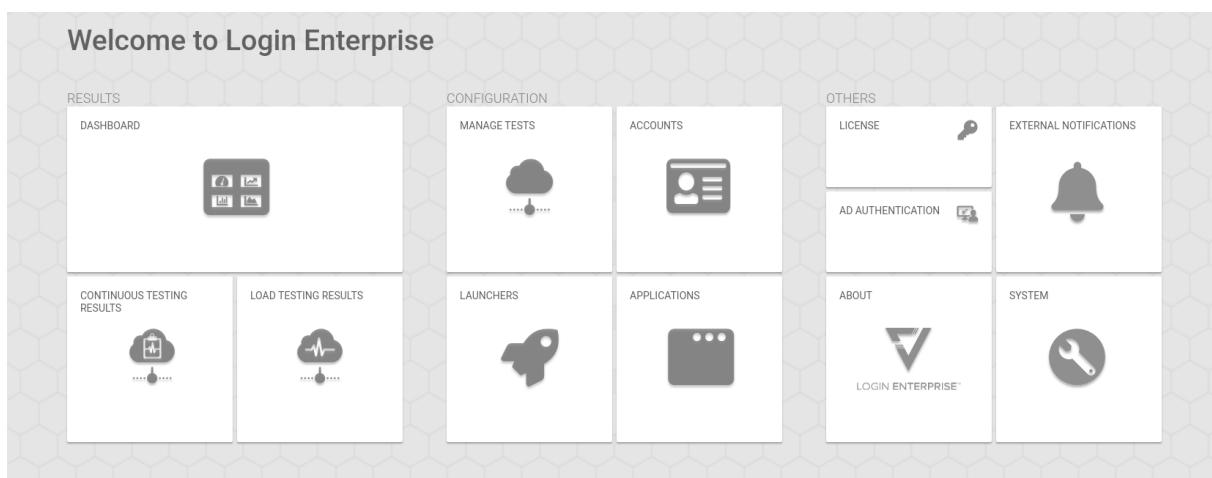
This how-to explains how to get a [Secret](#)(see page 343) to configure Login Enterprise Launcher.



1. Go to <https://yourServerURL>.  
Enter admin as a username and password and click **LOGIN**.



2. Go to **Launchers**.



3. Download a required .zip file under **Download Launcher Setup** and unpack it.

A screenshot of the IGEL OS web interface. At the top, there are tabs for "MANAGE TESTS", "ACCOUNTS", "LAUNCHERS" (which is highlighted in green), and "APPLICATIONS".  
  
**LAUNCHERS**: This section shows a table with columns: "Machine name" (sorted by ascending sessions), "Sessions", "Launcher version", and "OS Version". A message below the table says "Download launcher setup from below to install the PI launcher". At the bottom, there are pagination controls: "Items per page: 10", navigation arrows, and a page indicator "1/1".  
  
**LAUNCHER GROUPS**: This section shows a table with columns: "Group name" (sorted by ascending number of launchers), "No. launcher", "Type", and "Description". It displays the message "No groups to display." At the bottom, there are pagination controls: "Items per page: 10", navigation arrows, and a page indicator "1/1".  
  
**DOWNLOAD LAUNCHER SETUP**: This section shows a table with columns: "File name" and "Description". It lists two entries: "Windows x64" with the description "Extract complete zip file to folder before running Setup.MSI" and "Windows x86" with the description "Extract complete zip file to folder before running Setup.MSI". Each entry has a download icon to its right. At the bottom, there are pagination controls: "Items per page: 10", navigation arrows, and a page indicator "1/1".

#### 4. Open the appsettings.json file in the editor.

Name	Typ
appsettings	JSON-Datei
Setup	CAB-Datei
Setup	Windows Installer-Paket

Here you find the **Secret** for your Login Enterprise Launcher.



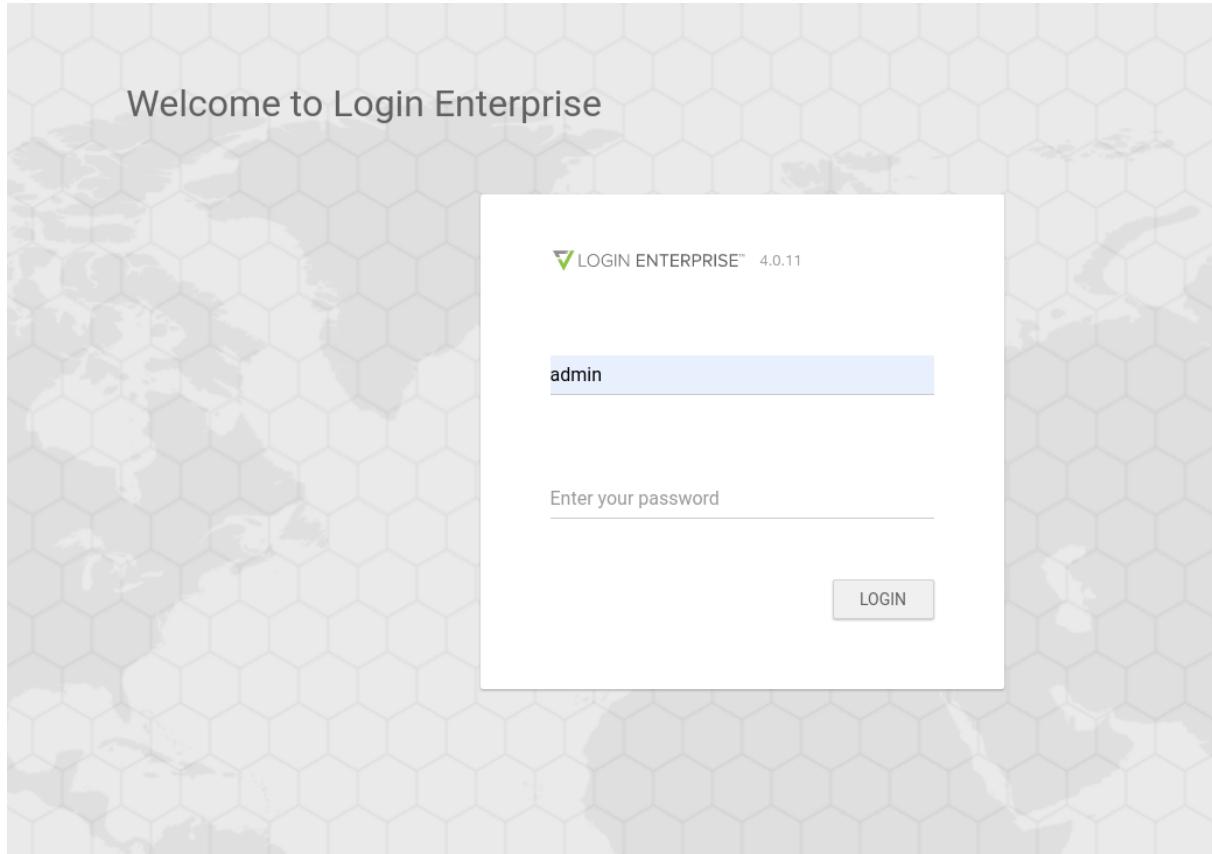
```
},
"ServerUrl": "https://loginipi.████████",
"IdentityProvider": {
    "ClientId": "Launcher",
    "Scope": "microservice",
    "Authority": "{ServerUrl}/identityServer",
    "Secret": "885F0D83DB88C7F840288F████████"
},
"Services": {
    "LaunchersUrl": "{ServerUrl}/launchers",
    "AccountsUrl": "{ServerUrl}/accounts",
    "EnvironmentsUrl": "{ServerUrl}/environments",
    "SessionRequestsUrl": "{ServerUrl}/sessionRequests"
}
```

Use the **Secret** without the quotation marks "".

### 2.13.3 Using the Login Enterprise Launcher within a VMware Horizon Session

If you want to use the Login Enterprise Launcher within a VMware Horizon Session on your IGEL OS device, note the following:

1. Go to <https://yourServerURL> and log in.



2. Go to **Manage Tests**.

A screenshot of the Login Enterprise dashboard. At the top, it says "Welcome to Login Enterprise". Below that is a grid of cards:

Welcome to Login Enterprise

RESULTS

DASHBOARD



CONTINUOUS TESTING RESULTS



LOAD TESTING RESULTS



CONFIGURATION

MANAGE TESTS



ACCOUNTS



OTHERS

LICENSE



EXTERNAL NOTIFICATIONS



LAUNCHERS



APPLICATIONS



ABOUT



SYSTEM



3. Click **Add new environment**.

A screenshot of the IGEL software interface. At the top, there's a navigation bar with tabs: "MANAGE TESTS" (which is active and highlighted in green), "ACCOUNTS", "LAUNCHERS", and "APPLICATIONS". Below the navigation bar, a section titled "CONTINUOUS TESTING" shows "04 environments". On the right side of this section is a button labeled "Add new environment" with a green plus sign icon. The main area below has columns for "Environment Name" (sorted by name), "Schedule", and "Connector".

Environment Name	Schedule	Connector	Description
test_VMware_Horizon_view			

4. Enter an **Environment name**.
5. Select **VMware Horizon View** under **Connector**.

A screenshot of the "Connector" dropdown menu. It is a list of options: Citrix Netscaler 12.1 and 13.0, Citrix StoreFront, Custom connector, Desktop, Microsoft RDS, and VMware Horizon View. The "VMware Horizon View" option is highlighted with a light gray background.

Environment name	Connector	Description
test_VMware_Horizon_view	Citrix Netscaler 12.1 and 13.0	
	Citrix StoreFront	
	Custom connector	
	Desktop	
	Microsoft RDS	
	VMware Horizon View	

6. Enter the **Server URL** and the **Resource**.



MANAGE TESTS ACCOUNTS LAUNCHERS APPLICATIONS

**INFO test\_Vmware\_Horizon\_view** All environments

Environment name	Connector	Description
test_Vmware_Horizon_view	VMware Horizon View	

Settings

Server Url	vcs71.horizon.test
Resource	sMartl
Connection command line	"/services/vvdm/bin/vmware-view" --serverURL={serverurl} --userName="{username}" --password="{password}" --domainName="{domain}" --desktopName="{resource}" --nonInteractive
Accounts	VM_horizon_users
Launchers	All launchers

## 7. Copy the following:

```
"/services/vvdm/bin/vmware-view" --serverURL={serverurl} --userName="{username}" --
password="{password}" --domainName="{domain}" --desktopName="{resource}" --nonInteractive
```

and paste it under **Connection command line**.

MANAGE TESTS ACCOUNTS LAUNCHERS APPLICATIONS

**INFO test\_Vmware\_Horizon\_view** All environments

Environment name	Connector	Description
test_Vmware_Horizon_view	VMware Horizon View	

Settings

Server Url	vcs71.horizon.test
Resource	sMartl
Connection command line	"/services/vvdm/bin/vmware-view" --serverURL={serverurl} --userName="{username}" -- password="{password}" --domainName="{domain}" --desktopName="{resource}" --nonInteractive
Accounts	VM_horizon_users
Launchers	All launchers



This is important if you use the Login Enterprise Launcher for IGEL OS devices!

For more information on the configuration, see <http://www.loginvsi.com>.

## 2.14 Nutanix

Nutanix enables IT teams to build and operate high-performance multi-cloud architectures. The enterprise cloud OS software combines private, public, and distributed cloud operating environments and provides centralized control to manage IT infrastructures and applications of all sizes.

Nutanix solutions are 100 % software-based and leverage the industry's most popular hyper-converged infrastructure (HCI) technology.

### Hyper-converged infrastructure (HCI)

Hyper-convergent infrastructures are a further development of convergent infrastructures in which hardware and software are also bundled.

They provide a complete infrastructure stack that combines computing, virtualization, storage, networking, and security to run any application of any size.

The Software runs across multiple cloud environments to harmonize IT operations and proved smooth mobility for all applications. For more information, see [nutanix.com](https://www.nutanix.com)<sup>152</sup>.

### 2.14.1 Frame on Nutanix

Frame is the easiest way to run virtual apps and desktops on your choice of infrastructure.

It's a new option to use Frame Desktop-as-a-Service (DaaS) with apps, desktops, and user data hosted on your Nutanix (AHV) infrastructure.

You have to create a browser profile and put in the address of your frame broker.

#### Setting Up Frame Connection

1. In the IGEL Setup, go to **Sessions > Firefox Browser > Firefox Browser Sessions**.

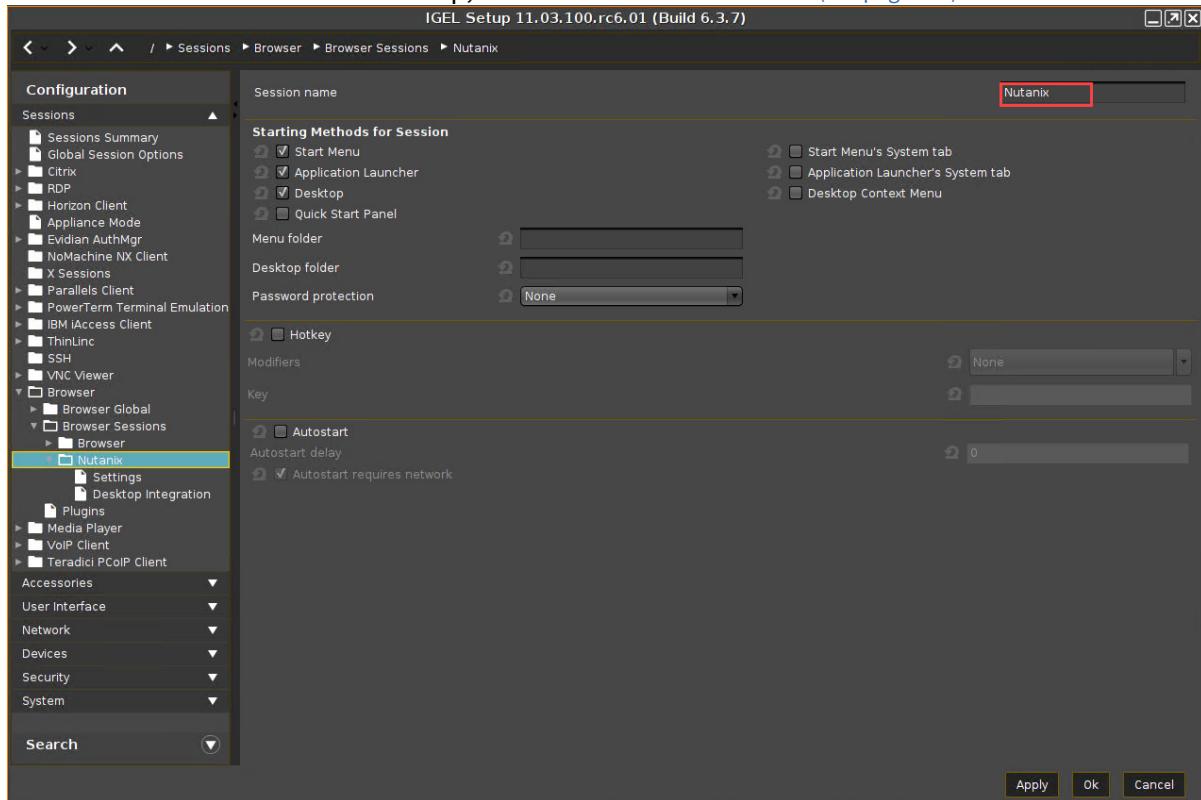
---

<sup>152</sup> <https://www.nutanix.com/en>



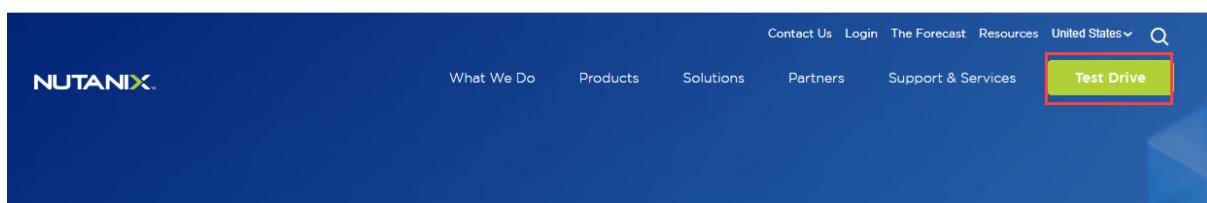
2. Click **[+]** to add a browser session.

For more information about the setup, see [Firefox Browser Session](#)(see page 978).



## 2.14.2 Running the Nutanix Test Drive on IGEL

1. Open the Firefox browser.
2. Enter <https://www.nutanix.com><sup>153</sup>.
3. Click **Test Drive**.



4. Enter the required data.
5. Click **Launch Test Drive**.

<sup>153</sup> <https://www.nutanix.com/en>



## Test Drive Nutanix Software

Start here

First Name *	Last Name *
Work Email *	
Phone Number *	
Company Name *	
Job Title *	

LAUNCH TEST DRIVE

Nutanix is committed to ensuring your privacy. Your email address will be used to deliver the information you have requested and may be used to deliver other news about Nutanix. You can unsubscribe at any time. Please review our [Privacy Statement](#) for additional details.

- 
6. Your **Nutanix Test Drive information** is shown.



7. Click **Start Test Drive**.

## Here is your Nutanix Test Drive information!

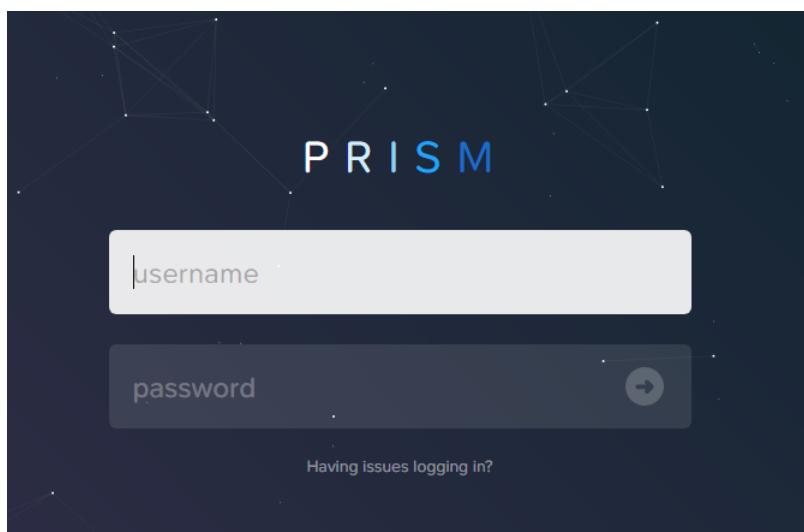
Username

Password 

Launch the test drive by proceeding through the certificate warning (IP addresses are dynamically generated).

**START TEST DRIVE**

8. Enter your credentials in the **PRISM (Planning tool for Resource Integration, Synchronization and Management)** login window.



For the next steps, follow the instructions of Nutanix.



## 2.15 Browser

- Define Multiple Start Pages for Your Browser(see page 355)
- Touchscreen: Multitouch/Gesture Support for Firefox(see page 356)
- Set Advanced User Preferences for the Browser(see page 357)
- Use the Firefox Browser in Kiosk Mode(see page 358)
- SSL/TLS Error with Firefox in Appliance Mode(see page 365)
- Browser Cannot Download Files(see page 366)
- Some PDFs are not opened by Firefox(see page 366)
- Can I Install Firefox Extensions?(see page 367)

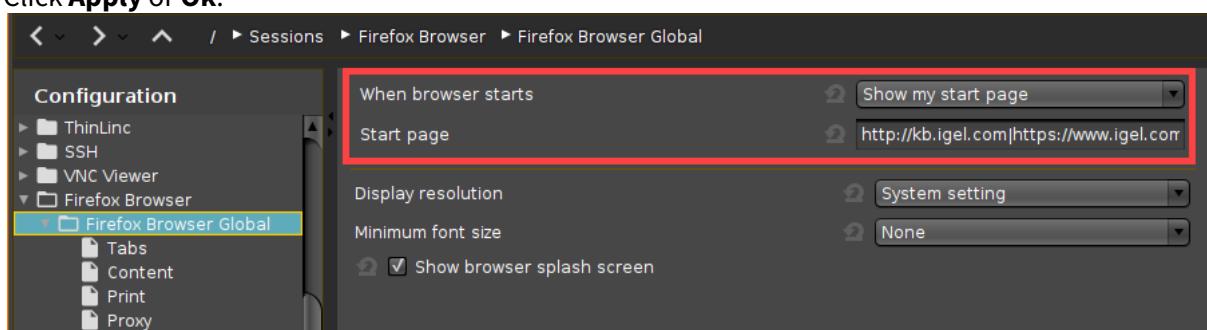
### 2.15.1 Define Multiple Start Pages for Your Browser

In some cases, a fixed set of start pages displayed in separate tabs may prove useful. For instance, if the browser is working in kiosk mode, reusing a set of tabs from an earlier session is not an option.

Here is how to define multiple start pages to be opened at browser startup.

#### Firefox

1. Open the IGEL Setup and go to **Sessions > Firefox Browser > Firefox Browser Global**.
2. Set **When browser starts** to **Show my start page**.
3. Set **Start page** to the URLs that the browser should open at startup. Use "|" as a separator.
4. Click **Apply or Ok**.



#### Chromium

1. Open the IGEL Setup and go to **Sessions > Chromium Browser > Chromium Browser Global > General**.
2. Set **On Startup** to **Open a specific page or set of pages**.
3. Set **Startup page** to the URLs that the browser should open at startup. Use "|" as a separator.



#### **4. Click Apply or Ok.**

### 2.15.2 Touchscreen: Multitouch/Gesture Support for Firefox

You can use multitouch/gestures in the Firefox browser that is built into IGEL OS 10 and IGEL OS 11. This is done by adding an environment variable.

To enable multitouch:

1. Open the local Setup or the UMS configuration dialog and go to **System > Firmware Customization > Environment Variables > Predefined**.
  2. In the first free **Variable name** field, enter MOZ\_USE\_XINPUT2
  3. In the corresponding **Value** field, enter 1
  4. Click **Ok**.

5. Reboot the device.
  6. To check if multitouch is working, open the Firefox browser and go to <https://www.paulirish.com/demo/multi>.

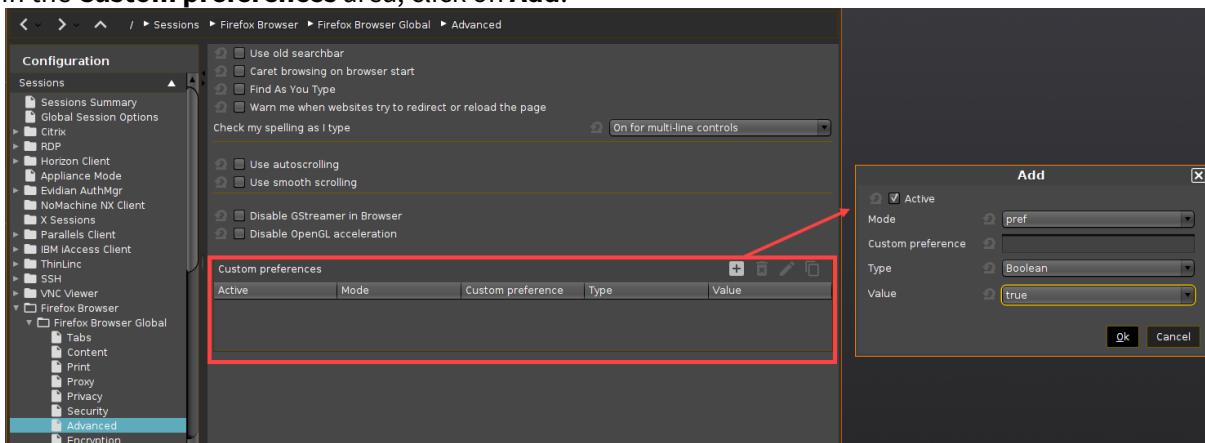
### 2.15.3 Set Advanced User Preferences for the Browser

The Mozilla Firefox browser included in IGEL OS offers a vast array of configuration options. They range from the sorting order of bookmarks over encryption algorithms to fixing quirks in web applications that are important to you. In total, they are too many to present them as individual items in IGEL Setup. However, as of IGEL Linux version 5.09.100, IGEL Setup lets you set any browser user preference in a generic way.

Changes to the advanced Firefox browser settings can impair its stability, security, and speed. IGEL Support is not responsible for problems caused by changing the browser configuration, even if the browser configuration was changed in IGEL Setup.

You will find information regarding the configuration parameters for Firefox in the MozillaZine Knowledge Base under [Firefox About:config entries](#)<sup>154</sup>.

1. In Setup, go to **Sessions > Firefox Browser > Firefox Browser Global > Advanced**.
2. In the **Custom preferences** area, click on **Add**.



3. Using the **Active** option, specify whether the configuration parameter is to be active.
  4. Specify the **Mode** of the configuration parameter - for many cases **pref** will do.
  5. Under **Custom preference**, give the name of the configuration parameter. Example:  
`ui.textSelectBackground`
  6. Specify the **Type** of the configuration parameter.  
Possible values:
    - **String:** The value is a string of characters.
    - **Integer:** The value is a whole number.
    - **Boolean:** The value is a Boolean value, i.e. `true` or `false`.
  7. Specify the **Value** of the configuration parameter. The possible entries depend on the **Type** selected.
  8. Click **Ok**.
- The configuration parameter will take effect the next time that the browser is launched.
- For more details on browser configuration, refer to the section [Firefox Browser Global](#)(see page 957) in the IGEL OS reference manual.

<sup>154</sup> [http://kb.mozilla.org/About:config\\_entries](http://kb.mozilla.org/About:config_entries)

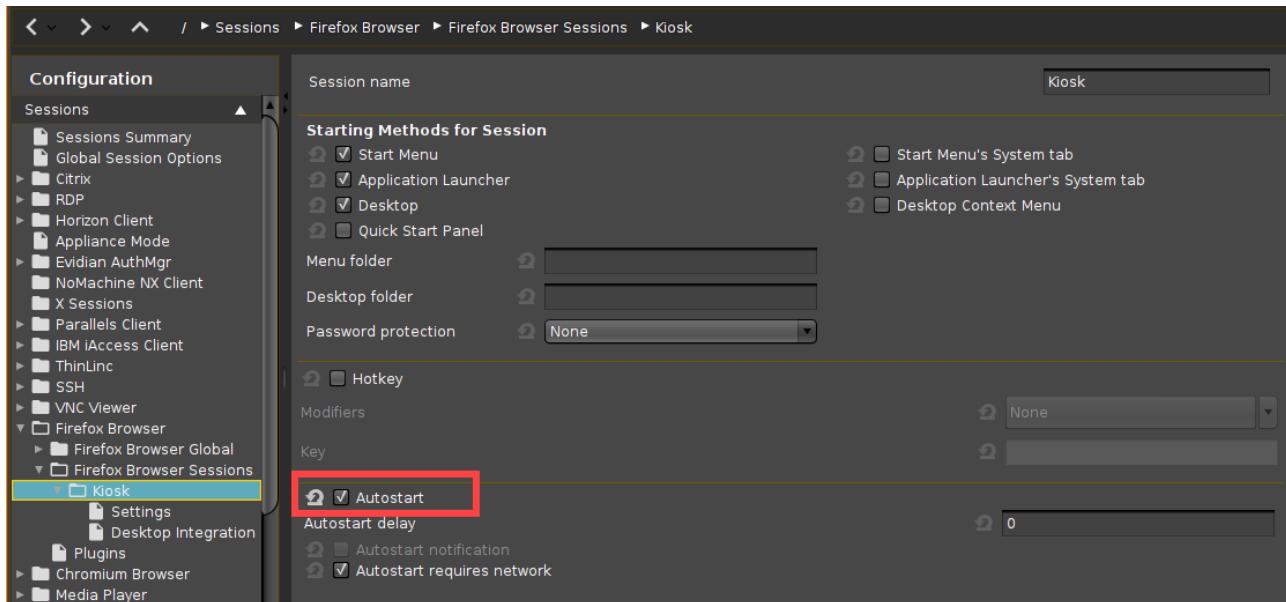
## 2.15.4 Use the Firefox Browser in Kiosk Mode

Browser kiosk mode is an option when you are operating any kind of public terminal with anonymous access, e.g.:

- Educational service in a museum
- Service terminals or ticket vending machines for public transport
- Entry portal for a corporate intranet

Albeit configuring an IGEL OS device for browser kiosk mode may seem quite extensive, you have the possibility to define your own flavor of kiosk mode. Consider the following settings.

Settings under Sessions > Firefox Browser > Firefox Browser Sessions > [Session Name]



► Activate **Autostart**.



## Settings under Sessions > Firefox Browser > Firefox Browser Sessions > [Session Name] > Settings

**Configuration**

- NoMachine NX Client
- X Sessions
- Parallels Client
- IBM Access Client
- ThinLinc
- SSH
- VNC Viewer
- Firefox Browser
  - Firefox Browser Global
  - Firefox Browser Sessions
    - Kiosk
      - Settings
      - Desktop Integration
      - Plugins
- Chromium Browser
- Media Player

**Related Configurations**

- User Interface - Display
- Firefox Browser Global

- ▶ Set **When browser starts** to **Global setting**.
- ▶ If necessary, select the correct **Start Monitor**.

## Settings under Sessions > Firefox Browser > Firefox Browser Global

**Configuration**

- ThinLinc
- SSH
- VNC Viewer
- Firefox Browser
  - Firefox Browser Global
    - Tabs
    - Content
    - Print
    - Proxy
    - Privacy
    - Security
    - Advanced
    - Encryption
    - Certificates
    - Smartcard Middleware
    - Restart
    - Window
    - Menus & Toolbars
    - Hotkeys
    - Context
    - Commands
  - Firefox Browser Sessions
  - Plugins

**Related Configurations**

- User Interface - Display

- ▶ Set **When browser starts** to **Show my start page**.
- ▶ Set **Start Page** to the desired start page.



## Settings under Sessions > Firefox Browser > Firefox Browser Global > Tabs

New pages should be opened in

- Warn me when closing multiple tabs
- Warn me when opening multiple tabs might slow down the browser
- When a link is opened in a new tab, switch to it immediately

- ▶ Set **New pages should be opened in** to **the current window** or to **a new tab**.

## Settings under Sessions > Firefox Browser > Firefox Browser Global > Content

Block pop-up windows

Load images automatically

Type of download directory

Download path

user-defined path /tmp

Enable JavaScript

- Enable JavaScript
- Raise or lower windows
- Move or resize existing windows
- Disable or replace context menus

Languages for Web Pages

- ▶ If applicable, activate **Block pop-up windows**.
- ▶ Activate **Load images automatically**.
- ▶ If required, activate **Enable JavaScript** and adapt the actions permitted for JavaScript according to your needs.



## Settings under Sessions &gt; Firefox Browser &gt; Firefox Browser Global &gt; Privacy

A screenshot of the IGEL OS Settings application. The left sidebar shows a tree view of session configurations, with 'Firefox Browser Global' selected. Under it, 'Privacy' is highlighted. The main pane displays privacy settings for the Firefox browser. A red box highlights the 'Save Browsing History (in days)' section, which includes options like 'Save information entered in forms and the Search Bar' and 'Remember Passwords'. Below this is a section for clearing private data, with checkboxes for 'Clear private data when closing browser' and 'Select the items to be cleared'. Under 'Select the items to be cleared', there are checkboxes for 'Browsing & Download History', 'Form & Search History', 'Saved Passwords', 'Cookies', 'Cache', and 'Active Logins'. Further down are sections for 'Allow private browsing feature', 'Always start in private browsing mode', 'Enable "Do Not Track" feature', and 'Enable built-in tracking protection'. At the bottom, there are checkboxes for 'Suggest visited sites in URL bar' and 'Suggest bookmarked sites in URL bar'.

Configuration

- SSH
- VNC Viewer
- Firefox Browser
  - Firefox Browser Global
    - Tabs
    - Content
    - Print
    - Proxy
    - Privacy
    - Security
    - Advanced
    - Encryption
    - Certificates
    - Smartcard Middleware
    - Restart
    - Window
    - Menus & Toolbars
    - Hotkeys
    - Context
    - Commands
  - Firefox Browser Sessions
  - Plugins
- Chromium Browser
- Media Player

Save Browsing History (in days)

Save information entered in forms and the Search Bar

Remember Passwords

Clear private data when closing browser

Select the items to be cleared

Browsing & Download History

Form & Search History

Saved Passwords

Cookies

Cache

Active Logins

Allow private browsing feature

Always start in private browsing mode

Enable "Do Not Track" feature

Enable built-in tracking protection

Suggest visited sites in URL bar

Suggest only typed visited sites

Suggest bookmarked sites in URL bar

Suggest open pages in URL bar

- ▶ Set **Save Browsing History (in days)** to **Do not save History**.
- ▶ Deactivate **Save information entered in forms and the Search bar**.
- ▶ Deactivate **Remember Passwords**.
- ▶ Activate **Clear private data when closing browser**.
- ▶ Activate all items in the area **Select the items to be cleared**.
- ▶ If you want to suppress any tracking of the user's activities, activate **Allow private browsing feature** and **Always start in private browsing mode**.
- ▶ If applicable, activate **Enable "Do Not Track" feature**.
- ▶ To make the browser block domains and websites which are known for tracking users, activate **Enable built-in tracking protection**.



## Settings under Sessions > Firefox Browser > Firefox Browser Global > Security

The screenshot shows the configuration interface with the following path: Sessions > Firefox Browser > Firefox Browser Global > Security. The left sidebar lists various configuration categories like SSH, VNC Viewer, and Firefox Browser, with Firefox Browser Global expanded. Under Firefox Browser Global, the Security tab is selected and highlighted in blue. On the right, there is a list of security options with checkboxes: Safe Browsing (checked), Malware Protection (checked), and Hide local filesystem (checked). A red box highlights this list of checkboxes.

- ▶ To enable phishing protection, activate **Safe Browsing**.
- ▶ To enable protection against malicious downloads, activate **Malware Protection**.
- ▶ Activate **Hide local filesystem**.

## Settings under Sessions > Firefox Browser > Firefox Browser Global > Restart

The screenshot shows the configuration interface with the following path: Sessions > Firefox Browser > Firefox Browser Global > Restart. The left sidebar lists various configuration categories, with Firefox Browser Global expanded. Under Firefox Browser Global, the Restart tab is selected and highlighted in blue. On the right, there are two checkboxes: 'Restart' (checked) and 'Restart after idle time' (checked). Below these, there is a field for 'Idle time after which a restart occurs' with a value of '3' and a unit dropdown set to 'Minutes'. A red box highlights the checkboxes and the restart configuration fields.

- ▶ Activate **Restart**. The browser will restart automatically if a user closes the browser window.
- ▶ If you want the browser to restart automatically after some idle time, activate **Restart after idle time** and specify **Idle time after which a restart occurs** in minutes or seconds.



## Settings under Sessions > Firefox Browser > Firefox Browser Global > Window

The screenshot shows the 'Configuration' tree on the left with 'Firefox Browser Global' selected. The right pane displays settings for 'Window'. A red box highlights two checkboxes: 'Start in full-screen mode' (checked) and 'Hide configuration page of the browser' (checked). There is also a 'Default' dropdown menu.

- ▶ If the browser shall run in full-screen mode, activate **Start in full-screen mode**.
- ▶ Activate **Hide configuration page of the browser**.

## Settings under Sessions > Firefox Browser > Firefox Browser Global > Menus & Toolbars

The screenshot shows the 'Configuration' tree on the left with 'Firefox Browser Global' selected. The right pane displays settings for 'Menus & Toolbars'. A red box highlights the 'Hide App Menu/Menu Bar' checkbox. Another red box highlights the 'User Customization of toolbars' checkbox in the 'Toolbarconfig' section. Other visible checkboxes include 'Use old Menu Bar', 'Hide Bookmarks menu', 'Hide Tools menu', 'Hide History entry', 'Hide Tabs Toolbar', 'Hide Bookmarks Toolbar' (which is checked), 'Hide Sidebar', 'Hide URL Input', 'Hide 'Print' Button', 'Hide 'Home' Button', 'Hide Search Input', and 'Hide 'Bookmarks' and 'RSS Feed' Button'.

- ▶ Activate **Hide App Menu/Menu Bar**.
- ▶ Select which menus and toolbars are to be hidden. In the kiosk mode, all menus, toolbars, and the address bar are commonly hidden.
- ▶ Deactivate **User Customization of toolbars**.



## Settings under Sessions > Firefox Browser > Firefox Browser Global > Context

The screenshot shows the 'Configuration' tree on the left with the following structure:

- Sessions
  - VNC Viewer
  - Firefox Browser
    - Firefox Browser Global
      - Tabs
      - Content
      - Print
      - Proxy
      - Privacy
      - Security
      - Advanced
      - Encryption
      - Certificates
      - Smartcard Middleware
      - Restart
      - Window
      - Menus & Toolbars
      - Hotkeys
      - Context** (highlighted with a yellow background)
      - Commands
  - Firefox Browser Sessions
  - Plugins
  - Chromium Browser

- ▶ Activate **Hide the browser's context menu**.

## Disabling Access to Developer Tools

To disable access to the developer tools, add the following custom preference.

For general instructions on adding custom preferences, see [Set Advanced User Preferences for the Browser](#)(see page 357).

<b>Mode</b>	pref
<b>Custom preference</b>	devtools.toolbox.host
<b>Type</b>	String
<b>Value</b>	(leave the value field empty)

## Disabling Crash Reports

To disable crash reports, add the following three custom preferences.

For general instructions on adding custom preferences, see [Set Advanced User Preferences for the Browser](#)(see page 357).

<b>Mode</b>	pref
<b>Custom preference</b>	datareporting.policy.dataSubmission



<b>Type</b>	Boolean
<b>Value</b>	false
<b>Mode</b>	pref
<b>Custom preference</b>	datareporting.healthreport.upload
<b>Type</b>	Boolean
<b>Value</b>	false
<b>Mode</b>	pref
<b>Custom preference</b>	toolkit.telemetry
<b>Type</b>	Boolean
<b>Value</b>	false

## 2.15.5 SSL/TLS Error with Firefox in Appliance Mode

### Symptom

Firefox on IGEL Linux 5.07.100 warns of an SSL/TLS error in appliance mode that does not occur in normal window mode. The error code is `ssl_error_unsupported_version`. This does not happen on IGEL Linux 5.06.x.

### Problem

You cannot connect to the affected HTTPS service.

### Solution

As a workaround you can instruct Firefox to ignore issues with SSL/TLS versions:

1. In IGEL Setup, go to **System > Firmware Customization > Custom Commands > Base Commands**
2. Enter the following command into the **After Session Configuration** input field:  
`echo "clearPref(\"security.tls.version.min\");" >> /services/fbrw/firefox/firefox.cfg`

There is also an IGEL Linux private build that addresses this issue.



## 2.15.6 Browser Cannot Download Files

### Symptom

You are trying to view or download a file with the browser, but you get error messages instead.

### Problem

The browser has no permissions for the file path you have selected for download. This is because the Firefox browser is being guarded by AppArmor for security reasons.

### Solution

Check whether one of the following possibilities for downloading files is applicable/available:

- Storage hotplug device (USB flash drive) which is mounted to /media/[device name] or /userhome/media/[device name]  
For hotplug storage configuration, see [Storage Hotplug\(see page 1228\)](#).
- Network drive which is mounted to /mnt/[folder name]
- Folder /userhome in the local file system; not persistent

## 2.15.7 Some PDFs are not opened by Firefox

### Symptom

When opening some PDFs from the Internet, the Mozilla Firefox browser opens a new window or tab, but fails to display the PDF contents.

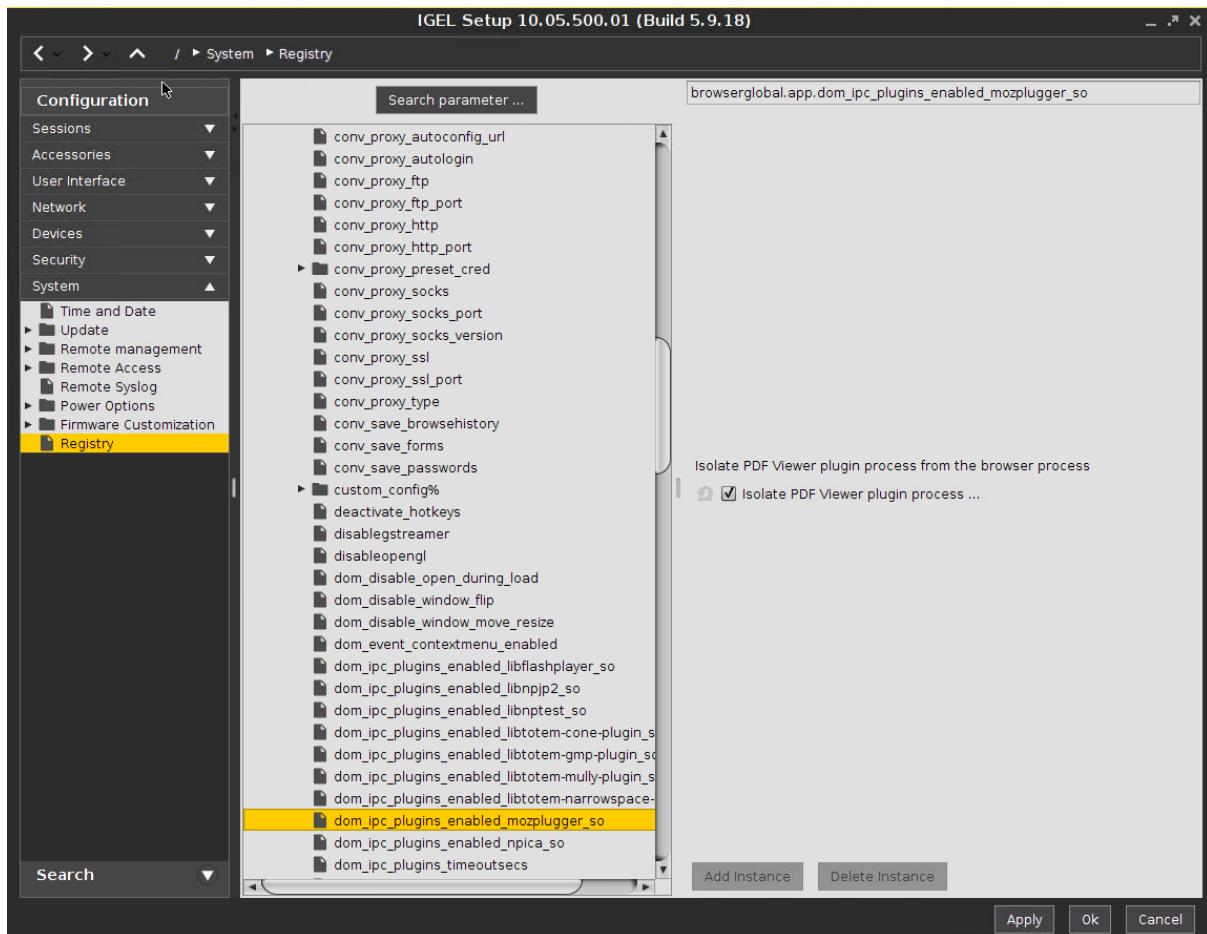
### Problem

This can be due to a malfunction of the mozplugger Firefox component.

### Solution

Disable mozplugger. Firefox will download the PDF document and open it with a local application (*IGEL Linux 5.07.100 or newer*):

1. Go to **System > Registry** in *IGEL Setup*.
2. Use **Search Parameter ...** to find the parameter  
`browserglobal.app.dom_ipc_plugins_enabled_mozplugger_so`.
3. Check **Completely disable mozplugger**.
4. Confirm the setting with **Apply** or **OK**.
5. Restart Firefox.



## 2.15.8 Can I Install Firefox Extensions?

### Question

Can Firefox extensions be installed?

### Answer

The installation of Firefox extensions is not possible. This applies to any version of both IGEL Linux v5.x and IGEL OS.

## 2.16 System

- [Resetting a Device with Unknown Administrator Password](#)(see page 368)
- [Error: "Unknown filesystem..."](#)(see page 369)
- [Custom Boot Commands Are Still Active after Factory Reset](#)(see page 370)



- Solving Issues with Signed Partitions(see page 371)
- How to Show the Boot Mode of IGEL OS(see page 375)
- Disabling Features to Reduce Firmware Size(see page 376)
- Fabulotech USB Redirection Server Component(see page 376)
- Which Features of IGEL OS Will Be Affected If the UMS Is Down?(see page 377)

## 2.16.1 Resetting a Device with Unknown Administrator Password

### Symptom

An administrator password has been set on IGEL OS (via **Setup > Security > Password > Administrator**) but it has been lost.

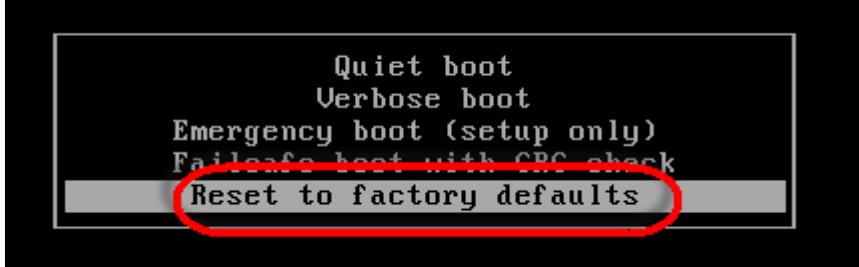
### Problem

The local setup is not accessible without the password. Also, resetting the device to factory defaults seems impossible.

### Solution

- Change the administrator password using IGEL UMS via **Setup > Security > Password > Administrator**  
or
- Reset the device using IGEL UMS via **Devices > Other commands > Reset to Factory Defaults** in the UMS menu.  
or
- Reset the thin client locally using a reset to defaults key provided by IGEL (as described below):

1. Press the [ESC] key repeatedly in rapid succession while the device is booting.  
This will bring up the boot menu.



2. Choose **Reset to factory defaults** and press [Enter].  
The following will be displayed:



```

Loading "German" keyboard layout.
The Administrator Password is required to reset the terminal settings.
If your Administrator Password is not available anymore, enter 3 times return.

Password:
Authentication: Authentication failure
Password:
Authentication: Authentication failure
Password: _

```

3. Press [Enter] three times without supplying a password.

```

Enter <r> if you want to reboot and type the password again.
Enter <c> if you want to continue and reset the terminal settings
      in case your Administrator Password is not available anymore.
<r> or <c>: _

```

4. Enter [c] and press [Enter].

The software will then display a terminal key. Make a note of it, as you need it for requesting the reset to defaults key from IGEL.

5. Request a reset to defaults key from IGEL. Write an email to [license@igel.com](mailto:license@igel.com)<sup>155</sup> containing
  - your terminal key
  - your email address as registered with IGEL support
  - your company address
  - your phone number

IGEL will send you the reset to defaults key.

6. In the current session, enter [e] and press [Enter] to shut down the device.
7. On receiving the reset to defaults key, repeat steps 1 to 3 to boot the device with the same terminal key.
8. Enter [c] and press [Enter]. You will be prompted to enter the reset to defaults key.

```

3) enter now the "reset to defaults key", you got by the service team
   for "terminal key" 39099-53083-29440-48934 and firmware version 5.03.100.01
   (you have only three tries to enter the key correctly!):
1. Try: _ ←

```

9. Enter the reset to defaults key. Enter yes and press [Enter] to confirm resetting the client. All local thin client settings will be lost.

Should you enter the wrong key or mistype the key you will have to resume from step 1.

## 2.16.2 Error: "Unknown filesystem..."

### Symptom

The boot process is aborted at an early stage; the error message is "Unknown filesystem. Couldn't find valid IGEL partition..."

---

<sup>155</sup> <mailto:license@igel.com>



## Environment

- IGEL OS (any version)

## Problem

One or more system partitions could not be found or are not valid.

## Solution

- Install IGEL OS anew on the device with IGEL OS Creator (OSC). For instructions, see the [Installation](#)(see page 1295) chapter of the [IGEL OS Creator Manual](#)(see page 1293).

### **Preserve Your Settings**

To prevent the device's settings from being deleted, ensure that **Migrate Old Settings** is activated in the installation settings; see [Installation Procedure](#)(see page 1302).

### **Data That Will Be Lost**

When IGEL OS is installed anew, the following data will be lost:

- All data on the writable partition /wfs
- All data that has been stored in a Custom Partition since its deployment; Custom Partitions will be reset to their original state.

### **Licenses Will Be Lost**

In this scenario, the licenses stored on the device will be lost. However, the licenses are cached in the UMS, so that they will be restored when the device registers with the UMS.

## 2.16.3 Custom Boot Commands Are Still Active after Factory Reset

### Symptom

You have reset your device to factory defaults, but the custom boot commands are still active.

### Problem

After a factory reset, the following settings will still be available:

- boot\_id
- uptime\_total
- product



- `force_Legacy`
- The bootreg entry `Splash` will be set to 1

## Solution

You can delete these settings manually with the following command:

1. Open a local terminal and log in as root.
2. Enter the following command to delete the settings:  
`bootreg delete /dev/igfdisk boot_cmd`

For further information about custom boot commands, see [Custom Boot Command](#)(see page 764).

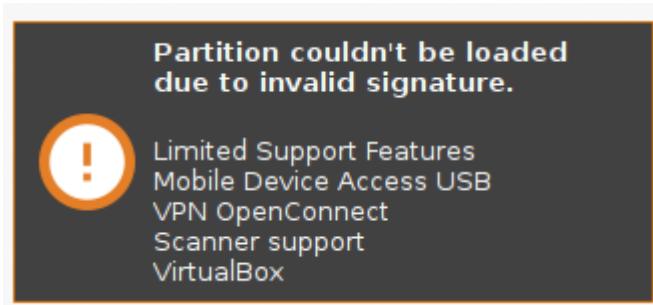
### 2.16.4 Solving Issues with Signed Partitions

- Error: "Partition couldn't be loaded due to invalid signature"(see page 371)
- Error: Device Plays a Beep Code Instead of Booting(see page 372)
- Error: "The new firmware is not signed. Update not allowed."(see page 374)
- Error: "Invalid signature - Failed to read from partition"(see page 375)

#### Error: "Partition couldn't be loaded due to invalid signature"

##### Symptom

During operation, a system message like this appears:



##### Environment

- IGEL OS 11.03 or higher

##### Problem

A system partition has been invalidated, which prevents system components from being loaded.



## Solution

1. Ensure that a valid update source is configured under **System > Update > Firmware Update** and the correct firmware is stored on the server. (For detailed information, see [Firmware Update\(see page 1252\)](#).) If the local Setup is not accessible, use the UMS.
2. Reboot the device.  
The device fetches the valid partition from the update source.

## Error: Device Plays a Beep Code Instead of Booting

### Symptom

The boot process fails, and a beep code is played. Two beep codes are possible:

- 3 short and 1 long beep, repeated 2 times (whole sequence repeats up to 1 minute)
- Long beep is played for 1,1 seconds, then 2,9 seconds pause (repeats up to 1 minute)

### Environment

- IGEL OS 11.03 or higher

### Problem

- 3 short and 1 long beep, repeated 2 times (whole sequence repeats up to 1 minute): The signature of the found system partition is invalid.
- Long beep is played for 1,1 seconds, then 2,9 seconds pause (repeats up to 1 minute): After up to 120 tries, no suitable system partition has been found at all.

### Diagnosis

To obtain further details:

1. Reboot the device and press [ESC] repeatedly.
2. Select **Verbose Boot**.

When the signature of the found system partition is invalid, the output looks like this:

```
init: boot id from cmdline: 191204080936053974571
init: boot id from /dev/igfddisk: 191204080936053974571
[ 3.356915] igel-flash: loading out-of-tree module taints kernel.
[ 3.359376] Going to add device for 'igf'
[ 3.386594] igel-loop: 1 -> verify_hash_info: -129
[ 3.387366] igel-loop: Signature verification failed: 1
[ 3.388185] igel-loop: Not adding 1 because hash info couldn't be built: -129
[ 3.440630] igel-loop: system partition rejected for non-verifiable partition signature!
insmod: can not insmod '/lib/modules/4.19.85/kernel/drivers/block/igel/igel-flash.ko' (errno 129): Key was rejected by service
[ 11.656993] random: crng init done
ERROR: Invalid signature of found SYS partition found abort.
[ 13.049396] sd 0:0:0:0: [sdal] Synchronizing SCSI cache
[ 13.068905] reboot: System halted
-
```



When no suitable system partition has been found at all, the output looks like this:

### Solution

- ▶ Install IGEL OS anew on the device with IGEL OS Creator (OSC). For instructions, see the [Installation](#)(see page 1295) chapter of the [IGEL OS Creator Manual](#)(see page 1293).



### Preserve Your Settings

To prevent the device's settings from being deleted, ensure that **Migrate Old Settings** is activated in the installation settings; see [Installation Procedure](#)(see page 1302).

### Data That Will Be Lost

When IGEL OS is installed anew, the following data will be lost:

- All data on the writable partition /wfs
- All data that has been stored in a Custom Partition since its deployment; Custom Partitions will be reset to their original state.

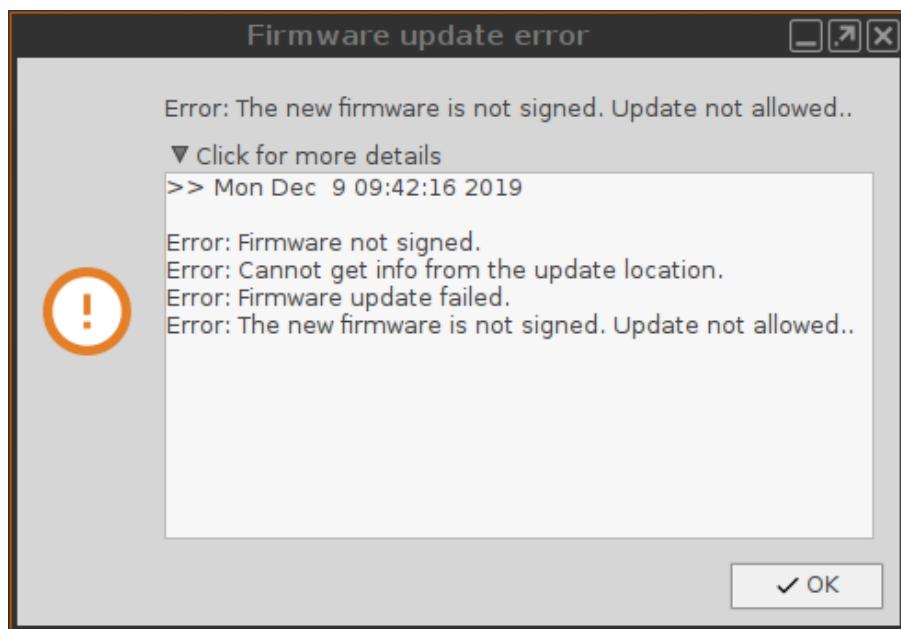
### Preservation of Licenses

When IGEL OS is installed anew, any licenses stored on the device are preserved, provided that the relevant partition is valid.

Error: "The new firmware is not signed. Update not allowed."

#### Symptom

During the update process, the following error messages are shown:



#### Environment

- IGEL OS 11.03 or higher



## Problem

The system expects signed system partitions, but the partitions of the update source are not signed. This will occur when you have tried to downgrade from IGEL OS 11.03 or higher to an older version of IGEL OS 11.

## Solution

- If you want to downgrade from IGEL OS 11.03 to IGEL OS 11.02, e. g. because you need certain older client versions, set the update source to IGEL OS 11.02.200.

IGEL OS 11.02.200 is a special variant of IGEL OS 11.02 which has signed partitions; this version can only be obtained from the IGEL Support Team.

## Error: "Invalid signature - Failed to read from partition"

### Symptom

During operation, a system message like this appears:



## Environment

- IGEL OS 11.03 or higher

## Problem

A system partition has been invalidated, which prevents system components from being loaded.

## Solution

1. Ensure that a valid update source is configured under **System > Update > Firmware Update** and the correct firmware is stored on the server. (For detailed information, see [Firmware Update\(see page 1252\)](#).) If the local Setup is not accessible, use the UMS.
2. Reboot the device.  
The device fetches the valid partition from the update source.

## 2.16.5 How to Show the Boot Mode of IGEL OS

To check the boot mode of IGEL OS, proceed as follows:

1. Open the IGEL start menu.
2. Click the i-icon.  
The **About** dialog opens.
3. Find the parameter **Boot Mode** under the **Hardware** section.  
Example: BIOS



## 2.16.6 Disabling Features to Reduce Firmware Size

### Symptom

You want to update your IGEL OS firmware to a higher release version, but the firmware update requires more disk space. Updating devices with less disk space than required leads to an error: Not enough space on local drive.

### Problem

The size of the new firmware

- with all enabled software features included
- with the NVIDIA graphics driver
- with the Firefox profile partition
- possibly with a custom partition
- possibly with custom wallpaper and bootsplash

exceeds the device's disk space (e.g. 2 GB).

### Solution

Disable firmware features not needed for productive operation to reduce the size of the firmware:

1. In IGEL Setup, go to **System > Firmware Customization > Features**.
2. Disable features not needed in your environment.
3. Activate your settings with **Apply** or **OK**.
4. Reboot the device.
5. Update the device.

Use profiles with UMS in order to deactivate features on a group of devices.

## 2.16.7 Fabulatech USB Redirection Server Component

### Issue

For Fabulatech USB Redirection, a special Fabulatech server component must be installed on the Citrix or RDP server (USB for Remote Desktop IGEL Edition). More detailed information on the function can be found on the [Fabulatech partner site<sup>156</sup>](#). On this site the server component is available for download.

Current versions are (as of 2017-05-29):

- USB for Remote Desktop IGEL Edition Ver.3.1.5

<sup>156</sup> <http://www.usb-over-network.com/partners/igel/>



- USB for Remote Desktop IGEL Edition V5 Ver. 5.0.2

## Problem

Which version is suitable for which IGEL Linux device?

Release notes of IGEL Linux only name the version of the *Fabulatech* client included but miss out the necessary server component version.

## Solution

- ▶ All Fabulatech clients version 3.x require server component version 3.x
- ▶ All Fabulatech clients version 5.x require server component version 5.x

So for IGEL Linux thin clients following requirements apply:

- IGEL Linux v4 devices up to current version 4.13.270 require server component version 3.x
- IGEL Linux v5 devices up to version 5.02.100 require server component version 3.x
- IGEL Linux v5 devices from version 5.03.100 and later require server component version 5.x
- IGEL Linux 10.x requires server component version 5.x.

## 2.16.8 Which Features of IGEL OS Will Be Affected If the UMS Is Down?

### Overview

In general, IGEL OS works independently of the Unified Management Suite (UMS). This includes, for instance, all remote desktop clients like Citrix, RDP, or VMware Horizon, and browsers.

Any configuration changes that are made via the UMS are stored on the device and thus remain stable when the UMS is down.

However, the Shared Workplace (SWP) feature and administration functions are affected by a UMS outage.

The following sections list the details.

### Productivity Features That Are Affected If the UMS Is Down

- Login via Shared Workplace (SWP); see [Shared Workplace \(SWP\)](#)<sup>157</sup>

### Administration Functions That Are Affected If the UMS Is Down

- Configuration changes
- License Management
- Secure Shadowing
- Secure Terminal

---

<sup>157</sup> <https://kb.igel.com/display/endpointmgmt606/SWP>



- Universal Firmware Update
- Firmware Customizations
- Transfer of files to the device, including Custom Partitions
- Remote commands, such as Wake-on-LAN or restart

## 2.17 Network

- Configuring Open VPN Sessions(see page 378)
- Running the OpenVPN Client with a Preconfigured Configuration File(see page 386)
- How Can I Configure OpenVPN with an .ovpn or .conf File?(see page 387)
- Configuring Wi-Fi Network Roaming(see page 393)
- Connecting to a Wi-Fi Network with Hidden SSID(see page 395)
- Improving WiFi Connectivity(see page 395)
- Preventing Permanent Storage of Wireless Network Keys(see page 398)
- Using WPA Enterprise / WPA2 Enterprise with TLS Client Certificates(see page 399)
- IPv6 Settings(see page 401)
- Extended Logging With Syslog, Tcpdump and Netlog(see page 403)
- Making a Telnet Connection from *IGEL Linux*(see page 413)
- Configuring Dynamic DNS Updates via DDNS(see page 414)
- Changing the SMB protocol version(see page 416)
- How to Launch the Wireless Manager within *IGEL OS* when the Taskbar Is Hidden(see page 416)

### 2.17.1 Configuring Open VPN Sessions

This document describes how to configure the *OpenVPN Client* on *IGEL Linux*.

#### Prerequisites

- A configured and running *OpenVPN 2.x* server
- Information about the *OpenVPN* server configuration (e.g. authentication method)
- A thin client with *IGEL Linux 10.01.100* or newer
- The certificate and private key files for the client, along with the root certificate of the CA that signed the client and server certificates.
- Optionally, a Smartcard or eToken supported by *IGEL Linux*.  
To learn how to distribute keys and certificates to the thin clients, refer to the How-To document "[Securely Distributing Keys and Certificates](#)(see page 385)".

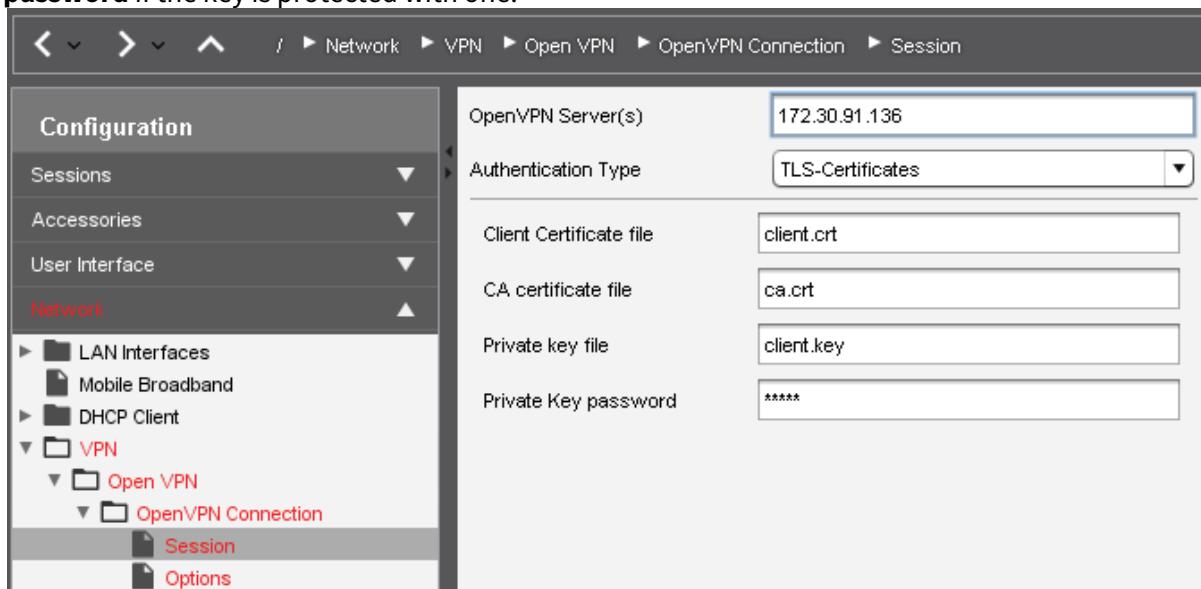
- 
- Authenticating with TLS Certificates(see page 379)
  - Authenticating with Name/Password(see page 379)
  - Authenticating with Name/Password with TLS Certificates(see page 380)
  - Authenticating with Static Key(see page 381)
  - Options and TLS Options(see page 382)
  - DNS and Routing Options(see page 382)
  - Proxy(see page 383)



- [Checking the VPN Connection](#)(see page 383)
- [Automatically Starting the VPN During Boot](#)(see page 384)
- [Further Information](#)(see page 384)
- [Securely Distributing Keys and Certificates for OpenVPN](#)(see page 385)

## Authenticating with TLS Certificates

1. Go to **Network > VPN > OpenVPN** and create a new connection.
2. In the **Session** section for the new connection, enter the name or public IP address of the **OpenVPN Server**.
3. Select **TLS-Certificates** as the **Authentication Type**.
4. Select the client certificate as the **Client Certificate file**.
5. Select the root certificate of the CA as the **Certificate Authority (CA) file**.
6. Select the client's private key as the **Private Key file**. Enter the passphrase in **Private Key password** if the key is protected with one.



7. Click an icon for the newly created session (e.g. in the Start Menu) to initiate the connection.

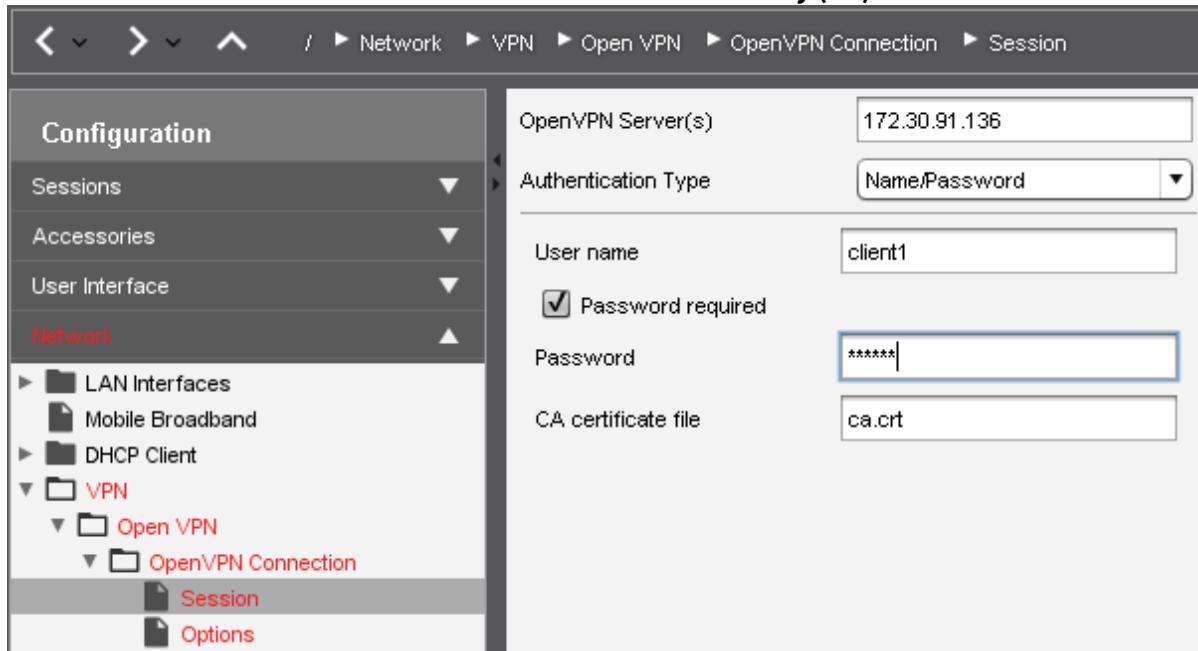
If a PKCS12 file is available, which includes the client certificate, the certificate authority and the private key, then you just need to enter the PKCS12 file name in the three corresponding fields. The advantage is that you only have to roll out one single file instead of three different files.

## Authenticating with Name/Password

1. Go to **Network > VPN > OpenVPN** and create a new connection.
2. In the **Session** section for the new connection, enter the name or public IP address of the **OpenVPN Server**.
3. Select **Name/Password** as the **Authentication Type**.



4. Enter the **Username**. If you leave this field blank the user will be prompted for the Username when connecting.
5. Check **Password required**.
6. Enter the **Password**. If you leave this field blank the user will be prompted for the password when connecting.
7. Select the root certificate file of the CAAs the **Certificate Authority (CA) file**.



8. Click an icon for the newly created session (e.g. in the Start Menu) to initiate the connection.

#### Authenticating with Name/Password with TLS Certificates

1. Go to **Network > VPN > OpenVPN** and create a new connection.
2. In the **Session** section for the new connection, enter the name or public IP address of the **OpenVPN Server**.
3. Select **Name/Password with TLS-Certificates** as the **Authentication Type**.
4. Enter the **Username**. If you leave this field blank the user will be prompted for the username when connecting.
5. Check **Password required**.
6. Enter the **Password**. If you leave this field blank the user will be prompted for the password when connecting.
7. Select the client certificate as the **Client Certificate file**.
8. Select the root certificate of the CA as the **Certificate Authority (CA) file**.
9. Select the client's private key as the **Private Keyfile**. Enter the passphrase in **Private Key password** if the key is protected with one.



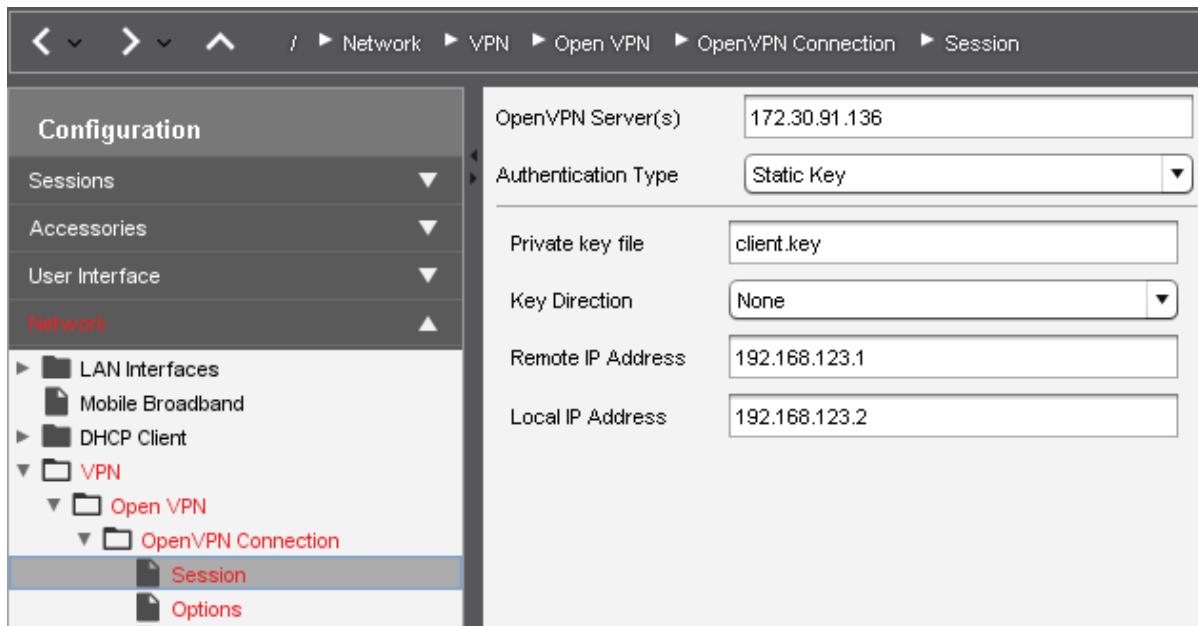
The screenshot shows the network configuration interface. On the left, a sidebar lists sessions, accessories, user interface, and network options. Under network, there are LAN interfaces, mobile broadband, DHCP client, and a VPN section which is expanded to show OpenVPN and OpenVPN Connection. The OpenVPN Connection item is further expanded to show Session and Options. The main panel displays configuration for the selected session. It includes fields for OpenVPN Server(s) (172.30.91.136), Authentication Type (Name/Password with TLS-Certificates), User name (client1), Password required (checked), Password (\*\*\*\*\*), Client Certificate file (client.crt), CA certificate file (ca.crt), Private key file (client.key), and Private Key password (\*\*\*\*\*).

- Click an icon for the newly created session (e.g. in the Start Menu) to initiate the connection.

If a PKCS12 file is available, which includes the client certificate, the certificate authority and the private key, then you just need to enter the PKCS12 file name in the three corresponding fields. The advantage is that you only have to roll out one single file instead of three different files.

## Authenticating with Static Key

- Go to **Network > VPN > OpenVPN** and create a new connection.
- In the **Session** section for the new connection, enter the name or public IP address of the **OpenVPN Server**.
- Select **Static Key** as the **Authentication Type**.
- Select the static key file as the **Private Key**.
- Select **None** as the **Key Direction**.
- Enter the server's VPN IP address as **Remote IP Address**.
- Enter your client's VPN IP address as **Local IP Address**.



- Click an icon for the newly created session (e.g. in the Start Menu) to initiate the connection.

## Options and TLS Options

### Options

Under **Network > VPN > OpenVPN > [Session Name] > Options**, you can set various options for the OpenVPN client. Usually, you can leave the default settings as they are. If the server uses compression, enable **Use LZO data compression**.

When using a proxy, set **Protocol used for communication to the host** to **tcp-client**.

### TLS Options

Under **Network > VPN > OpenVPN > [Session Name] > TLS-Options**, you can set various TLS-related options. In particular, you can configure whether the **remote peer certificate** will be verified.

For details about these settings, refer to [Configuring Open VPN Sessions](#)(see page 378) or [OpenVPN](#)(see page 1189).

## DNS and Routing Options

By default, OpenVPN automatically uses the server's settings for DNS and routing.

If you want to change these settings, go to **Network > VPN > Open VPN > [Session Name] > IPv4**. Here you can:

- Deactivate **Automatic DNS**
- Add **Extra nameserver(s)**
- Add **Extra search domains**
- Deactivate **Automatic Routes**
- Deactivate **VPN is the default route**



Additionally, you can enable three custom routes in **Network > VPN > Open VPN > [Session Name] > Route [0,1,2]**. For each enabled route you can configure:

- whether it is a **Network Route** or a **Host Route**
- **Network/Host IP**
- **Network Mask** (for Network Route only)
- Optional: **Gateway**
- Optional: **Metric** (a quality rating used for routing decisions, 0 being the best)

## Proxy

If you wish to configure a proxy for your VPN connection, go to **Network > VPN > OpenVPN > [Session Name] > Proxy**. Here you can configure:

- **Proxy Type: SOCKS or HTTP**, by default this is set to **None**
- **Proxy Address** and **Proxy Port**
- **Retry indefinitely when errors occur**

If you select the **HTTP** proxy type you can configure:

- **Proxy Username**
- **Proxy Password**

When using a proxy, set **Options > Protocol used for communication to the host** to **tcp-client**.

When experiencing issues with OpenVPN, read the messages in `/var/log/messages`, e.g. using the **System Log Viewer**.

## Checking the VPN Connection

As soon as a VPN connection is established, a lock icon with connected plugs is shown in the panel:



However, this only serves as an indicator. To be sure that the VPN connection really exists:

1. Open a **Local Terminal**.
2. Run the command `ifconfig`.
3. Check whether the output contains a `tun` device with an IP address from the private network.



Terminal

```

user@IGEL-000BCA050027:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0b:ca:05:00:27
          inet addr:172.30.91.219 Bcast:172.30.255.255 Mask:255.255.0.0
          inet6 addr: fe80::20b:caff:fe05:27/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:1091674 errors:0 dropped:47 overruns:0 frame:0
            TX packets:125138 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:79070067 (79.0 MB) TX bytes:58744380 (58.7 MB)
            Interrupt:105 Base address:0xa000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:65536 Metric:1
            RX packets:108954 errors:0 dropped:0 overruns:0 frame:0
            TX packets:108954 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:45078307 (45.0 MB) TX bytes:45078307 (45.0 MB)

tun0     Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.123.10 P-t-P:192.168.123.9 Mask:255.255.255.255
            UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
            RX packets:23080 errors:0 dropped:0 overruns:0 frame:0
            TX packets:48007 errors:0 dropped:74 overruns:0 carrier:0
            collisions:0 txqueuelen:100
            RX bytes:1266538 (1.2 MB) TX bytes:63784736 (63.7 MB)

user@IGEL-000BCA050027:~$ 
```

4. Additionally, check whether you can ping the VPN server's private IP address.

### Automatically Starting the VPN During Boot

If you want to update the firmware via the VPN, you need to enable **Autostart During Boot**. Enabling Autostart of the control application in **Network > VPN > OpenVPN > [session name]** is not adequate!

1. Go to **Network > VPN > OpenVPN**.
2. Check **Enable Autostart During Boot**.
3. Select one of the configured sessions.
4. Click **Set Auto**.

The session will be marked in the **Auto** column.

Click **Set Auto** again to deactivate autostarting the session.

The system will prompt you for key pass phrases or the eToken/smartcard PIN if necessary.

### Further Information

Further information about *OpenVPN* can be found in



- the [OpenVPN how-to<sup>158</sup>](#) and
- the [OpenVPN manual page<sup>159</sup>](#)

maintained by the *OpenVPN* project.

## Securely Distributing Keys and Certificates for OpenVPN

Use the file distribution mechanism in the *Universal Management Suite (UMS)* to securely distribute keys and certificates to the thin clients:

1. Select **Undefined** as the **Classification**.
2. Enter `/wfs/OpenVPN/` as **the thin client file location**.
3. Enable the **Read** permission for the **Owner** exclusively, and uncheck all remaining permissions.
4. Select **Root** as the **Owner**.

**New file**

**File source**

Upload local file to UMS server

Local file

Upload location (URL)

Select file from UMS server

File location (URL)

**File target**

Classification

Thin Client file location

**Access rights**

	Read	Write	Execute
Owner	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Others	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Owner	<input type="button" value="Root"/>	<input type="button" value="▼"/>	

**Ok** **Cancel**

<sup>158</sup> <https://openvpn.net/index.php/open-source/documentation/howto.html>

<sup>159</sup> <https://openvpn.net/community-resources/reference-manual-for-openvpn-2-0/>



## 2.17.2 Running the OpenVPN Client with a Preconfigured Configuration File

### Solution Based on Experience from the Field

This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

This article describes a basic solution for getting the built-in OpenVPN client running with a preconfigured configuration file. This is an alternative to using the Setup for configuration.

### Environment

This article is valid for the following environment:

- IGEL OS 10 or higher
- OpenVPN server

### Setting up an OpenVPN Connection with a Preconfigured Configuration File

1. In the UMS Console, open the context menu on **Files** and select **New File**.
2. Select your .ovpn file in the file system.
3. In the **File target** section, under **Devices file location**, enter "/wfs/".
4. Click **Ok**.  
The file is uploaded to the UMS.
5. Assign the file object to your device by clicking the "+" symbol in the **Assigned objects** area (upper right).
6. Create a profile with a suitable name, e. g. "OpenVPN Connection".
7. In the profile, go to **System > Firmware Customization > Custom Commands > Network**.
8. In the **Final network command** field, enter the following code, replacing example.ovpn with the correct filename:

```
while :; do if [ -z $(pgrep openvpn) ]; then echo "openvpn is not running"; openvpn --config /wfs/example.ovpn --auth-user-pass <(echo -e $(zenity --forms --text="Enter your VPN credentials" --add-entry=Username --add-password=Password --title=OpenVPN) | sed 's/|/\n/'); else echo "openvpn is running"; fi; sleep 1; done &
```

9. Click **Save** to save the profile.
10. Assign the profile to your device by clicking the "+" symbol in the **Assigned objects** area.
11. Reboot the device.  
After reboot, you should see a login window for OpenVPN.



## 12. Enter your OpenVPN credentials.

If the login was successful, a **Network connecting** popup appears briefly. No other indicator is shown. You can disconnect only by rebooting the device.

If the login has failed, the login window reappears.

### Removing the OpenVPN Connection

- ▶ To remove the OpenVPN connection from the settings, unassign the profile from the device and reboot it.

## 2.17.3 How Can I Configure OpenVPN with an .ovpn or .conf File?

### Solution Based on Experience from the Field

This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

### Overview

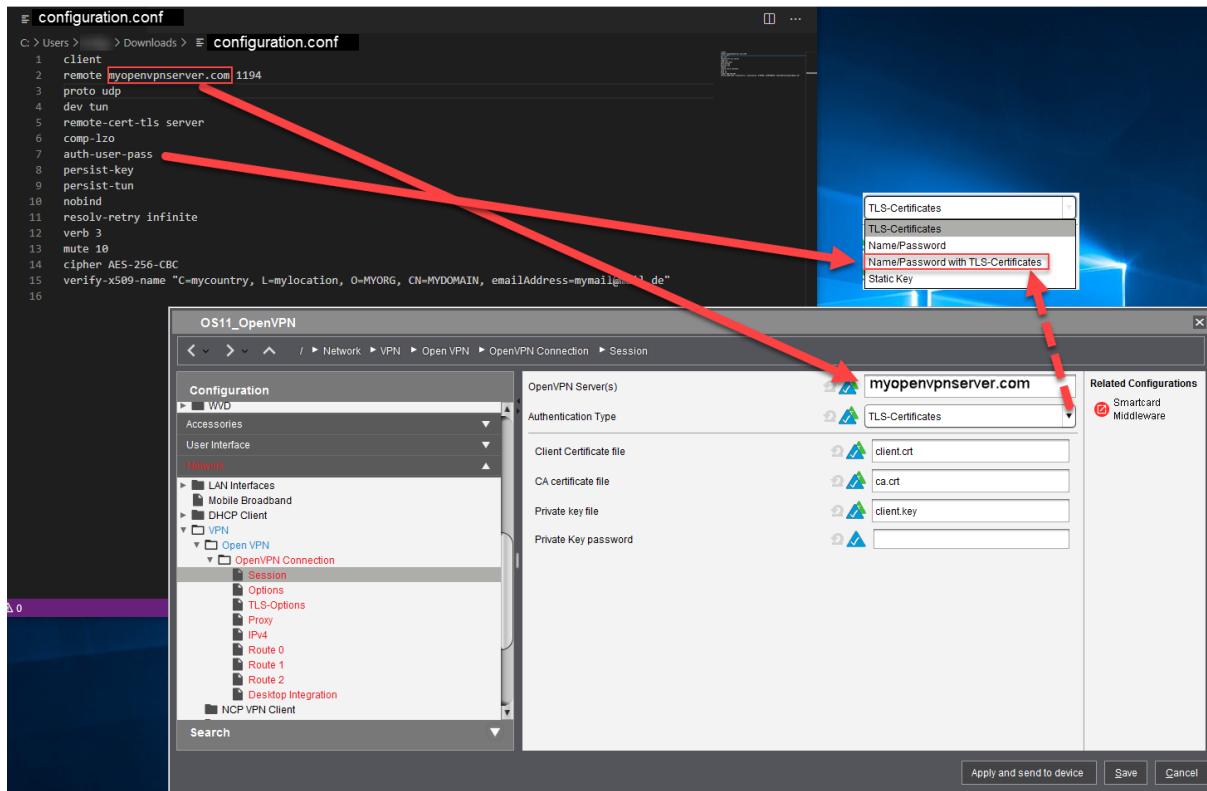
You can use the .ovpn or the .conf file from your firewall to configure OpenVPN for your IGEL OS device.

### Creating a Profile

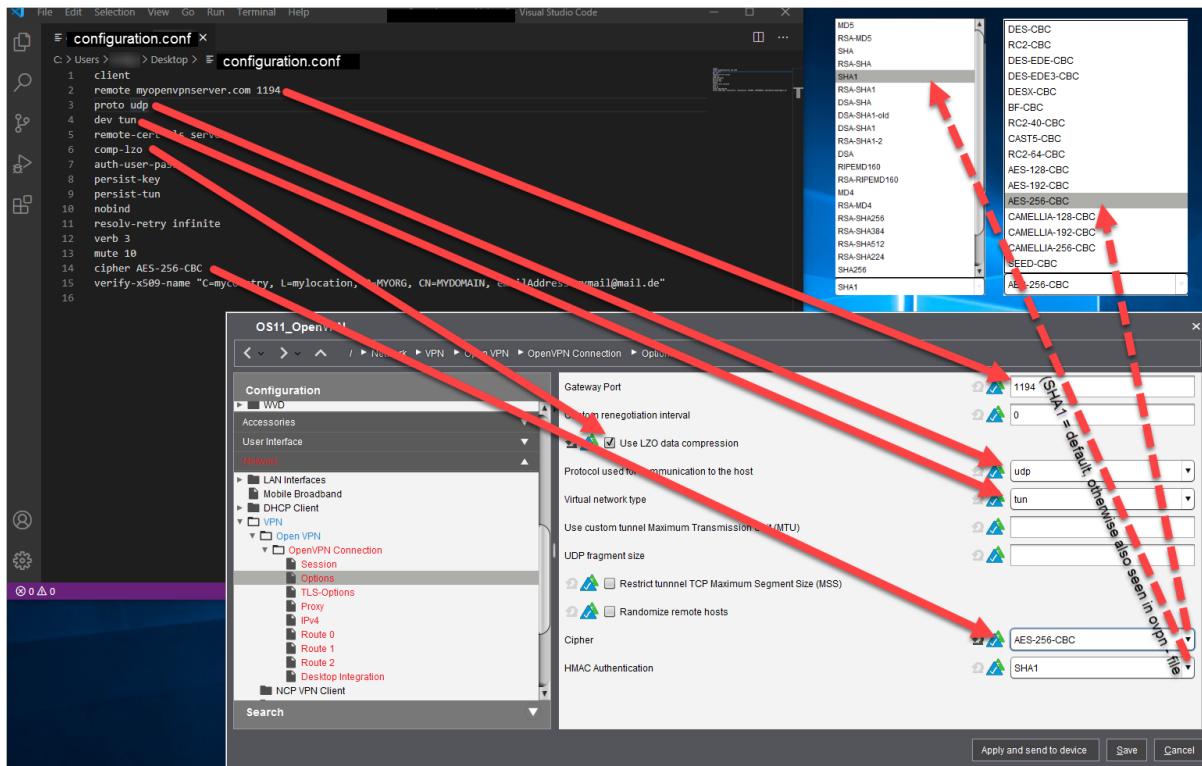
1. Open the .ovpn or the .conf file in “Microsoft Visual Studio Code” (freeware) or any other editor that can save files in UTF-8 and uses LF (not CR-LF) for a newline.
2. In the UMS, create a profile with an appropriate name, e.g. "OS11\_OpenVPN".
3. Go to **Network > VPN > Open VPN** and click to create an OpenVPN session.



4. Edit the settings of **Network > VPN > Open VPN > [your OpenVPN session] > Session** as follows:

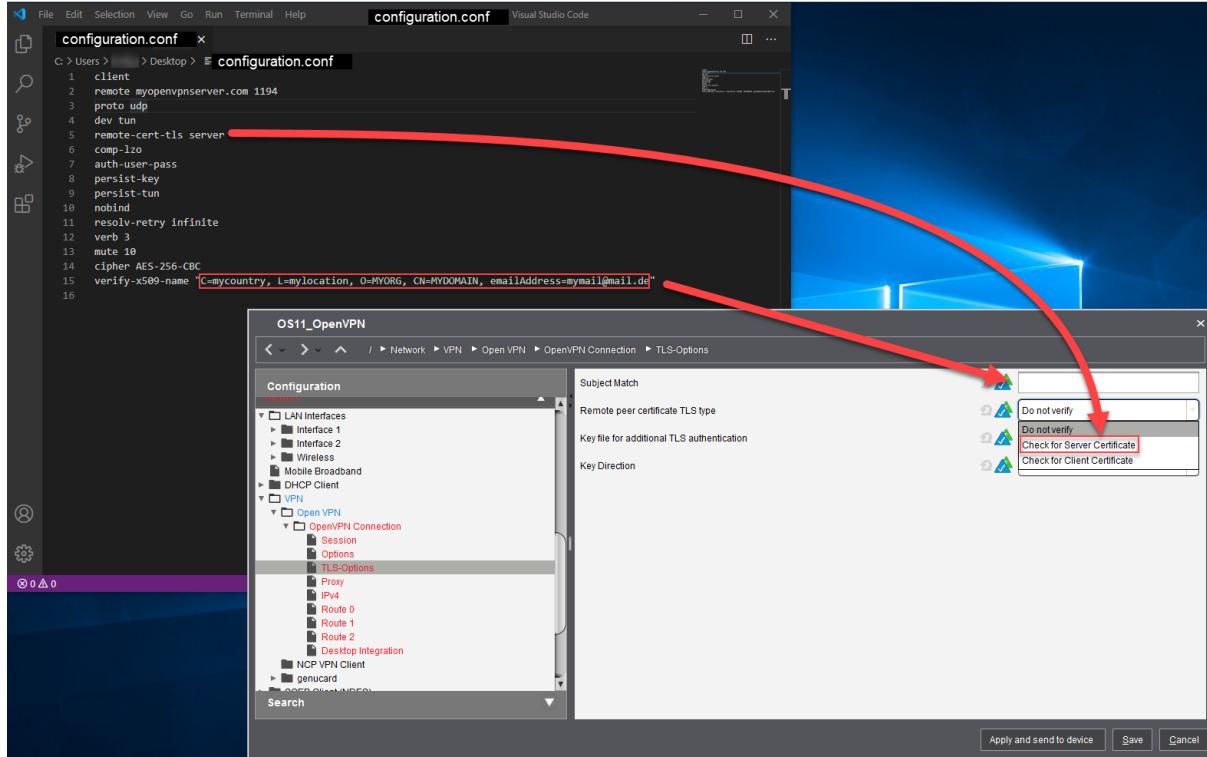


5. Go to **Network > VPN > Open VPN > [your OpenVPN session] > Options** and edit the settings as follows:





6. Go to **Network > VPN > Open VPN > [your OpenVPN session] > TLS Options** and edit the settings as follows:



## Creating the Certificate/Key Files

If you already have the following files, you can skip this section and jump to [Transferring the Files to the UMS\(see page 392\)](#):

- ca.crt
- client.crt
- client.key

If the certificates and the key are embedded in your .ovpn file, extract the certificates and key as follows:

1. Open the .ovpn file in your editor (must be able to save as UTF-8 and use LF, not CR-LF, for a newline).



2. Go to the section tagged as <ca> ... </ca> and copy the marked certificate, including -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----.

```

File Edit Selection View Go Run Terminal Help demo.ovpn - Visual Studio Code
demo.ovpn x
C:\> Users > [REDACTED] > Downloads > Test-ca > demo.ovpn
59 d2:9d:d7:30:6d:93:45:38:dc:3f:13:61:fd:4b:46:ff:c8:2a:
60 9c:89
61 -----BEGIN CERTIFICATE-----
62 MIICfDCCAcEwgAwIBAgIJAMNmYK8MaiTUMA0GCSqGSIb3DQEBCwUAMF8xCzAJBgNV
63 BAYTAmR1MRIwEAYDVQQHEwIeYXJtc3RhZHQxDAAKBgNVBAoTA0VSSzETMBEGA1UE
64 AxMKRVJLIFZQTiBDQTEZMBcGCSqGSIb3DQEJARYKYWRtQGVyay5kZTAeFw0wOTA3
65 MDgxMDQx LMRIwEAYDVQQH
66 EwIeYXJt LIFQTIbDQTEZ
67 MBCGC5qC 3AQEFAAA0BjQAw
68 gYkcgYE ZGAbQjee/DLV
69 WZWIA0mn 3ELyWoejMkUgW
70 6CmFFLc 3AwEAAaNAMD4w
71 HQDVROC FMAMB Af8wDwYD
72 VR0RBAgwBocEf wAAATANBgkqhkiG9w0BAQUFAAOBgQCDBbByikbQ0+4mv+yGgWsC6
73 xW34Wn2h7K10cdhBzwx2d71GBNhnRhdPiwe01au1cbwlRzEPni4CsdbA5joiic
74 7NnpXYS5xiBE+LGQl501SSEkO9UV+moxNxjYgaoguY8ne04QXC BhQi qFn5ndcw
75 bZNFO Nw/E2H950b/yCqcjQ==
76 -----END CERTIFICATE-----
77 </ca>
    
```

Ln 76, Col 26 (923 selected) Spaces: 4 UTF-8 LF Plain Text

3. Paste the text to the editor and save it to a file named ca.crt (file type "All files").  
 4. Go to the section tagged as <cert> ... </cert> and copy the marked certificate, including -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----.

```

File Edit Selection View Go Run Terminal Help demo.ovpn - Visual Studio Code
demo.ovpn x
C:\> Users > [REDACTED] > Downloads > Test-ca > demo.ovpn
133 9c:e8
134 -----BEGIN CERTIFICATE-----
135 MIIDcDCCAtmgAwIBAgIJAMNmYK8MaiVLMA0GCSqGSIb3DQEBCwUAMF8xCzAJBgNV
136 BAYTAmR1MRIwEAYDVQQHEwIeYXJtc3RhZHQxDAAKBgNVBAoTA0VSSzETMBEGA1UE
137 AxMKRVJLIFZQTiBDQTEZMBcGCSqGSIb3DQEJARYKYWRtQGVyay5kZTAeFw0xNjA3
138 MDUxMTE0NDNaFw0zNjExMjIxMDQzMjJaMEAxCzAJBgNVBAYTAmR1MRIwEAYDVQQH
139 DAIEYXJtc3RhZHQxMjAxMDQzMjJaMEAxCzAJBgNVBAYTAmR1MRIwEAYDVQQH
140 BgkhkiG9w0 /6cqeup+oSFw
141 0YbeRZwTS2L ?IpkTCN78hdz
142 er/JrXWqdK3 on2cEb81rzkd
143 USIVvOH3/n iQ8Wg9Ewwlyv
144 qRKkB6ZQF4 zkZ7iNrwoD6q
145 LmezFxiT7IE Dsk5PwIDAQAB
146 o4HOMIHLMB0 <QYDVR0jBIGJ
147 MIGGgBQhmhy 3hMCZGUxEjaQ
148 BgNVBAcTCURrciI2JGJRUQDEPfIAQGh1UCCyHMDRVS LPIRPhWQzDvQqo8wPfUksgv1B0
149 IENBMRkwFwYJKoZIhvvcNAQkBFGphZG1AZXJrLmRlgkkAw2ZgrwxqJNQwQyDVR0T
150 BAIwADALBgNVHQ8EBAMCBewDQYJKoZIhvvcNAQELBQADgYEAu63qTTjsWwPc7Fyr
151 JptP/eZwcJ5BeIKScx9Zux/U8jLY5rPm1ysBqN+vgD3hBvh+M3uxkABp70W0QQD
152 7GHVT460fRw4NfdedAggwFgtcR8zmNyex0e/m0bsupg3IJq70tlmaRyWc2fwFV
153 6ser81mVC1cPZnPewd73jWlsQn0g=
154 -----END CERTIFICATE-----
155 </cert>
156 -----BEGIN PRIVATE KEY-----
157 
```

Ln 154, Col 26 (1252 selected) Spaces: 4 UTF-8 LF Plain Text

5. Paste the text to the editor and save it to a file named client.crt (file type "All files").



6. Go to the section tagged as <key> . . . </key> and copy the marked key, including -----BEGIN PRIVATE KEY----- and -----END PRIVATE KEY-----.

```

File Edit Selection View Go Run Terminal Help demo.ovpn - Visual Studio Code
demo.ovpn x
C: > Users > [REDACTED] Downloads > Test-ca > demo.ovpn
156 <key>
157 -----BEGIN PRIVATE KEY-----
158 MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBwgSjAgEAAoIBAQCowcVivLbfju+w
159 YAg/pyp64/6hIXDRht5FnBNLYvalyALCFh1rPq4q8Kc1GU8x/TQDxfEsishULZT
160 6HFkimRNw3vyF3N6v8mtdap0rev0SfbTw3VC6lrmMuln1gyCADfgkxEmf+6auo1K
161 ymJufZwRvzWvOR1Rhi868ff+cw07mrwAFgnXZI8tVVZNP2282IQQUFYiPw/06P
162 uvRIdxaD0TDCXK+pEqQ0hpIAxhuCzw5EGC88RR+3C3ERgg/UDV8EJHhuB1CdVYn0
163 z0XRnuI2wCgPqouZ7MXGJPsgRTG/VbF88Xec+yB03BK21/VEA8BeKBz1FyxnZpc
164 jaUoYTk/ wjb91xr4J
165 Coc+nJQK jLGMe9+Snb
166 rncgy6xF wSsqj2JN87
167 V2HcUGAt /mA9VXvrVn
168 3X6F4eVa :N03vFwz/2
169 UX0kxxfUh leRb3XxzHa
170 FOFxx27F 'iS42cA3gg
171 q1EzlwJb 'mkK7BePdN
172 NowCOYlp .Tms1cnmkU
173 Vvauz1vz tL4JApgcL
174 kcg/jm8K l1i3vb1gbx
175 y5jfRy32 :POxpUklm1
176 TU9WNOS8 wbaqB0G3bc
177 VUnL8gVsPPRagXIAJxsHe1AcU4bb5xx4AHFKbNFrkzpY6sX75tf0BbIBAoGBAJJW
178 qTgkT1hkEMoXBw8K1XF9ZWM08uI5WYd+GIMt+Ae/XJwIt2m32Za05Lhs30Utg
179 jmRjMbw4/YH9sTD+X+HjLs481ugjt8AKTRmFipGwUXmYDPkfvVT0grFWEOru3/X
180 5cgjqZOY1EQ/947kf2Hmozq9qpBDj5S8AUQKdrzAoGAE30aX9P558/6NE0un113
181 3KG0/dgm9evz7WS9t1b6jFa0vwyp1/GDE8dePpjkt7aUGvY10HuRfeNzJ01AHF
182 TEDvMP64atacGJxh8Ipjoalstb2sKH1FyHMAwlks3an13Fg0BUd69AjK87+ENzNN
183 mvhbjsCx/zHqytHSah+Tqt8=
184 -----END PRIVATE KEY-----
185 </key>
186
187

```

Ln 184, Col 26 (1703 selected) Spaces: 4 UTF-8 LF Plain Text ⚙️ 🗑️

7. Paste the text to the editor and save it to a file named client.key (file type "All files").

## Transferring the Files to the UMS

1. In the UMS, create a file object for each certificate/key file; set **Classification** to "Common Certificate (all purpose)". For details, see [Registering a File on the UMS Server](#)<sup>160</sup>.
2. Assign the file objects to the endpoint devices on which you want to use the OpenVPN connection. For details, see [Transferring a File to a Device](#)<sup>161</sup>.

## Adjust the Profile

1. In the UMS, open the profile you have created for your OpenVPN connection and go to **Network > VPN > Open VPN > [your OpenVPN connection] > Session**.

<sup>160</sup> <https://kb.igel.com/display/endpointmgmt605/Registering+a+file+on+the+UMS+server>

<sup>161</sup> <https://kb.igel.com/display/endpointmgmt605/Transferring+a+file+to+a+device>



2. Edit the file locations as follows:

The screenshot shows the 'OS11' configuration interface with the path: Network > VPN > Open VPN > OpenVPN Connection > Session. The left sidebar shows 'Configuration' and 'Network' sections. In the main pane, under 'OpenVPN Server(s)', the server is set to 'myopenvpnserver.com' and the authentication type to 'Name/Password with TLS-Certificates'. Under 'Session', the 'Client Certificate file' field contains 'Mfs/ca-certs/client.crt', which is circled in red. Other fields include 'CA certificate file' (Mfs/ca-certs/ca.crt) and 'Private key file' (Mfs/ca-certs/client.key). Buttons at the bottom include 'Apply and send to device', 'Save', and 'Cancel'.

3. Apply the profile to the endpoint devices on which you want to use the OpenVPN connection.

## 2.17.4 Configuring Wi-Fi Network Roaming

### Issue

Different wireless network instances have been configured for a mobile device. The device should switch over to the strongest network automatically.

### Solution

Parameters to configure Wi-Fi roaming options can be found in the IGEL registry (**Setup > System > Registry**). These settings should be changed by experts only.

- Parameters for better control of Wi-Fi roaming capabilities with access points that share the same SSID:

**network.interfaces.wirelesslan.device0.lock\_initial**

Default: false

If true, the device will stick to the access point it is connected to even if candidates with better signal quality are present.

Setting this parameter to true is a last resort for problems that are caused by too much roaming.

**network.interfaces.wirelesslan.device0.bgscan.module**

Only active with encryption methods WPA Enterprise and WPA2 Enterprise.



Default: none

Possible values:

`none` : No background scanning is done.

`simple` : The Wi-Fi module tries to scan for a potentially better signal in the background.

**`bgscan.module simple`** provides following options:

**`network.interfaces.wirelesslan.device0.bgscan.simple.signal_strength`** (default: -45 dBm)

This defines a threshold that determines which of the following two parameters shall be effective:

**`network.interfaces.wirelesslan.device0.bgscan.simple.short_interval`** (default: 30 s)

Interval between background scans (in seconds) if the actual signal level of the currently connected access point is worse than `signal_strength`.

**`network.interfaces.wirelesslan.device0.bgscan.simple.long_interval`** (default: 300 s)

Interval between background scans (in seconds) if the actual signal level of the currently connected access point is better than `signal_strength`.

If parameter `lock_initial` is true, it is recommended to set **`bgscan.module`** to none.

- Parameters to control Wi-Fi roaming between Wi-Fi networks with different SSIDs:

**`network.interfaces.wirelesslan.device0.mssid_check_interval`** (default: 10 s)

The interval in seconds between checking if automatic roaming might be necessary. This includes detecting that a connection has been lost and a new one should be established.

**`network.interfaces.wirelesslan.device0.mssid_quality_threshold`** (default: 20)

If the current connection's quality percentage is below this value, scanning will be performed to find a potentially better network.

**`network.interfaces.wirelesslan.device0.mssid_quality_difference_threshold`** (default: 40)

A candidate for automatic roaming is only considered if its quality percentage is this much better than the current connection's quality.

**`network.interfaces.wirelesslan.device0.mssid_previously_used_threshold`** (default: 55)

During boot: If the previously used SSID's quality percentage is above this threshold, it is preferred.

**`network.interfaces.wirelesslan.device0.mssid_user_selection`** (default: false)

If true, the user can initiate roaming to a network via the Wi-Fi tray icon's context menu (must be enabled).

If automatic roaming shall not interfere with the user's choice, the following values are appropriate:

`network.interfaces.wirelesslan.device0.mssid_quality_threshold = 0`

`network.interfaces.wirelesslan.device0.mssid_quality_difference_threshold = 101`

`network.interfaces.wirelesslan.device0.mssid_previously_used_threshold = 0`

## 2.17.5 Connecting to a Wi-Fi Network with Hidden SSID

### Symptom

The device does not connect to a wireless network with hidden SSID.

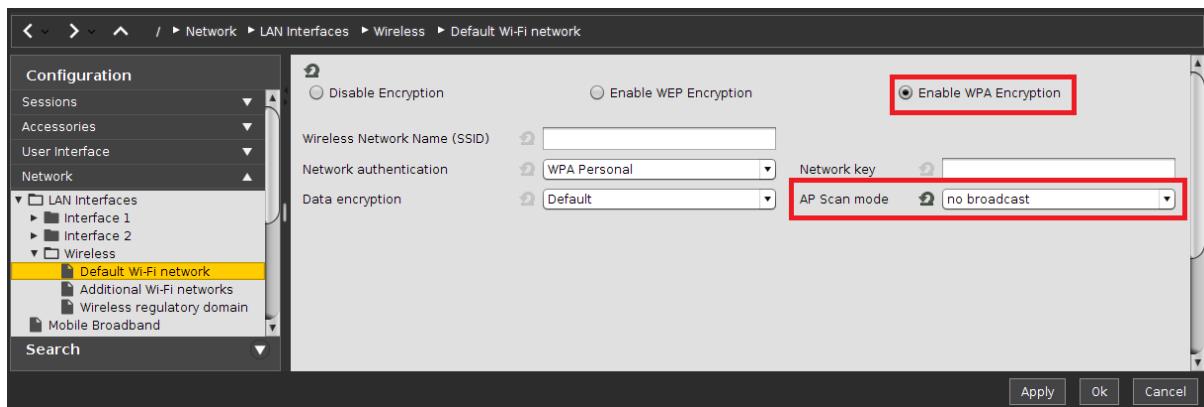
### Problem

An option in the device's network configuration is missing.

### Solution

If you need to configure a hidden access point, proceed as follows:

1. Start IGEL Setup or open the device configuration dialog in the UMS.
2. Go to **Network > LAN Interfaces > Wireless > Default Wi-Fi network** (or **Additional Wi-Fi networks** depending on your configuration).
3. Choose **Enable WPA Encryption**.
4. Set parameter **AP Scan mode** to "**no broadcast**".
5. Click **Apply** or **Ok** to save the settings.



## 2.17.6 Improving WiFi Connectivity

### Problem

Your WiFi connection is unstable, or weak, or both.



## Environment

- UDC with IGEL Linux v5??? or IGEL OS??? or higher???
- UD Pocket IGEL Linux v5??? or IGEL OS??? or higher???

## Possible Causes and Solutions

There are many circumstances and parameters which influence the quality of a device's WiFi connection. To find a suitable solution to your problem, check out the following collection of possible causes and suggested solutions, workarounds and hints for debugging.

### Several Access Points (APs) Are Using the Same Channel

If more than one Access Points visible to the thin client are using the same WiFi channel, interference issues may arise.

- ▶ Reconfigure the Access Point (AP) in question to use different channels.

### Roaming within One Network (Same SSID)

When the device is configured to roam within its network, it tries to make sure that it is using the strongest/nearest Access Point (AP) within its network. Dependent on the given situation, it might be feasible to disable or to optimize roaming.

See also [Configuring Wi-Fi Network Roaming](#)(see page 393).

### Avoid Roaming

- ▶ In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > lock\_initial** (Registry key: `network.interfaces.wirelesslan.device0.lock_initial`) and activate **Avoid roaming within the same network**.

If roaming is deactivated, **System > Registry > network > interfaces > wirelesslan > device0 > bgscan > module** should be set to **none**.

### Select the Access Point with the Best Signal

With the following setting, the thin client selects the Access Point that emits the best signal when the device starts up.

- ▶ In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > bssid** (Registry key: `network.interfaces.wirelesslan.device0.bssid`) and enter `bestsignal` in the **BSSID** field.

### Automatic Roaming

Automatic roaming is feasible if the device is moved around frequently, and several Access Points are available.

In the following example, the device is configured to start scanning for another Access Point 10 seconds after the signal of the current Access Point has dropped below -78 db, while a routine scan is executed every 60 seconds, :



1. In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > bgscan > module** (Registry key: network.interfaces.wirelesslan.device0.bgscan.module) and select **simple**.
2. Set **System > Registry > network > interfaces > wirelesslan > device0 > bgscan > module > simple > long\_interval** (Registry key: network.interfaces.wirelesslan.device0.bgscan.module.simple.long\_interval) to 60.
3. Set **System > Registry > network > interfaces > wirelesslan > device0 > bgscan > module > simple > short\_interval** (Registry key: network.interfaces.wirelesslan.device0.bgscan.module.simple.short\_interval) to 10.
4. Set **System > Registry > network > interfaces > wirelesslan > device0 > bgscan > module > simple > signal\_strength** (Registry key: network.interfaces.wirelesslan.device0.bgscan.module.simple.signal\_strength) to -78.

#### 40 MHz Bandwidth in the 2.4 GHz Band

With some Access Points, it may be feasible to disable the 40 MHz bandwidth in the 2.4 GHz band.

- ▶ In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > driver > cfg80211 > cfg80211\_disable\_40mhz\_24ghz** (Registry key: network.interfaces.wirelesslan.device0.driver.cfg80211.cfg80211\_disable\_40mhz\_24ghz) and deactivate **Disable 40 MHz channel bandwidth in 2.4 GHz band**.

#### High Throughput Option

In some environments, the high throughput functionality built into the driver may not produce optimal results. You can disable this functionality and check if the connection has improved.

- ▶ In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > driver > disable\_ht** (Registry key: network.interfaces.wirelesslan.device0.driver.disable\_ht) and deactivate **Disable HT**.

#### 2.4 GHz Band Only

In some environments, it might be better to use only the 2.4 GHz band.

- ▶ In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > band** (Registry key: network.interfaces.wirelesslan.device0.band) and select **2.4 GHz**.

If one or more alternative WiFi networks (SSIDs) are configured, do the following for each alternative SSID:

- ▶ In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > alt\_ssid[number] > band** (Registry key: network.interfaces.wirelesslan.device0.alt\_ssid[number].band) and select **2.4 GHz**.



## Frame Aggregation

It might be helpful to disable the frame aggregation feature of IEEE 802.11n.

- ▶ Disable frame aggregation on your Access Point (AP).

On your Access Point, this feature may have a different name.

Also note that IGEL cannot give a guarantee that the Access Point will function properly after the suggested configuration changes.

## WiFi Driver Scans And Selects Access Point

By default, the WPA supplicant initiates scanning and the selection of an Access Point. You can change this behavior and assign this task to the driver.

1. In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > wpa > ap\_scan** (Registry key: `network.interfaces.wirelesslan.device0.wpa.ap_scan`) and select **WLAN driver initiates scanning and AP selection**.
2. Restart the thin client.

## Whitelist of BSSIDs

You can restrict the number of Access Points to be scanned by creating a whitelist. This whitelist contains only the BSSIDs of those Access Points that the device should scan.

In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > bssid\_whitelist** (Registry key: `network.interfaces.wirelesslan.device0.bssid_whitelist`) and enter the BSSIDs of those Access Points that should be scanned, separated by whitespaces.

## Debugging

If none of the methods described above work, you can create a log file and send it to the IGEL Support Team.

1. In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > wpa > debug** (Registry key: `network.interfaces.wirelesslan.device0.wpa.debug`) and select **very verbose**.
2. Restart the thin client.
3. Send the file `/tmp/wpa_debug.all` to the IGEL Support Team.

## 2.17.7 Preventing Permanent Storage of Wireless Network Keys

This document describes how to prevent users from storing wireless network keys/passwords for **Wireless Manager** on the endpoint device.

1. In Setup, go to **System > Registry**.
2. Go to the `network.applet.wireless.allow_storing_credentials` parameter.
3. Uncheck **Allow permanently storing credentials**, which is checked by default.
4. Click **Apply**.



This will affect the **Wireless Manager** dialogs for wireless networks with the network authentication methods in their variants requiring passwords:

- WPA Personal
- WPA Enterprise
- WPA2 Personal
- WPA2 Enterprise

In particular, users will not have check boxes labeled **Permanently store identity and password** or **Permanently store network key** available.

## 2.17.8 Using WPA Enterprise / WPA2 Enterprise with TLS Client Certificates

This document describes how to use UMS to configure Wi-Fi connections on IGEL OS with WPA Enterprise / WPA2 Enterprise and TLS client certificates.

There are two options for supplying client certificates and keys to devices:

### Via SCEP (NDES)

SCEP allows the automatic provisioning of client certificates via an SCEP server and a certification authority (CA).

Learn how to configure it, using How-To [Certificate Enrollment and Renewal with SCEP \(NDES\)](#)(see page 457).

### Via Files Served from UMS

You need:

- a client certificate in PEM (base64) format
- a client private key (needs to be passphrase-protected) in PEM (base64) format

Alternatively,

- a PKCS#12 file containing both client certificate and private key (needs to be passphrase-protected).

In both cases, SCEP and files from UMS, the device needs to have a working Ethernet or Wi-Fi connection to the SCEP server or the UMS first, so that it can fetch the necessary certificates before it can connect to the target Wi-Fi.

- [Deploying Client Certificates and Keys](#)(see page 399)
- [Configuring the Network Interface](#)(see page 400)

### Deploying Client Certificates and Keys

To deploy client certificates and keys via UMS, follow these steps for the client certificate and client private key files (or the PKCS#12 files containing both):



1. In the **UMS Console** navigation tree, right-click **Files** and select **New file** from the context menu.  
The **New file** dialog opens
2. Under **File source**, use the file chooser to choose the file as the **Local file**.
3. Under **File target**, leave the classification as **Undefined**.
4. Set the **Thin Client file location** to `/wfs/wpa-tls/`
5. Under **Access rights**, set check **Read** and **Write** for the **Owner** and none for **Others**.
6. Set the **Owner** to **Root**.
7. Click **OK** to upload the file.
8. Drag the file icon onto a thin client or thin client directory in order to assign the file.

## Configuring the Network Interface

This describes how to configure the Wi-Fi interface.

In both cases, SCEP and files from UMS, the device needs to have a working Ethernet or Wi-Fi connection to the SCEP server or the UMS first, so that it can fetch the necessary certificates before it can connect to the target Wi-Fi.

### Using SCEP (NDES)

1. In Setup go to **Network > LAN Interfaces > Wireless**.
2. Check **Activate Wireless Interface**.
3. Go to **Default WiFi-network**.
4. Select **Enable WPA Encryption**.
5. Enter the **Wireless Network Name (SSID)**.
6. Select **WPA Enterprise** or **WPA2 Enterprise** according to your preferences.
7. Set **EAP Type** to **TLS**  
or set **EAP Type** to **PEAP** and **Auth Method** to **TLS**.
 

IGEL OS supports both EAP-TLS and PEAP-EAP-TLS. Choose one that is supported by your infrastructure.
8. Leave **Validate Server Certificate** enabled.
9. Enter the path to a **CA Root Certificate** if you use a CA other than [those supported by IGEL OS](#)(see [page 470](#)).
10. Check **Manage Certificates with SCEP (NDES)**.
11. Click **Save**.

### Using Certificate and Key Files

1. In Setup go to **Network > LAN Interfaces > Wireless**.
2. Check **Activate Wireless Interface**.
3. Go to **Default Wi-Fi network**.
4. Select **Enable WPA Encryption**.
5. Enter the **Wireless Network Name (SSID)**.
6. Select **WPA Enterprise** or **WPA2 Enterprise** according to your preferences.



7. Set **EAP Type** to **TLS**

or set **EAP Type** to **PEAP** and **Auth Method** to **TLS**

IGEL OS supports both EAP-TLS and PEAP-EAP-TLS. Choose one that is supported by your infrastructure.

8. Leave **Validate Server Certificate** enabled. Enter the path to a **CA Root Certificate** if you use a CA other than [those supported by IGEL OS](#)(see page 470).
9. Enter the path to the **Client Certificate** file in PEM (base64) format, e.g. /wfs/wpa-tls/client.crt.  
Leave this field blank if you use a PKCS#12 file containing both certificate and private key.
10. Enter the path to the **Private Key** file in PEM (base64) format.  
If you use a PKCS#12 file containing both certificate and private key, enter its path here.
11. Specify the **Identity** to be used if your key/certificate contains more than one entry.
12. Enter the **Private Key Password**.
13. Click **Save**.

## 2.17.9 IPv6 Settings

*IGEL Linux version 5.07.100 or newer and IGEL Linux version 10.01.100 or newer offer new options for configuring network interfaces for IPv6.*

### Application Scenario

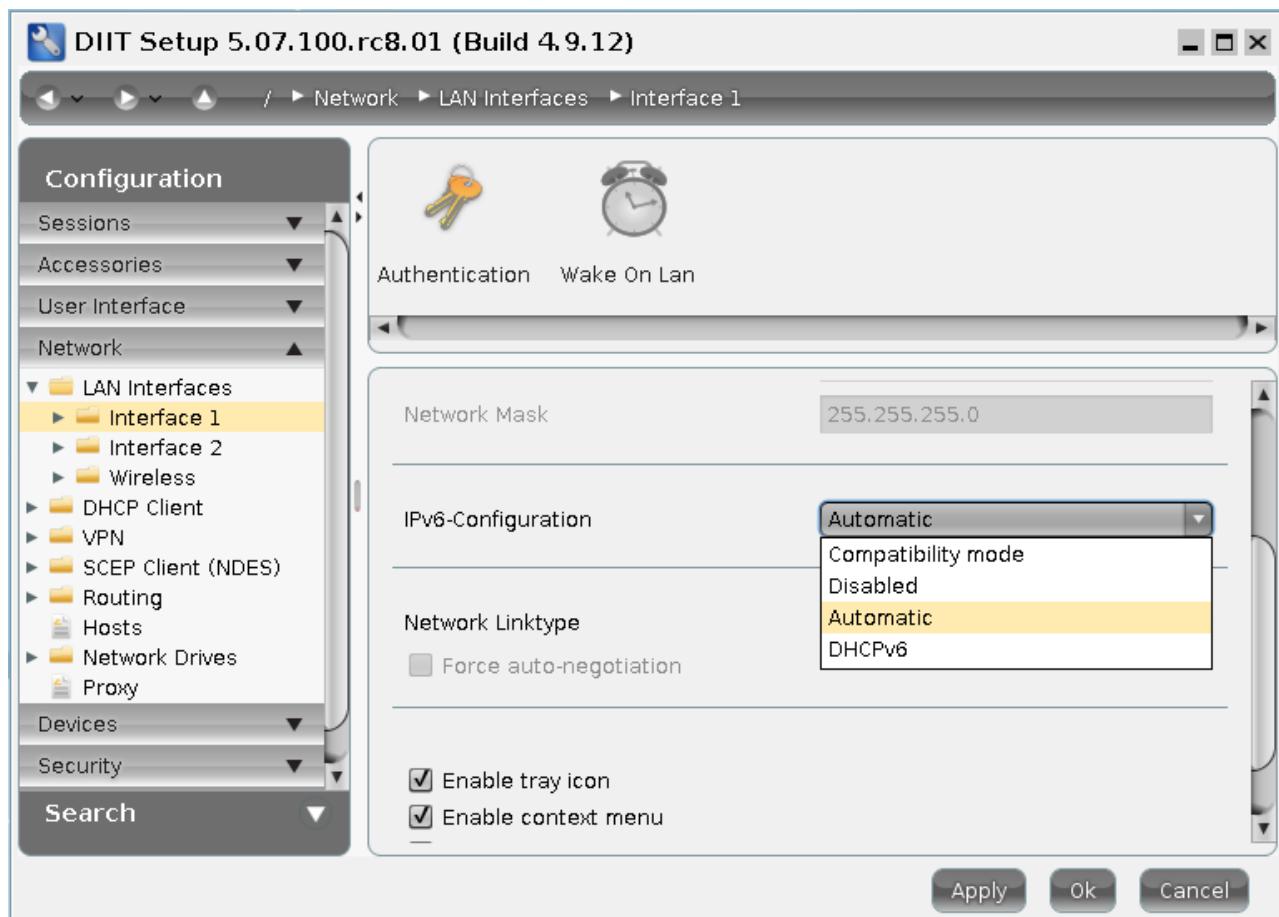
IGEL devices cannot so far communicate with the UMS via IPv6. Therefore, the major application scenario for IPv6 is as follows:

- Devices still receive their IPv4 configuration and potentially *IGEL*-specific DHCP options from a DHCPv4 server.
  - Most of the settings are received from the *UMS* via IPv4.
  - Only the default options are requested from the DHCPv6 server. These are as follows:
    - IPv6 address
    - nameservers
    - DNS search list.
  - Regarding DNS, only IPv6 nameserver addresses should be delivered (in router advertisements or DHCPv6 options). The resolver should be able to use these for retrieving AAAA records and also A records if necessary.
  - Clients and servers use IPv6 if they are prepared to do so.
- Examples:
- An NTP server (**System > Time and date > NTP time server**) can be specified as an IPv6 address or as a name for which the DNS has only an AAAA record available.
  - Similarly, in a web browser session, IPv6 will be used when the DNS has AAAA records available for servers.
- 
- [Available Configurations](#)(see page 402)
  - [Timeouts in Automatic Configuration](#)(see page 403)



## Available Configurations

IPv6 support is configured by network interface in **Network > LAN Interfaces**:



The following configurations are available:

Value	Effect
<b>Compatibility mode</b>	Equivalent to former versions of IGEL Linux: NetworkManager ignores the device, but the kernel performs some basic configuration. In particular, it assigns an IPv6 link local address to the device.
<b>Disabled</b>	IPv6 is disabled completely.
<b>Automatic</b>	The device tries to perform an IPv6 stateless or stateful autoconfiguration based on router advertisements. Depending on the router advertisements, this involves DHCPv6 (see RFC 4861).



<b>DHCPv6</b>	This option is supported by NetworkManager. It can be used when a DHCPv6 server is available but no router advertisements. Routing has to be configured by other means. In most cases <b>Automatic</b> will be preferable.
---------------	--

In all cases IPv4 is configured in the usual way.

### Timeouts in Automatic Configuration

If **Automatic** is selected, there is a configurable timeout for the dual stack mode. This is the time that the system waits after the first of the stacks IPv4 or IPv6 has completed its configuration for the other stack to complete its own configuration. After this time has elapsed, it runs the scripts that depend on the network being up. The default timeout value is 15 seconds.

The timeout can be configured with the following parameters in **System > Registry**:

Parameter	Device
network.interfaces.ethernet.device0.dual_stack_timeout	First ethernet device
network.interfaces.ethernet.device1.dual_stack_timeout	Second ethernet device
network.interfaces.wirelesslan.device0.dual_stack_timeout	Wireless LAN device

Use the **Search parameter ...** function with the string `dual_stack` to find these parameters quickly.

### 2.17.10 Extended Logging With Syslog, Tcpdump and Netlog

The IGEL OS **Registry** offers a number of extended logging options that can help customers, Support and PreSales debug system and network issues.

For instructions on how to send log files to the IGEL support team via the UMS, see [Sending Device Log Files to IGEL Support](#)(see page 720).

- [Debuglog Partition](#)(see page 403)
- [Syslog](#)(see page 405)
- [Tcpdump](#)(see page 405)
- [Netlog](#)(see page 407)

#### Debuglog Partition

Logfiles can get very large quite fast. This is why they are stored in a separate partition. It is mounted at `/debuglog`.



## Enabling and Configuring the Debuglog Partition

The partition is enabled and configured in the **Registry**:

<b>IGEL Setup &gt; System &gt; Registry</b>		
<b>&gt; Enable debuglog partition</b>	debug.tools.log_partition.enabled	enabled / <u>disabled</u>
Enables the debuglog partition.		

<b>IGEL Setup &gt; System &gt; Registry</b>		
<b>&gt; Size of debuglog partition in MiB</b>	debug.tools.log_partition_size	50 ... 500 / <u>100</u>
Resizing the debuglog partition will delete its contents!		

## Debuglog Partition Contents

Depending on which logging options you enable (see the following topics), you may find the following files in the debuglog partition:

- Syslog
  - messages (the current syslog)
  - messages[1-9].gz (compressed and rotated syslog)
- Ethtool
  - netlog-ethtool-[device].log
- Ping
  - netlog-host-[0-9]-ping.log (ping log)
  - netlog-host-[0-9]-ping[n].log.gz (compressed and rotated ping log)
- Ifconfig
  - netlog-ifconfig-[device].log
- Netstat
  - netlog-netstat.log (netstat log)
  - netlog-netstat[n].log.gz (compressed and rotated netstat log)
- Socket Status
  - netlog-socket\_status.log (socket status log)
  - netlog-socket\_status[n].log.gz (compressed and rotated socket status log)
- Tcpdump



- `tcpdump[0-3]_capture_current[n]` (tcpdump capture)
- `tcpdump[0-3]_capture-[n].pcap.{lzo,gz,bzip2,xz}` (compressed and rotated tcpdump captures)
- Tcpdump triggered by an error
  - `ERROR_[timestamp]/tcpdump[0-3]_capture-[n].pcap.{lzo,gz,bzip2,xz}` (compressed and preserved tcpdump captures)

## Syslog

It is possible to send all syslog messages that are written to `/var/log/message` (IGEL Linux version 5.10.250 and versions 5.11.x) or to the systemd journal (IGEL Linux version 10.01.100) to the debuglog partition as well. The logfile will be rotated and compressed as needed. This preserves the log if the thin client crashes, and logs from several previous boots.

Configure it in the **Registry**:

<b>IGEL Setup &gt; System &gt; Registry</b>		
<b>&gt; Enable syslog log to debuglog partition</b>	<code>debug.tools.syslog0.enabled</code>	true/ <u>false</u>
<b>IGEL Setup &gt; System &gt; Registry</b>		
<b>&gt; Number of Rotate Files</b>	<code>debug.tools.syslog0.num_rotate_files</code>	<u>2 ... 9</u>
Number of files to be kept while rotating.		
<b>IGEL Setup &gt; System &gt; Registry</b>		
<b>&gt; Logfile rotate size in MiB</b>	<code>debug.tools.syslog0.rotate_size</code>	<u>2, 4 , 8, 16</u>
Rotate when the size of the compressed file reaches this size in MiB.		

## Tcpdump

Tcpdump will help you debug network issues by capturing packets from up to 4 individual network interfaces.

Using the [Netlog](#)(see page 407) facility, it is possible to copy capture files to a subdirectory, triggered by an error in another log, so the captures before and after the error will be preserved for your analysis.



You can use Wireshark on an external system for analyzing capture files.

Find out more about Tcpdump from its homepage<sup>162</sup>.

### IGEL Setup > Registry

<b>&gt; Resolve addresses/ports to names</b>	debug.tools.tcpdump[0-3].addr_resolution	enabled / <u>disabled</u>
--	--	---------------------------

### IGEL Setup > Registry

<b>&gt; Compression Method</b>	debug.tools.tcpdump[0-3].compression	lzop, gzip, bzip2, xz
--------------------------------	--------------------------------------	-----------------------

The compression method affects file size as well as system performance while compressing. The default lzop method is relatively light on the CPU.

### IGEL Setup > Registry

<b>&gt; Interface for tcpdump logging</b>	debug.tools.tcpdump[0-3].interface	user editable string / <u>eth0</u>
---	------------------------------------	------------------------------------

Note: Names eth0, eth1, wlan0, etc. are treated as symbolic names and will internally be replaced by the correct PNINs automatically. For details on PNINs, see [LAN Interfaces](#)(see page 1172).

### IGEL Setup > Registry

<b>&gt; Number of Rotate Files</b>	debug.tools.tcpdump[0-3].num_rotate_files	3 ... 10
------------------------------------	---	----------

Number of files to be kept while rotating.

### IGEL Setup > Registry

<b>&gt; Only Log Package Headers</b>	debug.tools.tcpdump[0-3].only_headers	enabled / <u>disabled</u>
--------------------------------------	---------------------------------------	---------------------------

### IGEL Setup > Registry

<sup>162</sup> <http://www.tcpdump.org>



<b>&gt; Enable promisc tcpdump logging</b>	debug.tools.tcpdump[0-3].promisc	enabled / <u>disabled</u>
Enable promiscuous mode on the network interface to also capture packets not intended for this host.		

### IGEL Setup > Registry

<b>&gt; Logfile rotate size in MiB</b>	debug.tools.tcpdump[0-3].rotate_size	10, 15, 20, 25, 30, 40
Rotate when the size of the uncompressed file reaches this size in MiB.		

### IGEL Setup > Registry

<b>&gt; Logfile rotate time in s</b>	debug.tools.tcpdump[0-3].rotate_time	0 / user editable integer
Time in seconds after which the logfile is rotated and compressed. If set to 0 no time-based rotation happens.		

### IGEL Setup > Registry

<b>&gt; Additional Parameters for tcpdump</b>	debug.tools.tcpdump[0-3].tcpdump_additional_parameters	user editable string
Use with care.		

### IGEL Setup > Registry

<b>&gt; Enable tcpdump</b>	debug.tools.tcpdump[0-3].tcpdump_enabled	enabled / <u>disabled</u>

### IGEL Setup > Registry

<b>&gt; tcpdump filter expression</b>	debug.tools.tcpdump[0-3].tcpdump_filter	user editable string
Tcpdump filter expression. For the expression syntax, see the <a href="#">pcap-filter(7)</a> <sup>163</sup> manpage.		

## Netlog

The netlog facility combines the following network diagnosis tools:

- ethtool
- ifconfig

<sup>163</sup> <http://www.tcpdump.org/manpages/pcap-filter.7.html>



- netstat
- ping
- ss (socket status)

It can also trigger tcpdump.

### IGEL Setup > Registry

<b>&gt; Enable netlog logging</b>	debug.tools.netlog.enabled	enabled / <u>disabled</u>
-----------------------------------	----------------------------	---------------------------

### IGEL Setup > Registry

<b>&gt; period between netlog logs in</b> debug.tools.netlog.period	<u>s</u>	1, 5, 10, 20, 30, 60, 120
---	----------	---------------------------

Ping logging is not affected by this and uses its own timing.

- Ehtool(see page 408)
- Ifconfig(see page 409)
- Netstat(see page 410)
- Ping(see page 411)
- Socket Status (ss)(see page 412)

### Ehtool

Ehtool is the standard Linux utility for getting diagnostic information about wired Ethernet devices and their drivers.

### IGEL Setup > Registry

<b>&gt; Disable ehtool logging</b>	debug.tools.netlog.ethtool.disabled	true / <u>false</u>
------------------------------------	-------------------------------------	---------------------

By default Ehtool logging is included in Netlog logging. However, you can disable it here.

### IGEL Setup > Registry

<b>&gt; Log only if ehtool output changes</b>	debug.tools.netlog.ethtool.log_on_changes	<u>true/false</u> <u>_only</u>
---	---	-----------------------------------

Log only if ehtool output changes (on bootup there will always be at least one log entry)

### IGEL Setup > Registry

<b>&gt; Number of Rotate Files</b>	debug.tools.netlog.ethtool.num_rotate_files	<u>2 ... 4</u>
------------------------------------	---	----------------



Keep up to this number of rotated files (also compressed), the current log not included (which is limited to 600 lines)		
<b>IGEL Setup &gt; Registry</b>		
<b>&gt; Logfile rotate size in MiB</b>	debug.tools.netlog.ethtool.rotate_size	2, 4, 6
Rotate when the size of the uncompressed file reaches this size in MiB.		

Ifconfig

Ifconfig

Apart from configuring network devices, ifconfig also gives diagnostic information such as RX bytes, TX bytes and dropped packets.

<b>IGEL Setup &gt;</b>		
<b>&gt; Disable ifconfig logging</b>	debug.tools.netlog.ifconfig.disabled	true / false
By default Ifconfig logging is included in Netlog logging. However, you can disable it here.		

<b>IGEL Setup &gt;</b>		
<b>&gt; Log only if ifconfig output changes</b>	debug.tools.netlog.ifconfig.log_on_changes	no,error_counter,_only,all
<ul style="list-style-type: none"> <li>• <b>no:</b> log on every netlog run</li> <li>• <b>error_counter:</b> log only if an error counter or the address changes</li> <li>• <b>all:</b> log on every change of ifconfig output</li> </ul>		
<b>IGEL Setup &gt;</b>		
<b>&gt; Number of Rotate files</b>	debug.tools.netlog.ifconfig.num_rotate_files	2 ... 4
Keep up to this number of rotated files (also compressed), the current log not included (which is limited to 600 lines).		
<b>IGEL Setup &gt;</b>		
<b>&gt; Logfile rotate size in MiB</b>	debug.tools.netlog.ifconfig.rotate_size	2, 4, 6



	Rotate when the size of the uncompressed file reaches this size in MiB.
<b>IGEL Setup &gt;</b>	
<b>&gt; Trigger tcpdump log</b>	debug.tools.netlog.ifconfig.trigger_tcpdump true / <u>false</u> <u>_save</u>
Trigger the saving of tcpdump logs if an error counter increases or if the IP address changes.	

## Netstat

Netstat displays a variety of network statistics for the local machine.

<b>&gt; Disable netstat logging</b>	debug.tools.netlog.netstat.disabled true / <u>false</u>
By default netstat -s logging is included in Netlog logging. However, you can disable it here.	
<b>&gt; Number of Rotate files</b>	debug.tools.netlog.netstat.num_rotate_file 2 ... 4 s
Keep up to this number of rotated files (also compressed), the current log not included (which is limited to 600 lines).	
<b>&gt;LogFile rotate size in MiB</b>	debug.tools.netlog.netstat.rotate_size 2, 4, 6
Rotate when the size of the uncompressed file reaches this size in MiB.	
<b>&gt;Log only if triggered</b>	debug.tools.netlog.netstat.trigger_log <u>net_error_changes</u> , <u>net_changes</u> , <u>ifconfig_changes</u> , <u>ethtool_changes</u> , <u>no_trigger</u>



- **net\_error\_changes**: log if ethtool output changes or ifconfig error counter or address changes
- **net\_changes**: log if ethtool or ifconfig output changes
- **ifconfig\_changes**: log if ifconfig output changes
- **ethtool\_changes**: log if ethtool output changes
- **no\_trigger**: log on every netlog run

## Ping

<b>IGEL Setup &gt;</b>		
<b>&gt; Enable ping check</b>	debug.tools.netlog.ping_host[0-9].enabled	true / <u>false</u>

<b>IGEL Setup &gt;</b>		
<b>&gt; Log only if ping fails</b>	debug.tools.netlog.ping_host[0-9].log_only_on_error	true / <u>false</u>
Log only if any one of the configures pings [0-9 fails.]		
<b>IGEL Setup &gt;</b>		
<b>&gt; Number of Rotate Files</b>	debug.tools.netlog.ping_host[0-9].num_rotate_files	2 ... 4
Keep up to this number of rotated files (also compressed), the current log not included (which is limited to 600 lines).		
<b>IGEL Setup &gt;</b>		
<b>&gt; Logfile rotate size in MiB</b>	debug.tools.netlog.ping_host0.rotate_size	2 ... 4
Rotate when the size of the uncompressed file reaches this size in MiB.		
<b>IGEL Setup &gt;</b>		
<b>&gt; Trigger tcpdump save</b>	debug.tools.netlog.ping_host0.trigger_tcpdump_save	2 ... 4
Trigger the saving of tcpdump logs if an error counter increases or if the IP address changes.		



<b>IGEL Setup &gt;</b>		
<b>&gt; Ping target</b>	debug.tools.netlog.ping_host0.ping_target	user-editable string
Target IP/hostname to ping (if none is given ping will be considered as disabled!)		
<b>IGEL Setup &gt;</b>		
<b>&gt; Time between pings</b>	debug.tools.netlog.ping_host0.ping_time	1, 5, 10, 30, 60, 120
Time between pings in seconds.		
<b>IGEL Setup &gt;</b>		
<b>&gt; Type of ping</b>	debug.tools.netlog.ping_host0.type	icmp, http request, https request
<ul style="list-style-type: none"> <li><b>icmp</b>: use normal ping command</li> <li><b>http request</b>: send an http request (fails if no HTTP/*.* * OK answer is received)</li> <li><b>https request</b>: send an https request (fails if no CONNECTED is returned by openssl)</li> </ul>		

Socket Status (ss)

Socket Status (ss)

<b>IGEL Setup &gt;</b>		
<b>&gt; Disable socket status Logging</b>	debug.tools.netlog.socket_status.disabled	true / false
By default socket_status logging is included in Netlog logging. However, you can disable it here.		
<b>IGEL Setup &gt;</b>		
<b>&gt; Number of Rotate Files</b>	debug.tools.netlog.socket_status.num_rotate_files	true / false
Keep up to this number of rotated files (also compressed), the current log not included (which is limited to 600 lines).		



<b>IGEL Setup &gt;</b>		
<b>&gt; Logfile rotate size in MiB</b>	debug.tools.netlog.socket_status.rotate_size	true / <u>false</u>
Rotate when the size of the uncompressed file reaches this size in MiB.		
<b>IGEL Setup &gt;</b>		
<b>&gt; Log only if triggered</b>	debug.tools.netlog.socket_status.trigger_log	<u>ping_errors</u> , no_trigger
<ul style="list-style-type: none"> <li>• <b>ping_errors</b>: log only if ping test fails</li> <li>• <b>no_trigger</b>: log on every netlog run</li> </ul>		

## 2.17.11 Making a Telnet Connection from IGEL Linux

### Issue

You want to connect to a Telnet service and can't find a Telnet command on the device.

### Solution

Using Ericom Powerterm (Requires the Ericom Powerterm Firmware Feature):

1. In Setup, go to **Sessions > PowerTerm Terminal Emulation > PowerTerm Sessions**.
2. Create a new session.
3. Edit the session.
4. Under **Connection**, make the following settings:
  - a. Select **TELNET** as **Session Type**.
  - b. Enter an IP address or a name in **Host Name**.
  - c. If you want to use a graphical login dialog, activate **Enable Login Dialog**.



Session Type **TELNET**

<b>Parameters</b>			
Host Name	<input type="text" value="172.30.91.158"/>	Port Number	<input type="text" value="23"/>
Terminal Name	<input type="text"/>	Keep Alive Timeout	<input type="text" value="0"/>
<input checked="" type="checkbox"/> Enable Login Dialog	<input type="checkbox"/> Save last user name		
Script File	<input type="text"/>		
<input checked="" type="checkbox"/> Set Window Size			
<input type="checkbox"/> Force Binary Mode			

5. Under **Desktop Integration** enter a **Session Name** and enable the desired **Starting Methods for the Session**.
6. Click **Apply** to save your settings or **OK** to save and exit.
7. Start the new session and enter your username and password.

### 2.17.12 Configuring Dynamic DNS Updates via DDNS

Issue:

You want to register a device's IP address with your DNS server.

You are not using DHCP.

Solution:

Use the DDNS tools contained in */GEL Linux*, which can be configured by Setup.

This only works for BIND9 or other nameservers supporting TSIG, not for Microsoft Active Directory servers.

Distribute your nameserver's shared TSIG key with the UMS:

1. Create a **New File**.
2. Set the **Device Storage Path** to `/wfs/ddns`.
3. Enable **Read** permission for the **Owner** and disable all other permissions.
4. Set the **Owner** to **Root**.

Set up Dynamic DNS Registration:



1. Go to **Network > LAN Interfaces** in *Setup*.
2. Enable **Specify an IP Address**.
3. Enter an **IP Address** and **Network Mask**.
4. Enter a **Terminal Name**.
5. Check **Enable DNS**.
6. Enter a **Default Domain**.
7. Enter at least one **Nameserver** IP address.
8. Enable **Dynamic DNS Registration**.
9. Select **DNS as Dynamic DNS Registration Method**.
10. If the nameserver expects a TSIG key: Select the **TSIG key file**. Otherwise, leave the input field blank.
11. Click **Apply** or **OK** to confirm your settings.

The screenshot shows the 'Activate default interface (Ethernet)' configuration page. It includes fields for IP Address (192.0.0.1), Network Mask (255.255.255.0), Default Gateway, Terminal Name, and several DNS-related settings. The 'Enable DNS' checkbox is checked, and the 'Dynamic DNS Registration' checkbox is also checked. The 'Dynamic DNS Registration Method' dropdown is set to 'DNS'. The 'TSIG key file for additional DNS authentication' field contains the value '/wfs/ddns/ddns.private'. At the bottom, there are 'Apply', 'Ok', and 'Cancel' buttons.

Activate default interface (Ethernet)

Get IP from DHCP Server  
Specify an IP Address

IP Address: 192.0.0.1

Network Mask: 255.255.255.0

Default Gateway: enable

Terminal Name:

Enable DNS

Default Domain: dynamic.igel.local

Nameserver: 172.30.178.1

Nameserver:

Manually overwrite DHCP settings

Dynamic DNS Registration

Dynamic DNS Registration Method: DNS

TSIG key file for additional DNS authentication: /wfs/ddns/ddns.private

Apply Ok Cancel



### 2.17.13 Changing the SMB protocol version

Depending on which Windows (Samba) server you are using, you will need a specific SMB protocol version.

Due to security reasons, Microsoft recommends to disable SMB version 1.0 support on Windows ,so you need to switch to at least version 2.0 to be further able to access systems with disabled SMBV1.

IGEL Linux version 10.04.100 and higher offer several SMB protocol versions.

To change the version setting:

1. In the IGEL Setup go to **System > Registry**.
2. Go to parameter `network.smbmount.smb_version`.
3. Select the appropriate **SMB protocol version**.

Possible options:

- 1.0
- 2.0
- 2.1
- 3.0

4. Click **Save** or **Apply and send to thin client**.

The windows shares are configurable at **IGEL Setup > Network > Network Drives > Windows Drive**.

### 2.17.14 How to Launch the Wireless Manager within IGEL OS when the Taskbar Is Hidden

#### Problem

The taskbar or system tray has been disabled for some reason (**User Interface > Desktop > Taskbar / Taskbar Items**; also **User Interface > Screenlock /Screensaver > Taskbar**). As a result, a systray icon for the [Wireless Manager](#)(see page 1180) can't be accessed anymore, and the user can't manage wireless networks.

Notice that also the Wi-Fi switch will be inaccessible if you disable the taskbar or system tray, see [Switch for the Wi-Fi Connection](#)(see page 1182). See also "Enable Wi-Fi automatic switch" under [Wireless](#)(see page 1178).

#### Environment

- IGEL OS 10.06 or higher

#### Solution

You can configure the Wireless Manager as a custom application and define the way it can be launched.



1. Go to **Network > LAN Interfaces > Wireless** and check that the wireless interface and the Wireless Manager are enabled.
2. Go to **System > Firmware Customization > Custom Application** and click **[+]**.
3. Specify the **Session name** and configure the **Starting methods** according to your needs.

**Session name:** WLAN Manager

**Starting Methods for Session:**

- Start Menu
- Application Launcher
- Desktop
- Quick Start Panel

Menu folder: [empty]

Application Launcher folder: [empty]

Desktop folder: [empty]

Password protection: None

Hotkey: None

Modifiers: None

Key: None

Autostart: None

Restart: None

Autostart delay: 0

Autostart notification: None

Autostart requires network: checked

Appliance Mode Access: None

4. Under **Settings**, specify the **Icon name** and enter the following **Command**: `/bin/start-wireless-manager`

**Icon name:** applications-other

**Command:** /bin/start-wireless-manager

Buttons: Apply, Ok, Cancel



5. Click **Apply** or **OK**.

The Wireless Manager can now be launched via the configured starting methods.

## 2.18 Security

- [Securing IGEL OS Endpoints](#)(see page 418)
- [Secure Shell \(SSH\) Access to IGEL OS with Keys](#)(see page 439)
- [Secure Terminal \(Telnet with TLS/SSL\)](#)(see page 443)
- [Secure Shadowing \(VNC with TLS/SSL\)](#)(see page 443)
- [Cherry eGK Channel Substitution](#)(see page 446)
- [Single Sign-on for the Browser Proxy](#)(see page 448)
- [Limiting the Number of Permitted Login Attempts](#)(see page 452)
- [How to Deploy Device Encryption](#)(see page 452)
- [Security: Timeout for Secure Shadowing and Secure Terminal](#)(see page 456)

### 2.18.1 Securing IGEL OS Endpoints

This document describes settings for IGEL OS that will increase security.

It applies to the following types of devices:

- IGEL UD devices
  - Devices which are temporarily converted by UD Pocket
  - Devices which are permanently converted by IGEL OS Creator (OSC)
- 
- [Introduction](#)(see page 418)
  - [Setting Passwords](#)(see page 419)
  - [Keeping the System Up-To-Date](#)(see page 422)
  - [Disabling Access to Components](#)(see page 426)
  - [Minimizing the Attack Surface](#)(see page 429)
  - [Configuring Remote Access and Management](#)(see page 434)
  - [Wi-Fi and Bluetooth](#)(see page 438)
  - [Using UD Pocket for BYOD Devices](#)(see page 439)

#### Introduction

This document describes various settings to make IGEL OS more secure. In general, the more of these settings you apply, the better device security will be. However, it is up to you to strike a balance between security and enabling your users to do their work. Some settings may even be inappropriate for your use case, e.g. if you use Bluetooth peripherals, it does not make sense to disable Bluetooth.

In order to configure multiple devices, put the relevant settings into a Universal Management Suite (UMS) master profile, which you can assign to any number of devices. For more information, see [Master Profiles](#)<sup>164</sup>.

---

<sup>164</sup> <https://kb.igel.com/display/endpointmgmt601/Master+Profiles>



## Setting Passwords

You can restrict access to various system components by setting passwords.

- [Setting Local Passwords](#)(see page 419)
- [Password-Protecting Sessions and Accessories](#)(see page 419)
- [Using Screenlock](#)(see page 420)
- [Do Not Save Session Passwords](#)(see page 421)
- [Setting a UEFI Password](#)(see page 421)
- [Using Two-Factor Authentication \(2FA\)](#)(see page 422)

### Setting Local Passwords

#### Rationale

Passwords protect the system against local changes. They restrict access to the Local Terminal, Setup, and to the rescue shells on the virtual consoles. The administrator password is also needed to reset the system to factory defaults.

These passwords are saved in a way (salted and hashed) that prevents them from being recovered from the local storage.

By default, no passwords are set on IGEL OS. Set at least an administrator password:

#### Instructions

1. In IGEL Setup go to **Security > Password**.
2. In the **Administrator** area, check **Use Password**.
3. Enter a password twice when prompted.
4. Optional: If you want to grant unprivileged user access to IGEL Setup check **Use Password** in the **Setup user** area and enter a password twice when prompted.
5. Click **Apply**.

For configuration of the **User Account for Remote Access**, see [Using Secure SSH Settings](#)(see page 437).

Find further information on the [Passwords](#)(see page 1236) page in the IGEL OS manual.

### Password-Protecting Sessions and Accessories

#### Rationale

Sessions can be used to access corporate resources, while the accessories in IGEL OS can be used to make changes to the local system. If you do not want to disable certain sessions or accessories completely, you can set passwords to restrict access to them.

#### Instructions

By default, sessions do not have passwords set. In IGEL Setup, you can set a password on the **Desktop Integration** page of a session or accessory.



To enable password protection:

1. In the Setup, go to the relevant **Desktop Integration** page. The path has the following pattern: **Sessions > [session type] > [session name] > Desktop Integration**.  
For accessories, go to **Accessories > [accessory name]**.
2. Set **Password Protection** to
  - **Administrator** to require the Administrator password, or
  - **User** to require the User password, or
  - **Setup User** to require the Setup User password.
3. Click **Apply**.

## Using Screenlock

### Rationale

Leaving a screen unlocked enables attackers to access the system with the logged-in user's privileges. Manual or automatic locking the screen with a password prevents such access.

### Instructions for Enabling Manual Locking

By default, there is no way for the user to manually lock the screen. To enable manual locking, follow these steps:

1. In the Setup, go to **User Interface > Screenlock / Screensaver**.
2. Do one or both of the following:
  - Activate the **Quick start panel** starting method to give the user a button for locking the screen manually.
  - Activate **Use hotkey** and set a combination of keys that lets the user lock the screen manually, e.g. [Ctrl+Shift+L].
3. Click **Apply**.

### Instructions for Automatic Locking

By default, the screensaver is started automatically after 5 minutes, but the screen is not locked with a password. To enable locking, follow these instructions:

1. Go to **User Interface > User Interface > Screenlock / Screensaver > Options**.
2. Activate **Start automatically**.
3. Set the **Timeout**, i.e. the number of minutes of user inactivity before the screensaver starts automatically.
4. As a password, select **User password** (see [Setting Local Passwords\(see page 419\)](#)) or a separate **Screenlock password** (and set one).
5. If applicable, activate **Allow administrator password** to allow the administrator to unlock the screen.
6. Click **Apply**.



## Do Not Save Session Passwords

### Rationale

Passwords for sessions should not be stored on the endpoint device.

### Instructions

- ▶ When configuring a session, on the login page, leave the **Password** field empty. The user will then be prompted interactively for the password.
- ▶ Wherever possible use [Two-Factor Authentication \(2FA\)](#)(see page 422).

## Setting a UEFI Password

### Rationale

In the UEFI settings you can modify very fundamental system properties, e.g. disable booting from USB. Access to these settings should be protected by a password.

### Instructions for IGEL Devices

- ▶ If UEFI is not enabled, see the instructions under [UEFI Secure Boot Enabling Guides](#)<sup>165</sup>.

By default no UEFI password is set on IGEL UD devices. To set a password, do the following:

1. Hold down the [Del] key ([F2] key for UD2) while booting.  
The UEFI menu opens.
2. Using the arrow and return keys, go to **SCU**.  
The **Setup Utility** opens.
3. Using the arrow and return keys, go to **Security**.
4. Use the arrow keys to select **Set Supervisor Password**.
5. Hit [Return].
6. Enter the desired UEFI password and hit [Return]
7. Enter the same UEFI password again and hit [Return] twice.
8. Hit [F10] in order to save and exit.
9. Confirm **Exit Saving Changes?** by hitting [Return].  
The system boots, and the UEFI settings are now password-protected.

### Instructions for 3rd-Party Devices Converted with OS Creator (OSC)

- ▶ Refer to the instructions of your BIOS/UEFI vendor.

Alternatively, try pressing [F12] (in general), [F10] (Intel devices), or [F9] (Hewlett-Packard devices) to access the BIOS/UEFI settings. If this does not work, try pressing [Del], [F1], or [F2] during booting.

<sup>165</sup> <https://kb.igel.com/display/securitysafety/UEFI+Secure+Boot+Enabling+Guides>



## Using Two-Factor Authentication (2FA)

### Rationale

Two-factor authentication (2FA) combines two different factors to prove the user's identity, often a hardware device such as smartcard or smart token and a password or PIN. This improves protection against impostors, as they would have to gain both possession of the hardware device and knowledge of the password or PIN.

### Instructions

Use two-factor authentication with a smartcard or smart token where possible. IGEL OS supports this for the following sessions:

- [Smartcard authentication for sessions<sup>166</sup>](#)
  - [Citrix Storefront](#)(see page 494)
  - [RDP Sessions](#)(see page 495)
  - [Horizon Sessions](#)(see page 496)
  - [Web browser](#)(see page 497)
- [\(Kerberos\) Passthrough Authentication](#)(see page 734)

## Keeping the System Up-To-Date

### Rationale

Software updates fix newly discovered vulnerabilities in IGEL OS and applications. This means that keeping up with updates is one of the most important measures in securing IGEL OS systems.

To start and configure updates, you can use IGEL Setup and/or the [Universal Firmware Update<sup>167</sup>](#) feature of the Universal Management Suite (UMS).

The instructions described on this page use the Universal Firmware Update feature of the UMS. For defining a scheduled job, see the section "As a Job" in [Assigning Updates<sup>168</sup>](#); for configuring the update on a device, see [Firmware Update](#)(see page 1252).

### Instructions

- To be notified of security-critical IGEL OS updates and to receive the IGEL Technical Newsletter, subscribe to IGEL communications on [www.igel.com<sup>169</sup>](http://www.igel.com).

The upgrade procedure consists of the following steps:

- Getting the update from the IGEL download server
- Testing the update on one or a few devices
- Rolling out the update on all devices

---

<sup>166</sup> <https://kb.igel.com/display/igelos1101/Authentication+with+IGEL+Smartcard>

<sup>167</sup> <https://kb.igel.com/display/endpointmgmt601/Universal+Firmware+Update>

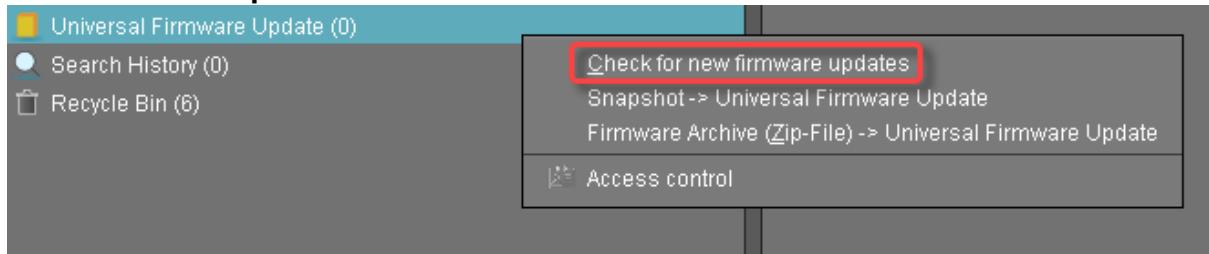
<sup>168</sup> <https://kb.igel.com/display/endpointmgmt601/Assigning+updates>

<sup>169</sup> <http://www.igel.com/>

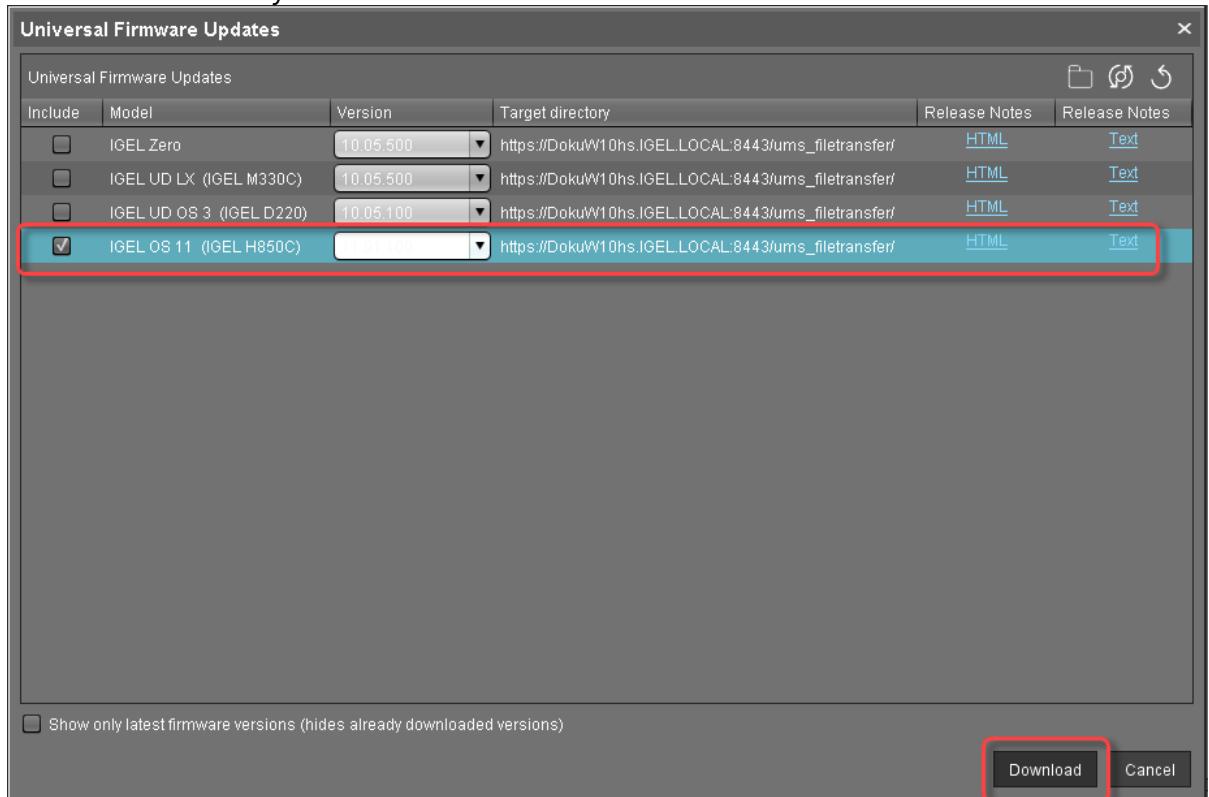


## Getting the Update from the IGEL Download Server

1. In the UMS Console, go to **Universal Firmware Update**, open the context menu, and select **Check for new firmware updates**.



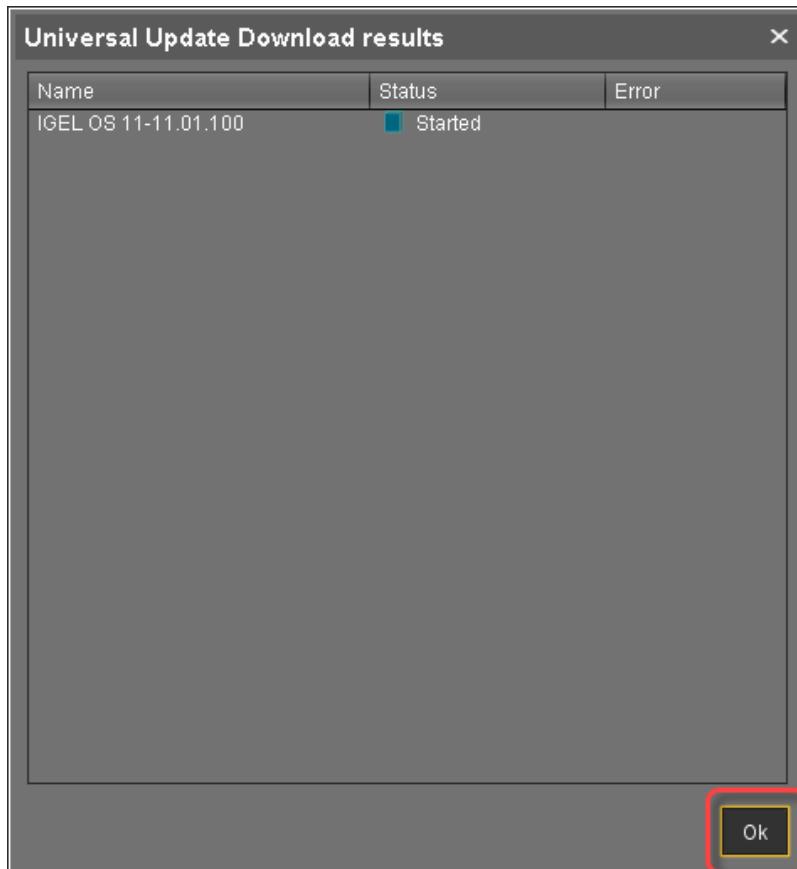
2. Activate the firmware you want to download and click **Download**.



The current status of the firmware download is shown.



3. Click **Ok**.



4. When the download has succeeded, the firmware is registered and stored in the UMS.

 A screenshot of the UMS (Universal Management System) interface. On the left is a sidebar with various navigation items:
 

- Profiles (0)
- Master Profiles (0)
- Template Keys and Groups (0)
- Firmware Customizations (0)
- Devices (2)
  - Remote Devices (0)
  - UDC3 (0)
  - VWOL (2)
    - ITC000BCA055018
    - ITC00E0C51143A5
- Mobile Devices (0)
- Shared Workplace Users
- Views (4)
  - EMP Expiry
  - Licenses required
  - Licensing
  - Maintenance Expiry
- Jobs (0)
- Files (0)
- Universal Firmware Update (1)
  - IGEL OS 11-11.01.100** (highlighted in blue)
- Search History (0)
- Recycle Bin (0)

 To the right of the sidebar is the main content area. It shows the following details for the selected firmware update:
 

Version: 11.01.100  
Release Notes: [HTML](#) [Text](#)

**Firmware Update Settings**

- User: IGEL\_INTERNAL\_FIRMWAREUPDATE\_USER
- Password: \*\*\*\*\*
- Host: DokuW10hs.IGEL.LOCAL
- Port: 8443
- Protocol: https
- Target URL: /ums\_filetransfer/IGEL\_OS\_11-11.01.100
- Snapshot file: [empty]

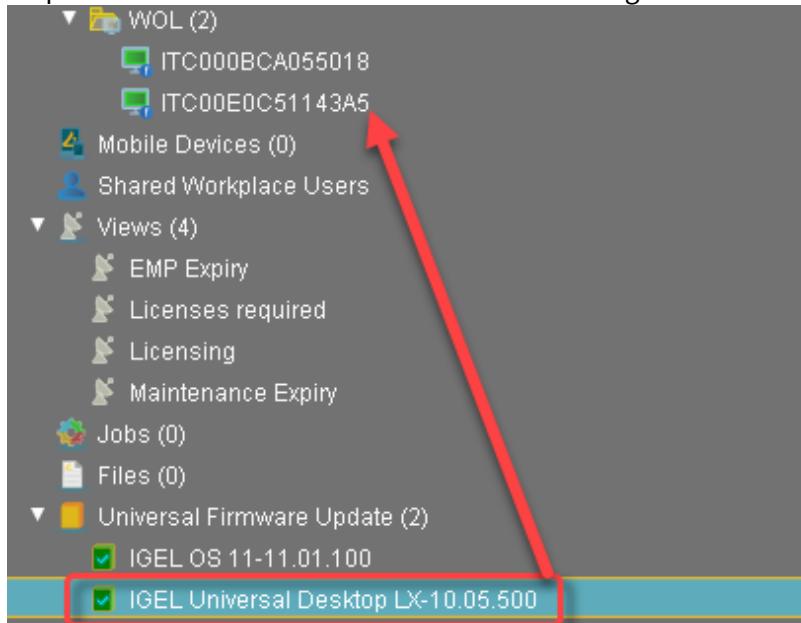
**Download Status**

- Status: OK Finished
- Error: [empty]

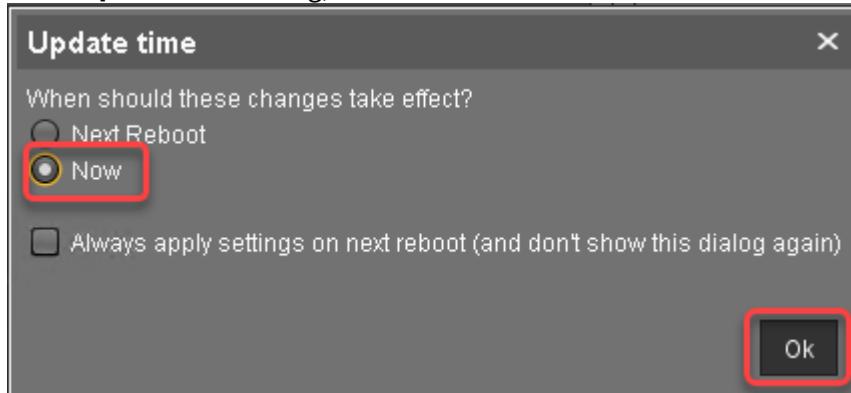


## Testing the Update on One or a Few Devices

1. In the UMS Console, go to **Universal Firmware Update**, select the desired firmware and drag and drop it on the test device or on the folder containing the test devices.



2. In the **Update time** dialog, select **Now** and click **Ok**.



The firmware is updated on the devices; during the update process, the devices reboot.

## Rolling out the Update on All Devices

You can either start the update immediately or use a scheduled job to start it at a defined time.

To start the update immediately:

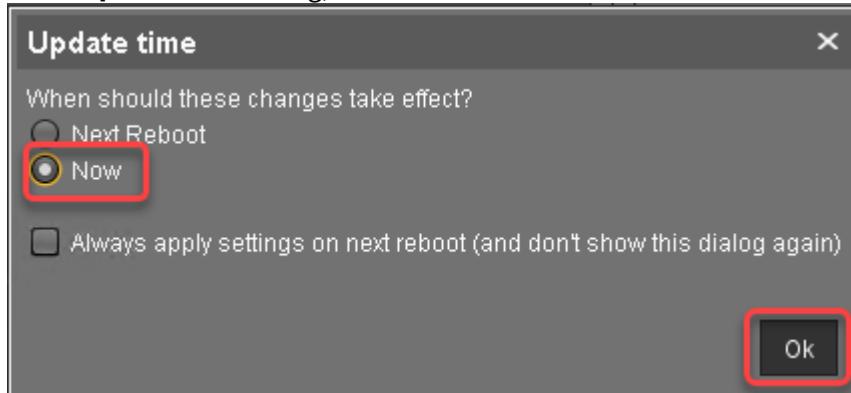


1. In the UMS Console, go to **Universal Firmware Update**, select the desired firmware and drag and drop it on the folder containing the devices that are to be updated.

The screenshot shows the UMS Console interface. On the left is a tree view of management objects:

- Devices (2)
  - Remote Devices (0)
  - UDC3 (0)
  - Update these devices (2)** (highlighted with a red arrow)
  - ITC000BCA055018
  - ITC00E0C51143A5
  - WOL (0)
- Mobile Devices (0)
- Shared Workplace Users
- Views (4)
  - EMP Expiry
  - Licenses required
  - Licensing
  - Maintenance Expiry
- Jobs (0)
- Files (0)
- Universal Firmware Update (3)
  - IGEL OS 11-11.01.100
  - IGEL Universal Desktop LX-10.05.500** (highlighted with a red box)
  - IGEL Universal Desktop OS 3-10.05.100

2. In the **Update time** dialog, select **Now** and click **Ok**.



The firmware is updated on the devices; during the update process, the devices reboot.

## Disabling Access to Components

You can hide IGEL OS components from the user that could be used to make changes to the system.

- [Disabling Local Terminal Access](#)(see page 427)
- [Disabling Virtual Console Access](#)(see page 427)
- [Using Appliance Mode](#)(see page 428)



- [Hiding Unused Accessories\(see page 428\)](#)

## Disabling Local Terminal Access

### Rationale

The **Local Terminal** accessory allows the user to execute commands or make changes to the system. By default, the local terminal is disabled, that is, no local terminal session is configured. To enhance security, you should do one of the following:

- Leave the local terminal disabled
- If a local terminal session is configured, but not needed, disable it.
- If a local terminal session is needed, password-protect it.

### Instructions

To remove an existing local terminal session:

1. In IGEL Setup, go to **Accessories > Terminals**.
2. Select a local terminal session you want to delete.
3. Click  to remove the selected session.
4. When prompted, confirm that you want to delete the session.
5. Click **Apply**.

Alternatively, you can password-protect the terminals.

To password-protect the local terminal:

1. Find the local terminal session under **Accessories > Terminals**.
2. Follow the instructions under [Password-Protecting Sessions and Accessories\(see page 419\)](#).

## Disabling Virtual Console Access

### Rationale

The virtual consoles `tty11` and `tty12` give the user access to a shell. Disabling these makes it more difficult to execute commands or make changes to the system.

### Instructions

By default, the user can access the virtual consoles with the `[Ctrl]+[Alt]+[F11]` and `[Ctrl]+[Alt]+[F12]` keyboard commands. To disable access, do the following:

1. In IGEL Setup go to **User Interface > Display > Access Control**
2. Activate **Disable Console switching** (Default: Console switching enabled)
3. Click **Apply**.



## Using Appliance Mode

### Rationale

By default, IGEL OS users are not presented with a full-screen remote session, but have access to the desktop and to the start menu. On the contrary, in the appliance mode, a single predefined session is presented full-screen to the user. As access to other applications is prevented, this reduces the system's potential exposure to attack.

### Instructions

The appliance mode is available for the following session types:

- [VMware Horizon](#)(see page 870)
- [Browser](#)(see page 871)
- [Citrix Self-Service](#)(see page 871)
- [RHEV/Spice](#)(see page 872)
- [Imprivata](#)(see page 872)
- [RDP MultiPoint Server](#)(see page 874)
- [XDMCP for This Display](#)(see page 875)

To enable the appliance mode for a session, proceed as follows:

1. In IGEL Setup, go to **Sessions > Appliance Mode**.
2. Pick the session and configure it according to the manual chapter [Appliance Mode](#)(see page 869).

You can combine most of the appliance mode sessions with [Two-factor Authentication](#)(see page 422) for increased security.

## Hiding Unused Accessories

### Rationale

Accessories can be used to make changes to the system. Restricting access to these accessories helps to keep the system secure.

### Instructions

To hide individual accessories (both in the start menu and the Application Launcher):

1. In IGEL Setup go to **Accessories > [accessory name]**.
2. Disable all **Starting Methods for Session**.
3. Click **Apply**.

To password-protect an accessory:

- Follow the instructions under [Password-Protecting Sessions and Accessories](#)(see page 419).

To hide the complete **System** icon of the start menu:

1. In IGEL Setup go to **User Interface > Desktop > Start Menu**.



2. Deactivate **System tab**.
3. Click **Apply**.

To hide the complete Application Launcher's **System** icon:

1. In IGEL Setup go to **Accessories > Application Launcher > Application Launcher Configuration**.
2. Activate **Hide system page**.
3. Click **Apply**.

## Minimizing the Attack Surface

Removing unused features and disabling unneeded network services reduces the parts of the system that can be attacked.

- [Removing the Local Web Browser](#)(see page 429)
- [Configuring the Browser \(Kiosk Mode\)](#)(see page 430)
- [Disabling Java in the Browser](#)(see page 431)
- [Disabling the PC/SC Daemon](#)(see page 431)
- [Disabling X Server TCP Connections](#)(see page 431)
- [Removing Unused Features](#)(see page 432)
- [Disabling Storage Hotplug](#)(see page 432)
- [Using USB Device Control](#)(see page 433)
- [Disabling USB Boot](#)(see page 433)
- [Leveraging AppArmor](#)(see page 434)

### Removing the Local Web Browser

#### Rationale

The local web browser may expose vulnerabilities to the internet and can be an entry point for malware. If the browser is not needed, it is safer to remove it.

Do not remove the local web browser if you use Citrix StoreFront sessions.

#### Instructions

By default, IGEL OS has a local web browser (Firefox and Chromium) installed, even if no web browser session is configured. To remove the browser:

1. In the IGEL Setup, go to **System > Firmware Customization > Features**.
2. Uncheck the **Local Browser (Firefox)** and **Local browser (Chromium)** feature.
3. Click **Apply**.
4. Reboot the device.



## Configuring the Browser (Kiosk Mode)

### Rationale

If you want to offer a local web browser, there are some settings that improve its security. Additionally, these settings add up to a kiosk mode, hiding the rest of IGEL OS from the user.

### Instructions

By default, the web browser makes all of its features and menus available. To achieve a restricted 'kiosk' mode, follow these instructions.

#### Firefox

1. In the IGEL Setup under **Sessions > Firefox Browser > Firefox Browser Global > Security**, activate the following options:
  - **Safe Browsing**
  - **Malware Protection**
  - **Hide local filesystem**
2. Under **Sessions > Firefox Browser > Firefox Browser Global > Content**, activate **Block pop-up windows**, if required.
3. Under **Sessions > Firefox Browser > Firefox Browser Global > Privacy**, activate the following options:
  - **Clear private data when closing browser** and all options in the area **Select the items to be cleared**
  - **Allow private browsing feature**
  - **Always start in private browsing mode**
  - **Enable "Do Not Track" feature** and **Enable built-in tracking protection**, if necessary
4. Under **Sessions > Firefox Browser > Firefox Browser Global > Restart**, activate **Restart**.
5. Under **Sessions > Firefox Browser > Firefox Browser Global > Window**, activate the following options:
  - **Start in full-screen mode**
  - **Hide configuration page of the browser**
6. Under **Sessions > Firefox Browser > Firefox Browser Global > Menus & Toolbars**, activate **Hide App Menu/Menu Bar**.
7. Under **Sessions > Firefox Browser > Firefox Browser Global > Context**, activate **Hide the browser's context menu**.
8. Under **Sessions > Firefox Browser > Firefox Browser Sessions > [session name] > Settings**, activate **Autostart**.
9. Click **Apply**.
10. Reboot the device.

For additional information, see also [Use the Firefox Browser in Kiosk Mode](#)(see page 358).

#### Chromium

1. In the IGEL Setup under **Sessions > Chromium Browser > Chromium Browser Global > Security**, activate **Safe browsing** and disable **File access**.
2. Under **Sessions > Chromium Browser > Chromium Browser Global**, activate **Automatic browser restart on exit**.



3. Under **Sessions > Chromium Browser > Chromium Browser Global > Content**, activate **Block pop-ups and redirects**, if required.
4. Under **Sessions > Chromium Browser > Chromium Browser Global > Privacy**, activate the following options:
  - **Clear browsing data** and all options in the area **Select the items to be cleared**
  - "Forced" for the setting **Allow incognito mode**
  - **Enable "Do Not Track" feature**, if necessary
5. Under **Sessions > Chromium Browser > Chromium Browser Global > Window**, activate **Enable kiosk mode**.
6. Under **Sessions > Chromium Browser > Chromium Sessions > [session name]**, activate **Autostart**.
7. Click **Apply**.
8. Reboot the device.

#### Disabling Java in the Browser

Java Applets and Java Web Start may constitute a potential security threat and are now regarded as deprecated. As of IGEL OS version 10.06.100, they are no longer included in IGEL OS. The registry keys under **System > Registry > java > deployment** are obsolete.

#### Disabling the PC/SC Daemon

##### Rationale

Unless you are running smartcard readers that use it, you can disable the PC/SC daemon. Running fewer daemons reduces the attack surface.

##### Instructions

To deactivate the PC/SC daemon:

1. In the IGEL Setup go to **Security > Smartcard > Services**.
2. Deactivate **Activate PC/SC Daemon**.
3. Click **Apply**.

#### Disabling X Server TCP Connections

##### Rationale

The X graphics server in IGEL OS has network functionality that could allow others to see your screen and read keyboard input. Leave it disabled to keep your data confidential.

##### Instructions

By default the network functionality of the X server is disabled. To disable it again at a later time, do the following:

1. In IGEL Setup go to **User Interface > Display > Access Control**
2. Make sure that **Access Control** is activated.
3. Make sure that **Disable TCP connections** is activated.



#### 4. Click **Apply**.

Removing Unused Features

##### Rationale

Reducing the amount of software running on a system reduces its attack surface. Therefore a basic security measure for IGEL OS 11 is to remove all unused features.

##### Instructions

To disable a feature:

1. In the IGEL Setup go to **System > Firmware Customization > Features**.
2. Deactivate all the features that you do not intend to use.
3. If you do not use local printers on the endpoint device that you want to share with others, activate:
  - **Printing (Internet Printing Protocol CUPS)**
  - **Printing (Line Printer LPD)**
  - **Printing (TCP/IP)**
  - **Printing (ThinPrint)**

Do not remove the **Custom Partition** feature if you have a custom partition that contains software or data for which you have no backup copy. After disabling the feature and a reboot the contents of the custom partition will be lost.

Do not remove **Fluendo Gstreamer Codec Plugins** or **Hardware Video Acceleration** if you use sessions that make use of these features.

#### 4. Click **Apply**.

5. Reboot the device.

Disabling Storage Hotplug

##### Rationale

Removable USB media can be used to steal data or to execute unauthorized software or even malware on the device.

##### Instructions

Storage hotplug is disabled by default. Should you want to disable it again at any later point, follow these instructions:

1. In IGEL Setup go to **Devices > Storage Devices > Storage Hotplug**.
2. Deactivate **Storage Hotplug**.
3. Click **Apply**.

Storage devices are no longer automatically mounted when they are plugged in.



## Using USB Device Control

### Rationale

USB devices such as pen drives, wireless controllers, or printers can be used to steal data or to execute unauthorized software or even malware. Deactivating as many USB device classes as possible increases security.

### Instructions

To enable and configure USB access control:

1. In IGEL Setup, go to **Devices > USB Access Control**.
2. Check **Enable**.

The activation of **USB Access Control** and setting the **Default rule to Deny** will block the use of USB devices locally and in the session and, thus, might disable devices needed for the users. Therefore, activate the USB access control only if your security policy requires that. In this case, set **Default rule to Deny** and configure **Allow** rules for the required USB devices and USB device classes.

It is recommended to make settings for **USB Access Control** as the last step in the device configuration. Before activating the USB access control, check that all your other settings for printers, Unified Communication, USB redirections, mapping settings for USB devices are working as expected.

Note that the USB access control is completely separate than USB redirection for remote sessions, see [When to Use USB Redirection](#)(see page 703).

Take also notice that the feature does not disable a USB port physically, i.e. power delivery will still work.

3. Set **Default rule to Deny**.

In combination with the preconfigured rule that allows Human Interface Devices (HID), no USB devices apart from e.g. mouse and keyboard are allowed.

4. Configure further rules as needed. For instructions, see [How to Configure USB Access Control](#)(see page 706).
5. Click **Apply**.
6. Reboot the device.

## Disabling USB Boot

### Rationale

Disabling USB boot prevents booting another operating system, which could be used to manipulate or (even accidentally) overwrite IGEL OS on mass storage.

### Instructions for IGEL Devices

USB boot is disabled in the factory settings on IGEL UD LX devices. If it has been enabled and you want to disable it again, follow the instructions given here:



1. Hold down the [Del] key ([F2] key for UD2) while the system is booting.  
The UEFI menu opens.
2. Use the arrow and return keys to go to **SCU**.
3. Enter the UEFI password if one is set.  
The **Setup Utility** opens.
4. Go to **Boot**.
5. Set **USB Boot** to **Disabled**.
6. Press [F10].
7. Confirm **Exit Saving Changes?**  
The device boots.

Additionally, set a [UEFI Password](#)(see page 421) so the boot settings cannot be changed back.

#### Instructions for 3rd-Party Devices Converted with OSC

- ▶ Refer to the instructions of your BIOS/UEFI vendor.

Alternatively, try pressing [F12] (in general), [F10] (Intel devices), or [F9] (Hewlett-Packard devices) to access the BIOS/UEFI settings. If this does not work, try pressing [Del], [F1], or [F2] during booting.

#### Leveraging AppArmor

AppArmor controls which privileges should be granted to an application that is running on the system. This way even vulnerabilities that are yet unknown can be mitigated.

The following applications are guarded by AppArmor:

- Firefox browser
- Cups print server
- Evince pdf viewer

The following system programs are guarded by AppArmor:

- tcpdump
- haveged
- dhclient

By default, AppArmor is enabled. They registry key is `system.security.apparmor`

#### Configuring Remote Access and Management

Remote management via UMS and remote access are powerful features of IGEL OS. Select secure settings and disable what you do not use.

- [Tying Endpoints to Your UMS instance](#)(see page 435)
- [Disabling Shadowing](#)(see page 435)
- [Using Secure VNC Settings](#)(see page 436)
- [Disabling SSH Access](#)(see page 436)



- [Disabling X11 Forwarding](#)(see page 437)
- [Using Secure SSH Settings](#)(see page 437)
- [Disabling Secure Terminal](#)(see page 437)

## Tying Endpoints to Your UMS instance

### Rationale

Devices that have remote management enabled but are not yet tied to a UMS instance can be taken over by an attacker's UMS. Make sure to register all IGEL devices on your network.

### Instructions

By default, remote management is enabled on IGEL OS devices. Use automatic registration to catch all devices in your corporate network:

1. Assign the DNS entry `igelrmserver` to the UMS host. For further instructions, see [Registering Devices Automatically](#)<sup>170</sup>.
2. In the UMS console go to **UMS Administration > Global Configuration > Device Network Settings**.
3. Activate **Enable automatic registration (without mac address import)**  
Now all new IGEL devices, UD Pockets and devices converted with OSC that are booting up in the network will automatically register with your UMS instance.
4. Optionally, put newly registered devices into a quarantine directory automatically with UMS [Default Directory Rules](#)<sup>171</sup>.
5. Optionally, assign a [Master Profile](#)<sup>172</sup> to this directory, thereby enforcing secure settings, e.g. a local administrator password.

Alternatively you can disable remote management in the local IGEL Setup under **System > Remote management**. Of course this means losing one of the most powerful features of IGEL OS. However, this may be an option for particular devices.

## Disabling Shadowing

### Rationale

Shadowing is made possible by a VNC server on IGEL OS, which is a network service. Reducing the number of running network services reduces the system's attack surface.

### Instructions

By default, Shadowing is not active on IGEL OS. However, if you want to disable it at any time, follow these steps:

1. In the IGEL Setup go to **System > Remote Access > Shadow**

<sup>170</sup> <https://kb.igel.com/display/endpointmgmt601/Registering+devices+automatically>

<sup>171</sup> <https://kb.igel.com/display/endpointmgmt601/Default+Directory+Rules>

<sup>172</sup> <https://kb.igel.com/display/endpointmgmt601/Master+Profiles>



2. Deactivate **Allow Remote Shadowing**.
3. Click **Apply**.

## Using Secure VNC Settings

### Rationale

If you intend to use shadowing on IGEL OS, there are a number of options that can make it more secure.

### Instructions

By default, Shadowing does not use encrypted network transport or a password. To activate these security features, do the following:

1. In IGEL Setup go to **System > Remote Access > Shadow**.
2. Make as many of the following settings as possible for your use case. Each setting improves security, and often also privacy:
  - Enable **Secure Mode**.
  - Enable **Use Password** and set a strong password (not needed in **Secure Mode**). The maximum length for this password is 8 characters.
  - Enable **Prompt User to allow Remote Session**.
  - Enable **Allow User to disconnect Remote Shadowing**.
  - Disable **Allow Input from Remote**.
3. Click **Apply**.

Secure mode for shadowing can be enabled globally in **UMS under UMS Administration > Global Configuration > Remote Access**. There you can also enable the logging of users who have used secure mode shadowing .

## Disabling SSH Access

### Rationale

The SSH server on IGEL OS is a network service. Reducing the number of running network services reduces the system's attack surface. Even more so in this case, as SSH by design enables a remote user to execute commands on the system.

### Instructions

By default, the SSH server is running on IGEL OS. To deactivate it, follow these steps:

1. In IGEL Setup go to **System > Remote Access > SSH Access**.
2. Deactivate **Enable**.
3. Click **Apply**.



## Disabling X11 Forwarding

When X11 forwarding is disabled, graphic applications cannot be run over SSH. By default, X11 forwarding is disabled.

If X11 forwarding is disabled, it is not possible to launch the IGEL Setup from an SSH session.

To ensure that X11 forwarding is disabled:

1. In the Setup, go to **System > Remote Access > SSH Access** and make sure that **Permit X11 forwarding** is deactivated.
2. Click **Apply** or **Ok**.

## Using Secure SSH Settings

### Rationale

If you intend to allow SSH connections to IGEL OS, there are a number of options that can make these more secure.

### Instructions

To secure the SSH settings of your devices, make as many of the following settings as possible for your use case

1. In IGEL Setup go to **System > Remote Access > SSH**.
2. Deactivate **Permit empty passwords**.
3. Deactivate **Permit administrator login**.
4. Deny **User access** for user, who can execute any command with regular user privileges.
5. Allow **User access** for ruser, whose access is restricted by the list **Applications access for remote user 'ruser'**.
6. Where needed, edit the list **Applications access for remote user 'ruser'**. It defines the commands that ruser can run from remote. By default, a local shell (`localshell`) and IGEL Setup (/config/sessions/setup0) are allowed.
7. Click **Apply**.
8. Go to **Security > Password**, under **User Account for Remote Access** activate **Use Password** and set a password
9. Click **Apply**.

## Disabling Secure Terminal

### Rationale

The secure terminal server on IGEL OS is a network service, providing a TLS/SSL-encrypted Telnet session. Reducing the number of running network services reduces the system's attack surface. Even more so in this case, as the secure terminal by design enables a remote user to execute commands on the system.

### Instructions

By default, the secure terminal is not active. Should you want to deactivate it at any time, do the following:



1. In IGEL Setup go to **System > Remote Access > Secure Terminal**
2. Deactivate **Secure Terminal**.
3. Click **Apply**.

Secure Terminal can be enabled globally in the UMS under **UMS Administration > Global Configuration > Remote Access**. There you can also enable the logging of users of the secure terminal.

## Wi-Fi and Bluetooth

Rogue or unencrypted Wi-Fi access points can put your data at risk, as can Bluetooth devices. If your device has Wi-Fi and Bluetooth, make sure to configure them securely or disable them.

- [Restricting Wi-Fi Access](#)(see page 438)
- [Disabling Bluetooth](#)(see page 439)

### Restricting Wi-Fi Access

#### Rationale

Using an unencrypted Wi-Fi network or falling for a rogue access point puts your users' data at risk. Enable strong encryption and restrict Wi-Fi access to a default network and optionally employ a whitelist of additional networks in order to prevent this.

#### Instructions

By default, Wi-Fi is not activated on IGEL OS. To activate it and preconfigure one or more allowed networks, follow these instructions:

1. In IGEL Setup go to **Network > LAN Interface > Wireless**.
2. Activate **Activate Wireless Interface**.
3. Do not activate **Enable wireless manager**, as this would give the user free choice of Wi-Fi networks.
4. Click **Apply**.
5. Go to **Network > LAN Interface > Wireless > Default Wi-Fi network**.
6. Check **Enable WPA Encryption**.
7. Enter the **Wireless network name (SSID)**.
8. Make authentication and encryption settings, see [Default Wi-Fi Network](#)(see page 1182) in the IGEL OS Manual.
9. Click **Apply**.
10. If needed, add further networks under **Network > LAN Interface > Wireless > Additional Wi-Fi networks**.



## Disabling Bluetooth

### Rationale

If your device has a Bluetooth interface it may be used to access data. Disabling the interface reduces the risk of data theft.

### Instructions

By default Bluetooth is deactivated on IGEL OS. Should you want to disable it at any time, do the following:

1. In the IGEL Setup go to **Devices > Bluetooth**.
2. Decativate **Bluetooth**.
3. Click **Apply**.

## Using UD Pocket for BYOD Devices

### Rationale

Letting users access company resources with their own devices (BYOD) and software poses a security risk: These systems may have insecure configurations or even contain malware. In addition, company data should not be saved on users' private devices.

### Instructions

- Use the IGEL UD Pocket. This ensures the use of secure and trusted software. As the UD Pocket does not access the device's mass storage, company data and private data will remain separated.

For details on the IGEL UD Pocket, see [UD Pocket \(UDP\) Reference Manual](#)(see page 1284).

For how to select the UD Pocket during the boot procedure, see [Boot Settings](#)(see page 1291) and [Starting Your UD Pocket](#)(see page 1292).

## 2.18.2 Secure Shell (SSH) Access to IGEL OS with Keys

IGEL OS has a built-in OpenSSH server that can be activated and configured via the Setup application. It lets you connect securely to the device over the network in order to issue commands or transfer files. While authentication can be done with a username-password combination, using a private-public key pair can increase convenience and/or security. This document describes how to generate and distribute the keys required.

- [Generating the SSH Key Pair](#)(see page 440)
- [Distributing the Public Key with UMS](#)(see page 441)
- [Configuring SSH Access on the Device](#)(see page 442)



## Generating the SSH Key Pair

### Prerequisites

- Linux/Unix operating system, typically on the administrator's workstation
- *OpenSSH* client software installed

### Introduction

The following procedure will generate two keys:

- **Public key:** This key is distributed to all machines the administrator wants to connect to. It can be made public.
- **Private key:** This key stays on the administrator's machine and has to be kept secret.

For the confidentiality of the encrypted connection to devices, it is essential to keep the private key secret.

An easily understandable explanation of private and public keys can be found in a [blog post by the programmer Blake Smith<sup>173</sup>](#).

### Generating the Key Pair

1. Open a terminal session on your workstation as the user who is going to make the SSH connections to the devices.
2. Issue the following command:  
`ssh-keygen`
3. When prompted for the location to store the key pair in, you can:
  - Hit return, which will accept the default file name `~/.ssh/id_rsa`

Using the default name may overwrite existing SSH key pairs!

4. When prompted for a passphrase, you can
  - Enter a passphrase (twice)

A passphrase protects the private key file in case it gets into the hands of an attacker. On the other hand, it may be inconvenient to enter the passphrase for every connection.

- Hit return in order to use no passphrase.

<sup>173</sup> <http://blakesmith.me/2010/02/08/understanding-public-key-private-key-concepts.html>



This increases convenience because you will be able to log in without entering the passphrase. However, it weakens security: The private key file will be unprotected if it gets into the hands of an attacker.

Two files have been generated (default names):

- `id_rsa` - the private key file
- `id_rsa.pub` - the public key file

### Distributing the Public Key with UMS

1. In *UMS Console*, right-click on **Files** in the navigation tree.
2. Select **New File**.
3. Upload the public key file (\*.pub) as a **Local File**.

Make sure that you do not upload the private key file by mistake.

4. Set the **Classification** to **Undefined**.
5. Specify the **Thin Client file location** as `/wfs/user/.ssh/authorized_keys`
6. Leave the **Access rights** as **Read, Write, Execute**.
7. Leave the **Owner** as **User**.
8. Assign the file to the desired thin clients, profiles or directories.



**New file**

**File source**

Upload local file to UMS server

Local file

Upload location (URL)

Select file from UMS server

File location (URL)

**File target**

Classification

Thin Client file location

**Access rights**

Read	Write	Execute
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Others	<input type="checkbox"/>	<input type="checkbox"/>

Owner

**Ok** **Cancel**

If you wish to authorize more keys for SSH connections to thin clients, prepare an authorized\_keys file containing all the public keys. Simply append them using a text editor.

## Configuring SSH Access on the Device

1. Go to **System > Remote Access > SSH Access** in the IGEL Setup or a profile.
2. Check **Enable**.
3. Optionally, if user `user` has an empty password, check **Permit empty passwords**.
4. Set **Deny** to **No** in the **User access** entry for `user`.

This configuration gives the remote user full shell access as if they were the local user on the client.

Now you can connect to the device from the administrator's machine with the following command:



`ssh user@[client name or IP address]`

Depending on whether you set a passphrase for the key, you may have to enter it or not.

### 2.18.3 Secure Terminal (Telnet with TLS/SSL)

IGEL Linux version 5.11.100 or newer and IGEL Linux version 10.01.100 or newer allow terminal access via UMS with transport encryption. In analogy to [secure shadowing](#)(see page 443), network traffic is encrypted with TLS/SSL. Secure terminal connections can only be initiated from the UMS whose certificate is stored on the device.

For details about setting up a secure terminal connection, see UMS manual [Secure Terminal \(Secure Shell\)](#)<sup>174</sup>.

Secure Terminal is the best way to create a remote access from the UMS (on Linux or Windows installed) to Linux devices, without installing an additional terminal software. Because the UMS includes the software.

### 2.18.4 Secure Shadowing (VNC with TLS/SSL)

The **Secure Shadowing** function improves security when remotely maintaining a device via VNC at a number of locations:

- **Encryption:** The connection between the shadowing computer and the shadowed device is encrypted.  
This is independent of the VNC viewer used.
- **Integrity:** Only devices in the UMS database can be shadowed.
- **Authorization:** Only authorized persons (UMS administrators with adequate authorizations) can shadow devices.  
Direct shadowing without logging on to the UMS is not possible.
- **Limiting:** Only the VNC viewer program configured in the UMS (internal or external VNC viewer) can be used for shadowing.  
Direct shadowing of a device by another device is likewise not permitted.

In addition, [IGEL Management Interface \(IMI\)](#)<sup>175</sup> in Version 2 or newer provides an API for Secure Shadowing.

- **Logging:** Connections established via secure shadowing are recorded in the UMS server log.  
In addition to the connection data, the associated user data (shadowing UMS administrator, optional) can be recorded in the log too.

Of course, this is only relevant to devices that meet the requirements for secure shadowing and have enabled the corresponding option. Other devices can be "freely" shadowed in a familiar manner and, if necessary, secured by requesting a password. If you would like to allow secure shadowing only, you can specify this in the UMS Console under **UMS Administration > Global Configuration > Remote Access**<sup>176</sup>.

<sup>174</sup> <https://kb.igel.com/pages/viewpage.action?pageId=22459969>

<sup>175</sup> <https://kb.igel.com/display/igelimiv2/IMI+Manual>

<sup>176</sup> <https://kb.igel.com/display/endpointmgmt605/Remote+Access>



- [Basic Principles and Requirements](#)(see page 444)
- [Shadow Devices Securely](#)(see page 445)
- [VNC Logging](#)(see page 445)

## Basic Principles and Requirements

The **Secure Shadowing** option can be enabled if the following requirements are met:

- IGEL Linux as of version 5.03.190 and 10.01.100 or IGEL Windows Embedded Standard 7 from version 3.09.100
- IGEL Universal Management Suite from version 4.07.100 onwards
- The device is registered on the UMS Server
- The device can communicate with the UMS Console and UMS Server (see below)

## Basic Technical Principles

Unlike with "normal" shadowing, the connection between the VNC viewer and the VNC server (on the device) is not established directly during secure shadowing. Instead, it runs via two proxies – one for the UMS Console and one for the VNC server on the device. These proxies communicate via a TLS/SSL-encrypted channel, while the local communication, e.g. between the VNC viewer application and the UMS proxy, takes place in the conventional unencrypted manner. As a result, a secure connection can also be established with external VNC programs that do not support TLS/SSL connections.

The two proxies (UMS Console and device) communicate with TLS/SSL encryption via the same port as the "normal" VNC connection: 5900. As a result, no special rules for firewalls need to be configured in order to perform secure shadowing.

If secure shadowing is active for a device under **Setup > System > Remote Access > Shadow > Secure mode**, the device generates a certificate in accordance with the X.509 standard and transfers it to the UMS Server when the system is next started. The UMS Server checks subsequent requests for a secure VNC connection using the certificate. The certificate in PEM format can be found in the `/wfs/client-certs/tc_ca.crt` directory on the device. The validity of the certificate can be checked on the (Linux) client using the command: `x11vnc -sslCertInfo /wfs/client-certs/tc_ca.crt`

If a UMS administrator calls up the **Shadowing** function in the UMS Console for the device, the console receives a signed request from the UMS Server which is then passed on to the device to be shadowed. This in turn passes on the request to the UMS Server which checks the validity of the request using the original certificate. If this check is successful, the console reports that the channel for the connection between the proxies can be established. The UMS proxy on the console connects to the server proxy on the device, and the server proxy, in turn, establishes on the device the connection to its VNC server.

Only when these connections have been established, the console calls up the VNC viewer which then connects to the console proxy. The VNC client and VNC server are now connected via the two proxies which transfer data with TLS/SSL encryption.

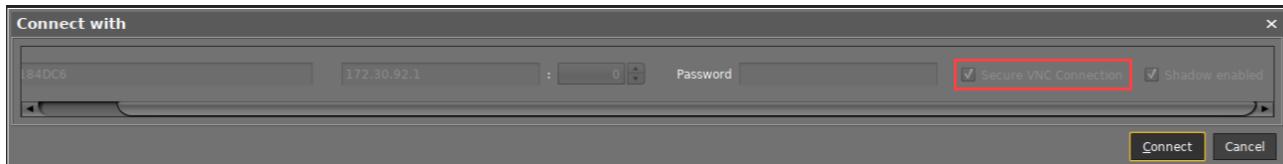
Secure shadowing can be enforced independently of the device configuration for all devices that support this function: **UMS Administration > Global Configuration > Remote Access > Enable secure VNC globally**.



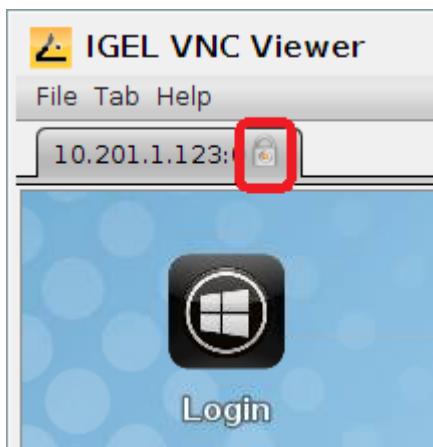
## Shadow Devices Securely

In order to shadow a device securely (with encryption), the administrator must log on to the server via the UMS console. When doing so, it is irrelevant whether a purely local UMS administrator account is used or the user was adopted via an Active Directory for example. As always, however, the UMS administrator must have the permission to shadow the object, see [Object-Related Access Rights](#)<sup>177</sup>.

The device to be shadowed is called up in the structure tree and, as usual, can be executed via **Shadow** in the context menu. The connection window, however, differs from the dialog for normal VNC shadowing. The IP and port of the client to be shadowed cannot be changed, and a password for the connection is not requested – this is superfluous after logging on to the console beforehand.



When a VNC connection has been established, the symbol in the connection tab indicates secure shadowing:



## VNC Logging

Connections via secure shadowing are always logged in the UMS. Via **UMS Administration > Global Configuration > Remote Access > Secure VNC**, you can configure whether the user name of the person shadowing is to be recorded in the log:

- **Log user for secure VNC**
- The user name is included in the log.

<sup>177</sup> <https://kb.igel.com/display/endpointmgmt/Object-related+access+rights>



- The user name is not included in the log. (default)

The VNC log can be called up via the **context menu** of a device or folder (for several devices, **Logging > Logging: Secure Access Logs**). The name, MAC address and IP address of the shadowed device, the time and duration of the procedure and, if configured accordingly, the user name of the shadowing UMS administrator are logged.

Remote Access Logs									
Filter: 00E0C51431C0									
Thin Client	MAC Address	Unit ID	Thin Client IP	User	Start time	Durat...	Comment	Protocol	
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 11:54:29 AM	0	Unknown Error	Secure VNC	▲
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 11:54:42 AM	58		Secure VNC	
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 11:56:31 AM	0	Shadowing triggered by IMI	Secure VNC	
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 11:56:31 AM	0	Shadowing triggered by IMI	Secure VNC	
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 11:57:31 AM	0	Shadowing triggered by IMI	Secure VNC	
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 12:03:34 PM	5		Secure VNC	
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 1:48:18 PM	219		Secure VNC	
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 2:32:40 PM	1007		Secure VNC	
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 3:25:24 PM	120		Secure VNC	

48 Logs found.

- To sort the list (e.g. according to user names), click on the relevant column header or filter the content shown by making entries in the **Filter** field.

## 2.18.5 Cherry eGK Channel Substitution

As of firmware version 10.05.100, the Cherry eGK Channel is no longer available. In the Igel Universal Desktop Firmware, Linux V5, the VirtualChannel for Cherry eGK devices is still included parallel to the Cherry USB2LAN Proxy. If you want to continue using the G87-1504/ST-1503 as before, with firmware version 10.05.100 and higher you have to activate the proxy. All settings are automatically applied and run through the connector in the network.

Using the G87-1504/ST-1503 with firmware version 10.05.100 and higher:

- Activate the proxy - this can also be done from the backend.
  - Cherry USB2LAN Proxy (Under Smartcard) (see screenshot)
  - IGEL device, valid for Cherry devices G87-1505, G87-1504/ST-1503 to USB



For IGEL Lx v5 and OS10:

- Activate **Cherry USB2LAN Proxy** under **IGEL Setup > Security > Smartcard > Services**.

The screenshot shows the 'Configuration' menu on the left with 'Smartcard' selected. On the right, under 'Services', the 'Cherry USB2LAN Proxy' checkbox is checked. Below it, the 'Network Interface' dropdown is set to 'auto'.

For IGEL Lx v5:

- Disable **Cherry Channel 0** and **Cherry Channel 1** under **IGEL Setup > Sessions > RDP > RDP Global > Mapping > Device Support**.
- Do not activate smartcard.

The screenshot shows the 'Sessions' menu on the left with 'RDP Global' selected. Under 'Device Support', the 'Enable smartcard' checkbox is unchecked. To the right, there is a list of various device support options, many of which have checkboxes next to them.

Install the Cherry eGK KVK software on the server. See [https://www.cherry.de/files/software/Cherry-eGK-KVK\\_Software\\_33.zip](https://www.cherry.de/files/software/Cherry-eGK-KVK_Software_33.zip)



Install the Cherry Linux software on the device.

- In the CT-API configuration the G87-1504/ST-1503 can be configured as network device.
- Link to Doku Client Server Integration: [https://www.cherry.de/files/manual/64410063-01\\_USBLANProxyClientServerUndCitrix.pdf](https://www.cherry.de/files/manual/64410063-01_USBLANProxyClientServerUndCitrix.pdf)
- Link to the software architecture documentation: [https://www.cherry.de/files/manual/Cherry-eGK-KVK\\_Software-Architektur\\_Windows-20130927-v04.pdf](https://www.cherry.de/files/manual/Cherry-eGK-KVK_Software-Architektur_Windows-20130927-v04.pdf)

The VirtualChannel was replaced due to the following difficulties and the future application of the telematics infrastructure (see also gematik anforderung lan)

- Independent of Citrix version (no need to check compatibility anymore)
- Independent of the server version (2008, 2012...), if the connection runs via RDP

## 2.18.6 Single Sign-on for the Browser Proxy

Using a proxy to handle a browser's internet traffic provides additional security and control. However, if the proxy is password-authenticated, the user has to enter their credentials, which adds some inconvenience.

With IGEL Linux *version 5.08* or newer and IGEL Linux *version 10.01.100* or newer, you can avoid this inconvenience by using the passthrough feature. As a prerequisite, user logon must be carried out via Kerberos.

To enable single sign-on for the browser proxy:

1. Open the Setup and go to **Security > Logon > Active Directory/Kerberos**.



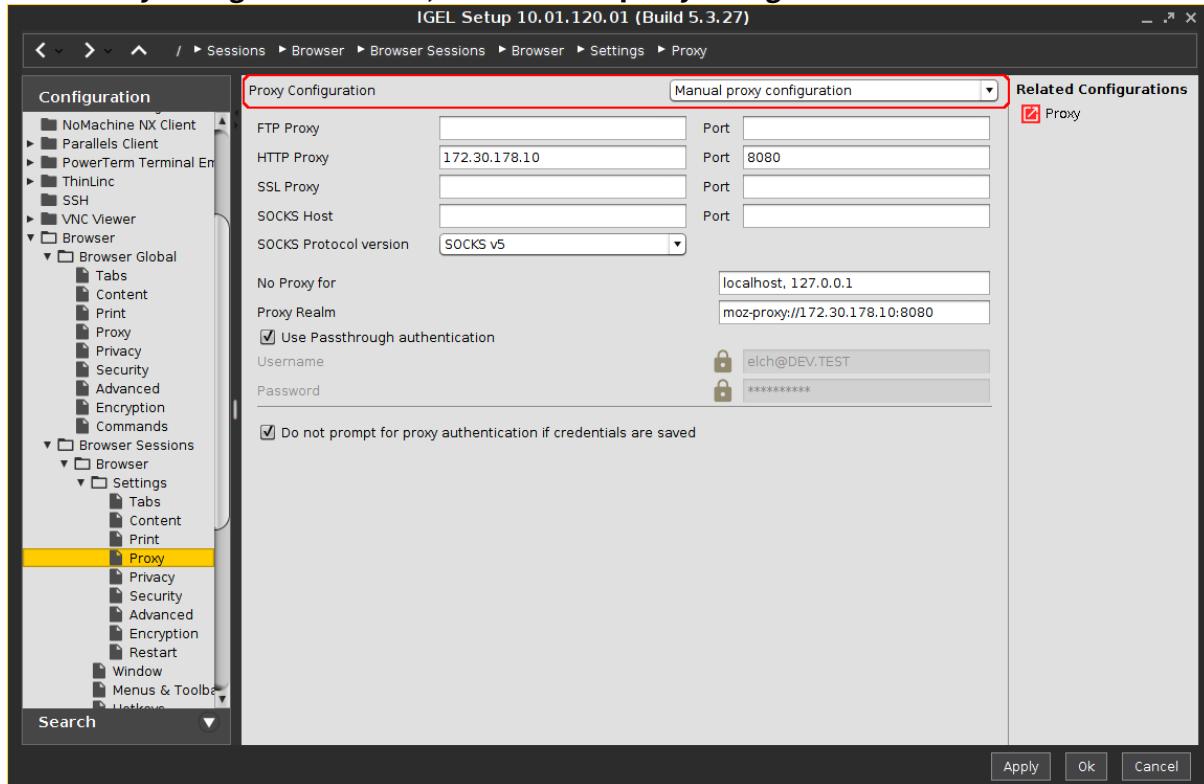
## 2. Activate Login to Active Directory/Kerberos.

The screenshot shows the 'IGEL Setup 10.01.120.01 (Build 5.3.27)' window. The left sidebar navigation tree is open, showing sections like Configuration, User Interface, Network, Devices, Security, Logon, Active Directory/Kerberos, and Smartcard. Under 'Logon', 'Active Directory/Kerberos' is selected. In the main panel, under 'Login methods:', the checkbox for 'Login to Active Directory Domain' is checked and highlighted with a red border. Other options include 'Explicit', 'Remember last user name', and 'Smartcard'. To the right, there's a 'Related Configurations' section with checkboxes for 'Active Directory / Kerberos', 'Post Session Command', and 'Smartcard Middleware'. At the bottom are 'Apply', 'Ok', and 'Cancel' buttons.

## 3. Go to Sessions > Browser > Browser Sessions > [name of the browser session] > Settings > Proxy.



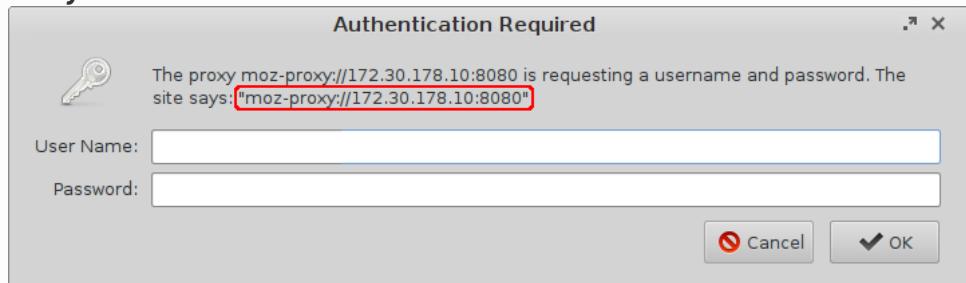
4. In the **Proxy Configuration** choice, select **Manual proxy configuration**.



5. For an HTTP proxy, define the following settings:

- **HTTP proxy:** IP address or hostname of the proxy to be used
- **Port:** Port of the proxy for HTTP
- **No proxy for:** IP addresses or hostnames of servers that can be accessed directly
- **Proxy realm:** Area in which the browser authenticates itself for the proxy. Together with the user name and password, this information is necessary for authentication.

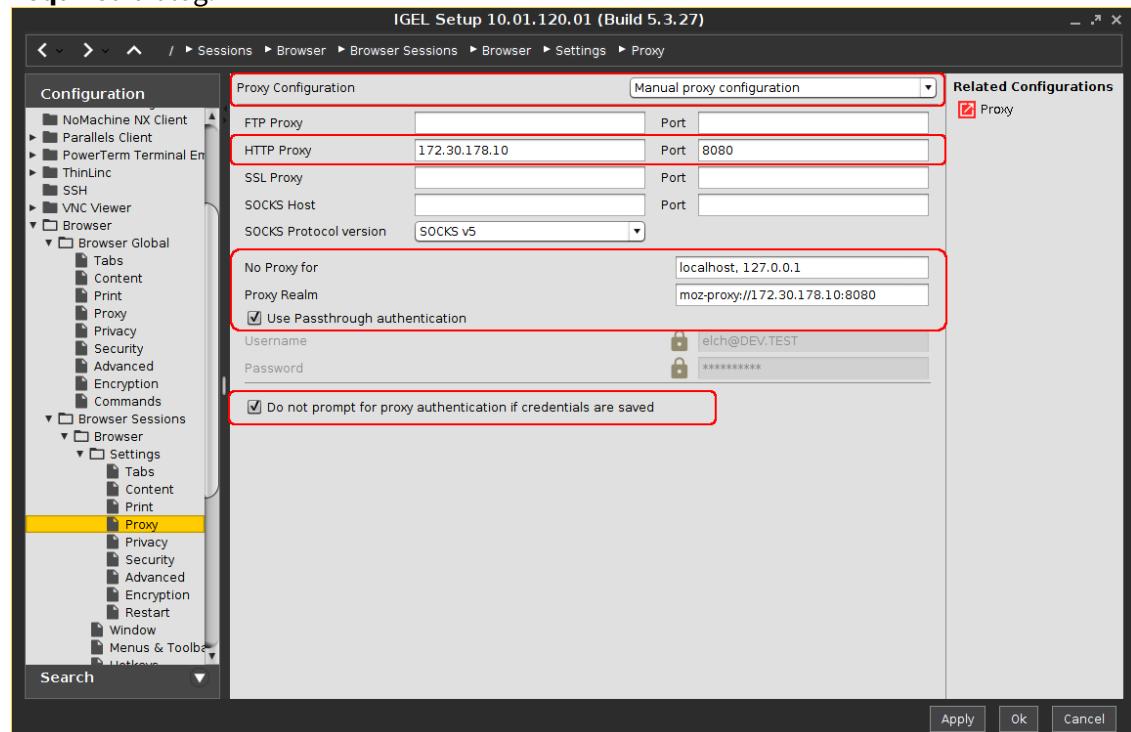
The **Proxy realm** field is internally pre-populated with the value `moz-proxy://[HTTP Proxy] : [Port]`. If the field is empty, this value will be used when authenticating the browser. If the proxy expects another unknown value for the proxy realm, you can determine this as follows: Leave the **User name** and **Password** fields empty and launch the browser. The dialog window which appears will contain the correct value for the **Proxy realm** field:



In the

example above, the value for the **Proxy realm** field is as follows: `moz-proxy://172.30.178.10:8080`

- **Use passthrough authentication:** Must be enabled to allow single sign-on for the browser proxy.
- **Do not prompt for proxy authentication if credentials are saved:** Must be enabled to enable seamless single sign on for the browser proxy; suppresses the **Authentication Required** dialog.



The next time the user logs in to the device, the browser proxy is ready to use.



## 2.18.7 Limiting the Number of Permitted Login Attempts

### Symptom

Users can attempt logging in as often and as fast as they want at the screen unlock prompt and local login prompts (e.g. for Kerberos, Shared Workplace, IGEL Smartcard).

### Problem

This leaves the system and remote sessions vulnerable to brute force login attacks.

### Solution

In IGEL OS 10.03.100 and newer, the number of login attempts is limited to 5 within 30 seconds.

These values can be changed in the system registry:

1. In Setup, go to **System > Registry**
2. Go to the auth.login.lockout\_threshold parameter to set the maximum number of login attempts within the specified interval.
3. Go to the auth.login.lockout\_duration parameter to set the interval in seconds.
4. Click **Apply** or **Ok**.

## 2.18.8 How to Deploy Device Encryption

### Overview

IGEL OS 11.06 or higher offers strong device encryption that is derived from a user password. The encryption is applied to all partitions that can contain user data, e.g. browser history or Custom Partitions.

#### Important Notes on Downgrading

- If you have encrypted your IGEL OS 11.06 device, downgrading to IGEL OS 11.05 or lower will imply data loss on the following partitions, due to different partition schemes:
  - Browsing history of the browsers Firefox and Chromium
  - Custom Partitions
- The device settings and the UMS connection are preserved.
- The device encryption password must be entered by the user.

### Instructions

1. In the UMS configuration dialog or the local Setup, go to **Security > Device Encryption**.



2. Set the parameters to meet your requirements. For details, see Device Encryption(see page 1235).

Device Encryption mode	keep
Authentication type	PW
Security level	Auto, constant-time
Target time delay (ms)	700
Password aggregation function	ll: Argon2id, 128M/3 ops
Minimum password length	8
Unwanted strings in password (comma separated)	
The password must contain	all
Minimum amount of lower case letters	1
Minimum amount of upper case letters	0
Minimum amount of numbers	0
Minimum amount of special characters	0
Special characters allowed	!"\$%/( )[]{}?+~-.^*



- Set **Device encryption mode** to "activate" and click **Apply and send to device** or **Save**.

A screenshot of a software interface for configuring device encryption settings. The main window has a dark background with light-colored input fields and buttons. A red box highlights the "Device Encryption mode" dropdown at the top right, which is set to "activate". Another red box highlights the "Apply and send to device" button at the bottom right of the dialog.

Device Encryption mode	activate
Authentication type	PW
Security level	Auto, constant-time
Target time delay (ms)	700
Password aggregation function	ll: Argon2id, 128M/3 ops
Minimum password length	8
Unwanted strings in password (comma separated)	
The password must contain	all
Minimum amount of lower case letters	1
Minimum amount of upper case letters	0
Minimum amount of numbers	0
Minimum amount of special characters	0
Special characters allowed	!"\$%/()[]{}?+~-*"

- When the settings have been sent to the device, a password dialog is presented to the user.
- The user enters an encryption password that meets the requirements and clicks **Apply**.



**Device Encryption**

The device encryption has been activated.

The password

- must be at least 8 characters long
- must contain at least 1 lower case letters

New password:

>Password strength   medium

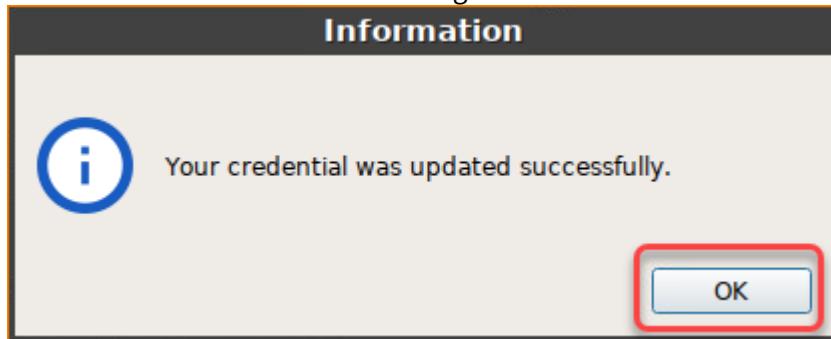
Re-Enter new password:

**Apply**

A red box highlights the "New password:" input field, another highlights the "Re-Enter new password:" input field, and a third highlights the "Apply" button.

Several partitions are re-encrypted. This might take up to 60 seconds, depending on your hardware capabilities and the size of your Custom Partition.

5. The user confirms the success message.



6. On system start, the user must enter the device encryption password.



## 2.18.9 Security: Timeout for Secure Shadowing and Secure Terminal

### Overview

To avoid a denial of service attack by blocking port 30022, which is used for secure shadowing (secure VNC) and secure terminal connections, a timeout can be configured. This timeout limits the establishing process for connections to port 30022. The duration is 180 seconds by default and can be changed via an environment variable.

### Configuring the Timeout

1. Open the UMS configuration dialog or the local Setup and go to **System > Firmware Customization > Environment Variables > Predefined**.
2. Enter the following data and then click **Ok**:
  - **Variable name:** IGEL\_TLS\_TUNNEL\_TIMEOUT
  - **Value:** Timeout in seconds. The range is 0 to 180. When the value is set to 0, there will be no timeout.



Variable name	Value
IGEL_TLS_TUNNEL_TIMEOUT	30
Variable name	Value

Some services are restarted on the device. Afterward, the timeout is set.

## 2.19 Certificates

- Certificate Enrollment and Renewal with SCEP (NDES)(see page 457)
- Deploying Trusted Root Certificates(see page 470)
- Which CA Certificates Are Contained in IGEL OS?(see page 474)

### 2.19.1 Certificate Enrollment and Renewal with SCEP (NDES)

SCEP is a protocol for certificate management which supports the secure issuance of certificates to network devices.

#### Requirements

- SCEP server  
The following SCEP server implementations can be used with IGEL Linux v5 or IGEL Linux 10:
  - Windows 2008 Server with the Network Device Enrollment Service (NDES) role



- Windows 2012 Server
- Windows 2016 Server

For information on how to deploy the NDES, see <http://aka.ms/ndes>.

- Connection between the SCEP server and the certification authority (CA).

This document explains the enrollment of certificates with SCEP.

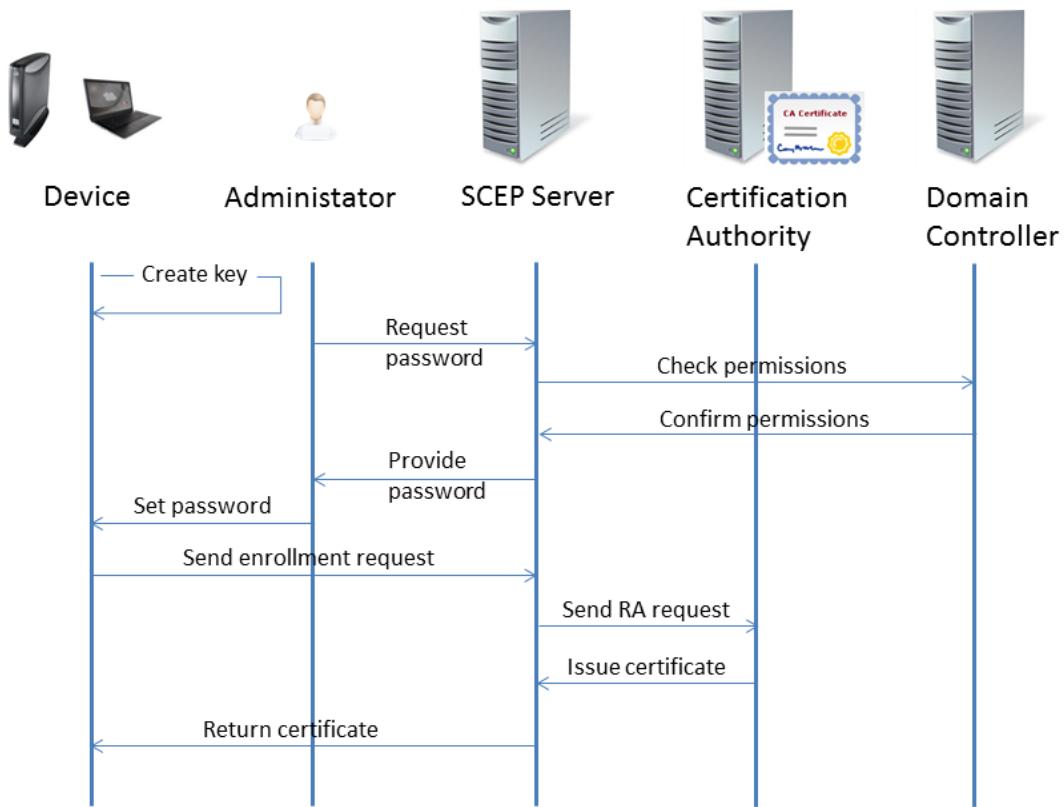
- [Technical Background](#)(see page 458)
- [Client Enrollment Details](#)(see page 460)
- [Configuration of the SCEP Client](#)(see page 461)
- [Files Involved](#)(see page 467)
- [Troubleshooting](#)(see page 468)

## Technical Background

The Simple Certificate Enrollment Protocol (SCEP) defines a way of automatically enrolling certificates for the authentication of network devices or VPNs. The client uses HTTP requests to fetch root certificates, to send certificate requests, and to fetch client certificates from the server.

For an in-depth description, see the Microsoft technet article "Network Device Enrollment Service (NDES) in Active Directory Certificate Services (AD CS)" under <http://aka.ms/ndes>.

Here is a typical certificate enrollment process:



1. The device creates an RSA public-private key pair.
2. The administrator requests a challenge password from the SCEP service (e.g. NDES).

The challenge password is only required for the first enrollment request. For certificate renewal, the current certificate is used for authentication.

3. The SCEP server asks the domain controller if the administrator holds the required permissions for the configured certificate templates.
4. The domain controller confirms that the administrator holds the required permissions.
5. The SCEP server creates a challenge password and hands it over to the administrator.

Typically, the challenge password expires after a defined time. With the NDES that is included in Windows 2008 Server, the default expiry time is 60 minutes.

6. The administrator provides the device with the challenge password, the CA identifier, and the fingerprint of the CA certificate.
7. The device sends the enrollment request to the SCEP server, using the challenge password to authenticate with the SCEP server. This action is triggered by the administrator.



8. The SCEP server signs the enrollment request with its enrollment agent certificate and sends it to the CA.
9. The CA issues the desired certificate and returns it to the SCEP server.
10. The SCEP server returns the certificate to the device.

## Client Enrollment Details

This section describes the actual certificate enrollment in detail. The process described here corresponds to step 7 to 10 in the [overall process](#)(see page 458).

The enrollment request and the response from the CA that contains the req

1. The client requests the CA's public certificate from the SCEP server.
2. The SCEP server sends the CA's public certificate to the client.
3. The client checks the CA's public certificate against the relevant fingerprint. The fingerprint has been provided by the administrator via a UMS profile; see [Defining the Certification Authority](#)(see page 464).
4. The client sends an enrollment request to the SCEP server. This enrollment request is an HTTP GET request that contains the following:

Signed data PKCS7	Enveloped data PKCS7	Certificate Signing Request (PKCS 10)
Version		
Hashing algorithm		
Signed (unencrypted) data:	Version	
Recipient and related encrypted data encryption key; the recipient is the CA.		
Encrypted data:	Version	
(encrypted with a randomly generated key that is encrypted with the recipient's public key)		
Requested subject name		
Public key of client		



Challenge password		
Requested extensions		
Signature algorithm		
Digital signature		
Client certificate		
Digital signature		
5. If the request was successful, the HTTP response from the SCEP server includes the following data:		
Signed data PKCS7	Enveloped data PKCS7	Degenerate Certificates (only PKCS7)
Version		
Hashing algorithm		
Signed (unencrypted) data:	Version	
List of recipients		
Encrypted data:	Version	
Issued X.509 certificate		
CA certificate		
Digital signature		

## Configuration of the SCEP Client

The configuration of the SCEP client on the IGEL OS device is carried out as follows:

- Creating a Profile in the UMS(see page 462)
- Activating the SCEP Client(see page 462)
- Entering the Data for the Certificate Signing Request (CSR)(see page 463)
- Defining the Certification Authority (CA)(see page 464)
- Providing the SCEP Server Data(see page 465)
- Applying the Profile to the Devices(see page 466)



## Creating a Profile in the UMS

1. In the UMS structure tree, go to **Profiles**, open the context menu and select **New Profile**.
2. Enter an appropriate **Profile Name**.
3. In the **Based on** menu, select the firmware version that is installed on the devices in question.
4. Click **OK**.  
The configuration dialog opens. The configuration dialog corresponds to the IGEL Setup available on the devices to which the profile is assigned.

## Activating the SCEP Client

1. Go to **Network > SCEP Client (NDES)**.
2. Enable **Manage Certificates with SCEP**.

The screenshot shows the UMS (User Management System) interface with the title bar "SCEP Certificate Enrollment". Below the title bar, the breadcrumb navigation shows "Network > SCEP Client (NDES)". On the left, there is a navigation tree under the heading "Configuration". The "Network" section is expanded, showing "LAN Interfaces", "Mobile Broadband", "DHCP Client", "VPN", and "SCEP Client (NDES)". The "SCEP Client (NDES)" node is selected and highlighted with a blue border. Under "SCEP Client (NDES)", there are three sub-options: "Certificate", "Certification Authority", and "SCEP". To the right of the navigation tree, there is a toolbar with a gear icon and a checkmark icon, followed by the text "Manage Certificates with SCEP". This text is enclosed in a red rectangular box, indicating it is the setting being enabled. The rest of the interface is mostly empty space.



## Entering the Data for the Certificate Signing Request (CSR)

► Go to **Network > SCEP Client (NDES) > Certificate** and enter the following data:

**Type of CommonName/SubjectAltName:** The characteristic for linking the certificate to the device.

- IP address: The IP address of the device.
- DNS name: The DNS name of the device.
- IP address (auto): The IP address of the device (inserted automatically).
- DNS name (auto): The DNS name of the device (inserted automatically).
- Email address: An email address.
- DNS name as UPN (auto)

If the client automatically obtains its network name, **DNS Name (auto)** is a good type for the client certificate.

The following parameter is available if **Type of CommonName/SubjectAltName** is set to **IP address**, **DNS name**, or **Email address**:

**CommonName/SubjectAltName:** Give a designation which matches the **Type of CommonName/SubjectAltName**. For certain types, this occurs automatically. No entry is then required.

The following parameter is available if **Type of CommonName/SubjectAltName** is set to **IP address (auto)**, **DNS name (auto)**, or **DNS name as UPN (auto)**:

**CommonName/SubjectAltName Suffix:** Specifies a suffix that will be added to CommonName/SubjectAltName. Possible values:

- "none- "dot + DNS domain (auto)": The system's current DNS domain name separated with a dot will be added. Example: .igel.local
- Free text entry: The manually entered suffix will be added. Take notice that the percent symbol "%" is used for introducing the escape sequence, and thus the following replacements take place automatically:
  - %D is replaced by the system's DNS domain name at the time the certificate signing request (CSR) is created. Example: @%D will be changed into @igel.de if the system's current DNS domain name is igel.de.
  - %% will be replaced by %. Example: A%%B will be changed into A%B.
  - Other combinations with % are currently discarded. Example: A%BC will be changed into AC.

If you have to specify the suffix manually, make sure you enter the separator.

**Organizational unit:** Stipulated by the certification authority.

**Organization:** A freely definable designation for the organization to which the client belongs.



**Locality:** Details regarding the device's locality. Example: "Augsburg".

**State:** Details regarding the device's locality. Example: "Bayern".

**Country:** Two-digit ISO 3166-1 country code. Example: "DE".

**RSA key length (bits):** Select a key length (one suited to the certification authority) for the certificate that is to be issued.

Possible values:

- "1024"
- "2048"
- "4096"

The RSA key length specified here must not be lower than the minimum key length configured on the server.

#### Defining the Certification Authority (CA)

1. Go to **Network > SCEP Client (NDES) > Certification Authority**.
2. Enter the details for the certification authority (CA):
  - **CA Identifier:** FQDN (fully qualified domain name) of the CA



- **CA Certificate Fingerprint (MD5):** Fingerprint of the CA certificate in the form 01:02:03:04:05:06:07:08:09:0A:0B:0C:0D:0E:0F:10

You can get the fingerprint from your NDES server: [https://<NDES Servername>/certsrv/mscep\\_admin](https://<NDES Servername>/certsrv/mscep_admin)

The screenshot shows the 'Configuration' menu on the left with 'Network' selected. Under 'Network', 'SCEP Client (NDES)' is expanded, and 'Certification Authority' is selected. On the right, there are two input fields: 'CA Identifier' containing 'ca.example.com' and 'CA Certificate Fingerprint (MD5)' containing ':04:05:06:07:08:09:0A:0B:0C:0D:0E:0F:10'. At the bottom are three buttons: 'Apply and send to thin client', 'Save', and 'Cancel'.

If the CA certificate fingerprint is specified, the client will use it to check the integrity of the CA certificate it receives from the SCEP server.

#### Providing the SCEP Server Data

1. Go to **Network > SCEP Client (NDES) > SCEP**.
2. Enter the following data:
  - **SCEP server URL:** URL by which the SCEP client communicates with the SCEP server.

HTTPS is not supported; however, all security critical data that are transferred between the SCEP client and other components are encrypted.

- **Proxy server for SCEP requests** (optional): IP address or host name of the proxy server that is used for the communication between the device and the SCEP server. If a web application



firewall is used instead of a proxy, its IP address or host name of the proxy server must be entered here.

- **Challenge password:** Password that the SCEP client must present to the SCEP server in its request (CSR).

On a Microsoft NDES server, you can retrieve the password by default under [https://certsrv/mscep\\_admin](https://certsrv/mscep_admin).

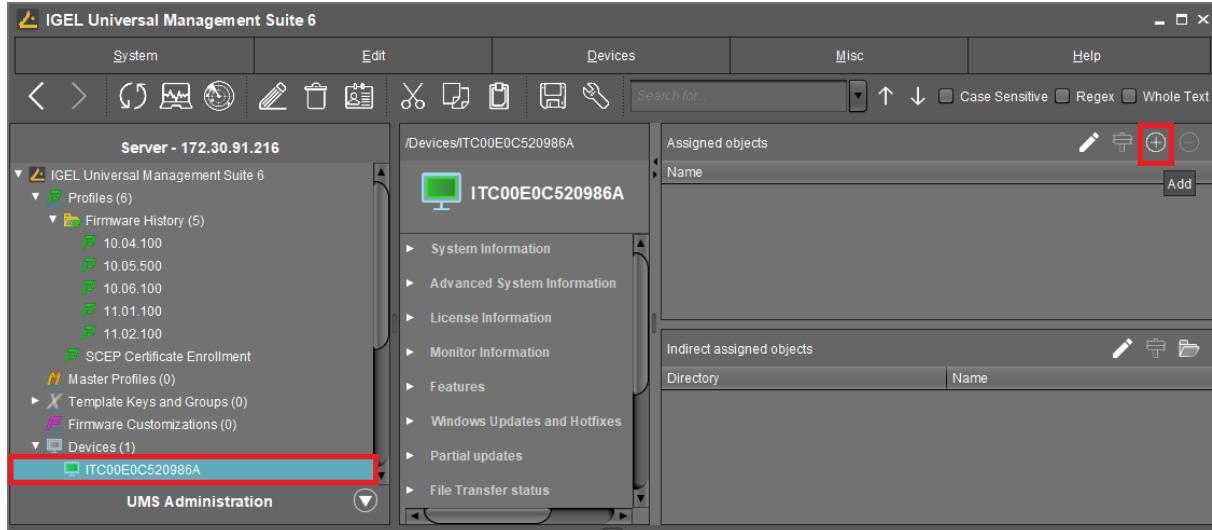
By default, the password on a Microsoft NDES server is valid for 1 hour and can be used only once. In order to use the password on numerous devices, additional settings must be made on the NDES server. For information, see the section "Password and Password Cache" on <https://social.technet.microsoft.com><sup>178</sup>.

- **Certificate renewal period (days):** Time interval before certificate expiry after which the certificate renewal procedure is started. (Default: 30)
- **Certificate expiry check interval (days):** Specifies how often the certificate is checked against its expiry date. (Default: 1)

### 3. Save the settings.

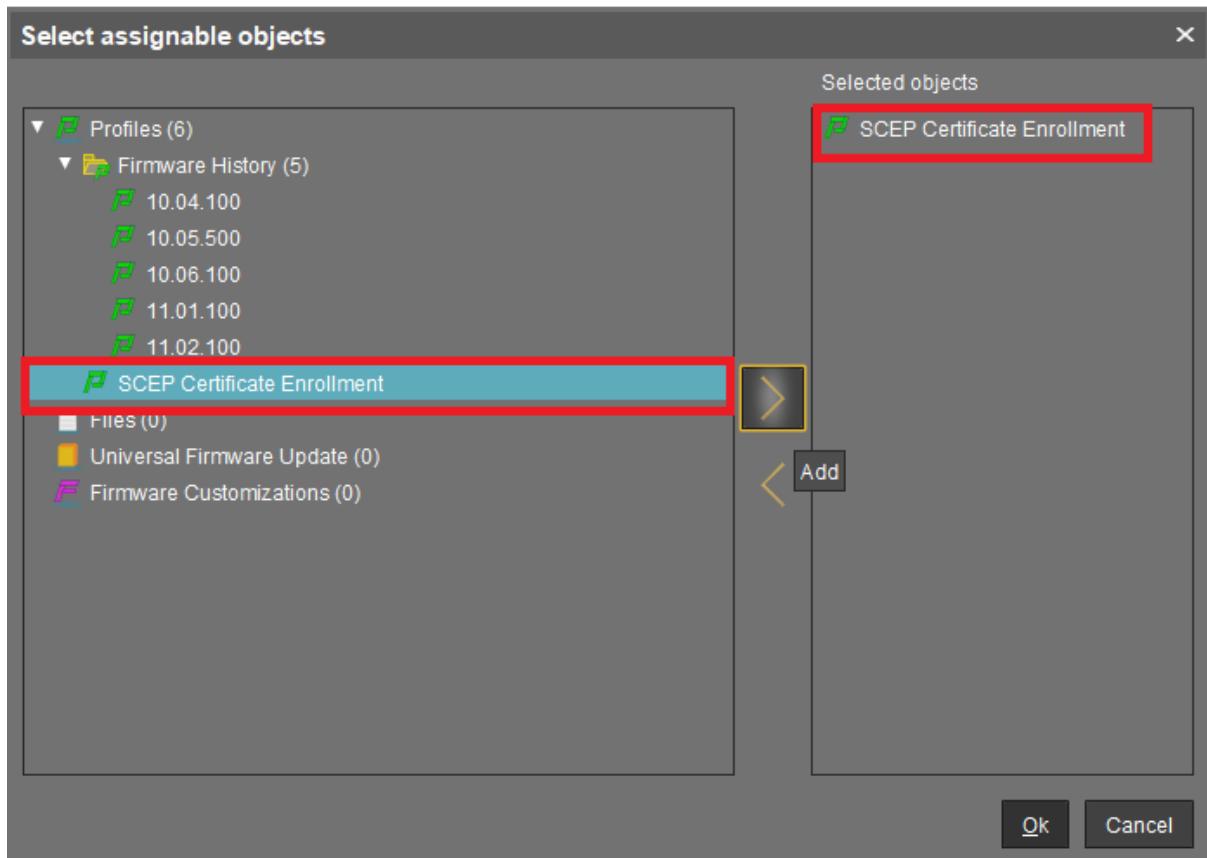
#### Applying the Profile to the Devices

1. In the UMS structure tree under **Devices**, select the devices you want to assign the profile to.
2. In the **Assigned objects** area, click 



3. In the **Select assignable objects** dialog, select the relevant profile and click  to assign it.

<sup>178</sup> <https://social.technet.microsoft.com/wiki/contents/articles/9063.active-directory-certificate-services-ad-cs-network-device-enrollment-service-ndes.aspx>



4. Click **Ok**.
5. In the **Update time** dialog, select **Now** and click **Ok**.  
The device performs the actions as described in [Client Enrollment Details](#)(see page 460).

## Files Involved

All files involved are stored in the directory `/wfs/scep_certificates/cert0`. The following fixed file names are used:

<code>cacert.pem</code>	CA certificate
<code>racert_enc.pem</code>	RA certificate used for encryption (optional)
<code>racert_sig.pem</code>	RA certificate used for signature (optional)
<code>client.csr</code>	Certificate signing request
<code>client.cert</code>	Client certificate



client.key	Private key of client certificate
------------	-----------------------------------

## Troubleshooting

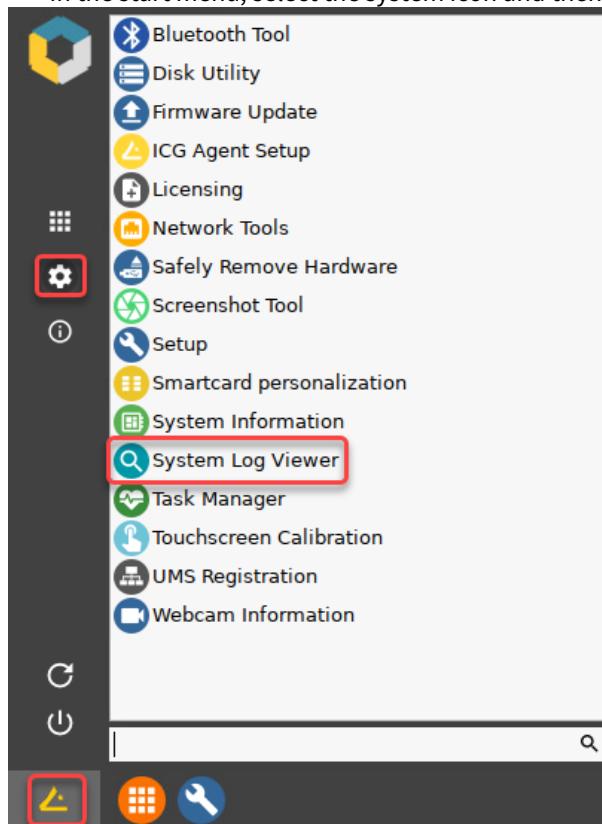
- [Diagnostics](#)(see page 468)

### Diagnostics

#### Preliminary: Tools

##### System Log Viewer

- In the start menu, select the system icon and then **System Log Viewer**.



For more information on starting, using, and configuring the system log viewer, see the [System Log Viewer](#)(see page 1070) chapter of the [IGEL OS Manual](#)(see page 750).

##### Local Terminal

- Start the local terminal, if available.

If a local terminal session has not been set up on your device, proceed as follows:

1. Open the Setup and go to **Accessories > Terminals**.
2. Click **+** to create a local terminal session.
3. Click **Ok** to save the setting and exit the Setup.



For more information on starting and using the local terminal, see the [Terminals](#)(see page 1042) chapter of the [IGEL OS Manual](#)(see page 750).

#### Checking the Current Status of the Client Certificate Enrollment

- ▶ In the local terminal, enter the command `cert_show_status`

The status for each certificate relating to SCEP is shown:

- CA certificate
- RA encryption certificate
- RA signature certificate
- Client certificate

#### Reviewing Log Messages

1. Open the system log viewer and select `/tmp/journal.log`
2. Press [Ctrl] + [F] and enter `cert_agent` to search for relevant messages.

Alternatively, you can open a local terminal and enter `journalctl | grep cert_agent`

#### Reviewing the Certificates and Certificate Requests in the File System

1. Open a local terminal and login as user.
2. Enter `ls /wfs/scep-certificates/cert0/`

#### Deleting a Certificate Request

1. Open a local terminal and login as root.
2. Enter `rm -rf /wfs/scep-certificates/cert0/`  
The directory that includes the certificate request, received certificates (if existing), and the device's own private client key, is deleted. This can be useful for debugging purposes, and if SCEP is no longer used.

#### Checking the CA

1. Open a local terminal and login as root.
2. Enter `scep_getca 0`

#### Generating an SCEP Request Manually

1. Open a local terminal and login as root.
2. Enter `scep_mkrequest 0`

#### Enrolling a Certificate Manually

1. Open a local terminal and login as root.
2. Enter `scep_enroll 0`



## Testing Certificate Renewal

1. Open a local terminal and login as root.
2. Generate an SCEP request and append "new" to the key file name: `scep_mkrequest 0 "new"`  
An SCEP request is issued. In the directory `/wfs/scep-certificates/cert0/`, the key file `clientnew.key` is created.
3. Renew the certificate: `scep_renew 0`
4. Overwrite the old certificate with the new one: `mv /wfs/scep-certificates/cert0/clientnew.cert /wfs/scep-certificates/cert0/client.cert`
5. Overwrite the old key with the new one: `mv /wfs/scep-certificates/cert0/clientnew.key /wfs/scep-certificates/cert0/client.key`

## 2.19.2 Deploying Trusted Root Certificates

### Purpose

IGEL OS comes with a number of trusted root certificates from certain Certificate Authorities (CA) pre-installed. For a complete list of pre-installed root certificates, see [Which CA Certificates Are Contained in IGEL OS?](#)(see page 474).

Certificates signed with these root certificates can be used for server authentication and encryption in ICA, RDP, Horizon and browser sessions. You can also verify the origin of Java applications.

Nevertheless, the root certificate you need might be missing. This document explains how to load and distribute it.

### Requirements

The certificates must be available in the Base64 file format encoded with the file extension `.pem`, `.crt` or `.cer`.

To check the file format, open the certificate with a text editor. It should look like this:

```
-----BEGIN CERTIFICATE-----
MIIDWzCCAk0gAwIBAgIQA64BW7UV06dG
MRQwEgYKCZImizPyLGQBGRYEdGVzdDETI
...
3iNjPsZgHJs9LmHM9mmmy5q29z8B0GZUJl
JUzn3SvfZTu2SXW+DXH9MdQPZvDCeMyx
-----END CERTIFICATE-----
```

### Solution

We advise you to use the following file transfer types for distributing the certificates via the UMS; see also [Registering a File on the UMS Server](#)<sup>179</sup>:

Type	To be used for

<sup>179</sup> <https://kb.igel.com/display/endpointmgmt/Registering+a+file+on+the+UMS+server>



Undefined	All-purpose class, you need to set the owner and access permissions manually.
Web Browser Certificate	Server authentication/encryption of HTTPS websites in browsers
SSL Certificate	Server authentication/encryption in ICA, RDP or Horizon sessions  Authentication via Active Directory (AD)
Java Certificate	Authentication/encryption for Java applications
IBM iAccess Certificate	Server authentication/encryption for IBM iAccess sessions
Common Certificate (all-purpose)	Multiple applications needing a certificate, e.g. if you want to launch an ICA session in a browser, or if you want to secure a Java session on a secure website.

With these file transfer types, you will not need to reboot after installing.

- [Deploying Certificates via UMS](#)(see page 471)
- [Installing Certificates Manually](#)(see page 472)

## Deploying Certificates via UMS

We advise you to use the Universal Management Suite for deploying certificates when you have a certain number of clients to be addressed.

Certificates can be deployed via the UMS in two steps:

- [Loading Certificates in the UMS](#)(see page 471)
- [Assigning Certificates to IGEL Thin Clients](#)(see page 472)

### Loading Certificates in the UMS

1. Open the **UMS console**.
2. Right-click **Files**.
3. Choose **New file** to open the **New file** mask.
4. Activate **Upload local file to UMS server**.
5. Browse your new certificate file under **Local file**.
6. Select the suitable **Classification** of the certificate under **File target**.



## 7. Confirm with **OK**.

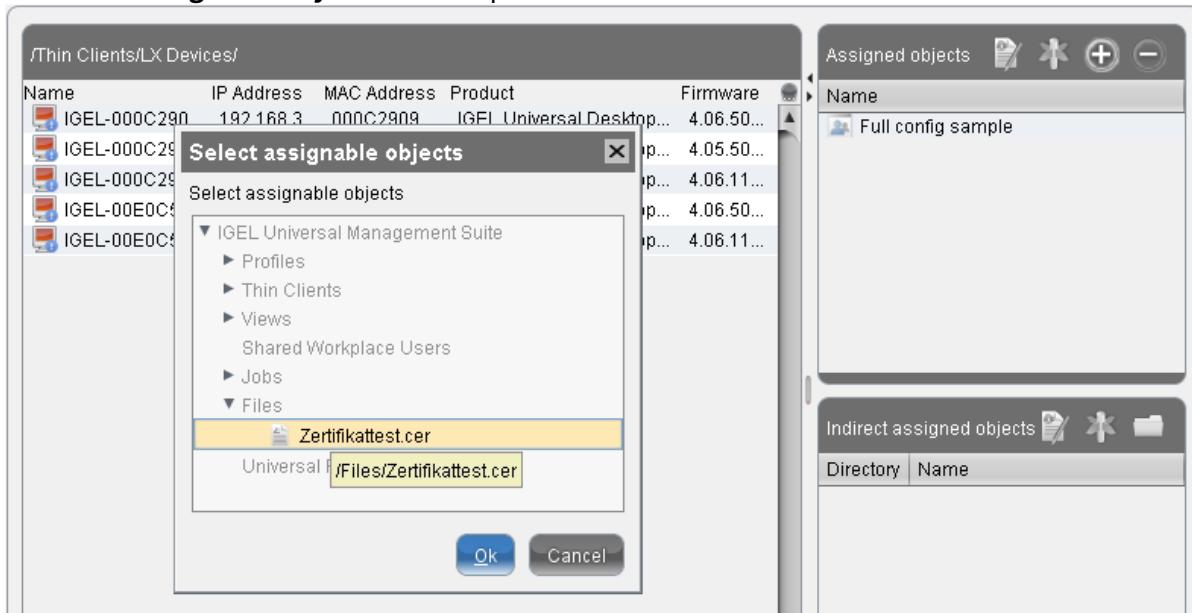
Your certificate is now listed in the **Files** window.

### Assigning Certificates to IGEL Thin Clients

After integrating the new certificates, you distribute them to the thin clients:

1. Choose one thin client or a group of thin clients in the UMS tree.
2. Click **Add** under **Assigned objects**.

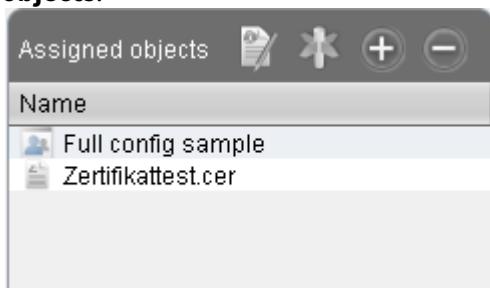
The **Select assignable object** window opens.



3. Select the new certificate and confirm by clicking on **OK**.

4. Select the **Update time** and confirm by clicking on **OK**.

The new certificate is now assigned to every thin client of the group and is listed under **Assigned objects**.



### Installing Certificates Manually

Use the **Firefox Certificate Manager** in order to install web browser certificates; see [Installing Web Browser Certificates](#)(see page 473).

Also a USB flash drive can be used for the manual import.



- Importing SSL Certificates (ICA, RDP, Horizon) (see page 473)
- Installing Web Browser Certificates (see page 473)

### Importing SSL Certificates (ICA, RDP, Horizon)

If a CA certificate is missing for *RDP*, *ICA* or *Horizon*, you can copy it from a USB storage device to the thin client:

1. Connect your USB storage device to the thin client.
2. Launch a **Terminal** session or press [CTRL]+[ALT]+[F11] to log in as **ROOT** on the Linux console of the thin client.
3. Create a directory for certificates:  
`mkdir /wfs/ca-certs`
4. Change to the directory:  
`cd /wfs/ca-certs`
5. Get the name of your USB storage device:  
`ls /userhome/media`
6. Copy the certificate to the client:  
`cp /userhome/media// /wfs/ca-certs`
7. Check whether the certificate was transferred:  
`ls -al /wfs/ca-certs`
8. End the terminal session or press [CTRL]+[ALT]+[F1] to exit the console.

The certificates you have saved will be available when you boot up the thin client next time.

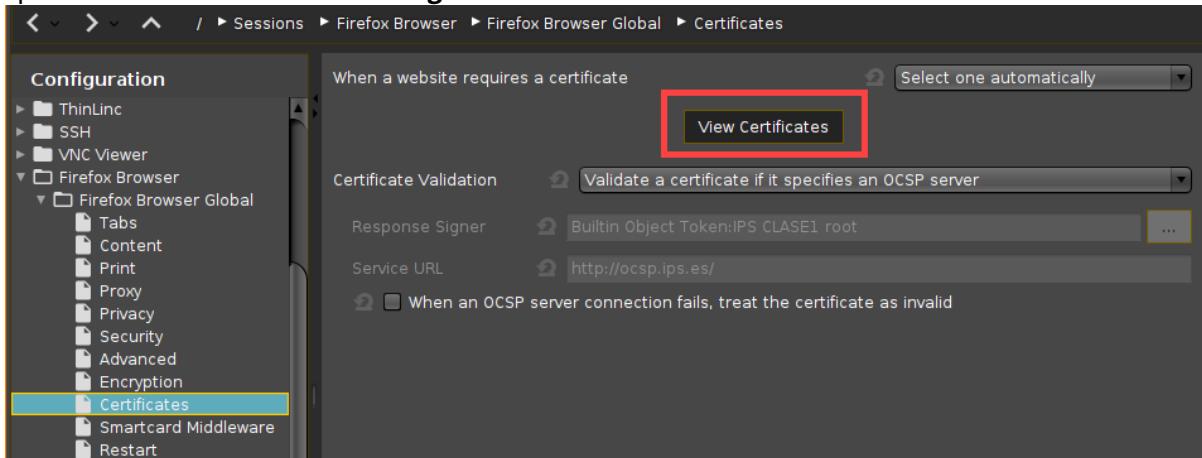
### Installing Web Browser Certificates

Installing web browser certificates manually:

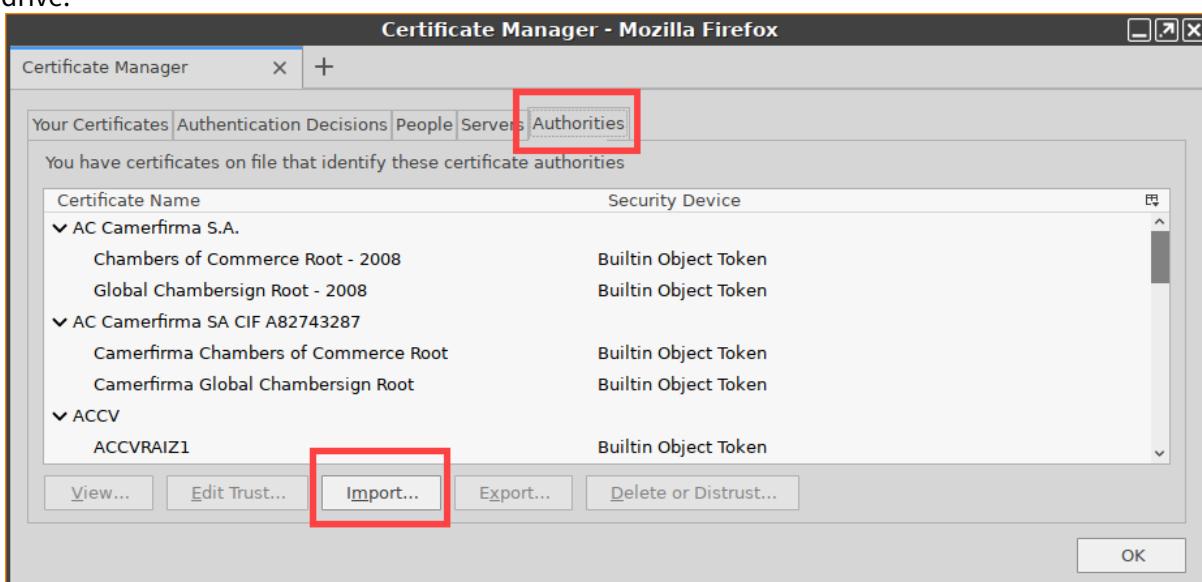
1. Open the IGEL Setup.



2. Click **Sessions > Firefox Browser > Firefox Browser Global > Certificates > View Certificates** to open the **Firefox Certificate Manager**.



3. Click **Import...** in the **Authorities** tab to import a new certificate from a directory or a USB flash drive.



Manually installed certificates will be saved permanently without any further configuration.

### 2.19.3 Which CA Certificates Are Contained in IGEL OS?

The following CA certificates are contained in IGEL OS 11.06.100:

Certificate name	Expiry date	File in /etc/ssl/certs
ACCVRAIZ1	Dec 31 09:37:37 2030 GMT	ACCVRAIZ1.crt



Certificate name	Expiry date	File in /etc/ssl/certs
AC RAIZ FNMT-RCM	Jan 1 00:00:00 2030 GMT	AC_RAIZ_FNMT-RCM.crt
Actalis Authentication Root CA	Sep 22 11:22:02 2030 GMT	Actalis_Authentication_Ro ot_CA.crt
AffirmTrust Commercial	Dec 31 14:06:06 2030 GMT	AffirmTrust_Commercial.c rt
AffirmTrust Networking	Dec 31 14:08:24 2030 GMT	AffirmTrust_Networking.c rt
AffirmTrust Premium	Dec 31 14:10:36 2040 GMT	AffirmTrust_Premium.crt
AffirmTrust Premium ECC	Dec 31 14:20:24 2040 GMT	AffirmTrust_Premium_ECC.c rt
Amazon Root CA 1	Jan 17 00:00:00 2038 GMT	AmazonRootCA1.pem)
Amazon Root CA 1	Jan 17 00:00:00 2038 GMT	Amazon_Root_CA_1.crt
Amazon Root CA 2	May 26 00:00:00 2040 GMT	Amazon_Root_CA_2.crt
Amazon Root CA 3	May 26 00:00:00 2040 GMT	Amazon_Root_CA_3.crt
Amazon Root CA 4	May 26 00:00:00 2040 GMT	Amazon_Root_CA_4.crt
Atos TrustedRoot 2011	Dec 31 23:59:59 2030 GMT	Atos_TrustedRoot_2011.crt
Autoridad de Certificacion Firmaprofesional CIF A62634068	Dec 31 08:38:15 2030 GMT	Autoridad_de_Certificacio n_Firmaprofesional_CIF_A6 2634068.crt
Baltimore CyberTrust Root	May 12 23:59:00 2025 GMT	BTCTRoot.pem)
Baltimore CyberTrust Root	May 12 23:59:00 2025 GMT	Baltimore_CyberTrust_Root .crt
Buypass Class 2 Root CA	Oct 26 08:38:03 2040 GMT	Buypass_Class_2_Root_CA.c rt



Certificate name	Expiry date	File in /etc/ssl/certs
Bypass Class 3 Root CA	Oct 26 08:28:58 2040 GMT	Bypass_Class_3_Root_CA.crt
CA Disig Root R2	Jul 19 09:15:30 2042 GMT	CA_Disig_Root_R2.crt
CFCA EV ROOT	Dec 31 03:07:01 2029 GMT	CFCA_EV_ROOT.crt
COMODO Certification Authority	Dec 31 23:59:59 2029 GMT	COMODO_Certification_Authority.crt
COMODO ECC Certification Authority	Jan 18 23:59:59 2038 GMT	COMODO_ECC_Certification_Authority.crt
COMODO RSA Certification Authority	Jan 18 23:59:59 2038 GMT	COMODO_RSA_Certification_Authority.crt
Certigna	Jun 29 15:13:05 2027 GMT	Certigna.crt
Certigna Root CA	Oct 1 08:32:27 2033 GMT	Certigna_Root_CA.crt
Certum Trusted Network CA	Dec 31 12:07:37 2029 GMT	Certum_Trusted_Network_CA.crt
Certum Trusted Network CA 2	Oct 6 08:39:56 2046 GMT	Certum_Trusted_Network_CA_2.crt
Chambers of Commerce Root - 2008	Jul 31 12:29:50 2038 GMT	Chambers_of_Commerce_Root_-_2008.crt
Class 3 Public Primary Certification Authority - G2 (c) 1998 VeriSign, Inc. - For authorized use only VeriSign Trust Network	Aug 1 23:59:59 2028 GMT	Class3PCA_G2_v2.pem)
Class 4 Public Primary Certification Authority - G2 (c) 1998 VeriSign, Inc. - For authorized use only VeriSign Trust Network	Aug 1 23:59:59 2028 GMT	Class4PCA_G2_v2.pem)
AAA Certificate Services	Dec 31 23:59:59 2028 GMT	Comodo_AAA_Services_root.crt



<b>Certificate name</b>	<b>Expiry date</b>	<b>File in /etc/ssl/certs</b>
Cybertrust Global Root	Dec 15 08:00:00 2021 GMT	Cybertrust_Global_Root.crt
D-TRUST Root Class 3 CA 2 2009	Nov 5 08:35:58 2029 GMT	D- TRUST_Root_Class_3_CA_2_2 009.crt
D-TRUST Root Class 3 CA 2 EV 2009	Nov 5 08:50:46 2029 GMT	D- TRUST_Root_Class_3_CA_2_E V_2009.crt
DST Root CA X3	Sep 30 14:01:15 2021 GMT	DST_Root_CA_X3.crt
DigiCert Global Root CA	Nov 10 00:00:00 2031 GMT	DigiCertGlobalRootCA.pem)
DigiCert Global Root CA	Mar 8 12:00:00 2023 GMT	DigiCertSHA2SecureServerC A.pem)
DigiCert Assured ID Root CA	Nov 10 00:00:00 2031 GMT	DigiCert_Assured_ID_Root_ CA.crt
DigiCert Assured ID Root G2	Jan 15 12:00:00 2038 GMT	DigiCert_Assured_ID_Root_ G2.crt
DigiCert Assured ID Root G3	Jan 15 12:00:00 2038 GMT	DigiCert_Assured_ID_Root_ G3.crt
DigiCert Global Root CA	Nov 10 00:00:00 2031 GMT	DigiCert_Global_Root_CA.c rt
DigiCert Global Root G2	Jan 15 12:00:00 2038 GMT	DigiCert_Global_Root_G2.c rt
DigiCert Global Root G3	Jan 15 12:00:00 2038 GMT	DigiCert_Global_Root_G3.c rt
DigiCert High Assurance EV Root CA	Nov 10 00:00:00 2031 GMT	DigiCert_High_Assurance_E V_Root_CA.crt



Certificate name	Expiry date	File in /etc/ssl/certs
DigiCert Trusted Root G4	Jan 15 12:00:00 2038 GMT	DigiCert_Trusted_Root_G4.crt
E-Tugra Certification Authority	Mar 3 12:09:48 2023 GMT	E-Tugra_Certification_Authority.crt
EC-ACC	Jan 7 22:59:59 2031 GMT	EC-ACC.crt
Entrust.net <sup>180</sup> Certification Authority (2048)	Jul 24 14:15:12 2029 GMT	Entrust.net_Premium_2048_Secure_Server_CA.crt
Entrust Root Certification Authority	Nov 27 20:53:42 2026 GMT	Entrust_Root_Certification_Authority.crt
Entrust Root Certification Authority - EC1	Dec 18 15:55:36 2037 GMT	Entrust_Root_Certification_Authority--EC1.crt
Entrust Root Certification Authority - G2	Dec 7 17:55:54 2030 GMT	Entrust_Root_Certification_Authority--G2.crt
Entrust Root Certification Authority - G4	Dec 27 11:41:16 2037 GMT	Entrust_Root_Certification_Authority--G4.crt
GDCA TrustAUTH R5 ROOT	Dec 31 15:59:59 2040 GMT	GDCA_TrustAUTH_R5_ROOT.crt
GlobalSign	Dec 15 08:00:00 2021 GMT	GSR2.pem)
GTE CyberTrust Global Root	Aug 13 23:59:00 2018 GMT	GTECTGlobalRoot.pem)
GTS Root R1	Jun 22 00:00:00 2036 GMT	GTS_Root_R1.crt
GTS Root R2	Jun 22 00:00:00 2036 GMT	GTS_Root_R2.crt
GTS Root R3	Jun 22 00:00:00 2036 GMT	GTS_Root_R3.crt
GTS Root R4	Jun 22 00:00:00 2036 GMT	GTS_Root_R4.crt

<sup>180</sup> <http://Entrust.net>



<b>Certificate name</b>	<b>Expiry date</b>	<b>File in /etc/ssl/certs</b>
GeoTrust Global CA	May 21 04:00:00 2022 GMT	GeoTrust_Global_CA.pem)
GeoTrust Primary Certification Authority - G2	Jan 18 23:59:59 2038 GMT	GeoTrust_Primary_Certification_Authority_-_G2.crt
GlobalSign	Jan 19 03:14:07 2038 GMT	GlobalSign_ECC_Root_CA_-_R4.crt
GlobalSign	Jan 19 03:14:07 2038 GMT	GlobalSign_ECC_Root_CA_-_R5.crt
GlobalSign Root CA	Jan 28 12:00:00 2028 GMT	GlobalSign_Root_CA.crt
GlobalSign	Dec 15 08:00:00 2021 GMT	GlobalSign_Root_CA_-_R2.crt
GlobalSign	Mar 18 10:00:00 2029 GMT	GlobalSign_Root_CA_-_R3.crt
GlobalSign	Dec 10 00:00:00 2034 GMT	GlobalSign_Root_CA_-_R6.crt
Global Chambersign Root - 2008	Jul 31 12:31:40 2038 GMT	Global_Chambersign_Root_-_2008.crt
Go Daddy Class 2 Certification Authority	Jun 29 17:06:20 2034 GMT	Go_Daddy_Class_2_CA.crt
Go Daddy Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	Go_Daddy_Root_Certificate_Authority_-_G2.crt
Hellenic Academic and Research Institutions ECC RootCA 2015	Jun 30 10:37:12 2040 GMT	Hellenic_Academic_and_Research_Institutions_ECC_RootCA_2015.crt
Hellenic Academic and Research Institutions RootCA 2011	Dec 1 13:49:52 2031 GMT	Hellenic_Academic_and_Research_Institutions_RootCA_2011.crt



Certificate name	Expiry date	File in /etc/ssl/certs
Hellenic Academic and Research Institutions RootCA 2015	Jun 30 10:11:21 2040 GMT	Hellenic_Academic_and_Research_Institutions_RootCA_2015.crt
Hongkong Post Root CA 1	May 15 04:52:29 2023 GMT	Hongkong_Post_Root_CA_1.crt
Hongkong Post Root CA 3	Jun 3 02:29:46 2042 GMT	Hongkong_Post_Root_CA_3.crt
ISRG Root X1	Jun 4 11:04:38 2035 GMT	ISRG_Root_X1.crt
IdenTrust Commercial Root CA 1	Jan 16 18:12:23 2034 GMT	IdenTrust_Commercial_Root_CA_1.crt
IdenTrust Public Sector Root CA 1	Jan 16 17:53:32 2034 GMT	IdenTrust_Public_Sector_Root_CA_1.crt
Imprivata Embedded Code Signing CA	Sep 7 16:20:00 2033 GMT	Imprivata.crt
Izenpe.com <sup>181</sup>	Dec 13 08:27:25 2037 GMT	Izenpe.com <sup>182</sup> .crt
Microsec e-Szigno Root CA 2009	Dec 30 11:30:18 2029 GMT	Microsec_e-Szigno_Root_CA_2009.crt
Microsoft ECC Root Certificate Authority 2017	Jul 18 23:16:04 2042 GMT	Microsoft_ECC_Root_Certificate_Authority_2017.crt
Microsoft RSA Root Certificate Authority 2017	Jul 18 23:00:23 2042 GMT	Microsoft_RSA_Root_Certificate_Authority_2017.crt
NAVER Global Root Certification Authority	Aug 18 23:59:59 2037 GMT	NAVER_Global_Root_Certification_Authority.crt
NetLock Arany (Class Gold) FÅ'tanÃºsÃtvÃ¡ny	Dec 6 15:08:21 2028 GMT	NetLock_Arany_=Class_Gold=_FÅ'tanÃºsÃtvÃ¡ny.crt

<sup>181</sup> <http://Izenpe.com><sup>182</sup> <http://Izenpe.com>



Certificate name	Expiry date	File in /etc/ssl/certs
Network Solutions Certificate Authority	Dec 31 23:59:59 2029 GMT	Network_Solutions_Certificate_Authority.crt
OISTE WISEKey Global Root GB CA	Dec 1 15:10:31 2039 GMT	OISTE_WISEKey_Global_Root_GB_CA.crt
OISTE WISEKey Global Root GC CA	May 9 09:58:33 2042 GMT	OISTE_WISEKey_Global_Root_GC_CA.crt
Class 3 Public Primary Certification Authority	Aug 1 23:59:59 2028 GMT	Pcs3ss_v4.pem)
QuoVadis Root Certification Authority	Mar 17 18:33:33 2021 GMT	QuoVadis_Root_CA.crt
QuoVadis Root CA 1 G3	Jan 12 17:27:44 2042 GMT	QuoVadis_Root_CA_1_G3.crt
QuoVadis Root CA 2	Nov 24 18:23:33 2031 GMT	QuoVadis_Root_CA_2.crt
QuoVadis Root CA 2 G3	Jan 12 18:59:32 2042 GMT	QuoVadis_Root_CA_2_G3.crt
QuoVadis Root CA 3	Nov 24 19:06:44 2031 GMT	QuoVadis_Root_CA_3.crt
QuoVadis Root CA 3 G3	Jan 12 20:26:32 2042 GMT	QuoVadis_Root_CA_3_G3.crt
SSL.com <sup>183</sup> EV Root Certification Authority ECC	Feb 12 18:15:23 2041 GMT	SSL.com_EV_Root_Certification_Authority_ECC.crt
SSL.com <sup>184</sup> EV Root Certification Authority RSA R2	May 30 18:14:37 2042 GMT	SSL.com_EV_Root_Certification_Authority_RSA_R2.crt
SSL.com <sup>185</sup> Root Certification Authority ECC	Feb 12 18:14:03 2041 GMT	SSL.com_Root_Certification_Authority_ECC.crt
SSL.com <sup>186</sup> Root Certification Authority RSA	Feb 12 17:39:39 2041 GMT	SSL.com_Root_Certification_Authority_RSA.crt
SZAFIR ROOT CA2	Oct 19 07:43:30 2035 GMT	SZAFIR_ROOT_CA2.crt

<sup>183</sup> <http://SSL.com><sup>184</sup> <http://SSL.com><sup>185</sup> <http://SSL.com><sup>186</sup> <http://SSL.com>



Certificate name	Expiry date	File in /etc/ssl/certs
SecureSign RootCA11	Apr 8 04:56:47 2029 GMT	SecureSign_RootCA11.crt
SecureTrust CA	Dec 31 19:40:55 2029 GMT	SecureTrust_CA.crt
Secure Global CA	Dec 31 19:52:06 2029 GMT	Secure_Global_CA.crt
Security Communication RootCA2	May 29 05:00:39 2029 GMT	Security_Communication_Ro otCA2.crt
Security Communication RootCA1	Sep 30 04:20:49 2023 GMT	Security_Communication_Ro ot_CA.crt
Sonera Class2 CA	Apr 6 07:29:40 2021 GMT	Sonera_Class_2_Root_CA.cr t
Staat der Nederlanden EV Root CA	Dec 8 11:10:28 2022 GMT	Staat_der_Nederlanden_EV _Root_CA.crt
Staat der Nederlanden Root CA - G3	Nov 13 23:00:00 2028 GMT	Staat_der_Nederlanden_Roo t_CA_-_G3.crt
Starfield Class 2 Certification Authority	Jun 29 17:39:16 2034 GMT	Starfield_Class_2_CA.crt
Starfield Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	Starfield_Root_Certificat e_Authority_-_G2.crt
Starfield Services Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	Starfield_Services_Root_C ertificate_Authority_-_ G2.crt
SwissSign Gold CA - G2	Oct 25 08:30:35 2036 GMT	SwissSign_Gold_CA_- _G2.crt
SwissSign Silver CA - G2	Oct 25 08:32:46 2036 GMT	SwissSign_Silver_CA_- _G2.crt
T-TeleSec GlobalRoot Class 2	Oct 1 23:59:59 2033 GMT	T- TeleSec_GlobalRoot_Class _2.crt



Certificate name	Expiry date	File in /etc/ssl/certs
T-TeleSec GlobalRoot Class 3	Oct 1 23:59:59 2033 GMT	T- TeleSec_GlobalRoot_Class_3.crt
TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1	Oct 25 08:25:55 2043 GMT	TUBITAK_Kamu_SM_SSL_Kok_Sertifikasi_-_Surum_1.crt
TWCA Global Root CA	Dec 31 15:59:59 2030 GMT	TWCA_Global_Root_CA.crt
TWCA Root Certification Authority	Dec 31 15:59:59 2030 GMT	TWCA_Root_Certification_Authority.crt
TeliaSonera Root CA v1	Oct 18 12:00:50 2032 GMT	TeliaSonera_Root_CA_v1.crt
TrustCor ECA-1	Dec 31 17:28:07 2029 GMT	TrustCor_ECA-1.crt
TrustCor RootCert CA-1	Dec 31 17:23:16 2029 GMT	TrustCor_RootCert_CA-1.crt
TrustCor RootCert CA-2	Dec 31 17:26:39 2034 GMT	TrustCor_RootCert_CA-2.crt
Trustis FPS Root CA	Jan 21 11:36:54 2024 GMT	Trustis_FPS_Root_CA.crt
Trustwave Global Certification Authority	Aug 23 19:34:12 2042 GMT	Trustwave_Global_Certification_Authority.crt
Trustwave Global ECC P256 Certification Authority	Aug 23 19:35:10 2042 GMT	Trustwave_Global_ECC_P256_Certification_Authority.crt
Trustwave Global ECC P384 Certification Authority	Aug 23 19:36:43 2042 GMT	Trustwave_Global_ECC_P384_Certification_Authority.crt
UCA Extended Validation Root	Dec 31 00:00:00 2038 GMT	UCA_Extended_Validation_Root.crt
UCA Global G2 Root	Dec 31 00:00:00 2040 GMT	UCA_Global_G2_Root.crt



Certificate name	Expiry date	File in /etc/ssl/certs
USERTrust ECC Certification Authority	Jan 18 23:59:59 2038 GMT	USERTrust_ECC_Certification_Authority.crt
USERTrust RSA Certification Authority	Jan 18 23:59:59 2038 GMT	USERTrust_RSA_Certification_Authority.crt
VeriSign Universal Root Certification Authority	Dec 1 23:59:59 2037 GMT	VeriSign_Universal_Root_Certification_Authority.crt
XRamp Global Certification Authority	Jan 1 05:37:19 2035 GMT	XRamp_Global_CA_Root.crt
certSIGN ROOT CA	Jul 4 17:20:04 2031 GMT	certSIGN_ROOT_CA.crt
certSIGN ROOT CA G2	Feb 6 09:27:35 2042 GMT	certSIGN_Root_CA_G2.crt
e-Szigno Root CA 2017	Aug 22 12:07:06 2042 GMT	e-Szigno_Root_CA_2017.crt
ePKI Root Certification Authority	Dec 20 02:31:27 2034 GMT	ePKI_Root_Certification_Authority.crt
emSign ECC Root CA - C3	Feb 18 18:30:00 2043 GMT	emSign_ECC_Root_CA_-_C3.crt
emSign ECC Root CA - G3	Feb 18 18:30:00 2043 GMT	emSign_ECC_Root_CA_-_G3.crt
emSign Root CA - C1	Feb 18 18:30:00 2043 GMT	emSign_Root_CA_-_C1.crt
emSign Root CA - G1	Feb 18 18:30:00 2043 GMT	emSign_Root_CA_-_G1.crt

## 2.20 Smartcard

- Authentication with IGEL Smartcard (see page 485)
- Smartcard Authentication (see page 492)



## 2.20.1 Authentication with IGEL Smartcard

Smartcards make the user experience more convenient by providing a single device that supports multiple authentication products across the enterprise. The user only has to remember a single PIN that unlocks the smart card to access the network.

### Prerequisites

Before using the IGEL smartcard, the relevant profiles and session information need to be written to the smartcard. We describe a best practice way of how to proceed. The names of folders and profiles are only examples and can be changed individually.

It is useful to use following folders and profiles on the Universal Management Suite (UMS):

Folder	Profile	Purpose
Smartcard Creation		Folder for devices which will be used for smartcard creation.
	Smartcard Key	This profile will apply the defined company key to the devices. This key will be written while creating the IGEL smartcard.
Smartcard Operation		Folder for devices whose authentication process will work only via IGEL smartcard.
	Smartcard Login	This profile will apply the company key to the devices and will activate the login with IGEL smartcard.

- ▶ Create two folders under **Profiles** in the Universal Management Suite (UMS), e.g. "Smartcard Operation" and "Smartcard Creation".
- ▶ Create the profile "Smartcard Login" for "Smartcard Operation".
- ▶ Create the profile "Smartcard Key" for "Smartcard Creation".

- 
- [Creating IGEL Smartcard Folders](#)(see page 486)
  - [Folder "Smartcard Operation"](#)(see page 486)
  - [Folder "Smartcard Creation"](#)(see page 487)
  - [Writing the IGEL Smartcard](#)(see page 487)

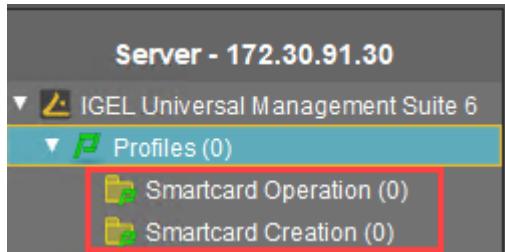


- Smartcard Readers Supported by IGEL Smartcards(see page 491)

## Creating IGEL Smartcard Folders

First, add two new profile folders for creating profiles and assigning them to devices:

- "Smartcard Operation";
- "Smartcard Creation".



### Folder "Smartcard Operation"

In this folder, you create a new profile "Smartcard Login":

1. Right-click the folder "Smartcard Operation".
2. Choose **New Profile**.
3. Enter a **Profile Name**, e.g. "Smartcard Login".
4. Click **Security > Logon > IGEL Smartcard**.
5. Enable **Login with IGEL smartcard**.
6. Enter your **Company key**.

Later on, this profile will be applied to all devices where the authentication process shall work only with a smartcard.

This way, the device will receive:

- the company key and
- the information that the authentication is only possible with the smartcard.

The company key is a private key shared between devices and smartcards. It should be chosen similarly to a good password. If the smartcard does not hold the same company key as the device, authentication will not be possible. Remember this company key because you will need later to write exactly the same key to the smartcard.

## Folder "Smartcard Creation"

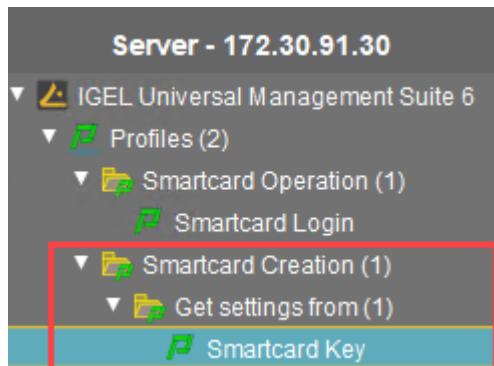
In this folder, you create a new profile "Smartcard Key":

1. Right-click the folder "Smartcard Creation".
2. Choose **New Profile**.
3. Enter a profile name, e.g. "Smartcard Key".
4. Click **Security > Logon > IGEL Smartcard**.
5. Enter the same **Company key** as in the profile "Smartcard Login".

Another additional folder is useful:

- Create the subfolder "Get settings from" under "Smartcard Creation".

In this folder, you create the profile with the session information you want to write to the smartcard.



You need this additional folder because the assignment of active profiles from the UMS to the IGEL smartcard can cause problems (firmware version < 5.06.100). Later on, you will copy the folder locally to your device.

## Writing the IGEL Smartcard

### Assigning the Profile "Smartcard Creation" to the Device

1. Prepare one device which has a smartcard reader/writer.
  2. Integrate this device in the UMS and put it into the folder "Smartcard Creation".
- Now the device automatically receives the company key from the profile. It will be used when writing the smartcard.



## Ensuring That the Profile Assignment Was Successful

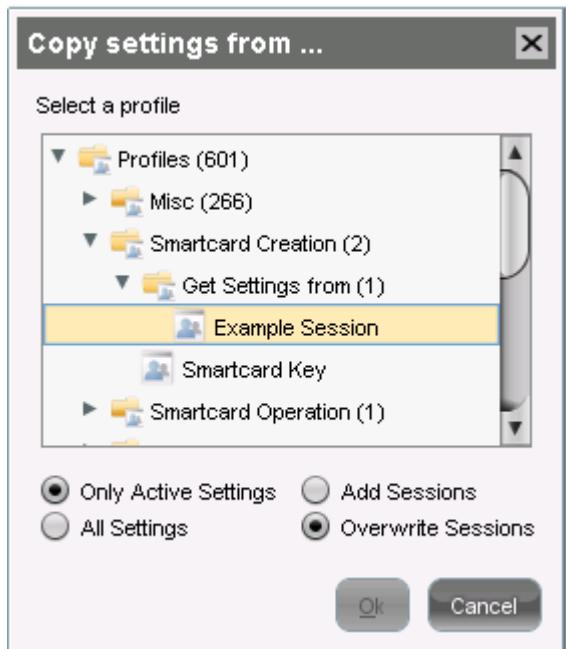
1. Open the local setup of your device.
2. Click **Security > Logon > IGEL Smartcard**.

You should now see a disabled field **Company key** with a lock symbol.

A screenshot of the IGEL local setup interface. The left sidebar shows a tree view with "Configuration" selected, followed by "Sessions", "Accessories", "User Interface", "Network", "Devices", and "Security". Under "Security", there are "Password", "Logon", and "Smartcard". "Smartcard" is expanded, showing "IGEL Smartcard" (selected), "Active Directory/Kerberos", "Auto Logoff", and "Active Directory/Kerberos". The main panel shows three icons: "IGEL Smartcard" (selected), "Active Directory/Kerberos", and "Auto Logoff". Below the icons are two checkboxes: "Login with IGEL Smart Card" and "Enable IGEL Smart Card without Locking Desktop". A "Company Key" field contains "\*\*\*\*\*" and has a lock icon. A button at the bottom says "Start application to write IGEL Smart Cards:" and a "Smart Card Personalization" button.

## Writing the Profiles to the Smartcard

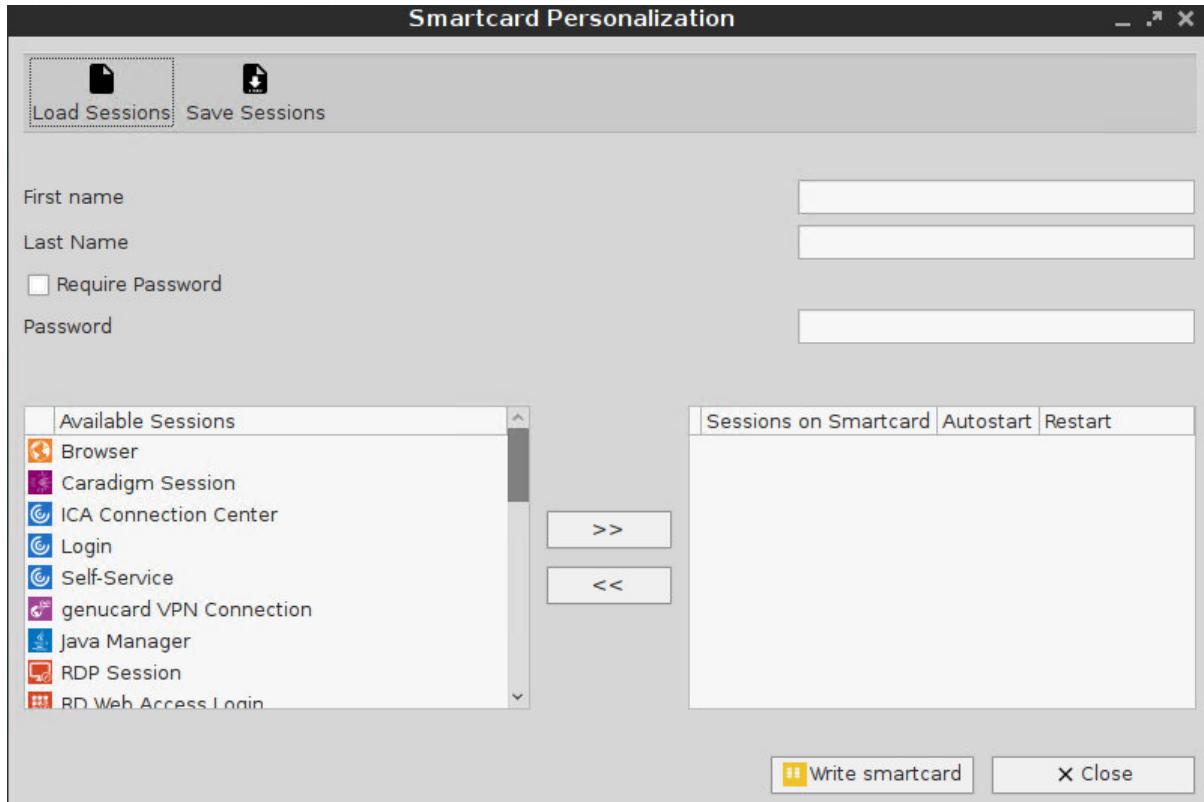
1. Open the folder "Smartcard Creation" in the UMS.
2. Right-click your device.
3. Choose **Take over settings from...** to copy the profile settings to the device.  
The dialog **Copy settings from...** opens.
4. Choose your profile from the folder "Smartcard Creation" > "Get settings from".
5. Enable **Overwrite Sessions**.



6. Click **OK** to copy the profile with the settings and the company key to the device.

#### Writing the Smartcard

1. Open the local setup of your device.
2. Click **Security > Logon > IGEL Smartcard**.
3. Click **Smartcard personalization**.  
The **Smartcard personalization** dialog opens.



4. Enter the **First name** and the **Last name** of the smartcard holder that should appear at the login prompt.
5. Activate **Require password** and specify the **Password** if a password has to be required for the smartcard login.
6. Select the local sessions you want to write to the smartcard.

Use the arrow buttons to add a session to the smartcard session list.

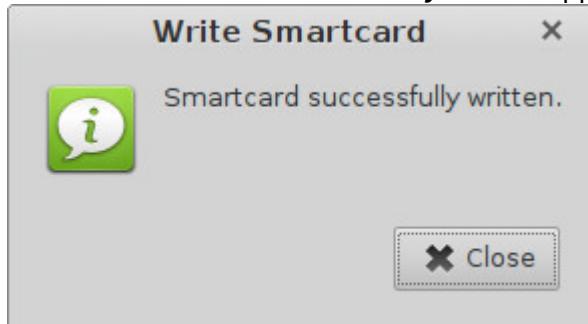
7. Activate **Autostart** for a session in the smartcard list if it should be automatically started at login. Check **Restart** if desired.

The configuration of the sessions can be saved and reloaded at a later time.

8. Click **Write smartcard** to start the writing process with the defined settings.
9. Confirm the security question with **Yes**.



The notice **Smartcard successfully written** appears.



## Testing the New IGEL Smartcard

1. Go to the UMS.
2. Register a new device in the UMS and put it in the folder "Smartcard Operation".  
The device gets the company key and the profile information that authentication is only possible with the IGEL smartcard.
3. Restart the device.  
The **Insert Smartcard...** dialog opens.
4. Insert the IGEL smartcard into your device and verify the selected configuration.

## Smartcard Readers Supported by IGEL Smartcards

IGEL smartcards are supported by the following third-party smartcard readers:

- OMNIKEY CardMan 3111
- OMNIKEY CardMan 3x21
- OMNIKEY CardMan 3621
- OMNIKEY CardMan 6121
- OMNIKEY CardMan 3821
- USB CCID Smart Card Reader
- USB CCID Smart Card Reader Keyboard
- Fujitsu Siemens Computers SmartCard-Reader USB 2A
- Fujitsu Siemens Computers SmartCard-Reader Keyboard USB 2A
- Fujitsu Siemens Computers SmartCard-Reader USB 2C
- Cherry SmartBoard XX44
- OMNIKEY CardMan 5121



- OMNIKEY CardMan 5x21
- HID Global OMNIKEY 3x21 Smart Card Reader
- Cherry KC 1000 SC
- Cherry KC 1000 SC/DI
- Cherry KC 1000 SC Z
- Cherry KC 1000 SC/DI Z
- Cherry SmartTerminal XX44 v2
- Cherry SmartTerminal XX44
- OMNIKEY CardMan
- CCID SC Reader
- Cherry SC Reader.

## 2.20.2 Smartcard Authentication

### Certificate Authentication

The smartcards discussed here can hold digital certificates (x.509) and corresponding private keys. The private key cannot be read from the card, but it can be used by the card itself for signing and decryption of data.

This enables the use of what is known as two-factor authentication: the user not only possesses the smartcard, he or she can also prove the knowledge of the smartcard PIN by signing data using the private key stored on the smartcard.

If you want to use Active Directory (AD), the certificate chain used by the key distribution center (domain controller) must be available on the device. For instructions on deploying certificate files, see [Registering a File on the UMS Server<sup>187</sup>](#) (set **Classification** to "SSL Certificate") and [Transferring a File to a Device<sup>188</sup>](#).

### Smartcard Readers

Smartcards are accessed via smartcard readers, using either a contact or contactless interface. The [IGEL Third Party Database<sup>189</sup>](#) lists the readers that are supported by the *Linux* firmware.

### PC/SC Resource Manager

The *PC/SC Resource Manager* is a common Application Programming Interface (API) that is available on *Windows* and *Linux* operating systems. It provides a standardized way for applications to handle smartcards and readers.

The *PC/SC Resource Manager* is active by default in the *Linux*-based firmware and can be controlled via the **Activate PC/SC Daemon** parameter on **IGEL Setup > Devices > Smartcard > PC/SC** or **IGEL Setup > Security > Smartcard > PC/SC** or **IGEL Setup > Security > Smartcard > Services** (depending on the firmware version).

---

<sup>187</sup> <https://kb.igel.com/display/endpointmgmt601/Registering+a+file+on+the+UMS+server>

<sup>188</sup> <https://kb.igel.com/display/endpointmgmt601/Transferring+a+file+to+a+device>

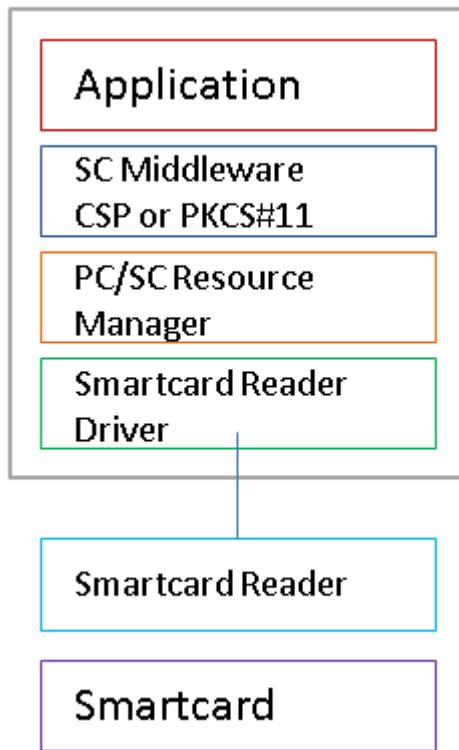
<sup>189</sup> <https://www.igel.com/linux-3rd-party-hardware-database/>

## Smartcard Middleware

In order to provide a generalized interface to different types of smartcard hardware, there is an additional software layer called smartcard middleware.

There are different types of middleware:

	Windows	Linux
<i>CSP, Cryptographic Service Provider</i>	✓	
<i>PKCS#11, Public-Key Cryptographic Standards</i>	✓	✓



Some of the smartcard authentication methods require *smartcard middleware* to be installed on the endpoint device. The following modules are available:

- Gemalto SafeNet
- cryptovision sc/interface
- Gemalto IDPrime
- Athena IDProtect
- A.E.T.SafeSign
- Secmaker Net iD
- Coolkey
- OpenSC



- 90meter

#### Licensed Feature

This feature requires an add-on license; see [Add-On Licenses](#)<sup>190</sup>. Please contact your IGEL sales representative.

For information on how to use a custom PKCS#11 library, refer to the article [Using a Custom PKCS#11 Library](#)(see page 588).

- Active Directory Logon with Smartcard(see page 494)
- Citrix StoreFront(see page 494)
- RDP Sessions(see page 495)
- Horizon Sessions(see page 496)
- Smartcard Authentication in Browser(see page 497)
- Local Login with Smartcard Certificate(see page 498)

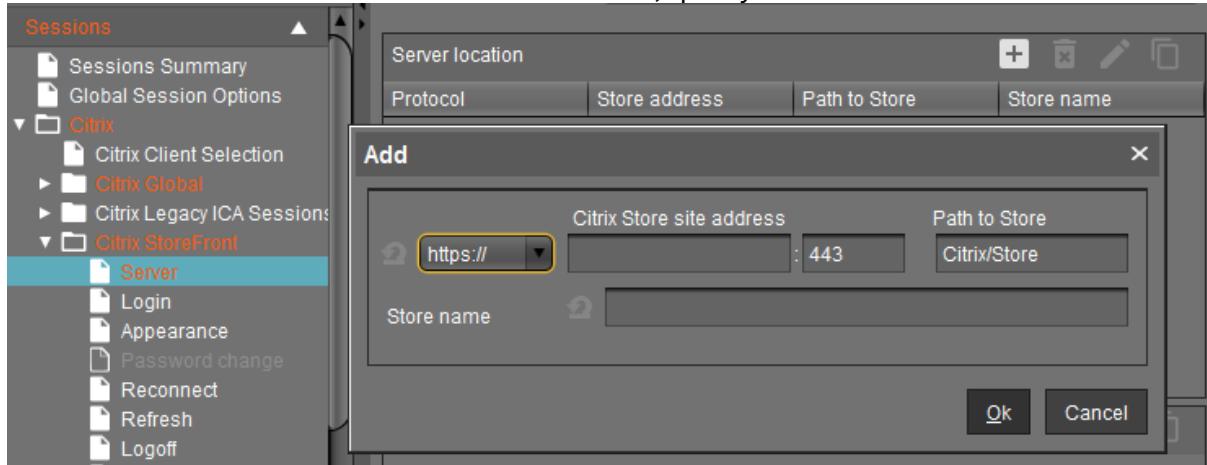
### Active Directory Logon with Smartcard

See the how-to [Passthrough Authentication](#)(see page 730).

### Citrix StoreFront

In this scenario, *Citrix Receiver 13.1* or newer is required. The root certificate of the web server certificate used by the *StoreFront* server has to be known as the trusted root certificate on the endpoint device - see [Deploying Trusted Root Certificates](#)(see page 470), **Certificate Type SSL Certificate**.

1. Under **Sessions > Citrix > Citrix StoreFront > Server**, specify the **Server location**.



2. Choose **Smartcard authentication** as **Authentication type** under **Sessions > Citrix > Citrix StoreFront > Login**.

<sup>190</sup> <https://kb.igel.com/display/licensesmoreigelos11/Add-on+Licenses>



When used in combination with **Active Directory Logon** the enabled **Use Passthrough authentication** activates single sign-on with smartcard.

3. Select the appropriate PKCS#11 module for the smartcard **Security > Smartcard > Middleware**.
  - Gemalto/SafeNet eToken
  - cryptovision sc/interface
  - Gemalto IDPrime
  - Athena IDProtect
  - A.E.T. SafeSign
  - Secmaker Net iD
  - 90meter

#### Licensed Feature

This feature requires an add-on license; see [Add-On Licenses](#)<sup>191</sup>. Please contact your IGEL sales representative.

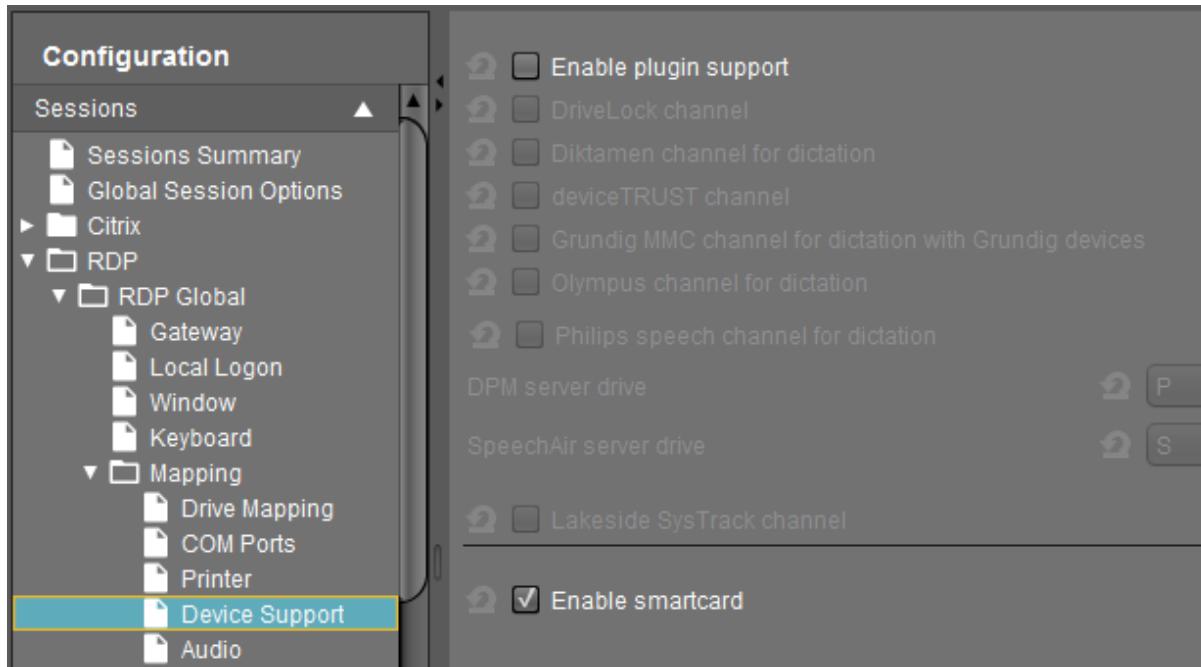
- Custom PKCS#11 module. See here also [Using a Custom PKCS#11 Library](#)(see page 588).

## RDP Sessions

In this scenario, the smartcard middleware has to be installed on the server side.

1. Enable **Activate PC/SC Daemon** under **Security > Smartcard > Services**.
2. Check **Enable Smartcard** under **Sessions > RDP > RDP Global > Mapping > Device Support**.

<sup>191</sup> <https://kb.igel.com/display/licensesmoreigelos11/Add-on+Licenses>



## Horizon Sessions

In this scenario, the smartcard middleware has to be installed on the virtual desktops as well as configured on the endpoint device side.

The View Connection Server has to be configured on the endpoint device side.

The View Connection Server has to be configured to accept connections via SSL/TLS secured https URLs. The root certificate of the certificate used for this service has to be known as the trusted root certificate on the thin client (see the how-to [Deploying Trusted Root Certificates](#)(see page 470), certificate type **SSL Certificate**).

1. Select the appropriate PKCS#11 support for the smartcard under **Sessions > Horizon Client > Horizon Client Global > Smartcard**.

- Gemalto/SafeNet eToken
- cryptovision sc/interface
- Gemalto IDPrime
- Athena IDProtect
- A.E.T. SafeSign
- Secmaker Net iD
- Coolkey
- OpenSC
- 90meter



#### Licensed Feature

This feature requires an add-on license; see [Add-On Licenses<sup>192</sup>](#). Please contact your IGEL sales representative.

For details on the custom PKCS#11 library, refer to the article [Using a Custom PKCS#11 Library\(see page 588\)](#).

2. Configure the **Server URL** under **Sessions > Horizon Client > Horizon Client Sessions > [session name] > Connection settings**.

Start the URL with https://!

## Smartcard Authentication in Browser

It is possible to authenticate using a smartcard at websites, e. g. *Citrix Web Interface* or *StoreFront*.

When connecting via an SSL/TLS secured https URL, the root certificate of the web server certificate has to be known as the **Trusted Root Certificate** on the endpoint device; see [Deploying Trusted Root Certificates\(see page 470\)](#), certificate types **Web Browser Certificate** and (!) **SSL Certificate**.

- ▶ Select the appropriate PKCS#11 module (security device) for the smartcard under **Sessions > Firefox Browser > Firefox Browser Global > Smartcard Middleware** or/and under **Sessions > Chromium Browser > Chromium Browser Global > Smartcard Middleware**.

- Gemalto/SafeNet eToken
- cryptovision sc/interface
- Gemalto IDPrime
- Athena IDProtect
- A.E.T. SafeSign
- Secmaker Net iD
- Coolkey
- OpenSC
- 90meter

#### Licensed Feature

This feature requires an add-on license; see [Add-On Licenses<sup>193</sup>](#). Please contact your IGEL sales representative.

For details on the custom PKCS#11 library, refer to the article [Using a Custom PKCS#11 Library\(see page 588\)](#).

<sup>192</sup> <https://kb.igel.com/display/licensesmoreigelos11/Add-on+Licenses>

<sup>193</sup> <https://kb.igel.com/display/licensesmoreigelos11/Add-on+Licenses>



## Local Login with Smartcard Certificate

### Overview

This is a method for local login at the endpoint device with a smartcard holding a certificate.

It can be used in two ways:

- As a standalone authentication method; see [Standalone Authentication Method\(see page 498\)](#)
- In combination with AD/Kerberos; see [Combination with the "AD/Kerberos with Smartcard" Method\(see page 505\)](#) (see also [Passthrough Authentication\(see page 730\)](#)). The AD/Kerberos login is tried first. If this has been successful, the login is successful. If not, login with the smartcard certificate is performed as a fallback.

For the login with a smartcard certificate, the pam\_pkcs11 module is used. For reference, see [https://github.com/OpenSC/pam\\_pkcs11](https://github.com/OpenSC/pam_pkcs11).

- 
- [Standalone Authentication Method\(see page 498\)](#)
  - [Combination with the "AD/Kerberos with Smartcard" Method\(see page 505\)](#)

### Standalone Authentication Method

#### Prerequisites

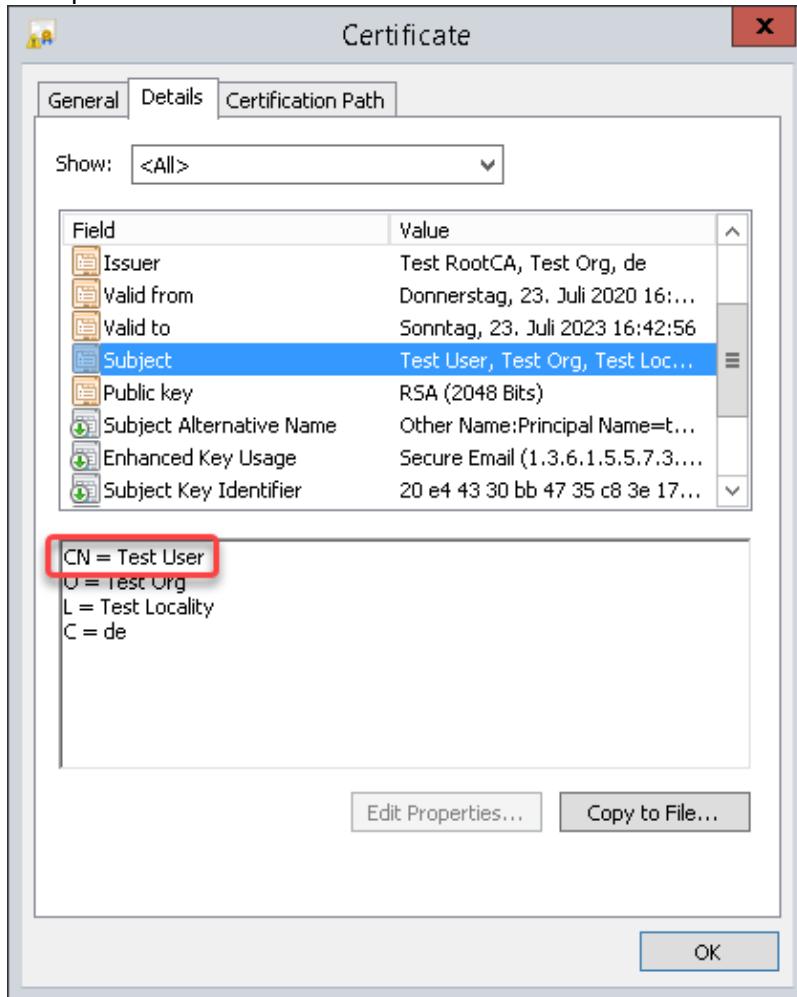
The following files are required:

- Root certificate and intermediate CA certificates, as applicable
- File cn\_map which contains mappings of common names to UPN names for each smartcard certificate

#### Creating the cn\_map File

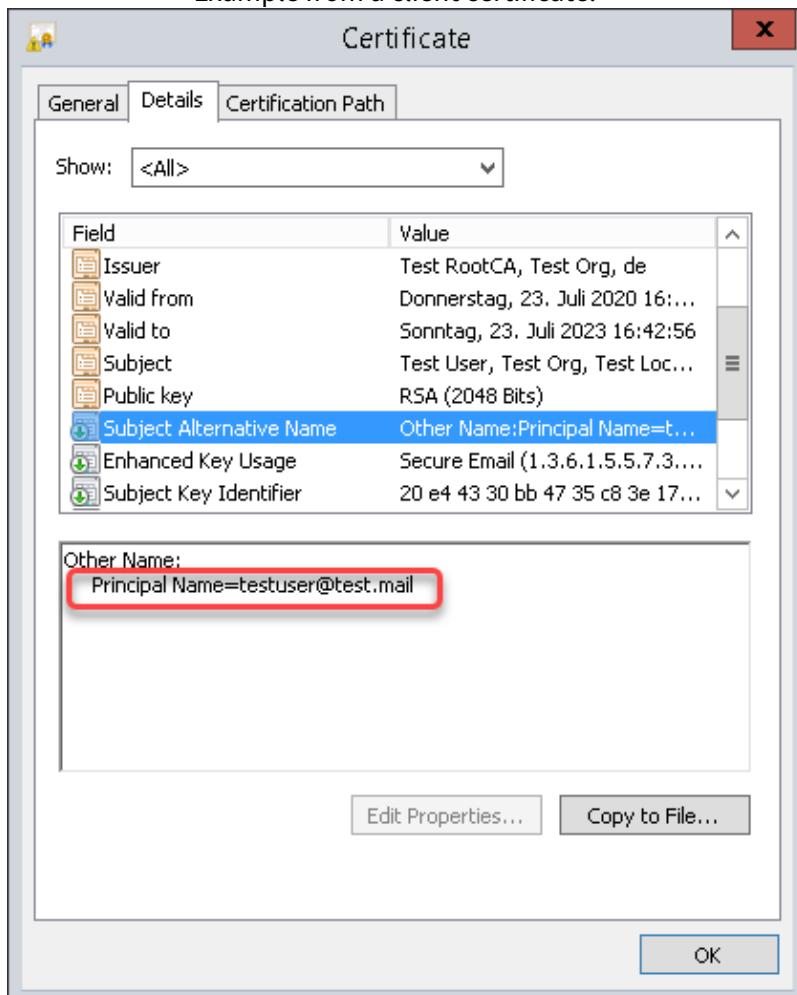
- Create a file named cn\_map in which each line is in the format <common name> -> <logon name> where

- <common\_name> is the common name part of the certificate's subject  
Example from a client certificate:



- <logon\_name> is the UPN name of the SubjectAltName extension of the certificate. The UPN name is dependent on whether Enterprise Kerberos names are enabled or disabled (the setting is described under [Configuring the Devices](#)(see page 504)):
  - When Enterprise Kerberos names are enabled, the user domain may differ from the default domain. In the following example, the user's domain is test.mail, while the default domain is MY.DOMAIN: testuser@test.mail@MY.DOMAIN

### Example from a client certificate:



- When Enterprise Kerberos names are disabled, the user domain is the same as the default domain. Example:

testuser@MY.DOMAIN

Example line: Test User -> testuser@test.mail@MY.DOMAIN

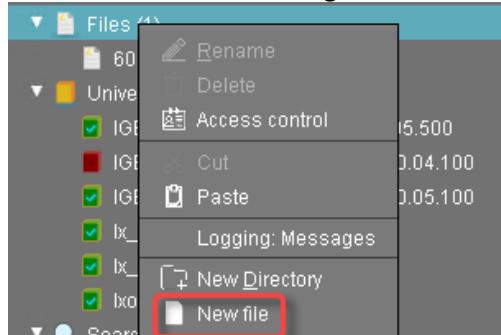
#### Transferring the cn\_map File to the Devices

The cn\_map file must be located in the directory /etc/pam\_pkcs11/cn\_map. This can be achieved via UMS file transfer.

To transfer the cn\_map file to the devices:

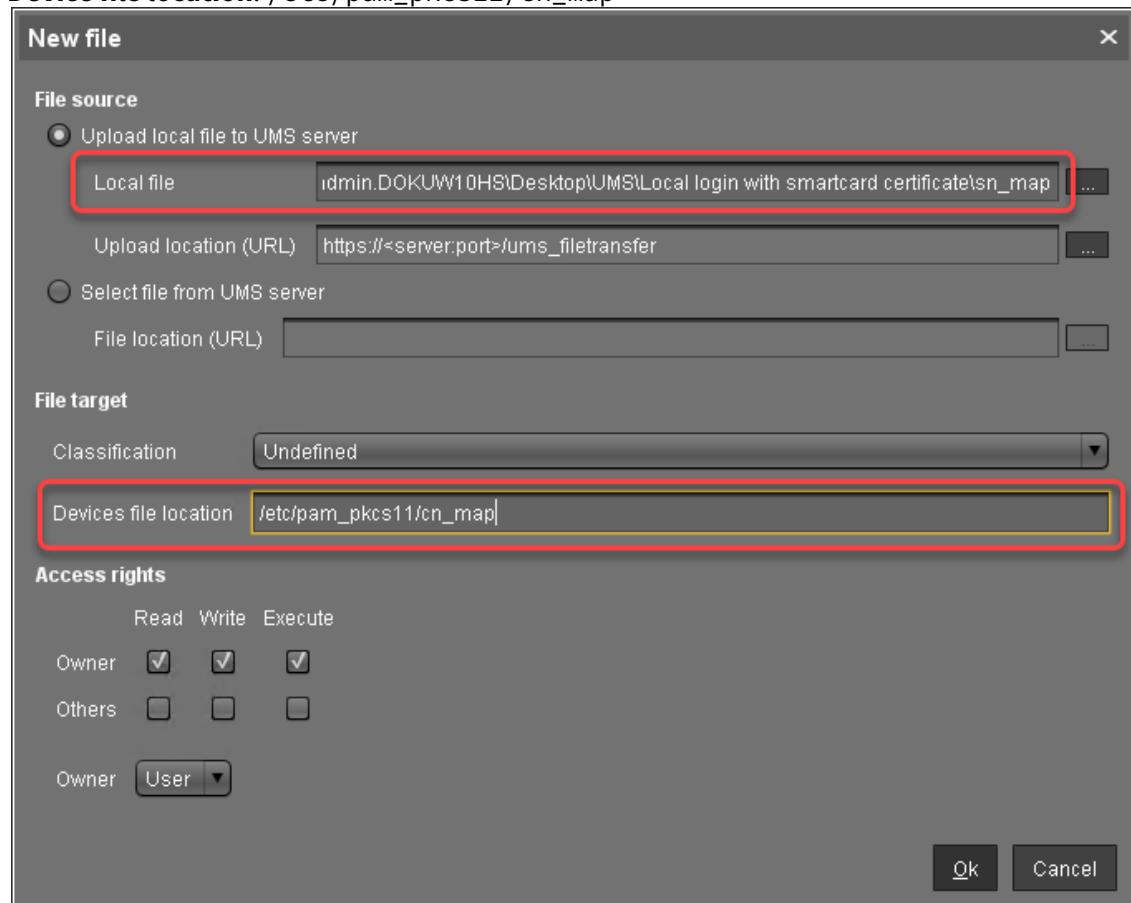


1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



2. In the **New file** dialog, configure the settings as follows:

- **Local file:** Local file path of the certificate. Use the file chooser by clicking .
- **Device file location:** /etc/pam\_pkcs11/cn\_map



3. Click **Ok**.

The file object is created in the UMS.

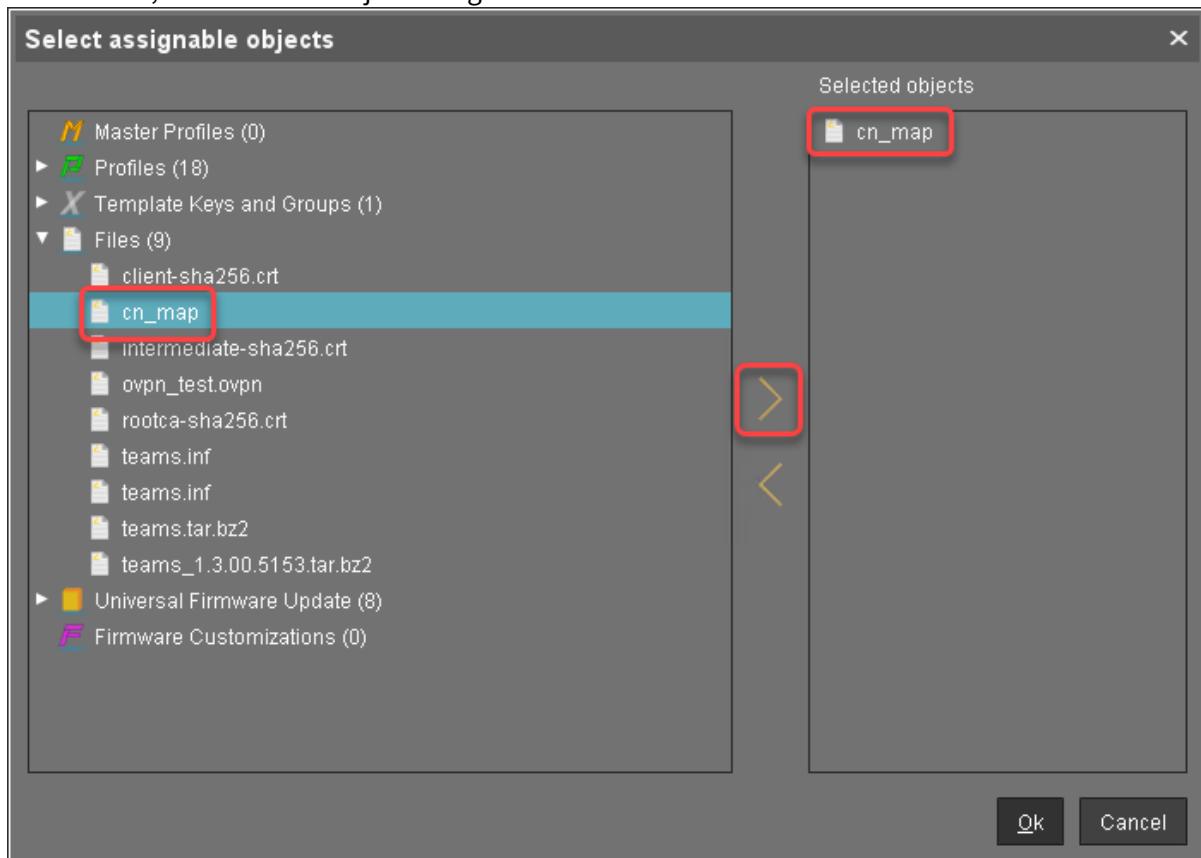
4. In the UMS structure tree, select the endpoints for which you want to configure the local login with a smartcard certificate. For mass deployment, it is recommended to use a directory containing the endpoint devices or a profile (see [Creating Profiles](#)<sup>194</sup>).

---

<sup>194</sup> <https://kb.igel.com/display/endpointmgmt605/Creating+Profiles>



5. In the **Assigned objects** area, click .
6. Under **Files**, select the file object using the button:



7. Click **Ok**.
8. In the **Update time** dialog, select **Now** and click **Ok**.  
The cn\_map file is transferred to the endpoint device.

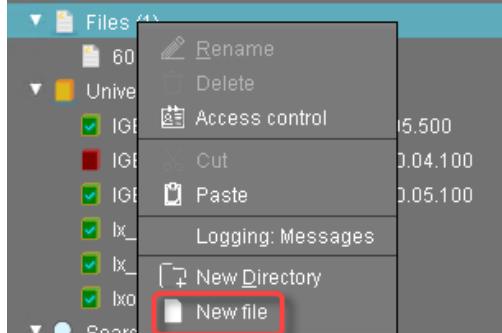
#### Transferring the Certificate Files to the Devices

##### Registering the Certificate Files as File Objects

To transfer the certificate files to the devices, perform the following steps for each certificate file:

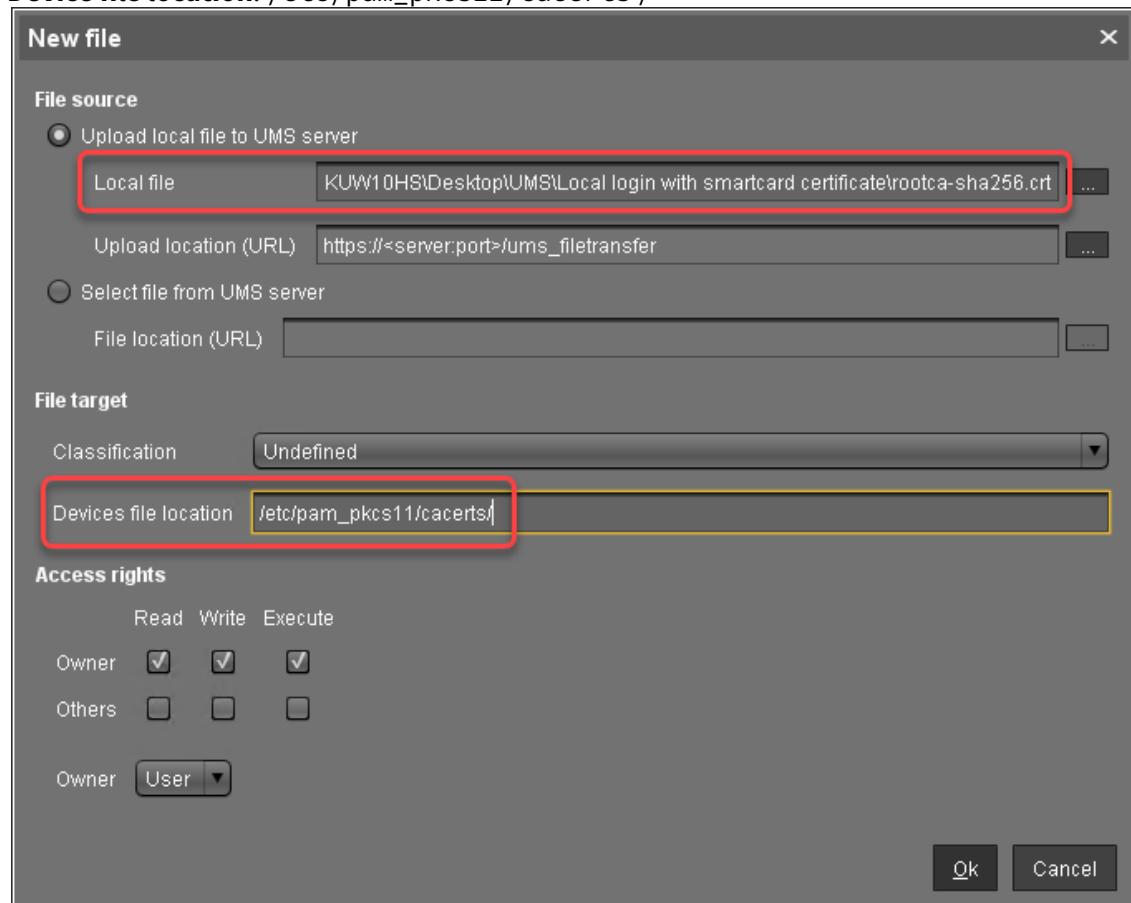


1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



2. In the **New file** dialog, configure the settings as follows:

- **Local file:** Local file path of the certificate. Use the file chooser by clicking .
- **Device file location:** /etc/pam\_pkcs11/cacerts /



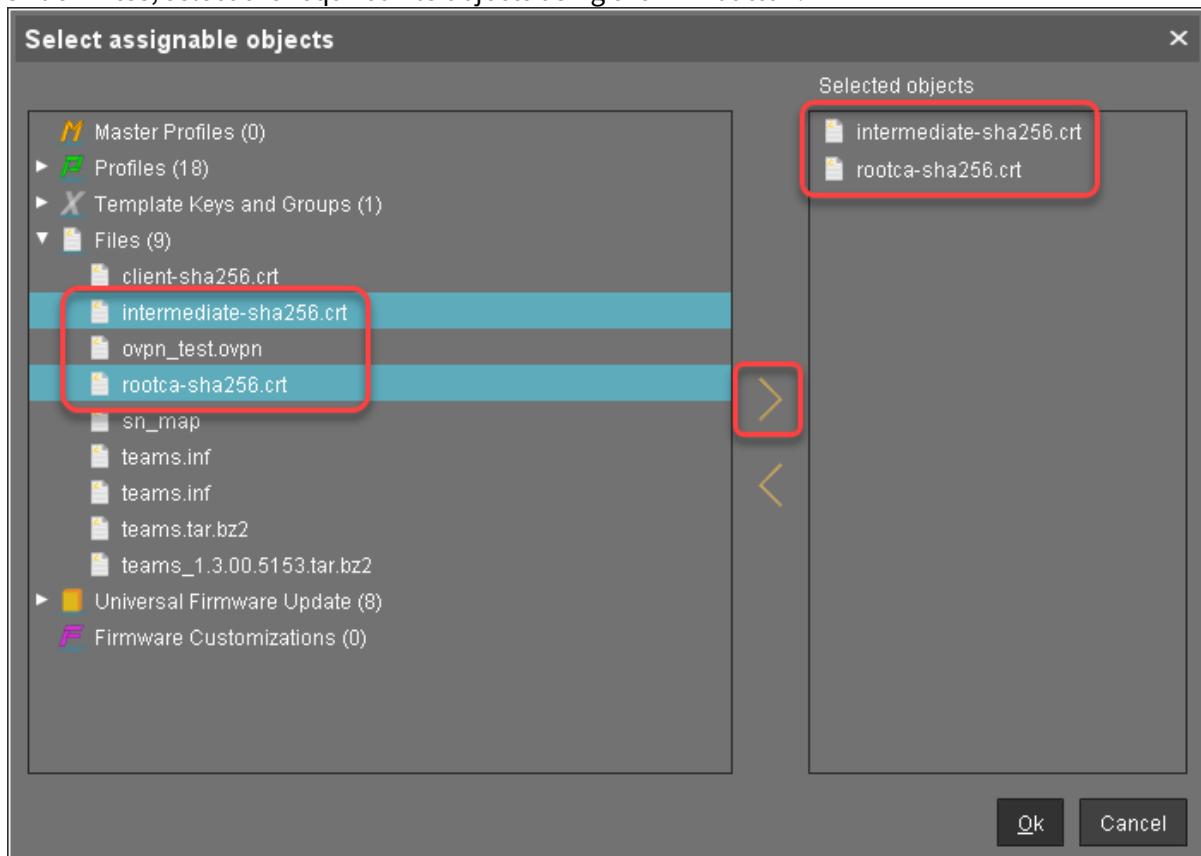
3. Click **Ok**.

The file object is created in the UMS.

Assign the Certificate Files to the Devices



1. In the UMS structure tree, select the endpoints for which you want to configure the local login with a smartcard certificate. For mass deployment, it is recommended to use a directory containing the endpoint devices or a profile (see [Creating Profiles](#)<sup>195</sup>).
2. In the **Assigned objects** area, click
3. Under **Files**, select the required file objects using the button:



4. Click **Ok**.
5. In the **Update time** dialog, select **Now** and click **Ok**.  
The certificates are transferred to the endpoint device.

## Configuring the Devices

To enable local login with a smartcard certificate, you must configure the devices appropriately. For mass deployment, it is recommended to use a profile.

1. Go to **Security > Smartcard > Middleware** and select the middleware to be used.
2. Go to **System > Registry > auth > login > pkcs11** (registry key: `auth.login.pkcs11`) and activate **Login with smartcard certificate**.
3. Go to **System > Registry > auth > login > pkcs11\_cert\_policy** (registry key: `auth.login.pkcs11_cert_policy`) and enter the methods for certificate verification that are to

<sup>195</sup> <https://kb.igel.com/display/endpointmgmt605/Creating+Profiles>



be used. For further information, see the documentation in [https://github.com/OpenSC/pam\\_pkcs11](https://github.com/OpenSC/pam_pkcs11).

4. If Kerberos enterprise names are used, go to **System > Registry > auth > login > krb5\_enterprise** and activate **Allow enterprise names**.

#### Debugging

- ▶ If you need to debug the smartcard certificate login, go to **System > Registry > auth > login > pkcs11\_debug** (registry key: auth.login.pkcs11\_debug) and activate **Enable debugging of smartcard certificate login**.

Logging messages will be available via syslog.

#### Combination with the "AD/Kerberos with Smartcard" Method

##### Prerequisites

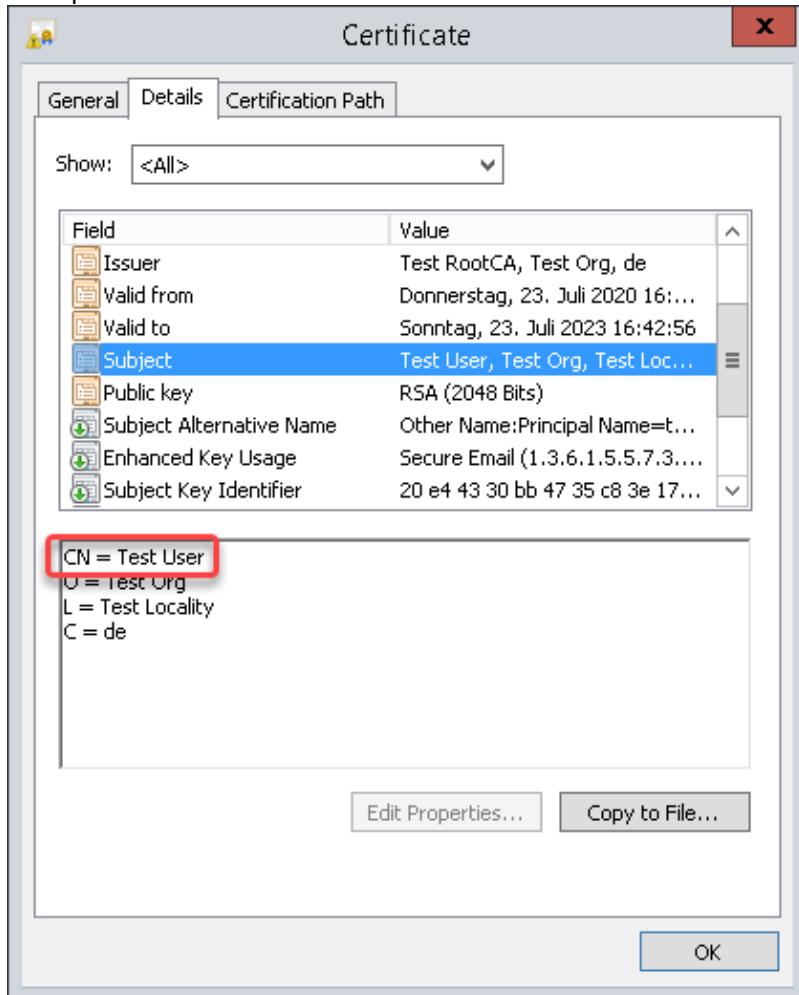
The following files are required:

- Root certificate and intermediate CA certificates, as applicable
- File cn\_map which contains mappings of common names to UPN names for each smartcard certificate

##### Creating the cn\_map File

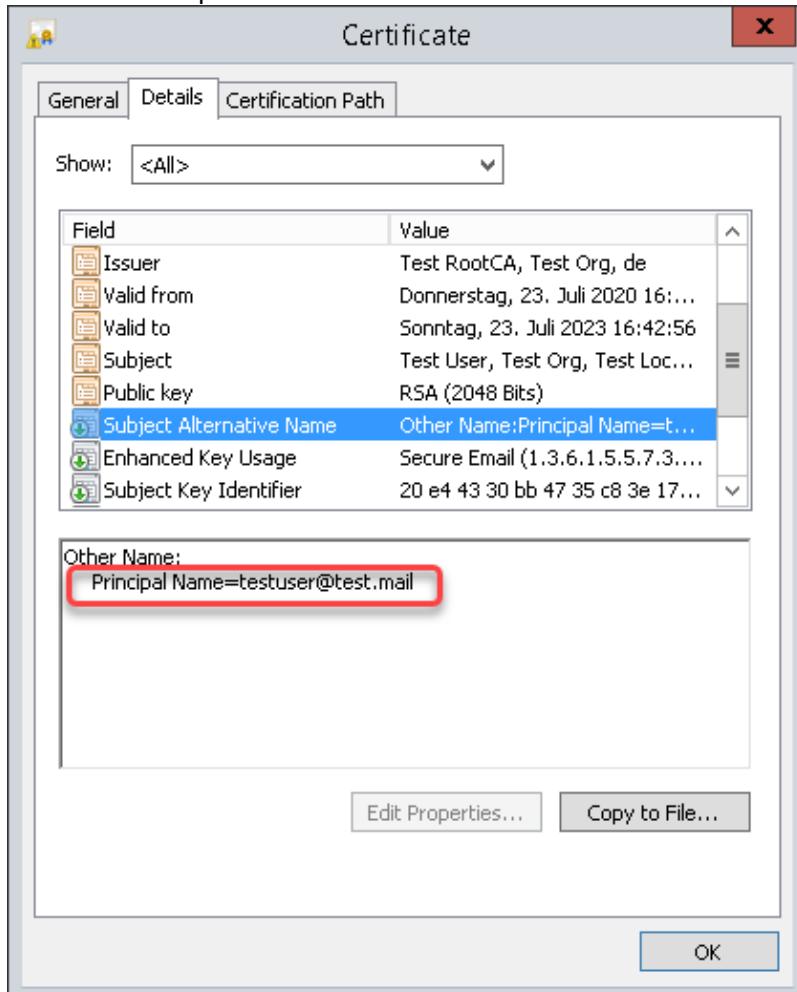
- ▶ Create a file named cn\_map in which each line is in the format <common name> -> <logon name> where

- <common\_name> is the common name part of the certificate's subject  
Example from a client certificate:



- <logon\_name> is the UPN name of the SubjectAltName extension of the certificate. The UPN name is dependent on whether Enterprise Kerberos names are enabled or disabled (the setting is described under [Configuring the Devices](#)(see page 511)):
  - When Enterprise Kerberos names are enabled, the user domain may differ from the default domain. In the following example, the user's domain is test.mail, while the default domain is MY.DOMAIN: testuser@test.mail@MY.DOMAIN

### Example from a client certificate:



- When Enterprise Kerberos names are disabled, the user domain is the same as the default domain. Example: testuser@MY.DOMAIN

Example line:

```
Test User ->
testuser@test.mail@MY.DOMAIN
```

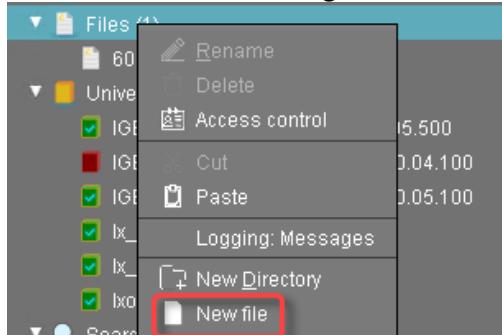
### Transferring the cn\_map File to the Devices

The cn\_map file must be located in the directory /etc/pam\_pkcs11/cn\_map. This can be achieved via UMS file transfer.

To transfer the cn\_map file to the devices:

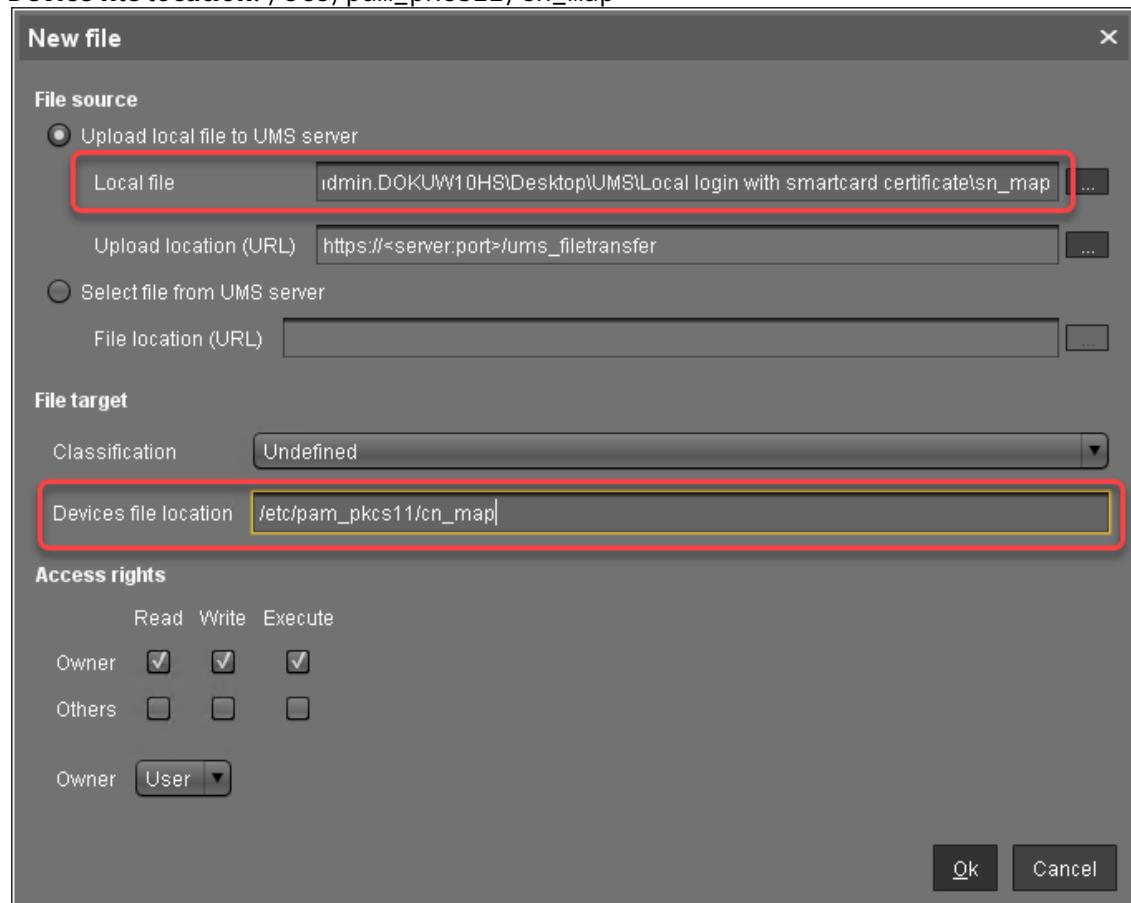


1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



2. In the **New file** dialog, configure the settings as follows:

- **Local file:** Local file path of the certificate. Use the file chooser by clicking .
- **Device file location:** /etc/pam\_pkcs11/cn\_map



3. Click **Ok**.

The file object is created in the UMS.

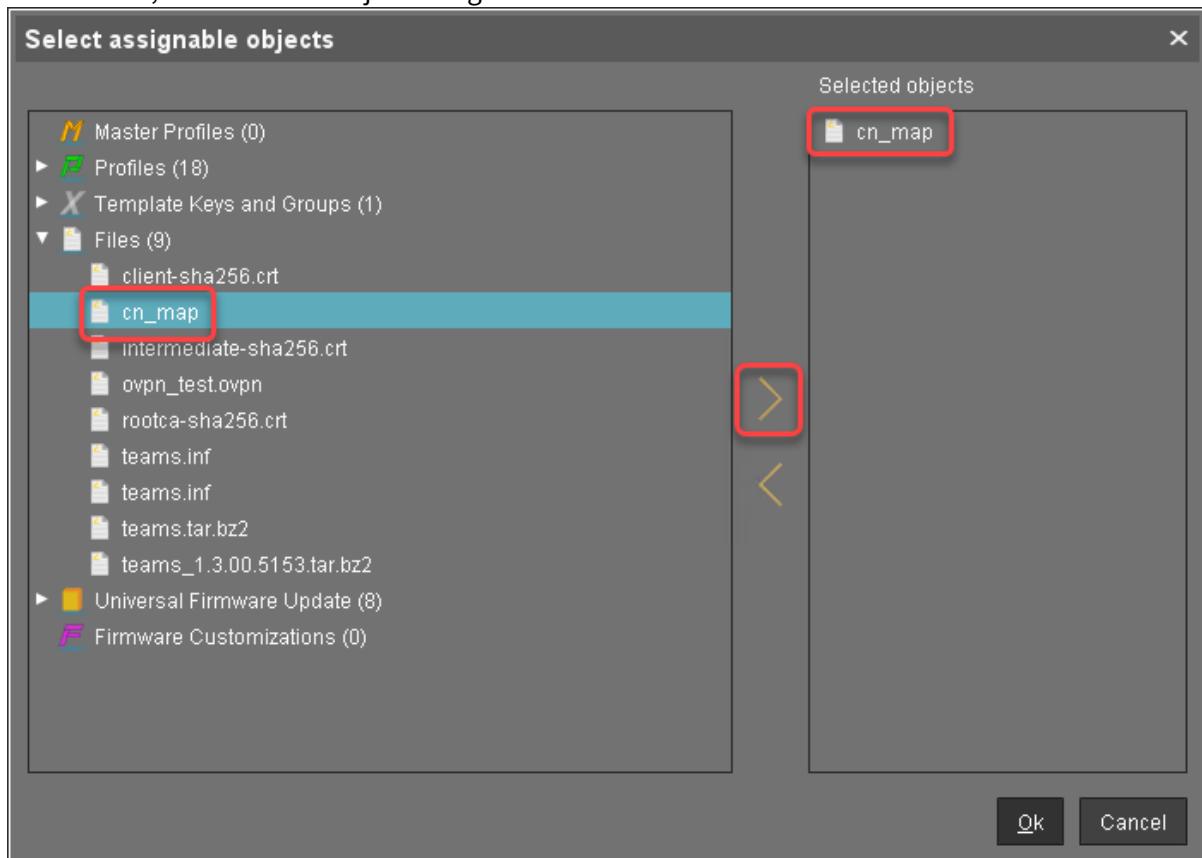
4. In the UMS structure tree, select the endpoints for which you want to configure the local login with a smartcard certificate. For mass deployment, it is recommended to use a directory containing the endpoint devices or a profile (see [Creating Profiles<sup>196</sup>](#)).

---

<sup>196</sup> <https://kb.igel.com/display/endpointmgmt605/Creating+Profiles>



5. In the **Assigned objects** area, click .
6. Under **Files**, select the file object using the button:



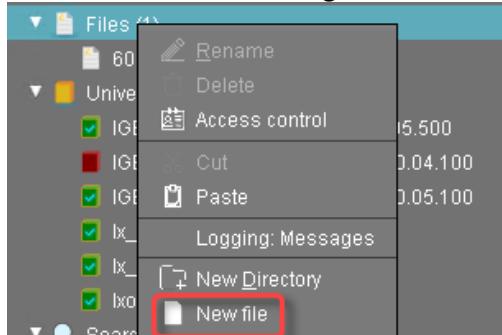
7. Click **Ok**.
8. In the **Update time** dialog, select **Now** and click **Ok**.  
The cn\_map file is transferred to the endpoint device.

#### Transferring the Certificate Files to the Devices

##### Registering the Certificate Files as File Objects

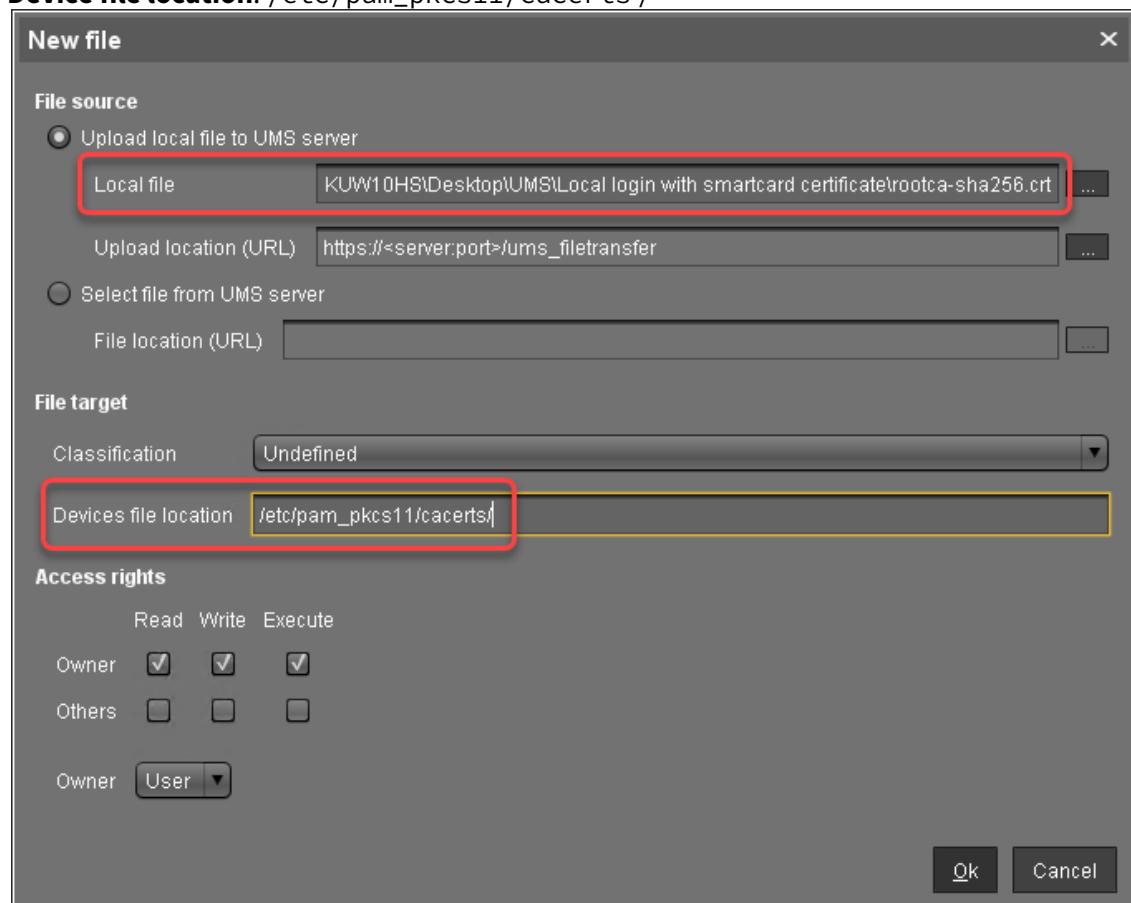
To transfer the certificate files to the devices, perform the following steps for each certificate file:

1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



2. In the **New file** dialog, configure the settings as follows:

- **Local file:** Local file path of the certificate. Use the file chooser by clicking .
- **Device file location:** /etc/pam\_pkcs11/cacerts /

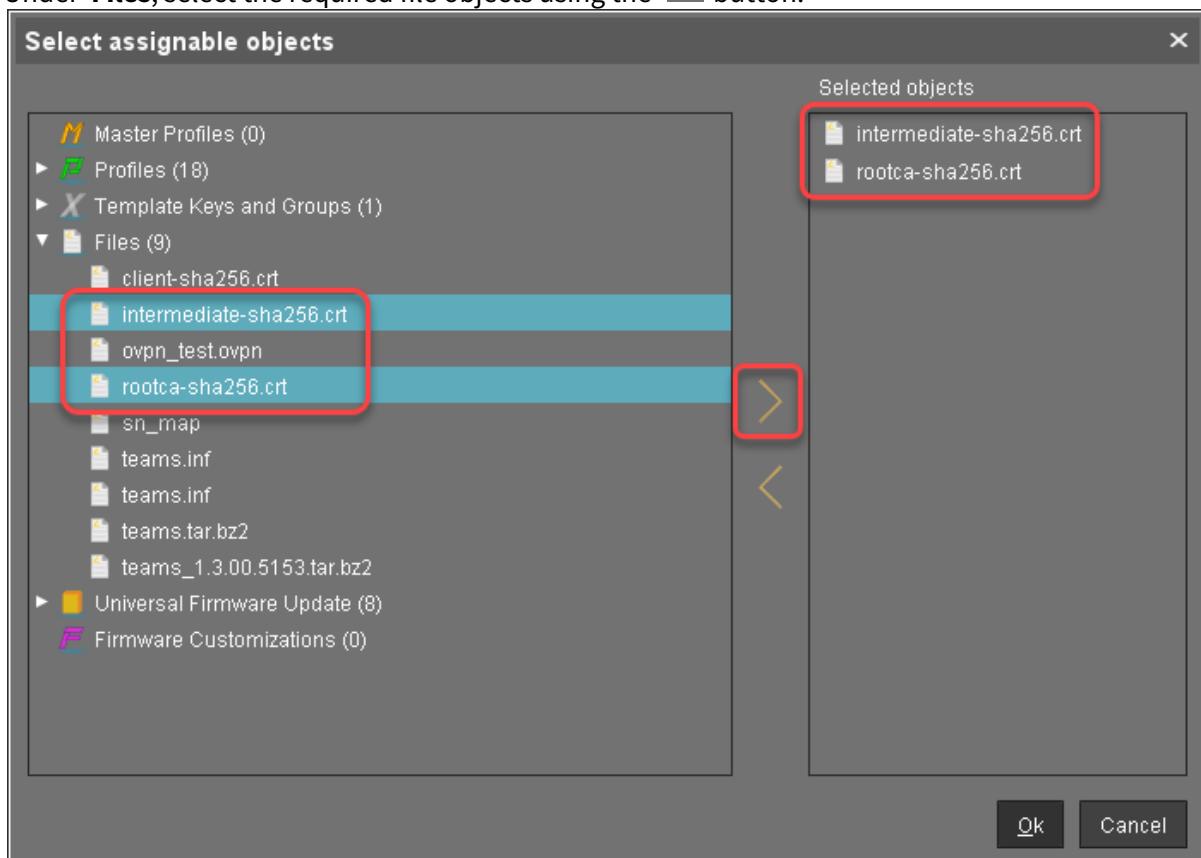


3. Click **Ok**.

The file object is created in the UMS.

Assign the Certificate Files to the Devices

1. In the UMS structure tree, select the endpoints for which you want to configure the local login with a smartcard certificate. For mass deployment, it is recommended to use a directory containing the endpoint devices or a profile (see [Creating Profiles](#)<sup>197</sup>).
2. In the **Assigned objects** area, click .
3. Under **Files**, select the required file objects using the  button:



4. Click **Ok**.
5. In the **Update time** dialog, select **Now** and click **Ok**.  
The certificates are transferred to the endpoint device.

## Configuring the Devices

To enable local login with a smartcard certificate, you must configure the devices appropriately. For mass deployment, it is recommended to use a profile.

1. Go to **Security > Smartcard > Middleware** and select the middleware to be used.
2. Go to **Security > Active Directory/Kerberos**, activate **Enable**, and set **Default domain (fully qualified domain name)**. For details, see [Active Directory/Kerberos](#)(see page 1247).
3. Go to **System > Registry > auth > login > pkcs11** (registry key: auth.login.pkcs11) and activate **Login with smartcard certificate**.

<sup>197</sup> <https://kb.igel.com/display/endpointmgmt605/Creating+Profiles>



4. Go to **System > Registry > auth > login > pkcs11\_cert\_policy** (registry key: `auth.login.pkcs11_cert_policy`) and enter the methods for certificate verification that are to be used. For further information, see the documentation in [https://github.com/OpenSC/pam\\_pkcs11](https://github.com/OpenSC/pam_pkcs11).
5. If Kerberos enterprise names are used, go to **System > Registry > auth > login > krb5\_enterprise** and activate **Allow enterprise names**.

#### Debugging

- If you need to debug the smartcard certificate login, go to **System > Registry > auth > login > pkcs11\_debug** (registry key: `auth.login.pkcs11_debug`) and activate **Enable debugging of smartcard certificate login**.

Logging messages will be available via syslog.

## 2.21 Desktop and Display

- [Display Configuration for Shared Workplace \(SWP\)](#)(see page 512)
- [Display Switch](#)(see page 513)
- [Multimonitor](#)(see page 517)
- [Showing and Hiding the On-Screen Software Keyboard Automatically](#)(see page 526)
- [Overcoming the Restrictions of a Full-Screen Session with the in-Session Control Bar](#)(see page 527)
- [Screen Issues When Redocking Notebook](#)(see page 528)
- [Using an External NVIDIA Graphics Card](#)(see page 528)

### 2.21.1 Display Configuration for Shared Workplace (SWP)

As of IGEL Universal Desktop Linux version 4.14.100 and version 5.06.100, Shared Workplace allows user specific screen resolutions and configurations. Resolution, layout, refresh rate, rotation, number of screens, monitor connectors (DVI, VGA, ...) can be set per user, but color depth cannot.

There are technical limitations to user-specific settings: For VIA graphics drivers/hardware, the maximum desktop size is set in the Screen section of the X configuration file. The name and location of the X configuration file depends on the firmware version:

- IGEL Linux *version 10*: `/config/Xserver/xorg.conf-0`
- IGEL Linux *version 5*: `/config/Xserver/xorg.conf-0` or `/etc/X11/xorg.conf` (this is a symbolic link that points to `/config/Xserver/xorg.conf-0`)

In the Screen section of the above-mentioned configuration file, you can find a line such as `Virtual 1920 1200`. The size defined here cannot be changed dynamically; it is a hard limit for the overall desktop size.



## Best practice

It is recommended to set the initial desktop configuration to the maximum number of screens and the resolutions to Autodetect. This way the user specific resolutions will not be restricted.

### Debugging

If the total framebuffer size of the user specific resolutions exceeds the limits of the `Virtual [width] [height]` setting from `/config/Xserver/xorg.conf-0` (or `/etc/X11/xorg.conf`), the user specific resolutions cannot be activated and the screen configurations are not changed dynamically.

There is no warning dialog or anything else to alert the user to this restriction. But you can find related log messages via `journalctl` or in `/var/log/messages`:

```
XRANDR: ERROR: CANNOT APPLY CHANGES ->
```

```
XRANDR: ERROR: -> Selected modes ([width]x[height]) would exceed the maximum framebuffer size ([width]x[height])
```

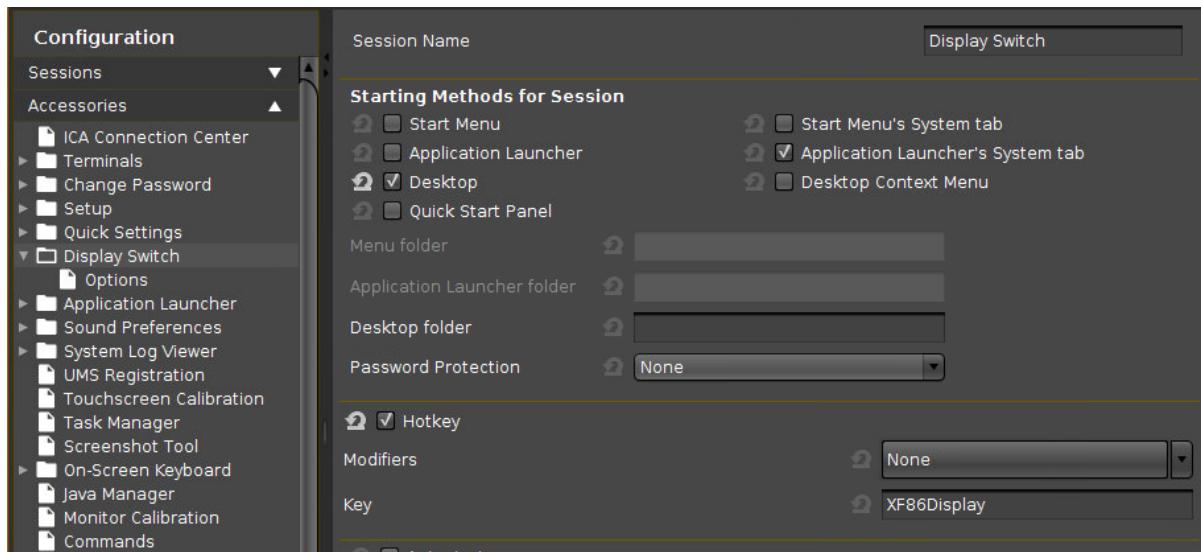
## 2.21.2 Display Switch

If you are using a notebook with IGEL UDC2, UDC3, or UD Pocket, you might want to connect an additional monitor. If you are using an IGEL thin client (UD series), you might want to use two monitors. Any thinkable display mode, like clone mode/mirroring or extended mode, is possible. Moreover, you can change between the display modes quickly.

### Configure a Starter for the Display Switch

There are many ways to start the display switch. The following example shows how to define a hotkey typical for a notebook.

1. Open the Setup and go to **Accessories > Display Switch**.
2. Activate **Hotkey**.



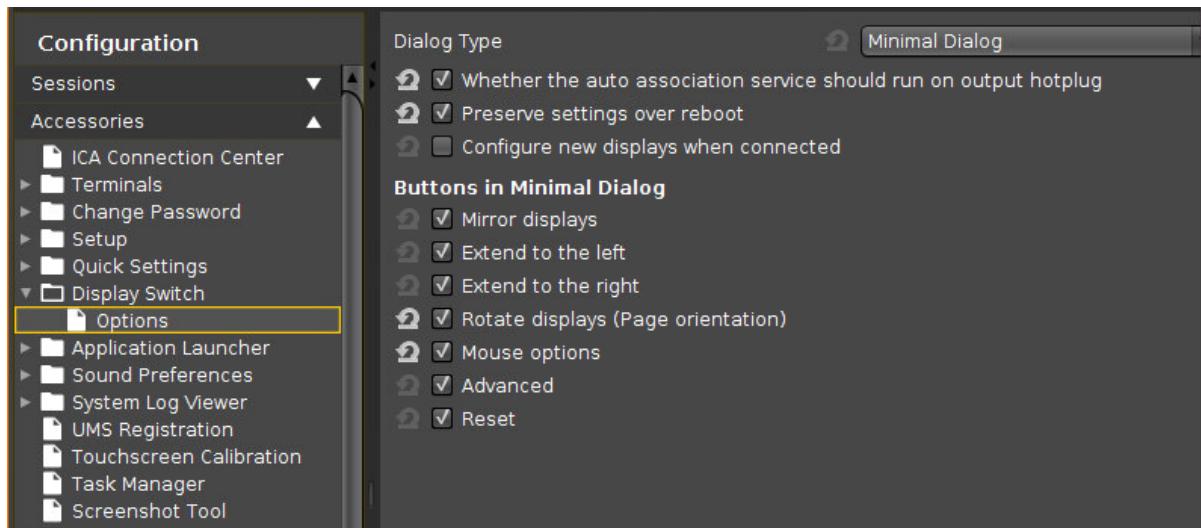
By default, [Fn]+[F7] (XF86Display) is defined as the hotkey for starting the display switch. You can change the hotkey by selecting or entering different keys in **Modifiers** and **Key**.

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field.  
Example: Tab in (keysym 0xff09, Tab)

3. Press **Apply** or **Ok**.

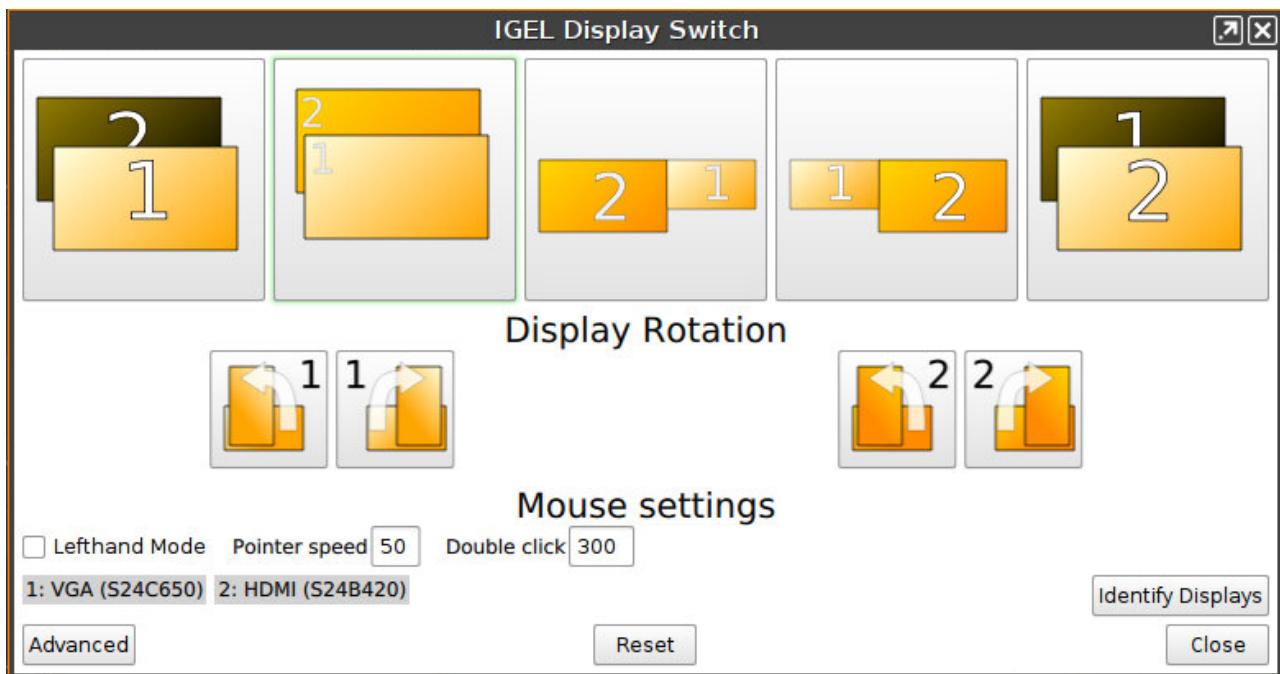
## Configure the Display Switch

1. Open the Setup and go to **Accessories > Display Switch > Options**.
2. Consider the following settings:
  - **Dialog Type:** In most cases, you can leave it at **Minimal Dialog**. The user can always switch to the advanced dialog, provided that **Advanced** in the **Minimal Dialog** area is activated.
  - **Smart display configuration:** Activate this option, if you want to save all your display configurations.
  - **Preserve settings over reboot:** Activate this if the settings made by the display switch are to remain unchanged after reboot.
  - **Configure new displays when connected:** Activate this if you want the display switch to start automatically as soon as a new monitor is connected.
  - To fine-tune the minimal dialog, change the settings under **Buttons in Minimal Dialog**.



## Use the Display Switch

The minimal dialog will look similar to this; details depend on your specific setup:



Button	Function

	Uses only display 1.
	Shows the same content on all screens, i.e. clone mode or mirroring.
	Extends the display area to the screen on the right.
	Extends the display area to the screen on the left
	Uses only display 2.
	Rotates the selected display to the left or to the right.

For more information, see the manual chapter [Using Display Switch](#)(see page 1061)



The **P** marks the primary Display.



### 2.21.3 Multimonitor

Working with two or more screens is becoming increasingly popular in professional working environments.

You can find out how to configure several screens and an extended desktop with the IGEL setup here.

There are different screen configuration options:

- [Automatic Configuration](#)(see page 517)
- [Manual Configuration](#)(see page 518)
- [Additional Settings](#)(see page 521)
- [Auto Switch Monitor Configuration for Laptops](#)(see page 524)

If you work with IGEL Universal Desktop or supported UDC2 hardware, multimonitor support is guaranteed.

Difficulties may arise if you work with UDC2 hardware and your hardware is not fully supported by IGEL.

Multimonitor configuration for unsupported hardware only works if native graphic driver support functions properly. You must ensure that the native driver really does work because the fallback VESA driver does not allow multimonitor configuration. Click **About** in the **Application Launcher** to determine which graphic chipset you work with. If VESA is listed there, the native driver will not work and multimonitor configuration will not be possible.

- See the [Linux 3rd party hardware database](#)<sup>198</sup> for supported graphic cards.

#### Automatic Configuration

The firmware recognizes the native graphic driver and will apply the screens automatically by default.

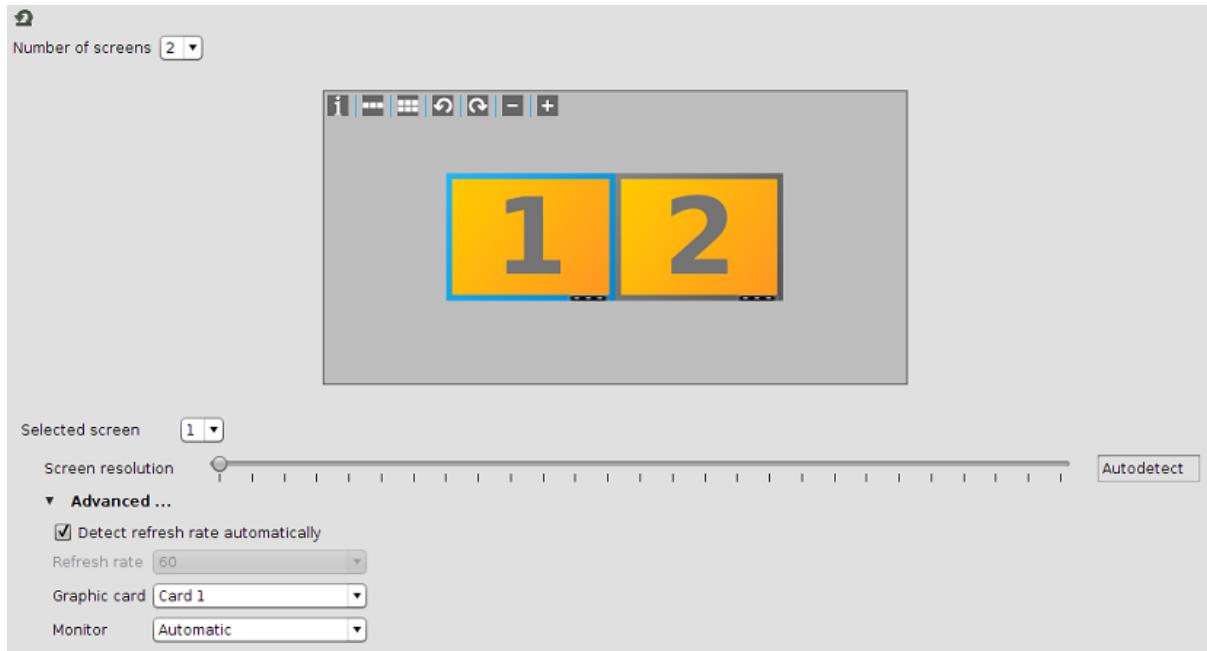
Define two or more monitors:

1. Go to **User Interface > Display** in the structure tree.
2. Select **2 (or more)** under **Number of screens**.

The number of monitors that you can select depends on your hardware. Using the Universal Management Suite (UMS), you can choose up to 8 monitors.

3. Choose the screen under **Selected screen** or by clicking it with a mouse.  
The selected screen is highlighted with a blue frame:

<sup>198</sup> <https://www.igel.com/linux-3rd-party-hardware-database/>



#### 4. Set **Screen Resolution** to **Autodetect** (default setting).

The operating system reads out the EDID (Extended Display Identification Data) of the monitors through DDC (Display Data Channel). With these data, the correct resolution for the monitors can be recognized and set.

If the **Autodetect** resolution is not available check **Monitor probing (DDC)** under **User Interface > Display > Options**. The **Monitor probing (DDC)** must be enabled (default setting).

With more than 2 monitors, the screen resolution has to be specified for each screen manually.

#### 5. Enable **Detect refresh rate automatically** (default setting) under **Advanced**.

#### 6. Set **Monitor** to **Automatic**.

The selected screen is automatically assigned to the graphic connector (monitor).

#### 7. Drag and drop the rectangles to position the screens.

Screen 1 is always the primary screen where the taskbar is situated.

#### 8. Click **Apply** or **OK** to save the settings.

## Manual Configuration

During automatic configuration, the following problems can sometimes arise:

- One of the screens remains black.

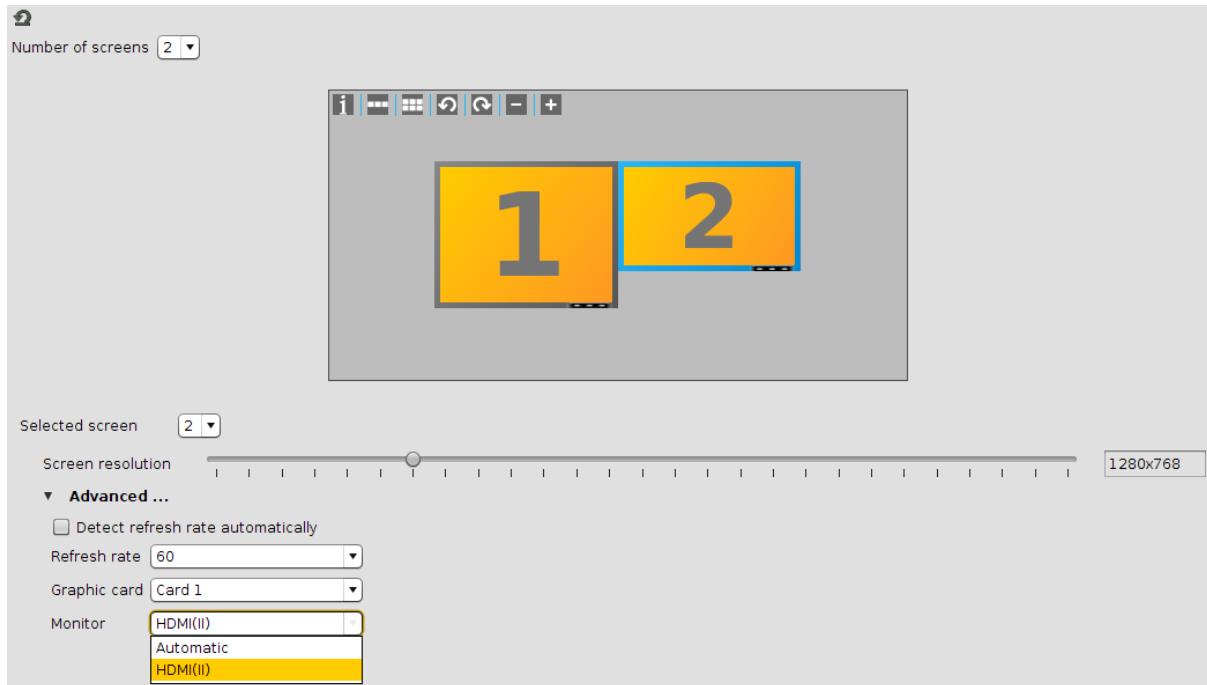


- There is the same display on all screens.

In this case, you can set the screens manually:



1. Go to **User Interface > Display** in the structure tree.



2. Select a screen number under **Selected screen**.
3. Specify the resolution manually under **Screen resolution**.

The standard resolution setting is **Autodetect**.

From IGEL Linux Version 10.03.100, you have the option of defining your own resolutions via the registry (`x.xserver0.custom_resolution`). In order for the values set there to take effect, the resolution must be set to **Autodetect** (the slider at the far left). The following parameters apply to the entry in the registry:

- WxH : W = width, H = height (example: 1920x1080)
- WxH@R : W = width, H = height, R = refresh rate (example: 1920x1080@60 or 1920x1200@59.8)

4. Select for all screens the respective connector under **Monitor**. The manual configuration can take effect only if you assign the monitor connector to all screens.

If you adjust the settings directly in IGEL Setup, only the connected monitors will be available in the selection list. If you want to configure the screens using the UMS profile, all possible connectors will be shown in the selection list and you will not know which one is relevant for your device.

**Tip:**



- Click in your client setup to obtain information about the connector names, screen resolutions and screen numbers.

This configuration cannot be accessed from the UMS.

The black field belongs to the screen number on the left side:



## Additional Settings

A number of useful tips are provided below:

- [Rotating a Screen \(Pivot\)](#)(see page 521)
- [Setting Different Backgrounds](#)(see page 522)
- [Useful Window Settings](#)(see page 523)

### Rotating a Screen (Pivot)

1. Click on a monitor field.
2. Select (**Rotates the selected screen counterclockwise**) or (Rotates the selected screen clockwise).



Two screens with autodetected resolutions are automatically aligned to the top.

- **Alignment:** If you enter the correct resolution, you can see the real size of the screens and you will be able to align them the way you want.

The individual screen areas must however be in contact with each other at one edge and corner, and cannot overlap.

### Setting Different Backgrounds

You can easily set different backgrounds for your screens.

- Click **User Interface > Desktop > Background** in the structure tree of the setup.  
There is a configuration page for each screen.

Setting	Value
Wallpaper (1st monitor)	blue (4x3)
Wallpaper Style (1st Monitor)	Streched
Color Style (1st Monitor)	Solid color
Desktop Color (1st Monitor)	Choose color
2nd Desktop Color (1st Monitor)	Choose color
Custom wallpaper download (1st monitor)	<input checked="" type="checkbox"/>
Custom Wallpaper file (1st Monitor)	[Empty input field]



- ▶ Select the wallpaper and define the style.

You may also upload your own **Custom Wallpaper**, e.g. a background with your corporate design. See [Creating Your Own Wallpaper](#)(see page 597).

## Useful Window Settings

### Setting the Start Monitor or Full-screen Mode:

1. Click the name of your session under **Sessions** in the IGEL Setup, e.g. **RDP > RDP Sessions**.
2. Click **[Session Name] > Window** to configure the window settings.

Number of colors	<span style="font-size: 2em;">⌚</span> Global setting
Window size	<span style="font-size: 2em;">⌚</span> fullscreen
Desktop scale factor	<span style="font-size: 2em;">⌚</span> Global setting
Display resolution	<span style="font-size: 2em;">⌚</span> Same as window size
Start monitor	<span style="font-size: 2em;">⌚</span> No configuration
Multi-monitor fullscreen mode	<span style="font-size: 2em;">⌚</span> Global setting

For the function "**2nd monitor as Start monitor**" the **Window size** has to be set to **fullscreen**.

### Setting the Multimonitor Full-screen Mode

1. Click **Window** in the global folder of your session, e.g. **RDP > RDP Global > Window**.
2. Configure the window settings.

Number of Colors	<span style="font-size: 2em;">⌚</span> Millions
Window size	<span style="font-size: 2em;">⌚</span> fullscreen
Desktop scale factor	<span style="font-size: 2em;">⌚</span> auto
<input checked="" type="checkbox"/> Enable Display Control	
<input type="checkbox"/> Control bar for RDP sessions	
<b>Multi Monitor</b>	
Multi-monitor fullscreen mode	<span style="font-size: 2em;">⌚</span> Restrict fullscreen session to one monitor



## Defining the Taskbar

1. Click **User Interface > Desktop > Taskbar**.
2. Define the **Taskbar** settings.

A screenshot of a software interface showing taskbar configuration options. At the top left is a checked checkbox labeled "Use Taskbar". Below it is a section titled "Taskbar Position" with a dropdown menu set to "Bottom". Under "Vertical Taskbar Mode", there is a dropdown menu set to "Deskbar". The "Taskbar Height/Width" is set to "40". In the "Number of rows/columns in taskbar" section, "Automatic" is selected. Under "Multi Monitor Taskbar Size", "Restrict taskbar onto one monitor" is chosen, and "1st monitor" is specified. There are also sections for "Monitor" and "Taskbar on top of all windows" (unchecked). Another section for "Taskbar Auto Hide" includes "Auto Hide Behavior" set to "Intelligently", "Taskbar Show Delay" set to "600", and "Taskbar Hide Delay" set to "400".

Setting	Value						
Taskbar Position	Bottom						
Vertical Taskbar Mode	Deskbar						
Taskbar Height/Width	40						
Number of rows/columns in taskbar	Automatic						
Multi Monitor Taskbar Size	Restrict taskbar onto one monitor						
Monitor	1st monitor						
Taskbar on top of all windows	(unchecked)						
Taskbar Auto Hide	<table border="1"><tr><td>Auto Hide Behavior</td><td>Intelligently</td></tr><tr><td>Taskbar Show Delay</td><td>600</td></tr><tr><td>Taskbar Hide Delay</td><td>400</td></tr></table>	Auto Hide Behavior	Intelligently	Taskbar Show Delay	600	Taskbar Hide Delay	400
Auto Hide Behavior	Intelligently						
Taskbar Show Delay	600						
Taskbar Hide Delay	400						

If you want to expand the taskbar onto all monitors, you have to ensure that the screens are aligned to the bottom. Otherwise, you will see only half of the taskbar on one monitor.

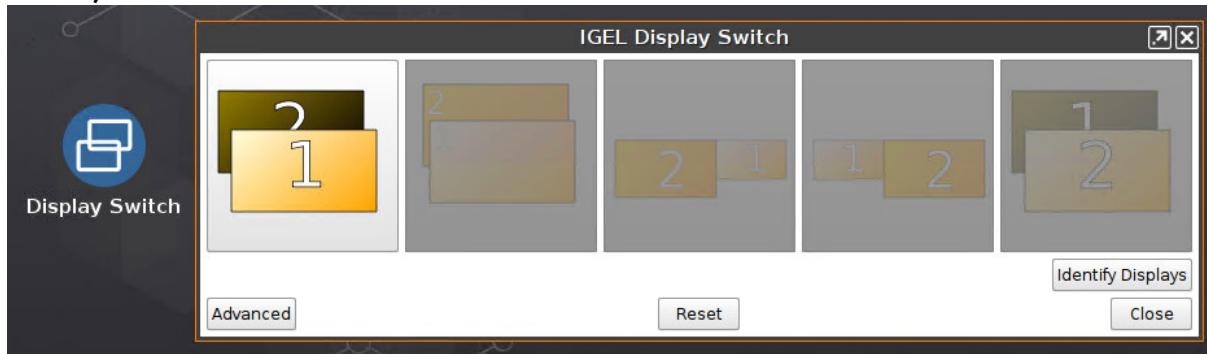
## Auto Switch Monitor Configuration for Laptops

This is one example of how to configure auto switch monitor for Laptops.

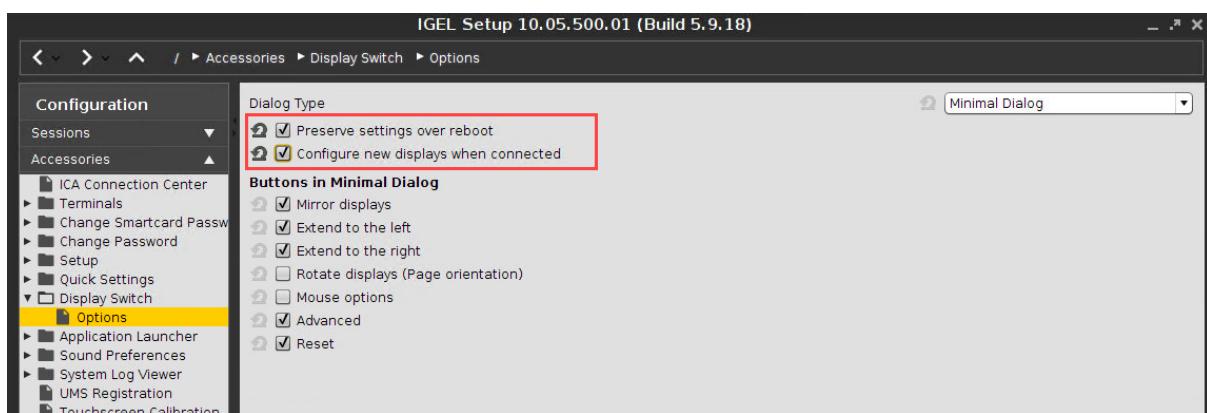
1. Connect the device and close/open lid.



2. Open the **Display Switch** utility (which has already been activated under **Accessories > Display Switch**).



3. In the advanced mode, you can drag & drop the displays for your intended configuration. The display will snap adjacent to others.
4. If a display should not be used, it can be dragged to the **Disabled** area on the top right - the screen will be reactivated when it is dragged back to the active area.
5. To show the same content on multiple displays, one display should be dragged onto an other active screen.  
The interface will show **Mirrors**. The mirroring monitor will be displayed on the lower right.
6. Press **Apply** to save the setting
7. Press **Yes** on the **Keep configuration** dialog so that the current settings will be saved to persistent storage and associated with the profile.  
You can configure advanced functionality (e.g. panning, scaling and resolutions) in drop-down boxes (hidden in a drawer on the right side)
  - Klick the > button on the right edge.
8. Go in IGEL Setup under **Accessories > Display Switch > Options**.
9. Enable **Preserve settings over reboot** and **Smart display configuration**. (Default: disabled)



10. The IGEL Display Switch utility is now used for NVIDIA graphic devices as well.

#### Configuration of the display setting for Notebook lid handling

You can configure the lid handling of a notebook so that the notebook goes into standby mode by closing the lid, regardless of whether the notebook is plugged in or not.



### Settings of the Standby Mode

If you want your notebook to go into standby mode by closing the lid, while your notebook is plugged in, you have to do following setting:

1. Go under **IGEL Setup** to **System > Registry > system > actions > lid > ac.**
2. Set **Lid close action while plugged in** to **Suspend.**(Default: Turn off display)
3. Click **Apply** or **Ok** to save the setting.

If you want your notebook to go into standby mode by closing the lid, while your notebook isn't plugged in, you have to do following setting:

1. Go under **IGEL Setup** to **System > Registry > system > actions > lid > battery.**
2. Set **Lid close action while not plugged in** to **Suspend.**(Default: Turn off display)
3. Click **Apply** or **Ok** to save the setting.

If you want that the notebook **turn off display** after closing the lid, it makes sense to set the following setting to switch off the notebook internally:

1. Go under **IGEL Setup** to **System > Registry > sessions > user\_display0 > options > lid\_events.**
2. Enable **React on lid open and close event.**
3. Click **Apply** or **Ok** to save the setting.

### 2.21.4 Showing and Hiding the On-Screen Software Keyboard Automatically

You can configure the on-screen software keyboard to appear or disappear automatically when an input box is selected or deselected (e. g. Firefox or screenlock).

#### Showing Automatically

With the following setting, a software keyboard will be shown automatically when an input box is focused.

1. In the Setup, go to **Registry > userinterface > softkeyboard > autoshow** (parameter: `userinterface.softkeyboard.autoshow`).
2. Enable **Automatically show on-screen keyboard when text field is selected.**

#### Hiding Automatically

With the following setting, the software keyboard will be hidden automatically when an input box is not focused anymore.

1. In the Setup, go to **Registry > userinterface > softkeyboard > autohide** (parameter: `userinterface.softkeyboard.autohide`)
2. Enable **Automatically hide on-screen keyboard when text field is deselected.**



If there are any problems, e. g. the keyboard does not hide automatically, you have to disable **Automatically hide on-screen keyboard when text field is deselected** and make sure that the following Setup parameters have been enabled:

- **Accessories > On-Screen Keyboard > Autostart**
- **Accessories > On-Screen Keyboard > Restart**

## 2.21.5 Overcoming the Restrictions of a Full-Screen Session with the in-Session Control Bar

Running a session in full-screen mode gives you the advantage that the complete real estate of your monitor is at the disposal of that session. However, you might still want to eject a hotplug drive, or to minimize or end the current session. The solution provided by IGEL Linux is called **in-session control bar**.

Activating the in-session control bar:

1. Open the Setup and go to **User Interface > Desktop > In-Session Control Bar**.
2. Activate **Use in-session control bar in all supported sessions** if you want to have an in-session control bar in all session types for which it is supported. If you want to have an in-session control bar only in sessions of certain types, activate the appropriate options, e.g. **Control bar for RDP sessions**.



3. In the **Start Monitor** choice, select the display on which you want the in-session control bar to appear. If unsure, leave it at **Automatic**.



4. Click **Apply** or **Ok**.

Using the in-session control bar:

1. Move the mouse to the upper edge of the desktop.  
The in-session control bar appears.



2. To perform the desired action, click the appropriate icon:
  - To eject a USB device, click ▲.
  - To minimize the session view, click □.
  - To end the session, click ✕.
  - To make the in-session control bar visible permanently, click ↗.

## 2.21.6 Screen Issues When Redocking Notebook

### Environment

UDC-converted notebooks running IGEL Linux 5 and above.

### Issue

When you take a notebook off the dock, e. g. to move to meeting rooms or other locations, and redock the notebook, the screen resolution ends up wrong, sometimes with a black screen and other similar screen issues.

### Solution

1. In Setup, go to **Accessories > Display Switch > Options**.
2. Enable **Configure new Displays when connected**.  
The display switch will start when the notebook is redocked.
3. Use the display switch to configure the display appropriately. For further information, see the Tips & Tricks article [Display Switch](#)<sup>199</sup>.
4. Click **Ok** to save the settings.

#### Legal Note

IGEL's [Terms & Conditions](#)<sup>200</sup> apply.

## 2.21.7 Using an External NVIDIA Graphics Card

### Goal

You want to use an external NVIDIA graphics card for your endpoint device and need to connect it with all graphics outputs.

### Environment

- IGEL OS 11.04.100 or higher

<sup>199</sup> <https://kb.igel.com/display/igelos/Display+Switch>

<sup>200</sup> <https://www.igel.com/terms-conditions/>



## Solution

1. In the IGEL Setup, go to **System > Registry**.
2. Set the registry key **x.drivers.preferred\_driver** to nvidia.
3. Enable the registry key **x.drivers.nvidia.use\_modeset**. This registry key should be used if you want to use PRIME.
4. Restart the device manually, e.g. by pressing the power switch.
5. Under **User Interface > Display**, orient and position your monitors.
6. For fine-tuning, use the **Display Switch** function, which can be enabled under **Accessories > Display Switch**. See [Using Display Switch](#)(see page 1061) and [Display Switch](#)(see page 1055).

Then the onboard graphics ports as well as the ports of the NVIDIA card can be used, which is the recommended mode since everything is rendered on the NVIDIA GPU.

## 2.22 Customizing

- [Custom Partition Tutorial](#)(see page 529)
- [Using a Custom PKCS#11 Library](#)(see page 588)
- [Adding an Icon for Browsing Removable Storage](#)(see page 590)
- [Adding an Icon for the Image Viewer](#)(see page 591)
- [Creating a Timed Command \(Cron Replacement\)](#)(see page 593)
- [Customizing IGEL OS Desktop](#)(see page 594)
- [How to Change the Font Color of the Desktop Icons](#)(see page 605)
- [How to Set up a Screensaver Countdown](#)(see page 607)
- [Installing a Calculator on IGEL Linux](#)(see page 611)
- [Keyboard Shortcuts for Managing Windows](#)(see page 612)
- [Make Frequent User Actions Easier by Defining Hotkeys](#)(see page 612)
- [Shutdown/Suspend Devices Automatically at the End of a Session](#)(see page 614)
- [Suspend to RAM - Wake Up by USB Mouse](#)(see page 615)
- [Taking Screenshots on IGEL Linux](#)(see page 616)
- [Setting the Device's System Time](#)(see page 617)
- [Updating Timezone Information \(Daylight Saving Time, DST\)](#)(see page 618)
- [Adding or Changing a MIME Type Handler](#)(see page 620)
- [Regional Settings in Sessions](#)(see page 623)

### 2.22.1 Custom Partition Tutorial

The Custom Partition mechanism solves the task of supplying additional software or other files to IGEL OS while still being able to update the system in the regular way.

This tutorial describes creating content for a Custom Partition for IGEL OS 11.01.100 or newer. In the examples, IGEL OS 11.03.500 is used. You may also find it useful for updating existing Custom Partitions in order to make them work on IGEL OS 11.01.100 or newer, as some details have changed.



The IGEL Support Team offers support for the deployment of Custom Partitions. However, it is not possible to offer support for any third-party software that is installed on a Custom Partition.

If you want to build a Custom Partition and give it to third parties, make sure you have redistribution permission for the software. This is usually the case for Open Source / Free Software, but not for proprietary software. Read the license agreements and respect them.

This tutorial contains the following sections:

- [A First Simple Custom Partition](#)(see page 530)
- [Packaging the Custom Partition](#)(see page 537)
- [A Real-World CP: Chromium](#)(see page 549)
- [Zoom as a Custom Partition](#)(see page 558)
- [Microsoft Teams as a Custom Partition](#)(see page 573)

## A First Simple Custom Partition

As a first step, this tutorial will guide you through creating a simple Custom Partition. It will open a message window greeting the user, which can be run by clicking a desktop icon. You will learn about some basic mechanisms of Custom Partitions in this section.

Read all the following chapters in the order given and follow the instructions.

1. [Development Environment](#)(see page 530)
2. [Activating the Custom Partition Functionality](#)(see page 530)
3. ["Hello World" Program](#)(see page 531)
4. [Creating the Custom Application](#)(see page 533)
5. [Using a Partition Parameter](#)(see page 535)

### Development Environment

For this first simple Custom Partition, you only need root access to a device with IGEL OS version 11.01.100 or higher.

### Next Step

>> [Activating the Custom Partition Functionality](#)(see page 530)

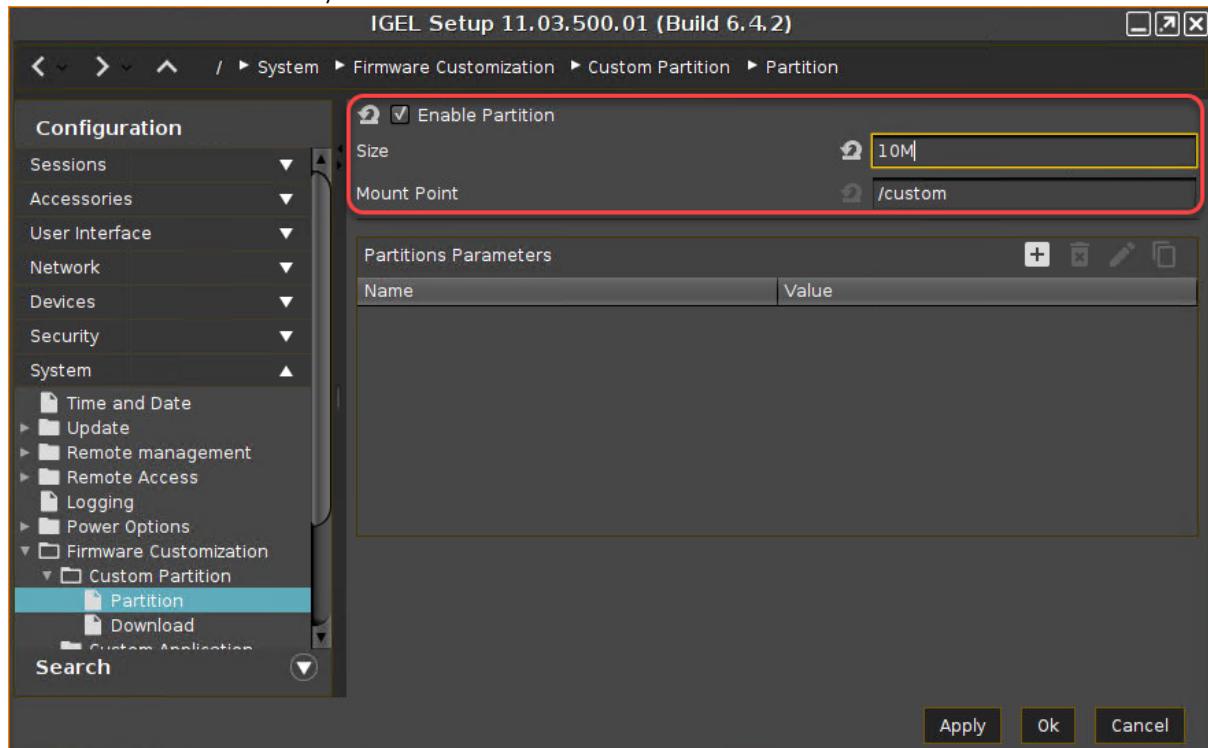
### Activating the Custom Partition Functionality

First, you must activate the Custom Partition functionality. It is deactivated by default.

1. Open the Setup and go to **System > Firmware Customization > Custom Partition > Partition**.
2. Check **Enable Partition**.
3. Set the **Size** to "10M" Megabyte).



4. Leave the **Mount Point** at `/custom`



5. Click **Apply**.

The Custom Partition is created on the device's mass storage, which is indicated by a message. When the Custom Partition is created and successfully mounted, the message reads:



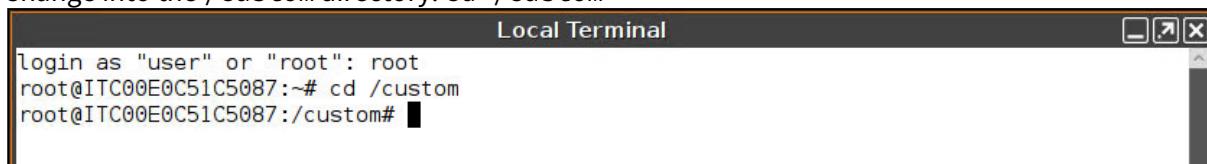
**Next Step**

>> ["Hello World" Program\(see page 531\)](#)

**"Hello World" Program**

Your first Custom Partition will contain a simple shell script that displays the message "Hello, world!" with the help of the `gtkmessage` utility.

1. Open the local terminal on your device and log in as root. If the local terminal has not been configured yet, see [Terminals\(see page 1042\)](#).
2. Change into the `/custom` directory: `cd /custom`





3. Make a hello directory for your Custom Partition contents: `mkdir hello`

```
root@ITC00E0C51C5087:/custom# mkdir hello
```

4. Change into the hello directory: `cd hello/`

```
root@ITC00E0C51C5087:/custom# cd hello/
```

5. Open a new plaintext file using the GNU nano editor: `nano hello.sh`

```
root@ITC00E0C51C5087:/custom/hello# nano hello.sh
```

The colors used by default for syntax highlighting in nano may be inconvenient for reading. You can change the colors with the following command: `sed -i "s#color cyan#color blue#; s#color brightyellow#color red#" /usr/share/nano/sh.nanorc`

Also, you can use the vi editor as an alternative; the commands for exiting and saving a file will be different then.

6. Put this content into the file:

```
#!/bin/bash
gtkmessage -m "Hello, World!" -t "Hello" -o "Close"
GNU nano 2.5.3                                     File: hello.sh

#!/bin/bash
gtkmessage -m "Hello $(customparam get NAME)!" -t "Hello" -o "Close"
```

<code>^G</code> Get Help	<code>^O</code> Write Out	<code>^W</code> Where Is	<code>^K</code> Cut Text	<code>^J</code> Justify	<code>^C</code> Cur Pos
<code>^X</code> Exit	<code>^R</code> Read File	<code>^\\</code> Replace	<code>^U</code> Uncut Text	<code>^T</code> To Linter	<code>^</code> Go To Line

7. Save the file by pressing [Ctrl]+[o], [Return].

8. Exit the GNU nano editor by pressing [Ctrl]+[x].

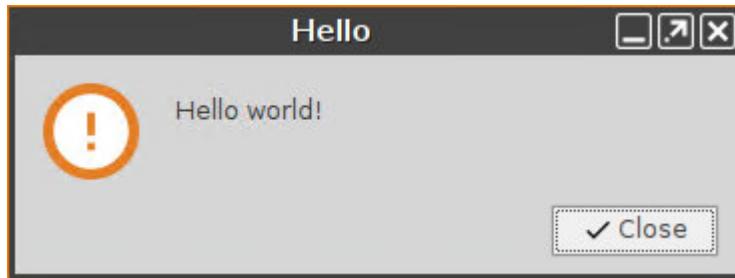
9. Make the file executable: `chmod a+x hello.sh`

```
root@ITC00E0C51C5087:/custom/hello# chmod a+x hello.sh
```

10. Run the shell script from the command line to test it: `./hello.sh`

```
root@ITC00E0C51C5087:/custom/hello# ./hello.sh
```

A message window like this should open:



You can close it with the **Close** button.

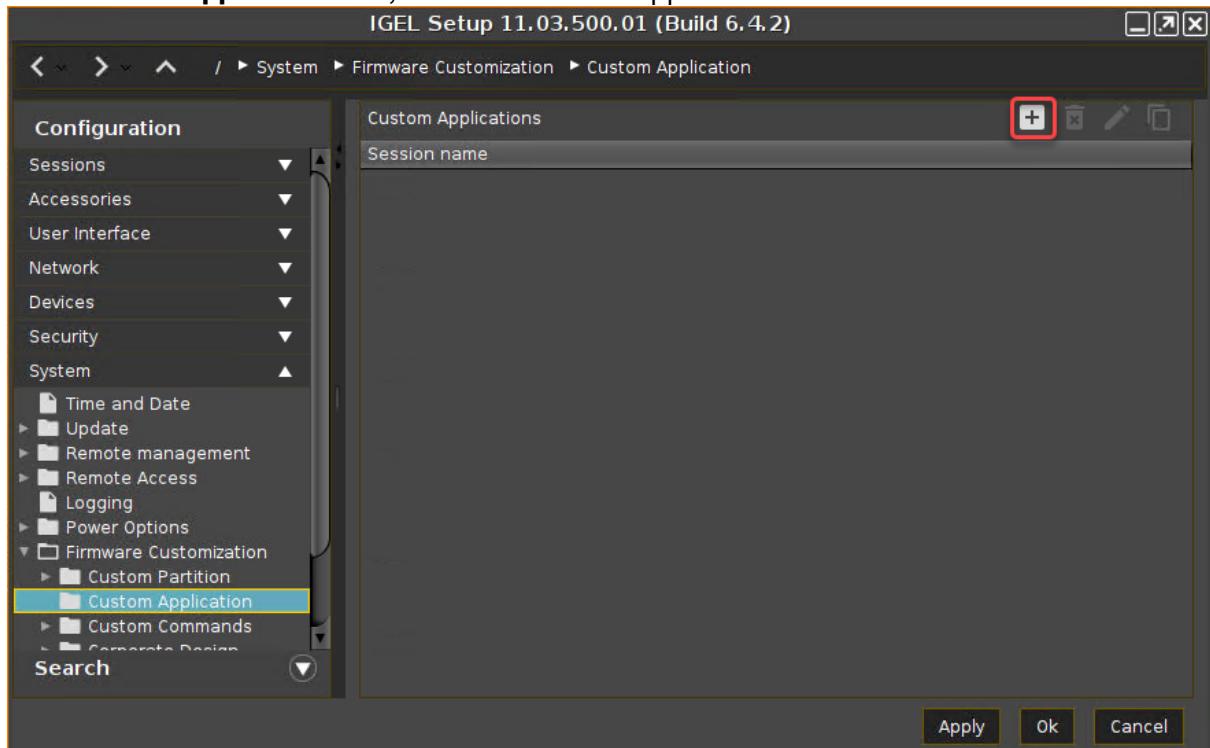
#### Next Step

>> [Creating the Custom Application\(see page 533\)](#)

#### Creating the Custom Application

In the previous step, you have created a little application and executed it from the command line. Now make it more convenient for end-users: Create a custom application and place an icon on the desktop that users can click.

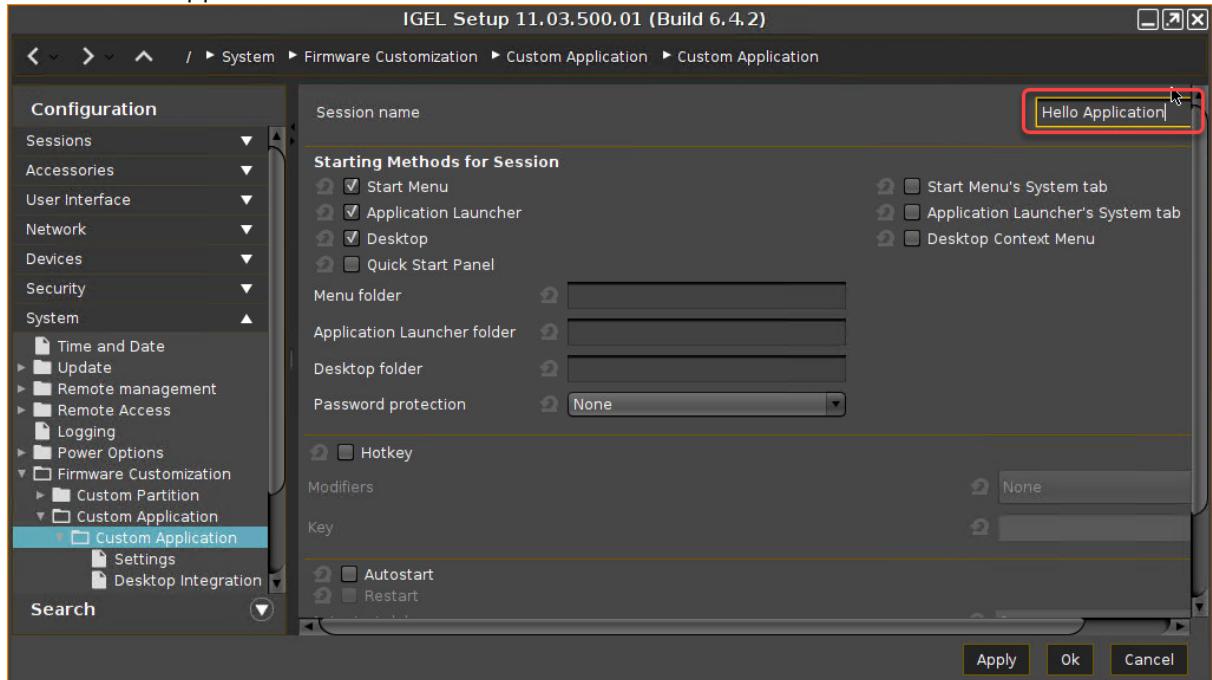
1. In the Setup, go to **System > Firmware Customization > Custom Application**.
2. In the **Custom Applications** list, click to add an application.



The **Desktop Integration** page opens.



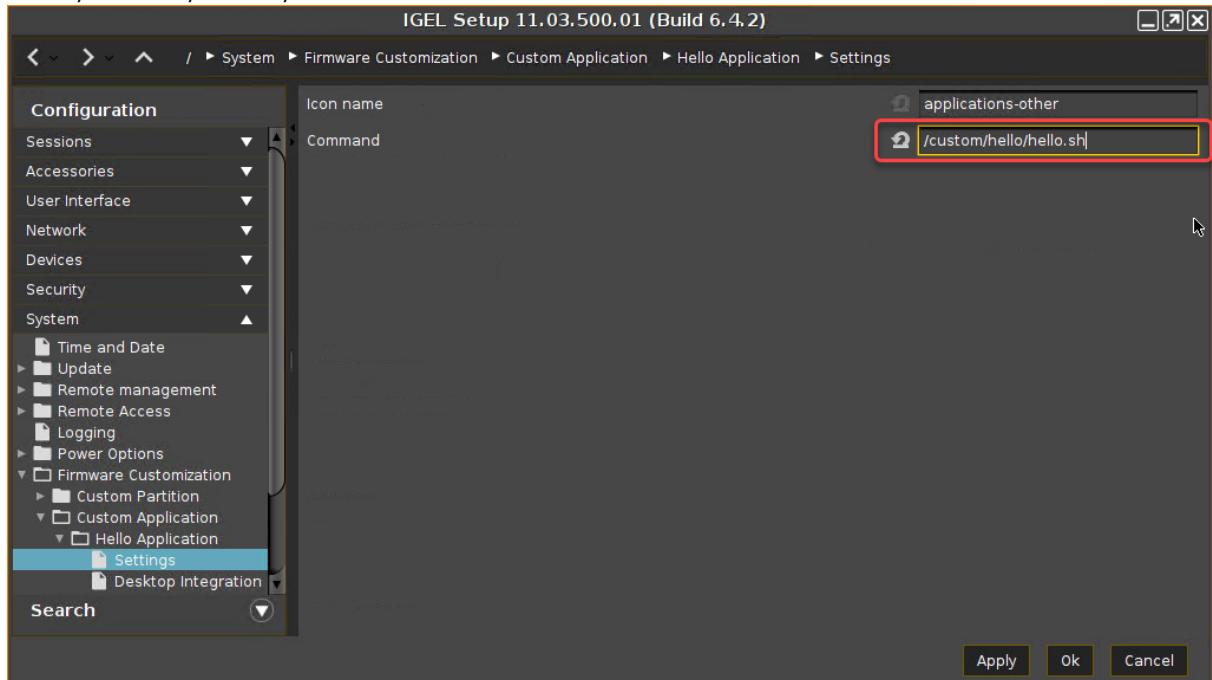
3. Enter Hello Application as the **Session name**.



4. Click **Apply**.

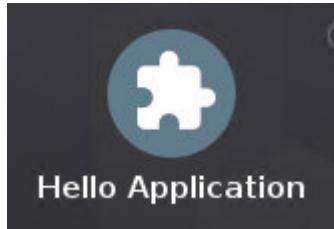
5. Go to **Settings**.

6. Enter /custom/hello/hello.sh as the **Command**.



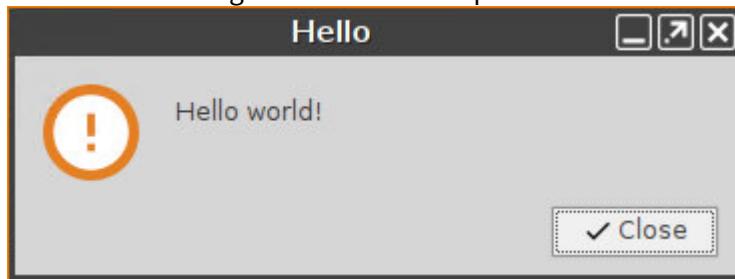
7. Click **OK**.

A **Hello Application** icon has appeared on the desktop.



8. Double-click the icon.

The "Hello" message window should open.



#### Next Step

>> [Using a Partition Parameter\(see page 535\)](#)

#### Using a Partition Parameter

When you roll out the same Custom Partition contents to many devices, you may still want the application to use different data or options on some of the devices. Partition parameters allow you to do this.

This is how you add a partition parameter to our "Hello World" program.

#### Setting a Partition Parameter in the Setup

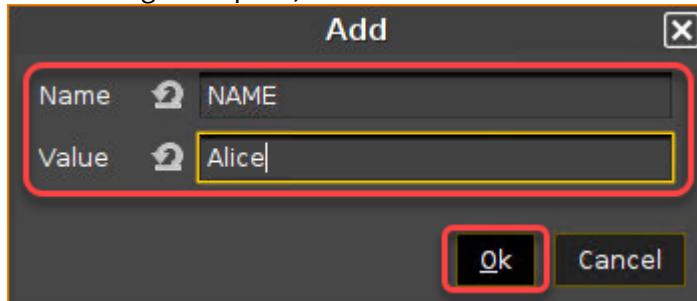
1. Go to **System > Firmware Customization > Custom Partition > Partition**.



2. In the **Partitions Parameters** list, click **+**.

The screenshot shows the 'Partitions Parameters' dialog in the 'Custom Partition > Partition' section of the setup tool. The left sidebar shows various configuration categories like Sessions, Accessories, User Interface, Network, Devices, Security, and System. Under System, there's a 'Firmware Customization' section with 'Custom Partition' selected. The main area has sections for 'Enable Partition' (checkbox checked), 'Size' (10M), and 'Mount Point' (/custom). Below these is a table for 'Partitions Parameters' with two columns: 'Name' and 'Value'. A '+' button is at the top right of the table. At the bottom are 'Apply', 'Ok', and 'Cancel' buttons.

3. In the dialog that opens, enter NAME as the **Name** and Alice as the **Value**. Click **OK**.



4. Click **Apply**.

#### Getting the Value of a Partition Parameter

This is the command line for getting or setting a Partition Parameter's value:

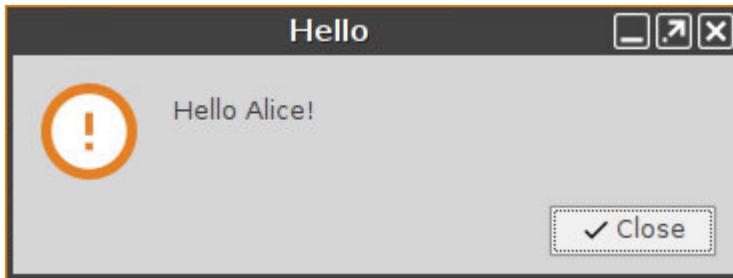
```
customparam [get|set] PARAMETER_NAME [PARAMETER_VALUE]
```

1. Change the hello.sh script to use this command to get the parameter value:

```
#!/bin/bash
gtkmessage -m "Hello $(customparam get NAME)!" -t "Hello" -o "Close"
```

2. Click the **Hello Application** desktop icon.

You should see the following:



## Packaging the Custom Partition

In the previous section, you developed Custom Partition contents locally on a device. Now, package it in order to deploy it to many devices via the Universal Management Suite (UMS).

Read all the following chapters in the order given and follow the instructions.

1. [Development Environment\(see page 537\)](#)
2. [Compressing the Custom Partition Contents\(see page 537\)](#)
3. [Writing the \\*.inf Metadata File\(see page 538\)](#)
4. [Uploading the Files to the UMS\(see page 538\)](#)
5. [Creating a Profile for the Custom Partition\(see page 544\)](#)
6. [Assigning the Profile\(see page 548\)](#)

When you have built this Custom Partition successfully, you can continue with a real-world partition. The following Custom Partitions are described in our tutorial:

- [Chromium\(see page 549\)](#)
- [Zoom\(see page 558\)](#)
- [Microsoft Teams\(see page 573\)](#)

### Development Environment

For this section, you need:

- a system with IGEL OS 11.01.100 or newer
- Universal Management Suite (UMS) 6.01.100 or newer

### Next Step

>> [Compressing the Custom Partition Contents\(see page 537\)](#)

### Compressing the Custom Partition Contents

The contents of a Custom Partition are packaged as a compressed tar file. Create it on the Linux command line, e.g. on a device that is running IGEL OS:

1. In the local terminal, become root and change to the /custom directory: cd /custom  

```
root@ITC00E0C51C5087:~# cd /custom
```
2. Compress the contents of the hello/ directory into an archive file named hello.tar.bz2:  
`tar cvf hello.tar.bz2 hello/`  

```
root@ITC00E0C51C5087:/custom# tar cvf hello.tar.bz2 hello/
```



The result is a `hello.tar.bz2` file, sitting side-by-side with the `hello/` directory. You will upload it to UMS later.

## Next Step

>> [Writing the \\*.inf Metadata File\(see page 538\)](#)

### Writing the \*.inf Metadata File

In addition to the compressed archive that you created in the previous step, a plain text file with essential information for the endpoint device is necessary. In this, step you will create the `hello.inf` file.

1. Change to the directory that contains the compressed contents of our Custom Partition (`hello.tar.bz2`): `cd /custom/`

```
root@ITC00E0C51C5087:/custom# cd /custom/
```

2. Create a new file named `hello.inf` and put the following into it:

```
[INFO]
[PART]
file="hello.tar.bz2"
version="1.0_igel1"
size="10M"
name="hello"
minfw="11.01.100"
```

The individual entries and their meaning are:

[INFO] Mandatory string

[PART] Mandatory string

file The filename of the `*.tar.bz2` archive

version The version of the contents, consisting of the vendor version (let's say this is "hello 1.0") and the IGEL package version (the first package we produced of the software), joined with an underscore.

size Size of the decompressed contents

name Name of this content, used for naming the subdirectory within the custom partition and for keeping track of installed contents

minfw Minimum firmware version required for these contents

3. Save the file.

## Next Step

>> [Uploading the Files to the UMS\(see page 538\)](#)

### Uploading the Files to the UMS

In this step, you upload the compressed `hello.tar.bz2` archive and the `hello.inf` metadata file to the UMS, which will serve them to other devices via HTTPS. To make the file available, you have to create a file object after transferring the physical file.



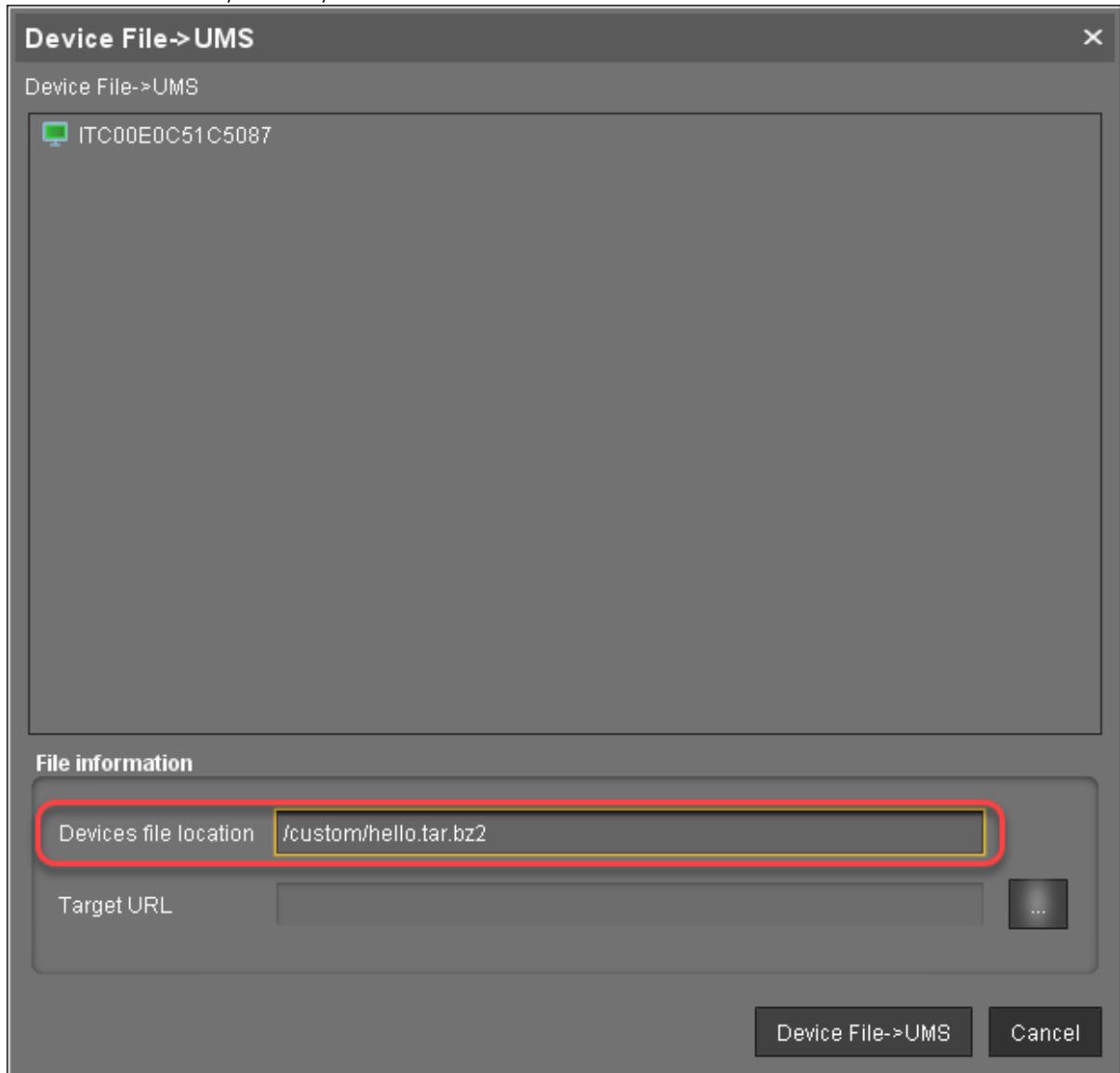
## Transferring the Files to the UMS

- In the structure tree of the UMS Console, go to the device on which you have created the files and select **Other commands > Device File->UMS**.

The screenshot shows the IGEL UMS Console interface. On the left, there's a tree view of devices under 'ITC00E0C51C5087'. In the center, a context menu is open for a specific device. The menu items include: Edit Configuration, Rename, Delete, Clear 'Configuration Change Status' flag, Access control, Cut, Copy, Paste, Shadow, Secure Terminal, Suspend, Shutdown, Wake up, Reboot, Update & snapshot commands, Other commands (which is expanded to show Take over settings from ..., Export Device Settings, Save device files for support, Release IGEL Cloud Gateway license), Logging, License manually..., Scan for devices, and a separator line followed by File UMS->Device, Device File->UMS (which is highlighted with a red box), Download Flashplayer, Remove Flashplayer, Store UMS Certificate, Remove UMS Certificate, Refresh license information, Refresh system information, and Refresh Asset Inventory data.



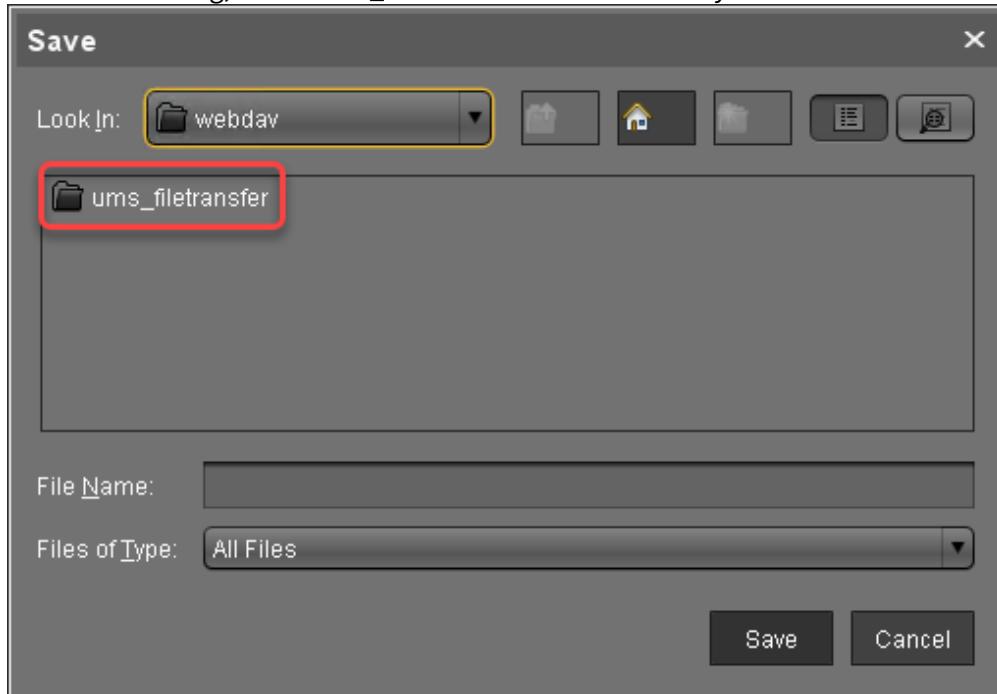
2. In the **Device File->UMS** dialog, under **Device file location**, enter the complete path and file name of the bz2 archive: "/custom/hello.tar.bz2"



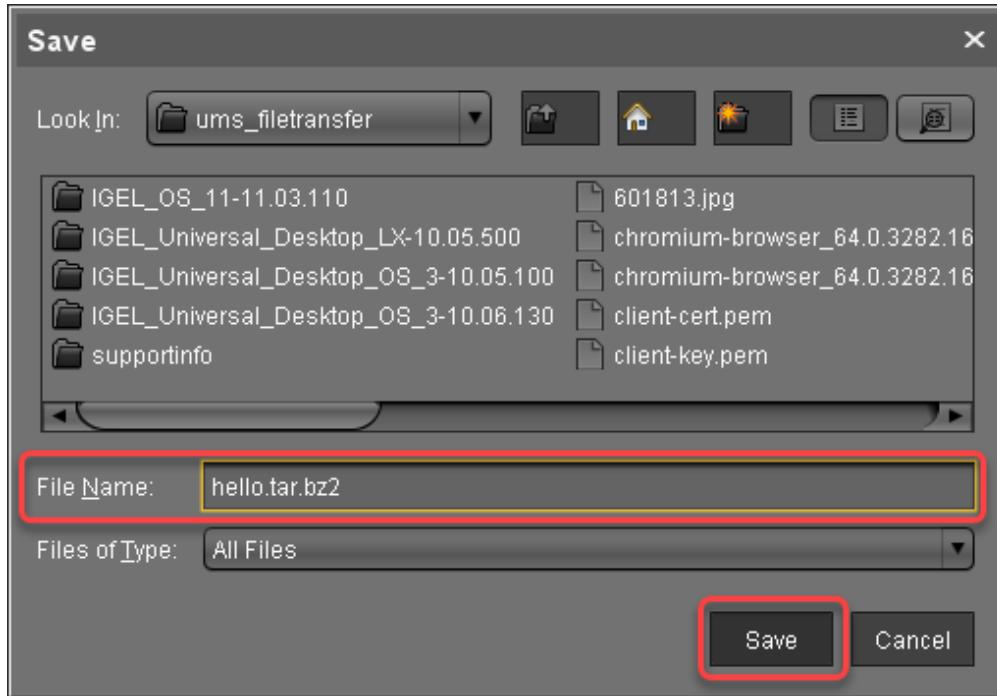
3. Click next to the **Target URL** to define the file path on the UMS Server.



4. In the **Save** dialog, select **ums\_filetransfer** as the directory.

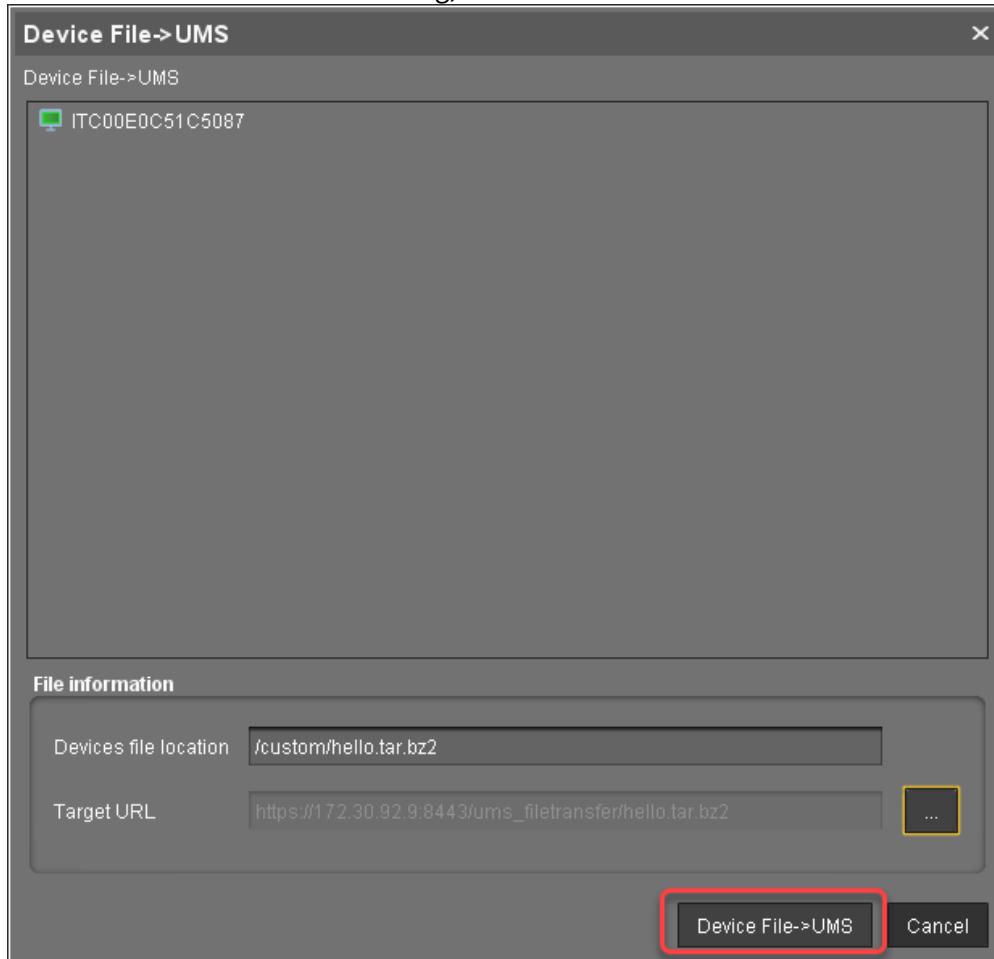


5. Enter "hello.tar.bz2" as the **File Name** and click **Save**.





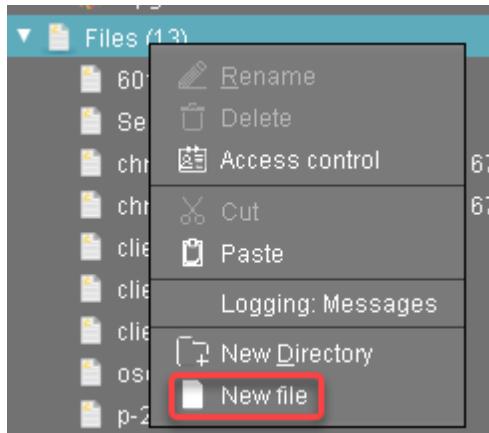
6. Back in the **Device File->UMS** dialog, click **Device File->UMS**.



7. Repeat steps 1 to 6 for the metadata file hello.inf.

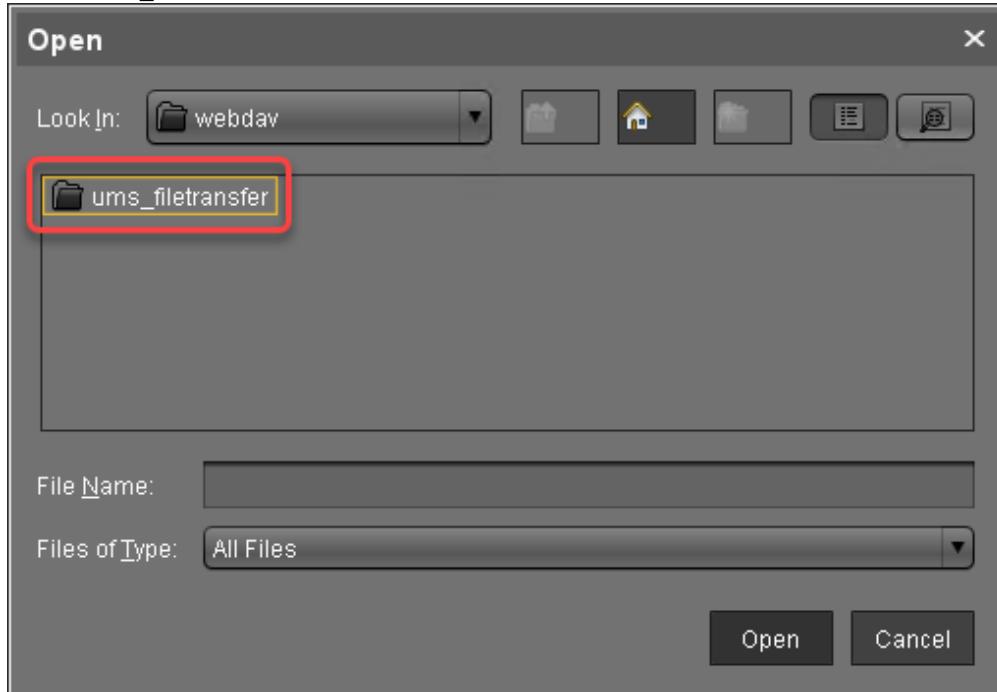
#### Creating File Objects

1. In the UMS Console, right-click the **Files** folder in the structure tree and select **New File** from the context menu.



The **New file** dialog opens.

2. Activate **Select from UMS server** and click  next to this option to open the file chooser.
3. Select **ums\_filetransfer**.



4. Select "hello.tar.bz2" and click **Open**.
5. Back in the **New file** dialog, click **Ok**.
6. Repeat steps 1 to 4 for the metadata file hello.inf.

#### Next Step

>> [Creating a Profile for the Custom Partition\(see page 544\)](#)

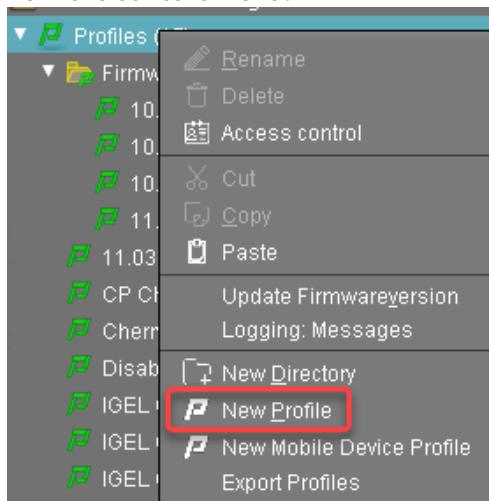


## Creating a Profile for the Custom Partition

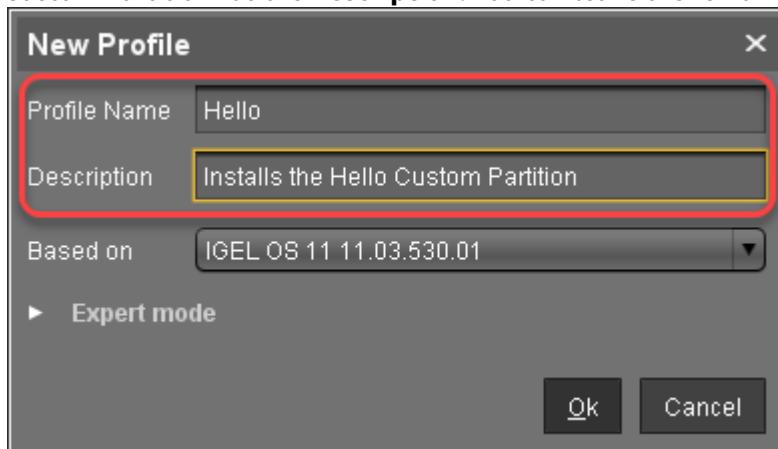
After you have uploaded the Custom Partition files to the UMS, you can now make the settings that will install the Custom Partition on any number of devices. For this purpose, we will create a profile.

### Activating the Custom Partition

1. In the structure tree of the UMS Console, right-click the **Profiles** folder and select **New Profile** from the context menu.



2. In the **New Profile** dialog, enter "Hello" as the **Profile Name** and something like "Installs the Hello Custom Partition" as the **Description**. You can leave the remaining fields.



3. Click **OK**.

The configuration dialog opens, where you will make the settings for this profile.

4. Go to **System > Firmware Customization > Custom Partition > Partition**.
5. Unlock the **Enable Partition** setting by clicking the orange triangle so that it turns blue.
6. Check **Enable Partition**.
7. Unlock the **Size** setting by clicking the orange triangle so that it turns blue, and enter "10M".



8. Leave the **Mount Point** at "/custom".

The screenshot shows the 'Hello' configuration interface. On the left, a tree view under 'System' shows 'Firmware Customization' and 'Custom Partition'. Under 'Custom Partition', 'Partition' is selected. In the main panel, there's a section titled 'Configuration' with various options like Sessions, Accessories, User Interface, Network, Devices, Security, and System. Under System, 'Firmware Customization' is expanded, and 'Custom Partition' is further expanded to show 'Partition'. To the right of this tree view is a form with fields: 'Enable Partition' (checkbox checked), 'Size' (set to 10M), and 'Mount Point' (set to '/custom'). Below this is a table titled 'Partitions Parameters' with one row: Name (Value). At the bottom are buttons for 'Apply and send to device', 'Save', and 'Cancel'.

#### Setting the Download Source

For this step, you need to determine the HTTPS download address for the hello.inf file first.

1. To find out the IP address of your UMS, go to **System > Remote Management** in the configuration dialog. You will find the IP address of the UMS Server your device is registered with.
2. Open a web browser and visit the following URL:  
`https://[IP or name of your UMS host]:8443/ums_filetransfer`
3. When prompted, authenticate with your UMS username and password.  
 You will see a directory listing of the files that can be downloaded from the UMS.



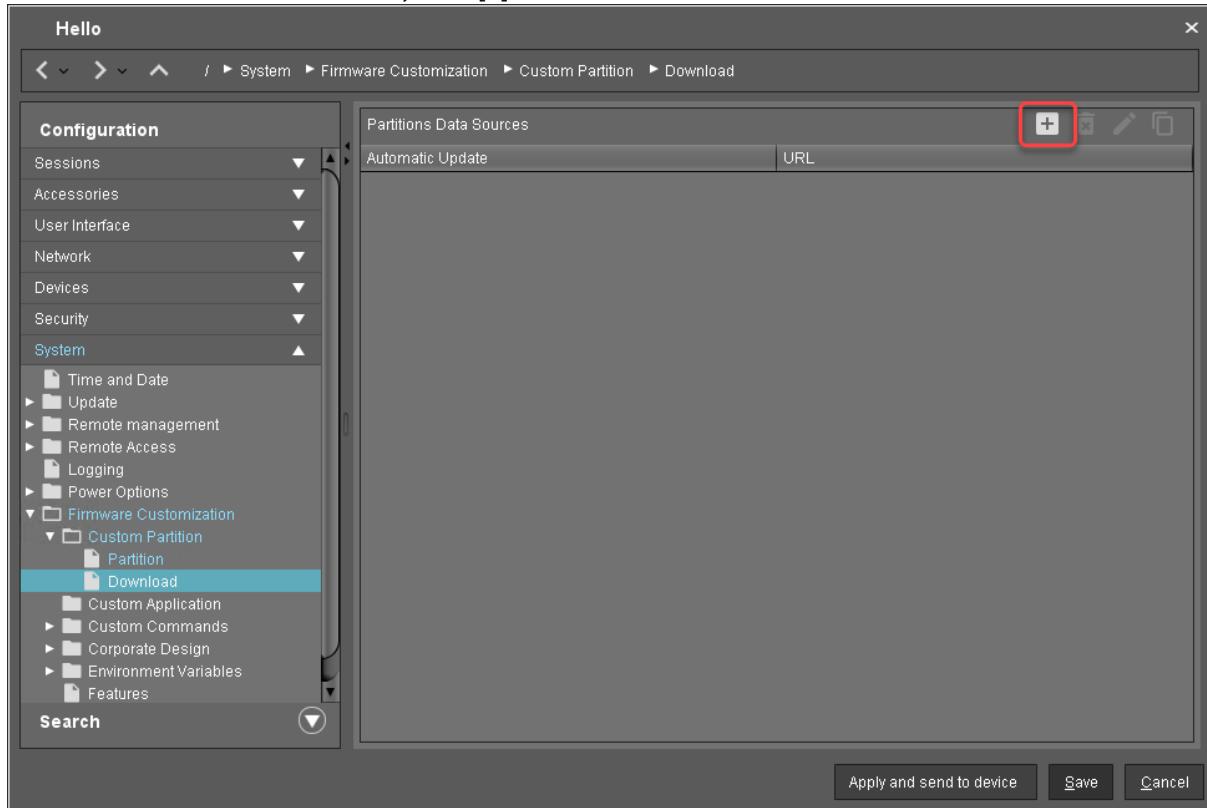
Directory Listing For [/]

Filename	Size	Last Modified
<a href="#">601813.jpg</a>	1138.8 kb	Fri, 29 Nov 2019 15:16:26 GMT
<a href="#">chromium-browser_64.0.3282.167.inf</a>	0.1 kb	Tue, 10 Mar 2020 15:35:45 GMT
<a href="#">chromium-browser_64.0.3282.167.tar.bz2</a>	68553.5 kb	Tue, 10 Mar 2020 15:34:09 GMT
<a href="#">client-cert.pem</a>	0.6 kb	Thu, 12 Dec 2019 12:21:12 GMT
<a href="#">client-key.pem</a>	0.2 kb	Thu, 12 Dec 2019 12:28:06 GMT
<a href="#">clientca-cert.pem</a>	0.6 kb	Thu, 12 Dec 2019 11:47:20 GMT
<a href="#">hello.inf</a>	0.1 kb	Mon, 11 May 2020 12:24:06 GMT
<a href="#">hello.tar.bz2</a>	0.2 kb	Mon, 11 May 2020 12:17:42 GMT
<a href="#">IGEL_OS_11-11.03.110/</a>		Wed, 11 Mar 2020 16:42:20 GMT
<a href="#">IGEL_Universal/Desktop/LX-10.05.500/</a>		Fri, 15 Mar 2019 13:55:11 GMT
<a href="#">IGEL_Universal/Desktop/OS_3-10.05.100/</a>		Mon, 18 Mar 2019 07:07:51 GMT
<a href="#">IGEL_Universal/Desktop/OS_3-10.06.130/</a>		Thu, 30 Jan 2020 16:09:01 GMT
<a href="#">installer-2.01.100.rc2.bin</a>	38964.0 kb	Thu, 10 Oct 2019 10:04:02 GMT
<a href="#">journalctl.txt</a>	218.8 kb	Fri, 20 Mar 2020 15:29:32 GMT
<a href="#">lx_10.05.700.rc7_public.zip</a>	856088.0 kb	Fri, 05 Apr 2019 14:15:46 GMT
<a href="#">osc.iso</a>	2184736.0 kb	Wed, 29 Apr 2020 14:06:05 GMT
<a href="#">p-20190712.pem</a>	0.7 kb	Thu, 12 Dec 2019 11:44:08 GMT

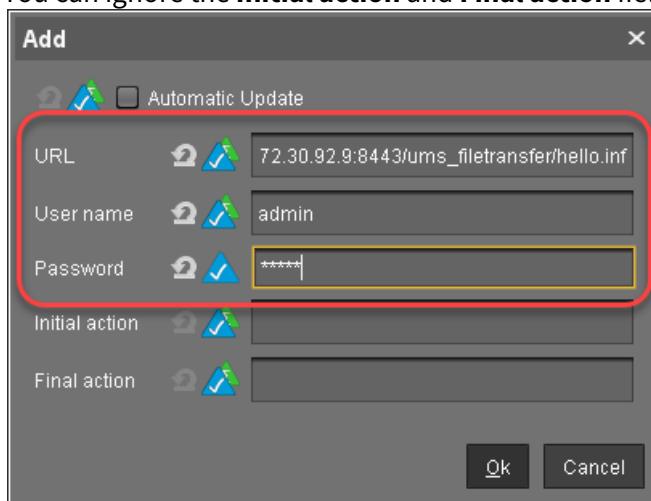
4. Right-click the `hello.inf` entry and select **Copy link address** (or the like, depending on your browser).
5. In the profile's settings, go to **System > Firmware Customization > Custom Partition > Download**.



6. Next to **Partitions Data Sources**, click [+].



7. The **Add** dialog opens.  
 8. Paste the URL you copied from the browser into **URL**.  
 9. Enter the **User name** and **Password** so that the device has access to your UMS.  
 You can ignore the **Initial action** and **Final action** fields for the time being.



10. Click **OK**.



## Creating a Custom Application

- Add a custom application to the profile by following the steps in [Creating the Custom Application](#)(see page 533).

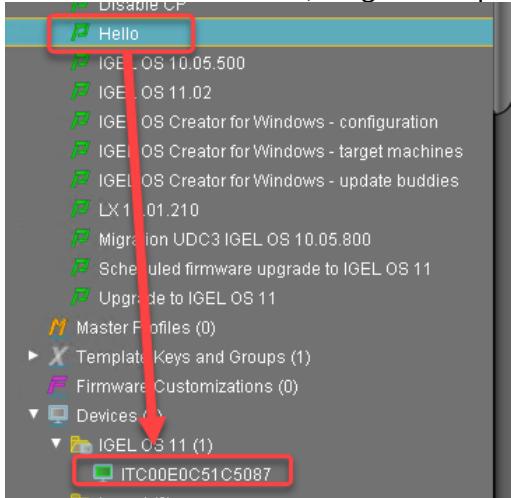
## Next Step

>> [Assigning the Profile](#)(see page 548)

## Assigning the Profile

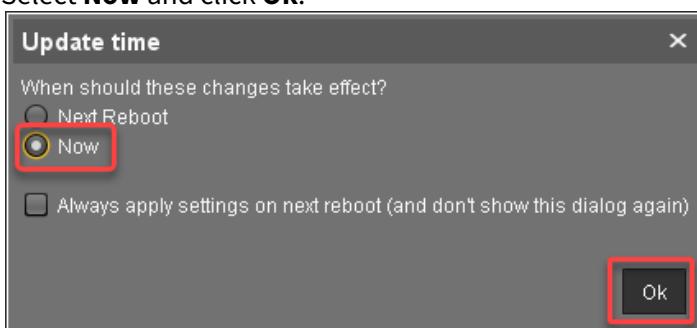
Now that you have put all the settings for installing the Custom Partition on a device into a profile, it is time to assign the profile.

1. In the UMS structure tree, drag and drop the icon of your profile onto the icon of a device.



The **Update time** dialog opens.

2. Select **Now** and click **Ok**.



The device receives the settings of the profile, creates the Custom Partition, downloads the contents of the Custom Partition and uncompresses them.

The **Hello Application** icon appears on the desktop.

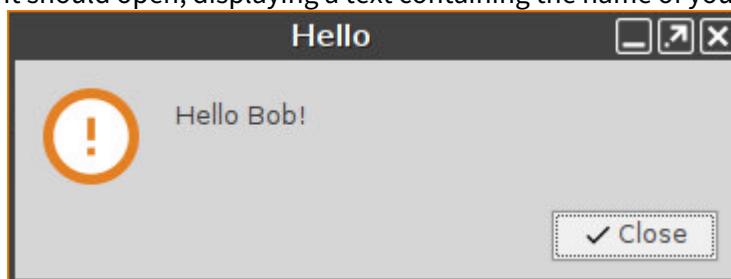
3. In the device's local Setup, go to **System > Firmware Customization > Custom Partition > Partition**.



4. Add a **Partition Parameter** with the **Name** "NAME" and a **Value** of your choice.



5. Back in the Setup, click **Ok**.  
 6. Click the icon to test the application.  
 It should open, displaying a text containing the name of your choice.



## A Real-World CP: Chromium

The previous example was simplified, but it taught you a lot of the IGEL Custom Partition fundamentals. Now build on top of these and try your hand at a real-world CP: the Chromium web browser - the Open Source sibling of Google Chrome, a complex application with a variety of features.

As you will be working with original Ubuntu packages, actual version numbers (or packages) may differ from this tutorial, as Ubuntu frequently update their packages. The method for building the CP, however, remains the same.

- [Development Environment\(see page 550\)](#)
- [Getting the Ubuntu Package\(see page 550\)](#)
- [Unpacking the Ubuntu Package\(see page 551\)](#)
- [Creating a Larger CP\(see page 551\)](#)
- [Setting Up Library Paths via Script\(see page 551\)](#)
- [The First Run\(see page 554\)](#)
- [Obtaining Libatomic\(see page 554\)](#)
- [Installing Libatomic\(see page 555\)](#)
- [Another Test Run\(see page 555\)](#)
- [Providing Libffmpeg\(see page 556\)](#)
- [Chromium Starts Successfully\(see page 556\)](#)
- [Packaging the Custom Application\(see page 557\)](#)
- [Advanced\(see page 558\)](#)



## Development Environment

For this section you need

- a system with IGEL OS version 10.03.100 or newer,
  - a Windows or Linux workstation with Universal Management Suite (UMS) in version 5.07.100 or newer,
  - a Debian or Ubuntu Linux workstation for unpacking the \*.deb package (can be the same as the Linux workstation hosting UMS),
  - a method to exchange files between the thin client and the workstation.
- While a USB pen or disk drive would do the trick, it is more convenient to have either a
- Windows fileshare or
  - an NFS export

that you can access both from the thin client and the workstation in order to exchange files.

[Learn how to mount network drives in the IGEL OS Manual.](#)<sup>201</sup>

## Getting the Ubuntu Package

As the Chromium web browser is Free Software it can be found in the package repositories of Linux distributions. To build Custom Partitions, use the software packages from exactly that Ubuntu version on which your version of IGEL OS is based. From IGEL OS 10.04 up to IGEL OS 11.03, this is Ubuntu 16.04 (Xenial Xerus). You need packages for the amd64 (also known as x86\_64) architecture.

This is how to find the right package and download it to your Linux workstation:

1. In a web browser, go to <https://packages.ubuntu.com>
2. Use the **Search package directories** form to search
  - a. Set **Keyword** to chromium
  - b. Set **Distribution** to xenial
  - c. Click **Search**.

## Search

### Search package directories

Keyword:	<input type="text" value="chromium"/>	<input type="button" value="Search"/>	<input type="button" value="Reset"/>		
Search on:	<input checked="" type="radio"/> Package names only <input type="radio"/> Descriptions <input type="radio"/> Source package names				
Only show exact matches:	<input type="checkbox"/>				
Distribution:	<input type="text" value="xenial"/>	▼	Section:	<input type="text" value="any"/>	▼

3. On the results page, click the **chromium-browser** package to go to its details page.
4. At the bottom of the details page, click the **amd64** link to download the package to a local directory on your Linux workstation.

---

<sup>201</sup> <http://edocs.igel.com/11105.htm>



## Unpacking the Ubuntu Package

Extract the Ubuntu package on your Debian/Ubuntu Linux workstation in order to access its files:

1. Open a terminal emulator.
2. Change to the directory where you saved the Ubuntu package.
3. Create a directory to extract the files to:  
`mkdir chromium-browser`
4. Extract the package to the new directory:  
`dpkg -x *.deb chromium-browser/`
5. Run the following command to see how much space the package contents need in total (in MB):  
`du -cms chromium-browser/*`  
 The total is 255 MB (your package may differ slightly). To be on the safe side let's memorize that we need approximately 400 MB of space for the CP contents.

## Creating a Larger CP

Create a larger Custom Partition so we can put all the Chromium package files into it.

1. On the thin client, make sure that you have closed all **Local Terminal** windows.
2. In UMS Console, navigate to your target thin client.
3. In **Assigned Objects**, remove the **Hello CP** profile from this thin client.
4. When prompted **When should these changes take effect?** select **Now**.  
 The existing Custom Partition is deleted.
5. Right-click the thin client and select **Edit Configuration**.
6. In Setup go to **System > Firmware Customization > Custom Partition > Partition**.
7. Check **Enable Partition**.
8. Set the **Size** to 400M (Megabyte) to be on the safe side.
9. Leave the **Mount Point** at /custom
10. Click **Save**.  
 The new Custom Partition is created.
11. On the thin client, open a **Local Terminal** and log in as root
12. Change into the Custom Partition: `cd /custom`
13. Check the size of the Custom partition: `df -h .`  
 It should be roughly 400M - if it is still roughly 10M, close **Local Terminal** and use **Setup** to first disable and then re-create the Custom Partition again.
14. Copy the complete `chromium-browser/` directory with all its contents from the Debian/Ubuntu machine into the Custom Partition on the thin client.

## Setting Up Library Paths via Script

With the whole package contents in place, you need to make sure that Chromium will be able to find its libraries and other needed files. There is a pre-fabricated script for this.

1. Log into **Local Terminal** as root.
2. Change into the `/custom/chromium-browser` directory.
3. Enter the command `ls -l`.



4. You will see that instead of a single script as in the previous example there are the etc / and usr / directories. They include many libraries and other files that Chromium will need to run. However, it expects these directories not within the /custom/chromium-browser / directory, but in the filesystem root, where system directories such as /usr are located. The Initialization Script for the Custom Partition will fix this by setting up symbolic links, so that for example /custom/chromium-browser/usr/lib/library.so will appear to be in /usr/lib/library.so, where Chromium expects it.
5. Use the GNU nano editor to create the file custompart-chromium-browser and put the following contents into it - alternatively, edit the file elsewhere and copy it into /custom/chromium-browser/:



```
#!/bin/sh
ACTION="custompart-chromium-browser_${1}"
# mount point path
MP=$(get custom_partition.mountpoint)
# custom partition path
CP="$MP/chromium-browser"
# output to systemlog with ID amd tag
LOGGER="logger -it ${ACTION}"
echo "Starting" | $LOGGER
case "$1" in
init)
    # Initial permissions
    chown -R root:system "${CP}" | $LOGGER
    chmod 755 "$MP" | $LOGGER
    # Linking files and folders on proper path
    find "${CP}" | while read LINE
    do
        DEST=$(echo -n "${LINE}" | sed -e "s|${CP}||g")
        if [ ! -z "${DEST}" -a ! -e "${DEST}" ]; then
            # Remove the last slash, if it is a dir
            [ -d $LINE ] && DEST=$(echo "${DEST}" | sed -e "s/\//${DEST}" | $LOGGER
        if [ ! -z "${DEST}" ]; then
            ln -sv "${LINE}" "${DEST}" | $LOGGER
        fi
    fi
done
ldconfig
;;
stop)
    killall -q -SIGTERM chromium-browser
    sleep 1
    killall -q -SIGKILL chromium-browser
;;
esac
echo "Finished" | $LOGGER
exit 0
```

Use this as a script template for your Custom Partitions, replacing all instances of chromium-browser with the directory name of your CP.



6. Make the script executable with the following command:

```
chmod a+x custompart-chromium-browser
```

7. Run the script:

```
./custompart-chromium-browser init
```

It should run and finish without any errors.

The library paths are set up now.

## The First Run

Now that the paths for the complete Chromium package contents have been set up, try running the program for the first time:

1. Log into **Local Terminal** as root.
2. Change into the /custom/chromium-browser/directory.
3. The `usr/bin/` and `usr/lib/` directories are good candidates for Chromium's main executable.

Try to run the following command:

```
./usr/lib/chromium-browser/chromium-browser
```

You will see the following error message:

```
/usr/lib/chromium-browser/chromium-browser: error while loading shared
libraries:
```

```
libatomic.so.1: cannot open shared object file: No such file or directory
```

This tells you that the program tries to load the shared library `libatomic.so.1`, but can't find it.

You will need to obtain `libatomic.so.1` and install it.

## Obtaining Libatomic

The source for Libatomic will be Ubuntu Package Search again:

1. In a web browser, go to <https://packages.ubuntu.com>
2. This time use the **Search the contents of packages** form to search.
  - a. Set **Keyword** to `libatomic.so.1`
  - b. Select **packages that contain files named like this**.
  - c. Set **Distribution** to `xenial`
  - d. Set **Architecture** to `amd64`
  - e. Click **Search**.

Keyword: <input type="text" value="libatomic.so.1"/>	<input type="button" value="Search"/>	<input type="button" value="Reset"/>	
Display:			
<input checked="" type="radio"/> packages that contain files named like this <input type="radio"/> packages that contain files whose names end with the keyword <input type="radio"/> packages that contain files whose names contain the keyword			
Distribution: <input type="text" value="xenial"/>	<input type="button" value="▼"/>	Architecture: <input type="text" value="amd64"/>	<input type="button" value="▼"/>

3. This time the results page lists a lot of packages. But with the background knowledge that IGEL OS libraries are located in `/usr/lib/x86_64-linux-gnu/` you will find that **libatomic1** is the desired package. Download it to a local directory on your Linux workstation.



/usr/lib/gcc-snapshot/libx32/libatomic.so.1	gcc-snapshot
/usr/lib/x86_64-linux-gnu/libatomic.so.1	libatomic1
/usr/lib32/libatomic.so.1	lib32atomic1

## Installing Libatomic

This step installs Libatomic and sets up a symbolic link so the Chromium will find it.

1. Extract the package contents with this command:

```
dpkg -x libatomic*.deb libatomic
```

2. Change into the extracted contents:

```
cd libatomic1/usr/lib/x86_64-linux-gnu/
```

3. List its contents in long form: ls -l

```
lrwxrwxrwx 1 huber huber 18 Nov 3 2016 libatomic.so.1 -> libatomic.so.1.1.0
-rw-r--r-- 1 huber huber 26760 Nov 3 2016 libatomic.so.1.1.0
```

This shows you that the library file is actually named libatomic.so.1.1.0 and that libatomic.so.1 is a symbolic link to it. We will recreate the link on the thin client later.

4. Transfer the libatomic.so.1.1.0 file to the thin client and place it in:

```
/custom/chromium-browser/usr/lib/chromium-browser/
```

5. Change into the directory:

```
cd /custom/chromium-browser/usr/lib/chromium-browser/
```

6. Create the symbolic link:

```
ln -s libatomic.so.1.1.0 libatomic.so.1
```

Now Libatomic is set up to be used by Chromium.

## Another Test Run

Test whether Chromium now has everything it needs to run.

1. Change into the Custom Partition directory on the thin client:

```
cd /custom/chromium-browser
```

2. Run Chromium:

```
./usr/lib/chromium-browser/chromium-browser
```

3. You will see this error message:

```
/usr/lib/chromium-browser/chromium-browser: error while loading shared
libraries:
```

```
libffmpeg.so: cannot open shared object file: No such file or
directory
```

It seems Libatomic is no longer a problem, but now Chromium needs a further library:

libffmpeg.so



## Providing Libffmpeg

To obtain Libffmpeg, repeat the process for [obtaining Libatomic\(see page 554\)](#). Hint: The Ubuntu package is named `chromium-codecs-ffmpeg`. It contains the file `libffmpeg.so`, which you need to transfer to the thin client. Place it in `/custom/chromium-browser/usr/lib/chromium-browser/`.

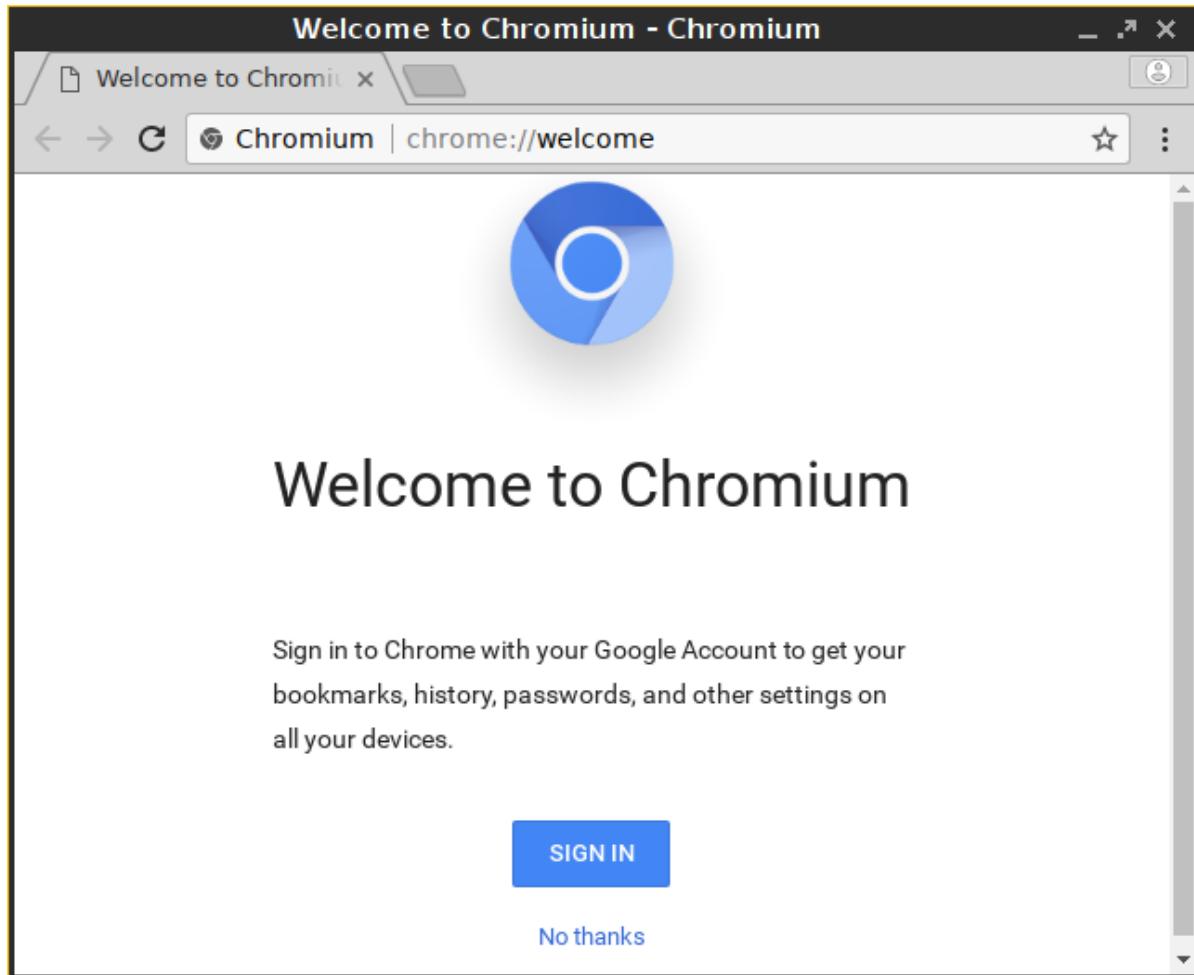
This is a procedure that you need to repeat until you have supplied all required libraries:

- Run the application from the commandline.
- Scan the error message for needed libraries.
- Obtain and install the required libraries.
- Run the application from the commandline.
- ...

## Chromium Starts Successfully

Now you are ready to give running Chromium another try. It does not like to be started by root, because it is much safer to run it as the non-privileged user.

1. Log into **Local Terminal** as user.
  2. Change into the `/custom/chromium-browser` directory.
  3. Enter the following command:  
`./usr/lib/chromium-browser/chromium-browser`
- Chromium starts for the first time. Congratulations, you now have working Chromium installation.



The next step will package the Custom Partition so it can be deployed to any number of thin clients from UMS:

#### Packaging the Custom Application

Now that the hardest part of creating the Custom Partition is done, package the CP for UMS. You are already familiar with most of the steps from earlier in this tutorial.

1. [Compress the CP Contents](#)(see page 537) into `chromium-browser.tar.bz2`
2. Upload the compressed file to UMS as a new **File**.
3. [Write the \\*.inf Metadata File](#)(see page 538) with 400M as **size**.
4. Upload the \*.inf Metadata File to UMS as a new **File**.
5. [Create a Profile for the CP](#)(see page 544) with the **Initializing Action** set to:  
`/custom/chromium-browser/custompart-chromium-browser init`  
and the **Finalizing Action** set to:  
`/custom/chromium-browser/custompart-chromium-browser stop`
6. [Create a Custom Application](#)(see page 533) with the **Command** set to:  
`/custom/chromium-browser/usr/lib/chromium-browser/chromium-browser`
7. Assign the CP to a new thin client in order to test everything.



## Advanced

Here are some advanced topics for you to try after you have completed this tutorial.

### Using ldd to Find Required Libraries

Using the `ldd` command is another way of determining the libraries that a binary requires.

1. Log into **Local Terminal** as root.
2. Find out which file the main binary of the Custom Partition is. It is usually found in `bin/`, `usr/bin/` or `usr/lib/` and is named similar to the application name.
3. Run the following command:  
`ldd /custom/[name]/[binary] | grep 'not found'`  
 This command line contains a filter, so that it will only show you those libraries that could not be found.

 A screenshot of a terminal window titled "Local Terminal". The window shows the command `root@GEORGE:/# ldd /custom/chromium-browser/usr/lib/chromium-browser/chromium-browser | grep 'not found'` being run. The output lists several shared libraries that were not found: `libatomic.so.1 => not found`, `libffmpeg.so => not found`, `libffmpeg.so => not found`, and `libffmpeg.so => not found`. The terminal prompt `root@GEORGE:/#` is visible at the bottom.

### Auto-updating Custom Partitions

The Custom Partition mechanism in IGEL OS can update the Custom Partition contents automatically when a newer version is available on UMS. To activate it, follow these steps:

1. In Setup, go to **System > Firmware Customization > Custom Partition > Download**.
2. Open the CP entry in the **Partitions Data Sources** list.
3. Enable **Automatic Update**.
4. Click **OK**.
5. Click **Apply** or **Save** in the Setup window.
6. On UMS, increase the `version` property in the `*.inf` metadata file.  
 When booting, the thin client checks whether there is a higher version of the Custom Partition available on UMS. If so, the new CP version will be downloaded automatically.

### Zoom as a Custom Partition

Now that you have learned the IGEL Custom Partition fundamentals, build on top of these and try your hand at a real-world Custom Partition: Zoom.

Read all the following chapters in the order given and follow the instructions.

1. [Development Environment](#)(see page 559)
2. [Getting the Packages](#)(see page 559)



3. Unpacking the Packages(see page 560)
4. Creating the Initialization Script(see page 560)
5. Compressing the Custom Partition Contents(see page 563)
6. Writing the \*.inf Metadata File(see page 563)
7. Uploading the Files to the UMS(see page 563)
8. Creating a Profile for the Custom Partition(see page 565)
9. Assigning the Profile and Testing the Application(see page 572)

## Development Environment

For this section, you need

- a system with IGEL OS 11.01.100 or newer,
- Universal Management Suite (UMS) 6.01.100 or newer,
- a Debian or Ubuntu workstation for unpacking the \*.deb package (can be the same as the Linux workstation hosting the UMS. Ideally, the machine is running Ubuntu 18.04 LTS.
- a method to exchange files between the endpoint device and the workstation.  
While a USB memory stick or disk drive would do the trick, it is more convenient to have either a
  - Windows fileshare or
  - an NFS export

that you can access both from the endpoint device and the workstation in order to exchange files.

[Learn how to mount network drives in the IGEL OS Manual.\(see page 1212\)](#)

## Next Step

[">>> Getting the Packages\(see page 559\)](#)

## Getting the Packages

Get the required packages for Ubuntu. Apart from the Zoom package, you need the package `libxcb-xtest0[version].deb` (contains the shared libraries `libxcb-test.so.0` and `libxcb-test.so.0.0.0` which are required by the Zoom package).

1. Open <https://zoom.us/download?os=linux> in a browser and select the following:
  - **Linux Type:** "Ubuntu"
  - **OS Architecture:** "64 bit"
  - **Version:** "16.04+"
2. Download the Ubuntu/Debian package `zoom_amd64.deb`

Version 5.0.399860.0429 has been tested by IGEL. Newer versions should work, too.

3. Change to the download directory on your workstation (typically `/home/[username]/Downloads`).
4. Download `libxcb-xtest0[version].deb` with the following command:  
`apt download libxcb-xtest0`

## Next Step

[">>> Unpacking the Packages\(see page 560\)](#)



## Unpacking the Packages

In this step, you extract the Ubuntu packages on your Linux workstation in order to access their files:

1. Open a terminal.
2. Change to the directory where you saved the packages.
3. Create a directory to extract the files to:  
`mkdir zoom`
4. Extract the packages to the new directory:  
`dpkg -x zoom*.deb zoom/`  
`dpkg -x libx*.deb zoom/`
5. Run the following command to see how much space the package contents need in total (in MB):  
`du -cms zoom/*`  
The total is 151 MB (your package may differ slightly). To be on the safe side, let's memorize that we need approximately 500 MB of storage space for the Custom Partition contents.

## Next Step

>> [Creating the Initialization Script](#)(see page 560)

## Creating the Initialization Script

In this step, you will create an initialization script that enables the application to work inside a Custom Partition. In a regular installation, the files of the Zoom application would be located in /usr, /opt and so on, whereas in the Custom Partition, they are located under /custom/zoom/usr, /custom/zoom/opt and so on. The initialization script will fix this by creating symbolic links so that for example /custom/zoom/usr/lib/library.so will appear to be in /usr/lib/library.so, where Zoom expects it.

1. On your workstation, go to the directory where the zoom directory is located.
2. Open your text editor of choice and enter the following script:



```

#!/bin/sh

ACTION="custompart-zoom_{1}"

# mount point path
MP=$(get custom_partition.mountpoint)

# custom partition path
CP="${MP}/zoom"

# wfs for persistent login and history
WFS="/wfs/user/.zoom/data"

# .zoom directory
ZOOM="/userhome/.zoom/"

# output to systemlog with ID and tag
LOGGER="logger -it ${ACTION}"

echo "Starting" | $LOGGER

case "$1" in
init)
    # Linking files and folders on proper path
    find ${CP} | while read LINE
    do
        DEST=$(echo -n "${LINE}" | sed -e "s|${CP}| |g")
        if [ ! -z "${DEST}" -a ! -e "${DEST}" ]; then
            # Remove the last slash, if it is a dir
            [ -d $LINE ] && DEST=$(echo "${DEST}" | sed -e "s|/|/|g")
            if [ ! -z "${DEST}" ]; then
                ln -sv "${LINE}" "${DEST}" | $LOGGER
            fi
        fi
    done

    # Linking /userhome/.zoom/data to /wfs/user/.zoom/data for some basic
    # persistency
    mkdir -p ${WFS}
    chown -R user:users ${WFS}
    mkdir -p ${ZOOM}/data
    chown -R user:users ${ZOOM}/data
    mkdir -p ${ZOOM}/data/VirtualBkgnd_Custom
    chown -R user:users ${ZOOM}/data/VirtualBkgnd_Custom
    mkdir -p ${ZOOM}/data/VirtualBkgnd_Default
    chown -R user:users ${ZOOM}/data/VirtualBkgnd_Default

    ln -sv ${WFS}/zoomus.db ${ZOOM}/data/zoomus.db | $LOGGER
    ln -sv ${WFS}/zoommeeting.db ${ZOOM}/data/zoommeeting.db | $LOGGER
esac

```



```

ln -sv ${WFS}/VirtualBkgnd_Custom ${ZOOM}/data/ | $LOGGER
ln -sv ${WFS}/VirtualBkgnd_Default ${ZOOM}/data/ | $LOGGER

chown user:users /wfs/user/.zoom
ln -sv /wfs/user/.zoom/zoomus.conf /userhome/.config/zoomus.conf |
$LOGGER

# remove all com.zoom.ipc* files from /wfs/user/.zoom/data - might
cause issues when updating zoom
rm ${WFS}/com.zoom.ipc*

# add /opt/zoom to ld_library
echo "${CP}/opt/zoom" > /etc/ld.so.conf.d/zoom.conf
ldconfig

${MP}/zoom_postinst | $LOGGER

;;
stop)
# unlink linked files
find ${CP} | while read LINE
do
      DEST=$(echo -n "${LINE}" | sed -e "s|${CP}||g")
      unlink $DEST | $LOGGER
done

# remove zoom.conf because it is not needed anymore
rm /etc/ld.so.conf.d/zoom.conf

;;
esac

echo "Finished" | $LOGGER

exit 0

```

The code line echo "\${CP}/opt/zoom" > /etc/ld.so.conf.d/zoom.conf tells the Zoom application via the configuration file zoom.conf to search for libraries in /custom/opt/zoom. This is expected by the Zoom application.

### 3. Save the file as custompart-zoom

Next Step

>> [Compressing the Custom Partition Contents\(see page 563\)](#)



## Compressing the Custom Partition Contents

To make the unpackaged software package usable in a Custom Partition, make the application files executable and put them into a compressed tar file.

1. On your Linux workstation, open a terminal and change to the directory that contains the zoom/ directory with the application files and the initialization script custompart-zoom.
2. Make the files in zoom/ and the initialization script executable:  
    chmod -R +x zoom  
    chmod +x custompart-zoom
3. Compress the zoom/ directory and the initialization script into an archive file named zoom\_[version].tar.bz2 (in our example: zoom\_5.0.399860.0429.tar.bz2):  
    tar cjvf zoom\_5.0.399860.0429.tar.bz2 zoom custompart-zoom

### Next Step

>> [Writing the \\*.inf Metadata File\(see page 563\)](#)

## Writing the \*.inf Metadata File

In addition to the compressed archive that you created in the previous step, a plain text file with essential information for the endpoint device is necessary. In this, step you will create the zoom.inf file.

1. Change to the directory that contains the compressed contents of our Custom Partition.
2. Create a new file named zoom.inf and put the following into it:

```
[INFO]
[PART]
file="zoom_5.0.399860.0429.tar.bz2"
version="5.0.399860.0429_igel1"
size="500M"
name="zoom"
minfw="11.01.100"
```

For an explanation of the settings, see the corresponding page in the section about building a simple Custom Partition: [Writing the \\*.inf Metadata File\(see page 538\)](#).

### Next Step

>> [Uploading the Files to the UMS\(see page 563\)](#)

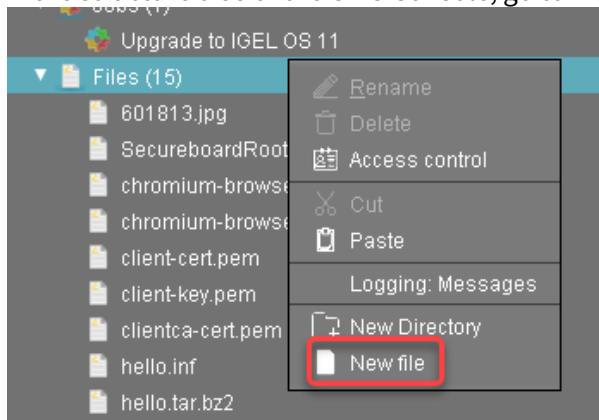
## Uploading the Files to the UMS

In this step, you upload the compressed zoom\_[version].tar.bz2 archive and the zoom\_[version].inf metadata file to the UMS, which will serve them to other devices via HTTPS. To make the file available, you have to create a file object after transferring the physical file.

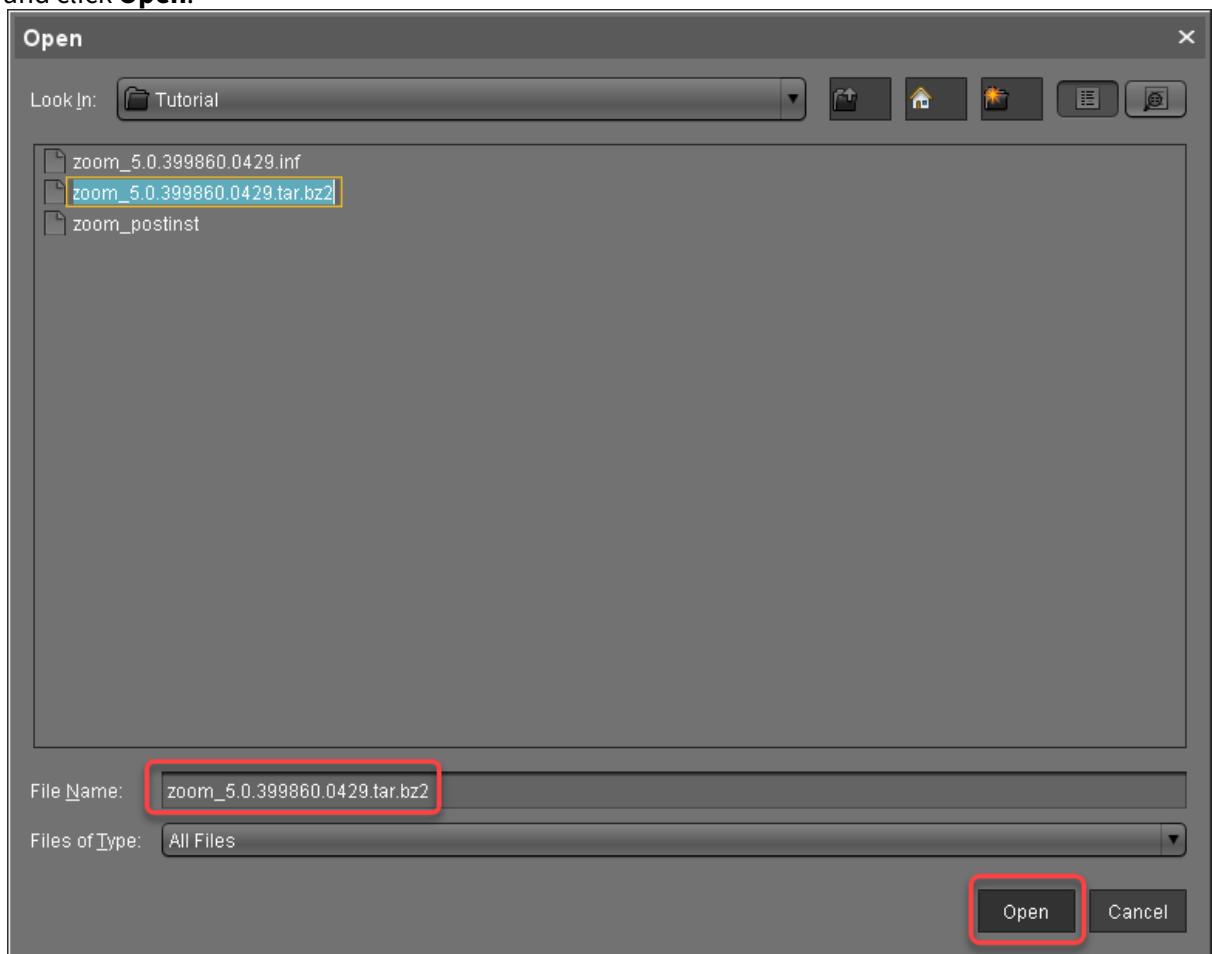


## Transferring the Files to the UMS

1. Make sure that the Zoom files can be accessed from the machine that hosts the UMS Console.
2. In the structure tree of the UMS Console, go to **Files** and select **New file** in the context menu.



3. Click  next to the **Local file** field, select zoom\_[version].tar.bz2 on your local machine, and click **Open**.





4. Click next to the **Target URL** to define the file path on the UMS Server.
5. Review the file name at **Local file** and click **Ok**.

**New file**

**File source**

Upload local file to UMS server

Local file

Upload location (URL)

Select file from UMS server

File location (URL)

**File target**

Classification

Devices file location

**Access rights**

	Read	Write	Execute
Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Others	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Owner

**Ok** **Cancel**

6. Repeat steps 1 to 5 for zoom\_[version].inf

#### Next Step

>> [Creating a Profile for the Custom Partition \(see page 565\)](#)

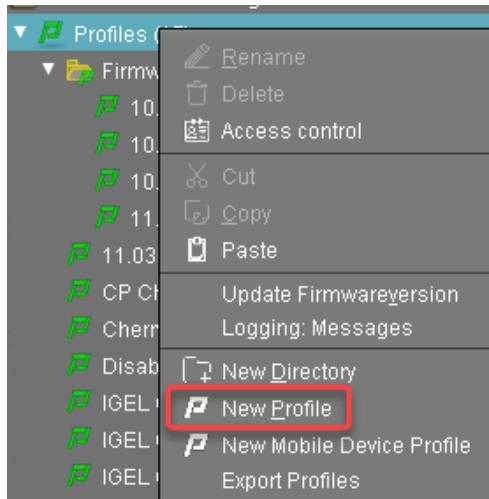
#### Creating a Profile for the Custom Partition

After you have uploaded the Custom Partition files to the UMS, you can now make the settings that will install the Custom Partition on any number of devices. For this purpose, you create a profile.

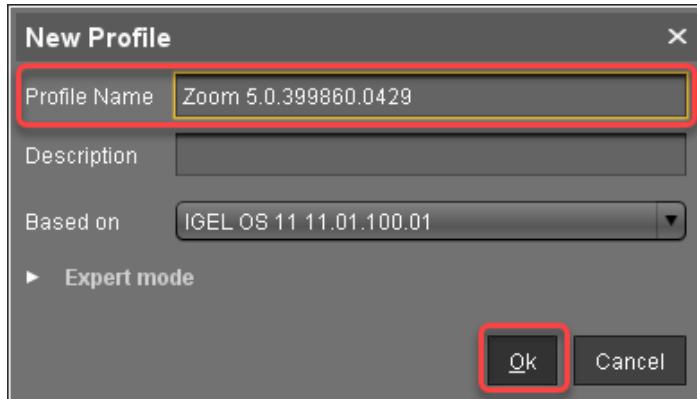


## Activating the Custom Partition

1. In the structure tree of the UMS Console, right-click the **Profiles** folder and select **New Profile** from the context menu.



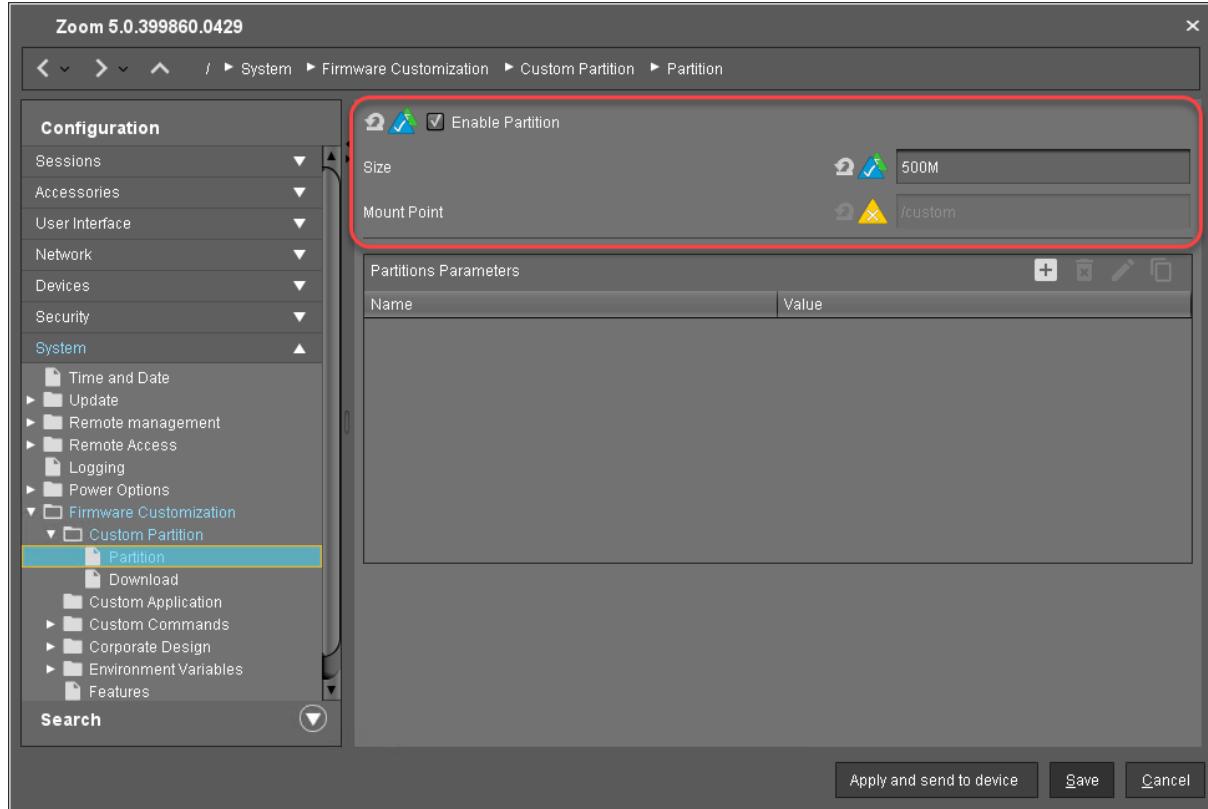
2. In the **New Profile** dialog, enter a **Profile Name**, e. g. "Zoom" followed by the version name, and click **Ok**.



3. Go to **System > Firmware Customization > Custom Partition > Partition**.
4. Unlock the **Enable Partition** setting by clicking the orange triangle so that it turns blue.
5. Check **Enable Partition**.
6. Unlock the **Size** setting by clicking the orange triangle so that it turns blue, and enter "500M".



7. Leave the **Mount Point** at "/custom".



#### Setting the Download Source

For this step, you need to determine the HTTPS download address for the zoom.inf file first.

1. To find out the IP address of your UMS, go to **System > Remote Management** in the configuration dialog. You will find the UMS Server your device is registered with and its IP address.
2. Open a web browser and visit the following URL:  
`https://[IP or name of your UMS host]:8443/ums_filetransfer`
3. When prompted, authenticate with your UMS username and password.  
 You will see a directory listing of the files that can be downloaded from the UMS.



4. Right-click the **zoom\_[version].inf** entry and select **Copy link address** (or the like, depending on your browser).

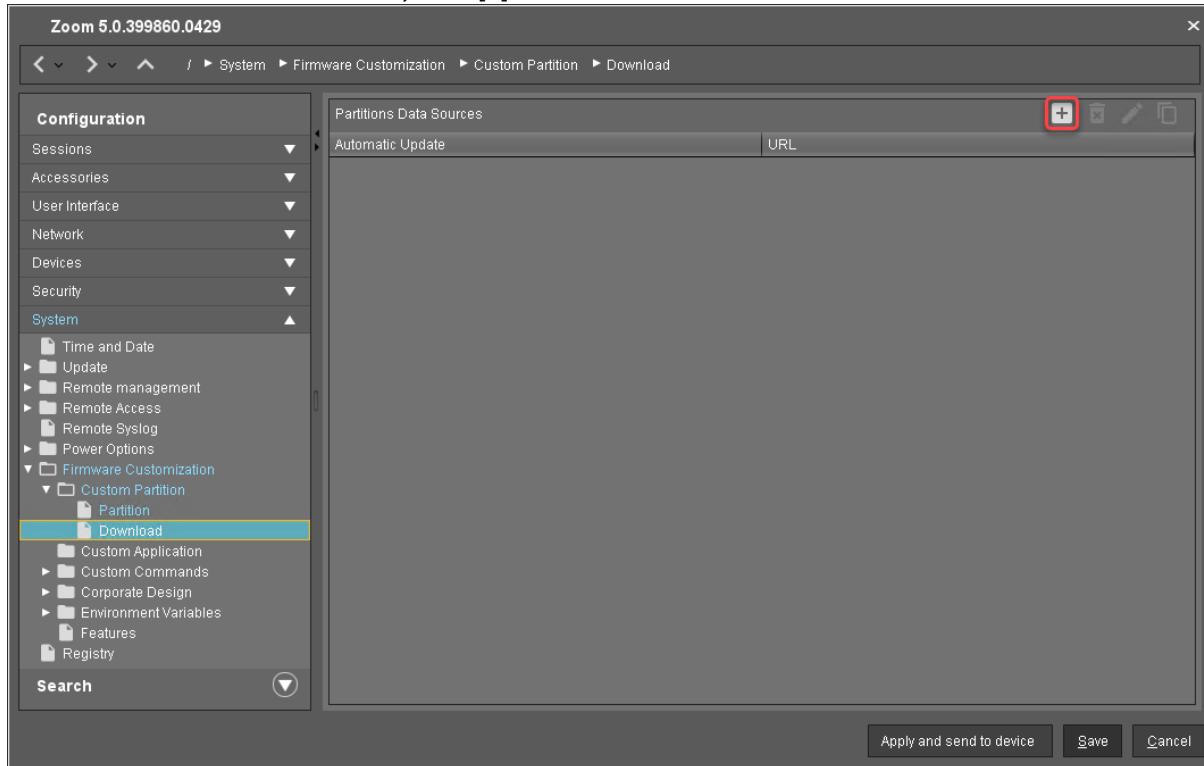
#### Directory Listing For [/]

Filename	Size	Last Modified
<a href="#">601813.jpg</a>	1138.8 kb	Fri, 29 Nov 2019 15:16:26 GMT
<a href="#">chromium-browser_64.0.3282.167.inf</a>	0.1 kb	Tue, 10 Mar 2020 15:35:45 GMT
<a href="#">chromium-browser_64.0.3282.167.tar.bz2</a>	68553.5 kb	Tue, 10 Mar 2020 15:34:09 GMT
<a href="#">client-cert.pem</a>	0.6 kb	Thu, 12 Dec 2019 12:21:12 GMT
<a href="#">client-key.pem</a>	0.2 kb	Thu, 12 Dec 2019 12:28:06 GMT
<a href="#">clientca-cert.pem</a>	0.6 kb	Thu, 12 Dec 2019 11:47:20 GMT
<a href="#">hello.inf</a>	0.1 kb	Mon, 11 May 2020 12:24:06 GMT
<a href="#">hello.tar.bz2</a>	0.2 kb	Mon, 11 May 2020 12:17:42 GMT
<a href="#">IGEL_OS_11-11.03.110/</a>		Wed, 11 Mar 2020 16:42:20 GMT
<a href="#">IGEL_Universal/Desktop/LX-10.05.500/</a>		Fri, 15 Mar 2019 13:55:11 GMT
<a href="#">IGEL_Universal/Desktop/OS_3-10.05.100/</a>		Mon, 18 Mar 2019 07:07:51 GMT
<a href="#">IGEL_Universal/Desktop/OS_3-10.06.130/</a>		Thu, 30 Jan 2020 16:09:01 GMT
<a href="#">installer-2.01.100.rc2.bin</a>	38964.0 kb	Thu, 10 Oct 2019 10:04:02 GMT
<a href="#">journalctl.txt</a>	218.8 kb	Fri, 20 Mar 2020 15:29:32 GMT
<a href="#">lx_10.05.700.rc7_public.zip</a>	856088.0 kb	Fri, 05 Apr 2019 14:15:46 GMT
<a href="#">osc.iso</a>	2184736.0 kb	Wed, 29 Apr 2020 14:06:05 GMT
<a href="#">p-20190712.pem</a>	0.7 kb	Thu, 12 Dec 2019 11:44:08 GMT
<a href="#">SecureboardRootCA.pem</a>	0.7 kb	Thu, 12 Dec 2019 11:40:35 GMT
<a href="#">supportinfo/</a>		Wed, 03 Apr 2019 10:35:27 GMT
<a href="#">tc_files_for_support_00E0C53627EE.zip</a>	133.7 kb	Wed, 29 Apr 2020 09:48:15 GMT
<a href="#">user-cert.der</a>	0.4 kb	Thu, 12 Dec 2019 12:13:25 GMT
<a href="#">user-key.pem</a>	0.2 kb	Thu, 12 Dec 2019 11:33:20 GMT
<a href="#">userca-cert.pem</a>	0.6 kb	Thu, 12 Dec 2019 16:30:59 GMT
<a href="#">zoom_5.0.399860.024.tar.bz2</a>	52687.5 kb	Thu, 14 May 2020 11:40:32 GMT
<a href="#">zoom_5.0.399860.024.tar.bz2</a>	0.1 kb	Thu, 14 May 2020 11:42:20 GMT
<a href="#">zoom_5.0.399860.024.tar.bz2</a>	52687.5 kb	Thu, 14 May 2020 12:55:31 GMT
<b>Apache Tomcat/8</b>		

5. Back in the profile, go to **System > Firmware Customization > Custom Partition > Download**.



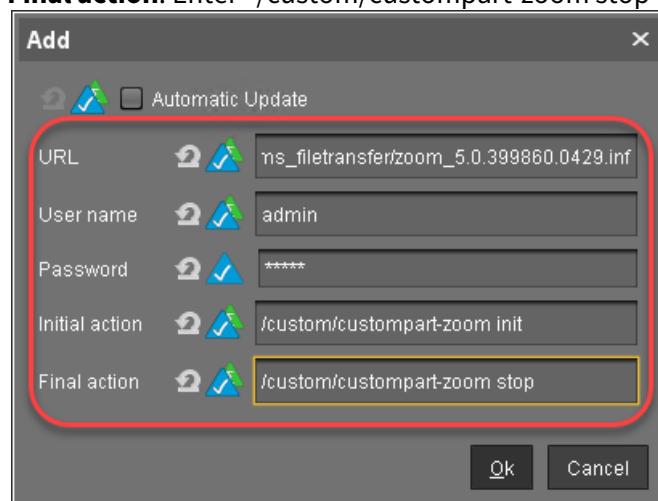
6. Next to **Partitions Data Sources**, click [+].



The **Add** dialog opens.

7. Edit the settings as follows:

- **URL:** Paste the URL you copied from the browser.
- **User name:** Username for accessing the UMS
- **Password:** Password for the username
- **Initial action:** Enter "/custom/custompart-zoom init".
- **Final action:** Enter "/custom/custompart-zoom stop".



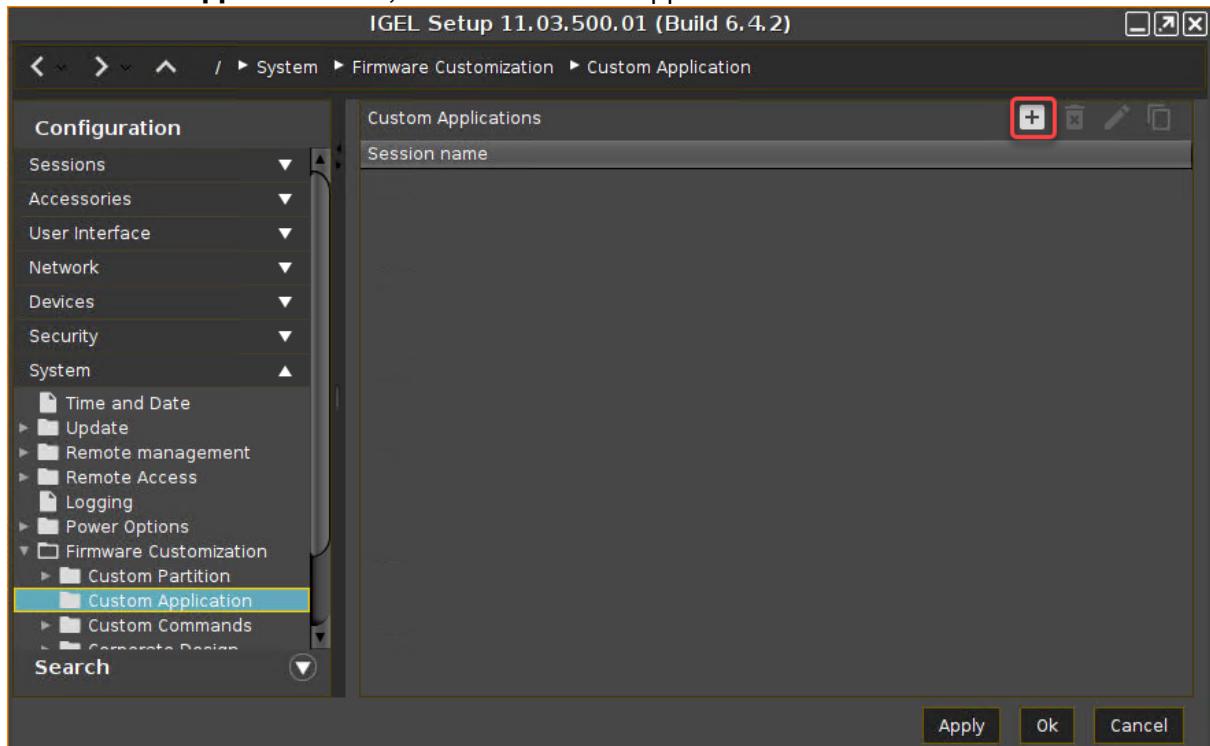
8. Click **OK**.



## Configuring the Custom Application

To create a convenient starting method for the user, create a custom application that includes a starter icon on the desktop.

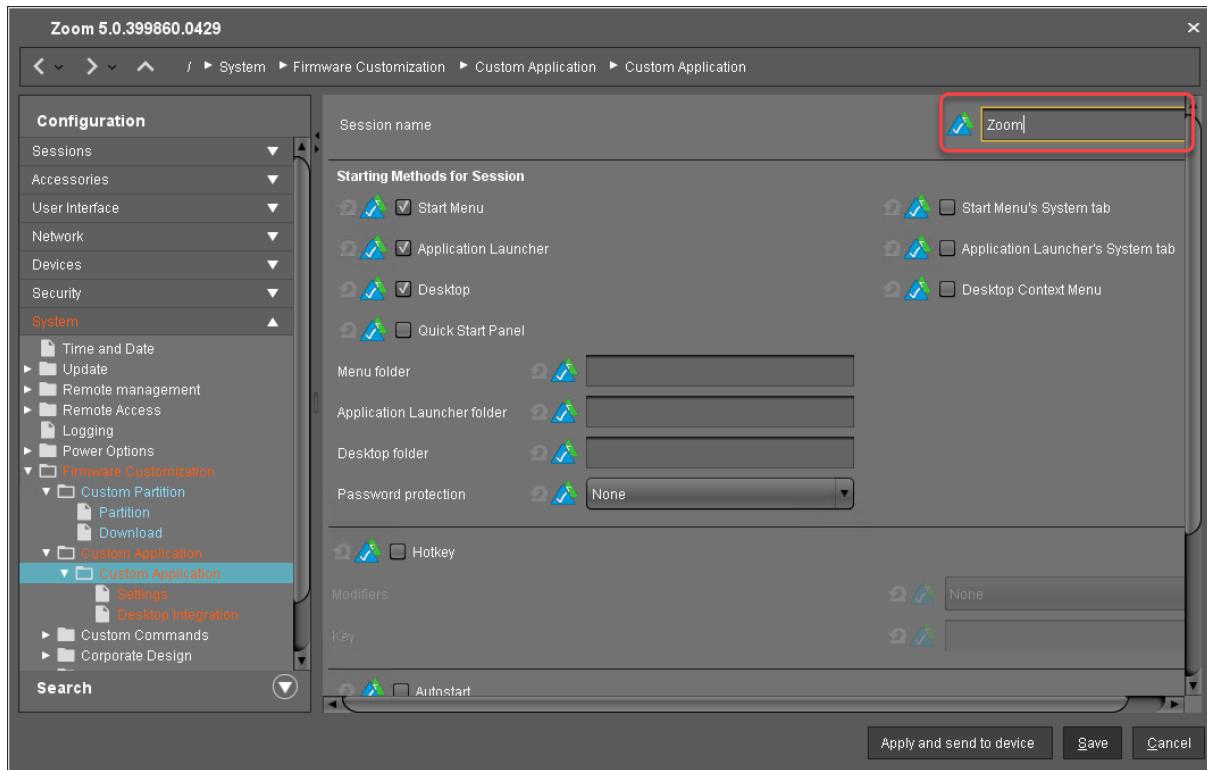
1. Go to **System > Firmware Customization > Custom Application**.
2. In the **Custom Applications** list, click to add an application.



The **Desktop Integration** page opens.



3. Enter "Zoom" as the **Session name**.



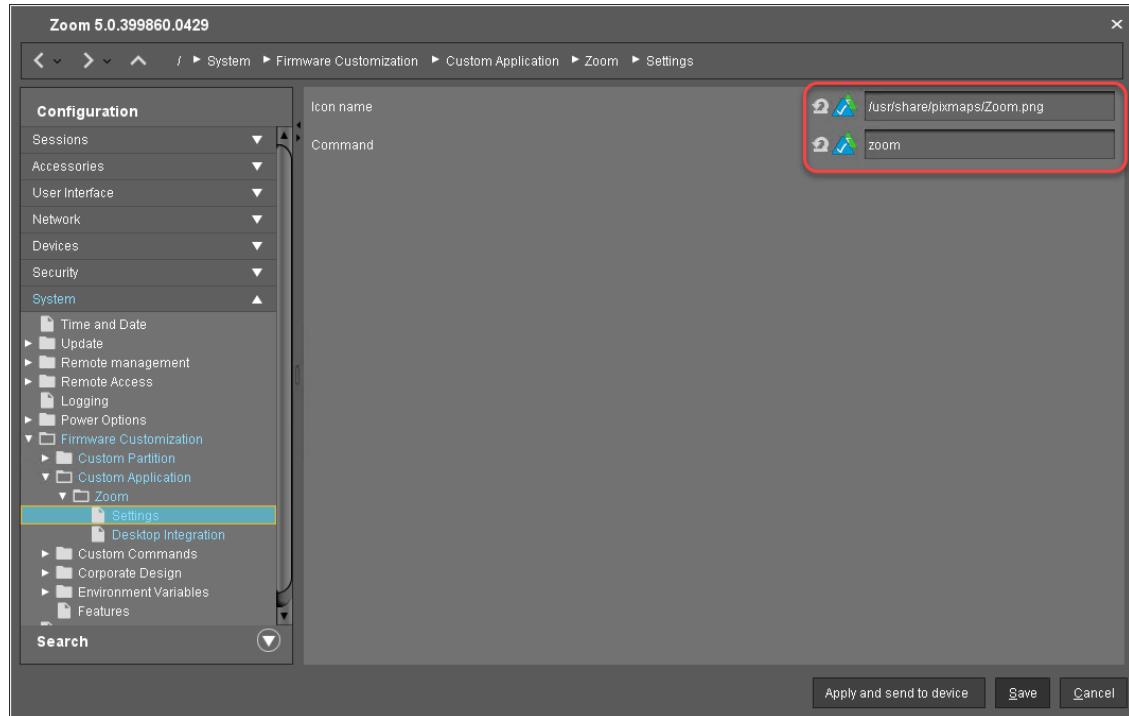
4. Go to **Settings**.

5. Edit the settings as follows:

- **Icon name:** Enter "/usr/share/pixmaps/Zoom.png".



- **Command:** Enter "zoom".



6. Click **Save**.

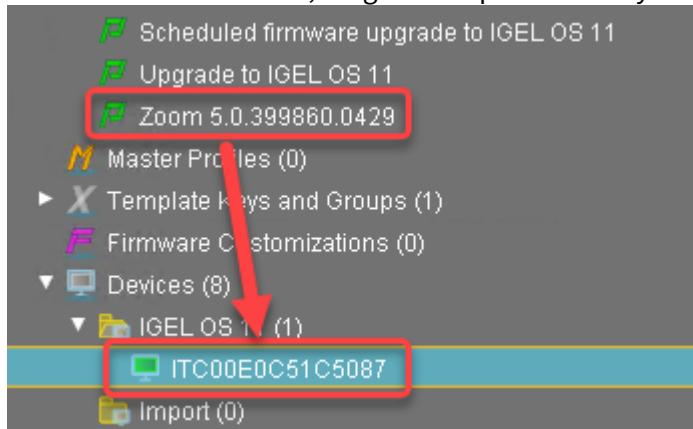
#### Next Step

>> [Assigning the Profile and Testing the Application](#)(see page 572)

#### Assigning the Profile and Testing the Application

Now that you have put all the settings for installing the Custom Partition on a device into a profile, it is time to assign the profile.

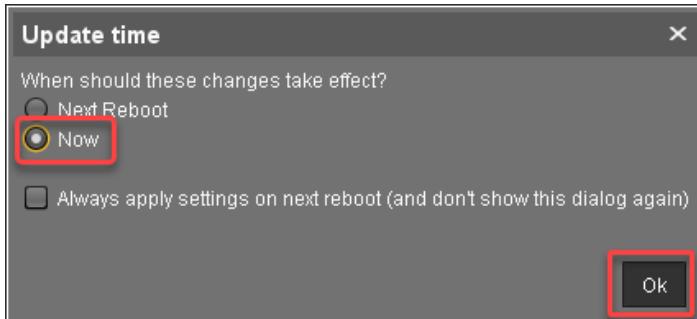
1. In the UMS structure tree, drag and drop the icon of your profile onto the icon of a device.



The **Update time** dialog opens.



2. Select **Now** and click **Ok**.



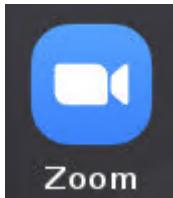
The device receives the settings of the profile, creates the Custom Partition, downloads the contents of the Custom Partition, and uncompresses them.

**Update Can Be Canceled After Timeout**

An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

On the desktop of the endpoint device, the Zoom icon should appear:



3. Click on the Zoom icon to test the Zoom application.

### Microsoft Teams as a Custom Partition

Now that you have learned the IGEL Custom Partition fundamentals, build on top of these and try your hand at a real-world Custom Partition: Microsoft Teams.

If you want to get an impression of how Microsoft Teams works on IGEL OS, watch this video:



Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:

<https://m.youtube.com/watch?v=3X0IKKu5eZY>

Read all the following chapters in the order given and follow the instructions.



1. Development Environment(see page 574)
2. Getting the Package(see page 574)
3. Unpacking the Packages(see page 575)
4. Creating the Initialization Script(see page 575)
5. Compressing the Custom Partition Contents+1(see page 577)
6. Writing the \*.inf Metadata File 1(see page 577)
7. Uploading the Files to the UMS(see page 578)
8. Creating a Profile for the Custom Partition(see page 580)
9. Assigning the Profile and Testing the Application(see page 587)

## Development Environment

For this section, you need

- a system with IGEL OS 11.01.100 or newer,
- Universal Management Suite (UMS) 6.01.100 or newer,
- a Debian or Ubuntu workstation for unpacking the \*.deb package (can be the same as the Linux workstation hosting the UMS). Ideally, the machine is running Ubuntu 18.04 LTS.
- a method to exchange files between the endpoint device and the workstation.  
While a USB memory stick or disk drive would do the trick, it is more convenient to have either a
  - Windows fileshare or
  - an NFS export

that you can access both from the endpoint device and the workstation in order to exchange files.

[Learn how to mount network drives in the IGEL OS Manual.](#)(see page 1212)

## Next Step

>> [Getting the Package](#)(see page 574)

## Getting the Package

Get the required package for Ubuntu.

1. Open <https://www.microsoft.com/en-us/microsoft-365/microsoft-teams/download-app#allDevicesSection> in a browser and click **Linux DEB (64-bit)**.

When you open the URL from a Windows machine, the Linux download button will probably not appear.

2. Download the package teams\_[version]\_amd64.deb (example:  
`teams_1.3.00.5153_amd64.deb`)
3. Change to the download directory on your workstation (typically `/home/[username]/Downloads`).

## Next Step

>> [Unpacking the Package](#)(see page 575)



## Unpacking the Packages

In this step, you extract the packages on your Linux workstation in order to access their files:

1. Open a terminal.
2. Change to the directory where you saved the packages.
3. Create a directory to extract the files to:  
`mkdir teams`
4. Extract the packages to the new directory:  
`dpkg -x teams*.deb teams/`
5. Run the following command to see how much space the package contents need in total (in MB):  
`du -cms teams/*`  
The total is 237 MB (your package may differ slightly). To be on the safe side, let's memorize that we need approximately 500 MB of storage space for the Custom Partition contents.

## Next Step

>> [Creating the Initialization Script](#)(see page 575)

## Creating the Initialization Script

In this step, you will create an initialization script that enables the application to work inside a Custom Partition. In a regular installation, the files of the Teams application would be located in /usr, whereas in the Custom Partition, they are located under /custom/teams/usr. The initialization script will fix this by creating symbolic links so that for example /custom/teams/usr/share/libffmpeg.so will appear to be in /usr/share/libffmpeg.so, where Teams expects it.

1. On your workstation, go to the directory where the teams directory is located.
2. Open your text editor of choice and enter the following script:



```

#!/bin/sh

ACTION="custompart-teams_${1}"

# mount point path
MP=$(get custom_partition.mountpoint)

# custom partition path
CP="${MP}/teams"

# only needed if application has an executable
BIN="/usr/bin/teams"

# output to systemlog with ID and tag
LOGGER="logger -it ${ACTION}"

echo "Starting" | $LOGGER

case "$1" in
init)
    # Linking files and folders on proper path
    find ${CP} | while read LINE
    do
        DEST=$(echo -n "${LINE}" | sed -e "s|${CP}| |g")
        if [ ! -z "${DEST}" -a ! -e "${DEST}" ]; then
            # Remove the last slash, if it is a dir
            [ -d $LINE ] && DEST=$(echo "${DEST}" | sed -e "s/\/$///g") | $LOGGER
            if [ ! -z "${DEST}" ]; then
                ln -sv "${LINE}" "${DEST}" | $LOGGER
            fi
        fi
    done
;;
stop)
    # unlink linked files
    find ${CP} | while read LINE
    do
        DEST=$(echo -n "${LINE}" | sed -e "s|${CP}| |g")
        unlink $DEST | $LOGGER
    done
;;
esac

echo "Finished" | $LOGGER

exit 0

```

3. Save the file as `custompart-teams`



## Next Step

>> [Compressing the Custom Partition Contents\(see page 577\)](#)

### Compressing the Custom Partition Contents

To make the unpackaged software package usable in a Custom Partition, make the application files executable and put them into a compressed tar file.

1. On your Linux workstation, open a terminal and change to the directory that contains the teams/ directory with the application files and the initialization script custompart-teams
2. Make the files in teams/ and the initialization script executable:  
    chmod -R +x teams  
    chmod +x custompart-teams
3. Compress the teams/ directory and the initialization script into an archive file named teams\_[version].tar.bz2 (in our example: teams\_1.3.00.5153.tar.bz2):  
    tar cvjf teams\_1.3.00.5153.tar.bz2 teams custompart-teams

## Next Step

>> [Writing the \\*.inf Metadata File\(see page 577\)](#)

### Writing the \*.inf Metadata File

In addition to the compressed archive that you created in the previous step, a plain text file with essential information for the endpoint device is necessary. In this, step you will create the teams.inf file.

1. Change to the directory that contains the compressed contents of our Custom Partition.
2. Create a new file named teams.inf and put the following into it:

```
[INFO]
[PART]
file="teams_1.3.00.5153.tar.bz2"
version="1.3.00.5153_igel1"
size="500M"
name="teams"
minfw="11.01.100"
```

For an explanation of the settings, see the corresponding page in the section about building a simple Custom Partition: [Writing the \\*.inf Metadata File\(see page 538\)](#).

## Next Step

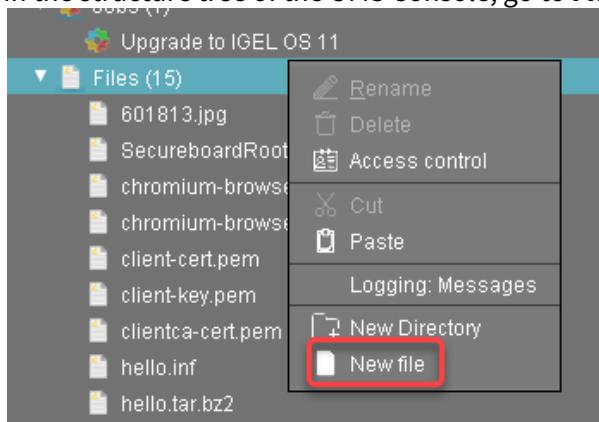
>> [Uploading the Files to the UMS\(see page 578\)](#)

## Uploading the Files to the UMS

In this step, you upload the compressed `teams_[version].tar.bz2` archive and the `teams_[version].inf` metadata file to the UMS, which will serve them to other devices via HTTPS. To make the file available, you have to create a file object after transferring the physical file.

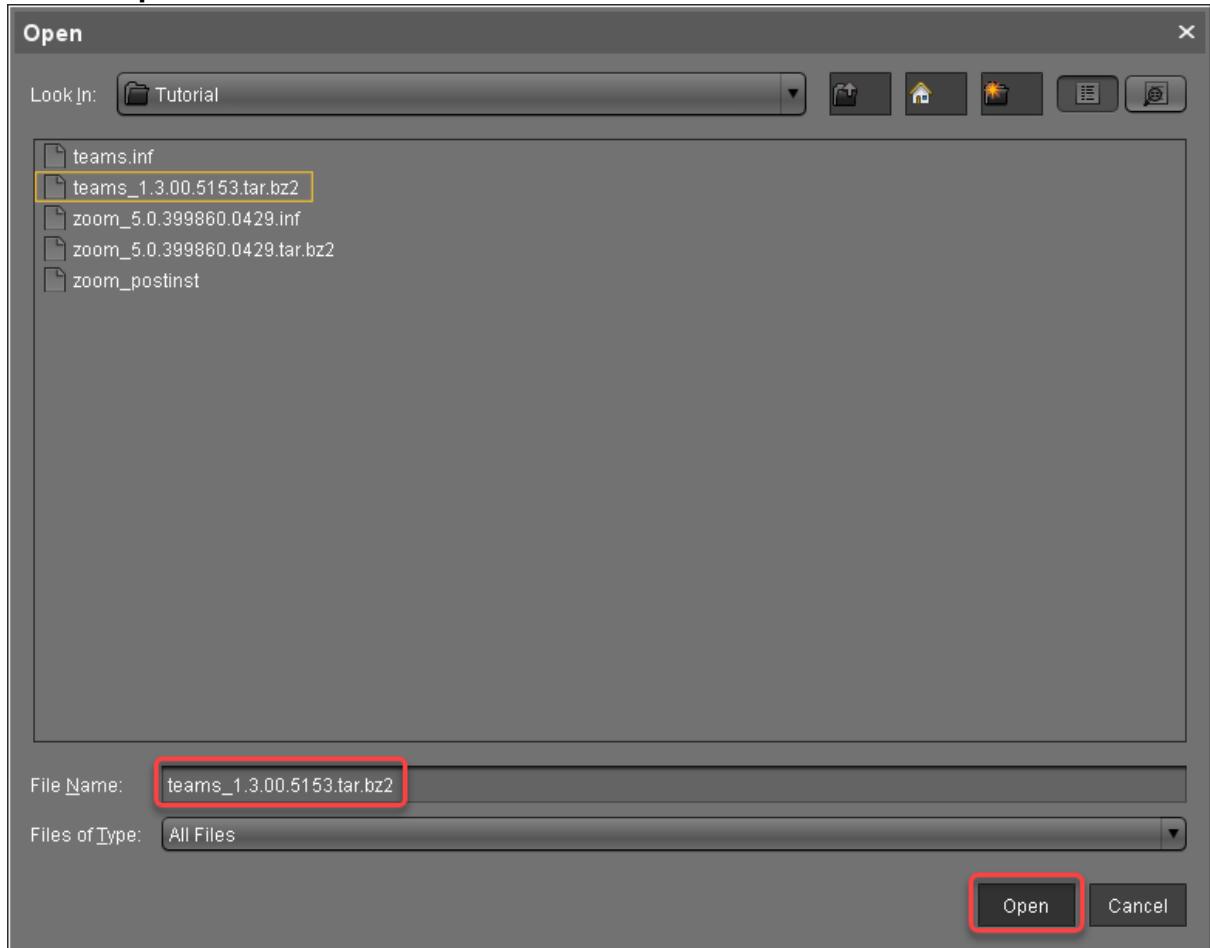
## Transferring the Files to the UMS

1. Make sure that the Teams files can be accessed from the machine that hosts the UMS Console.
2. In the structure tree of the UMS Console, go to **Files** and select **New file** in the context menu.





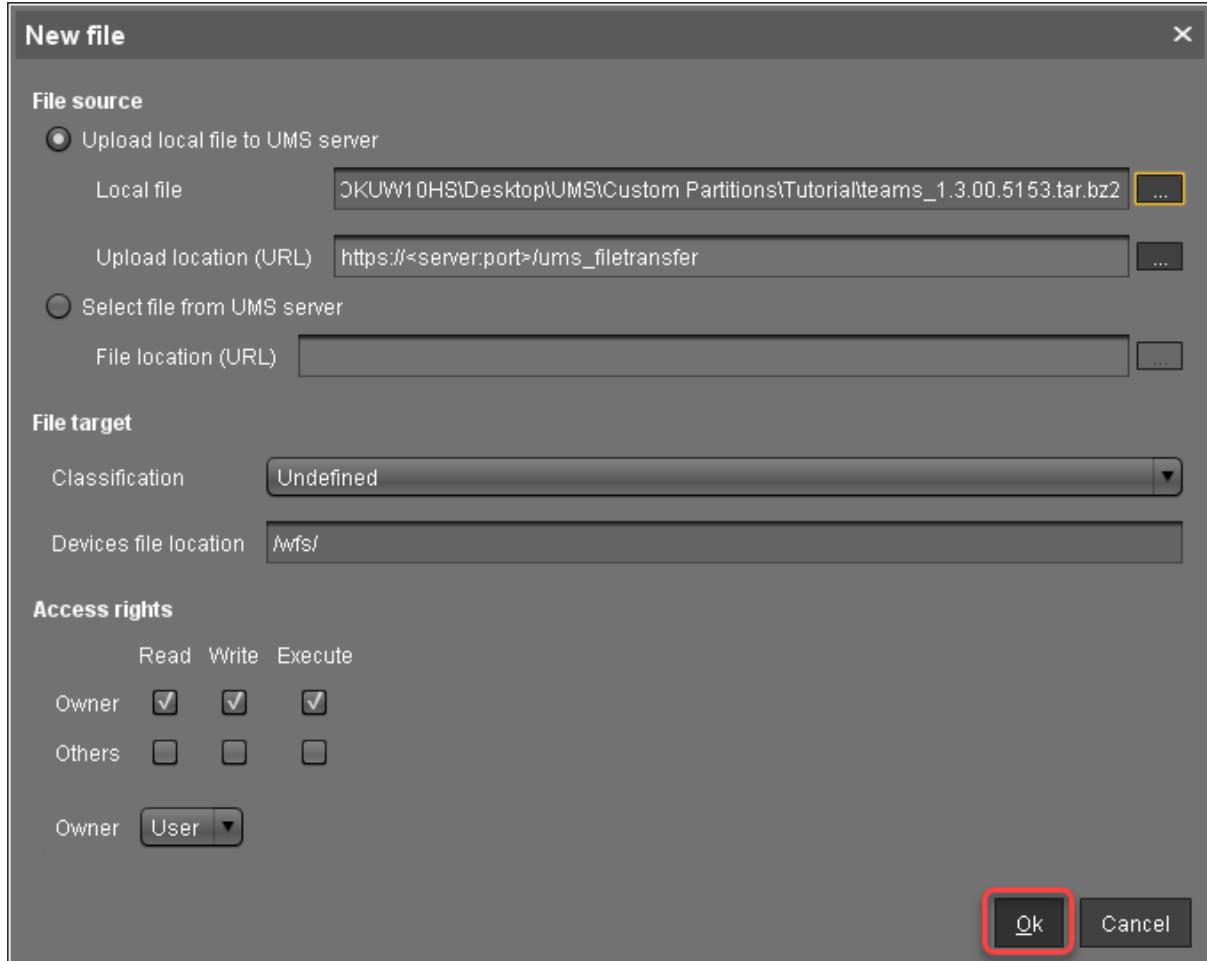
3. Click  next to the **Local file** field, select teams\_[version].tar.bz2 on your local machine, and click **Open**.



4. Click  next to the **Target URL** to define the file path on the UMS Server.



5. Review the file name at **Local file** and click **Ok**.



6. Repeat steps 1 to 5 for teams\_[version].inf

#### Next Step

>> [Creating a Profile for the Custom Partition](#)(see page 580)

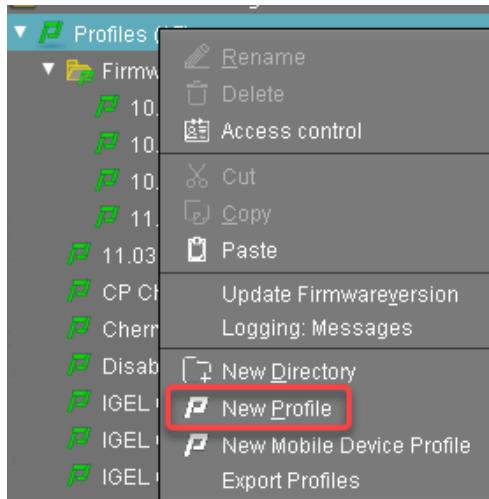
#### Creating a Profile for the Custom Partition

After you have uploaded the Custom Partition files to the UMS, you can now make the settings that will install the Custom Partition on any number of devices. For this purpose, you create a profile.

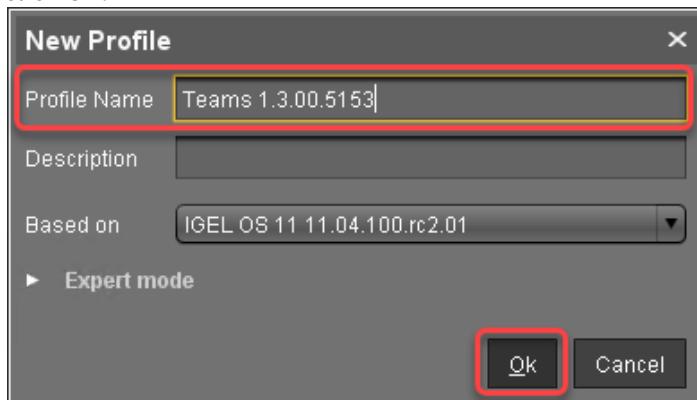


## Activating the Custom Partition

1. In the structure tree of the UMS Console, right-click the **Profiles** folder and select **New Profile** from the context menu.



2. In the **New Profile** dialog, enter a **Profile Name**, e. g. "Teams" followed by the version name, and click **Ok**.



3. Go to **System > Firmware Customization > Custom Partition > Partition**.
4. Unlock the **Enable Partition** setting by clicking the orange triangle so that it turns blue.
5. Check **Enable Partition**.
6. Unlock the **Size** setting by clicking the orange triangle so that it turns blue, and enter "500M".



7. Leave the **Mount Point** at "/custom".

The screenshot shows the 'Custom Partition' configuration screen in the Teams software. The 'Mount Point' field is highlighted with a red box and contains the value '/custom'. The 'Size' field is set to 500M. A message box in the center of the screen states: 'This feature requires an active Enterprise Management Pack subscription.' The left sidebar shows various system configuration categories like Sessions, Accessories, User Interface, Network, Devices, Security, and System. Under the System category, 'Firmware Customization' is expanded, and 'Custom Partition' is selected. The bottom right of the screen has buttons for 'Apply and send to device', 'Save', and 'Cancel'.

### Setting the Download Source

For this step, you need to determine the HTTPS download address for the teams.inf file first.

1. To find out the IP address of your UMS, go to **System > Remote Management** in the configuration dialog. You will find the UMS Server your device is registered with and its IP address.
2. Open a web browser and visit the following URL:  
[https://\[IP or name of your UMS host\]:8443/ums\\_filetransfer](https://[IP or name of your UMS host]:8443/ums_filetransfer)
3. When prompted, authenticate with your UMS username and password.  
 You will see a directory listing of the files that can be downloaded from the UMS.



4. Right-click the **teams\_[version].inf** entry and select **Copy link address** (or the like, depending on your browser).

Filename	Size	Last Modified
<a href="#">ovpn_test.ovpn</a>	3.6 kb	Tue, 26 May 2020 14:34:07 GMT
<a href="#">supportinfo/</a>		Tue, 26 May 2020 14:17:34 GMT
<a href="#">teams.inf</a>	0.1 kb	Fri, 12 Jun 2020 10:03:40 GMT
<a href="#">team</a>	79929.4 kb	Wed, 10 Jun 2020 10:31:14 GMT
<a href="#">team</a>	84073.9 kb	Fri, 12 Jun 2020 10:03:10 GMT

5. Back in the profile, go to **System > Firmware Customization > Custom Partition > Download**.

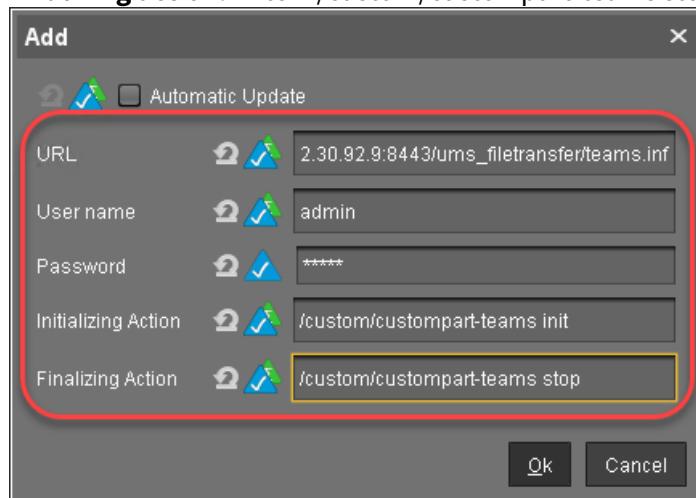
6. Next to **Partitions Data Sources**, click [+].

The **Add** dialog opens.



7. Edit the settings as follows:

- **URL:** Paste the URL you copied from the browser.
- **User name:** Username for accessing the UMS
- **Password:** Password for the username
- **Initializing action:** Enter "/custom/custompart-teams init".
- **Finalizing action:** Enter "/custom/custompart-teams stop".



8. Click **OK**.

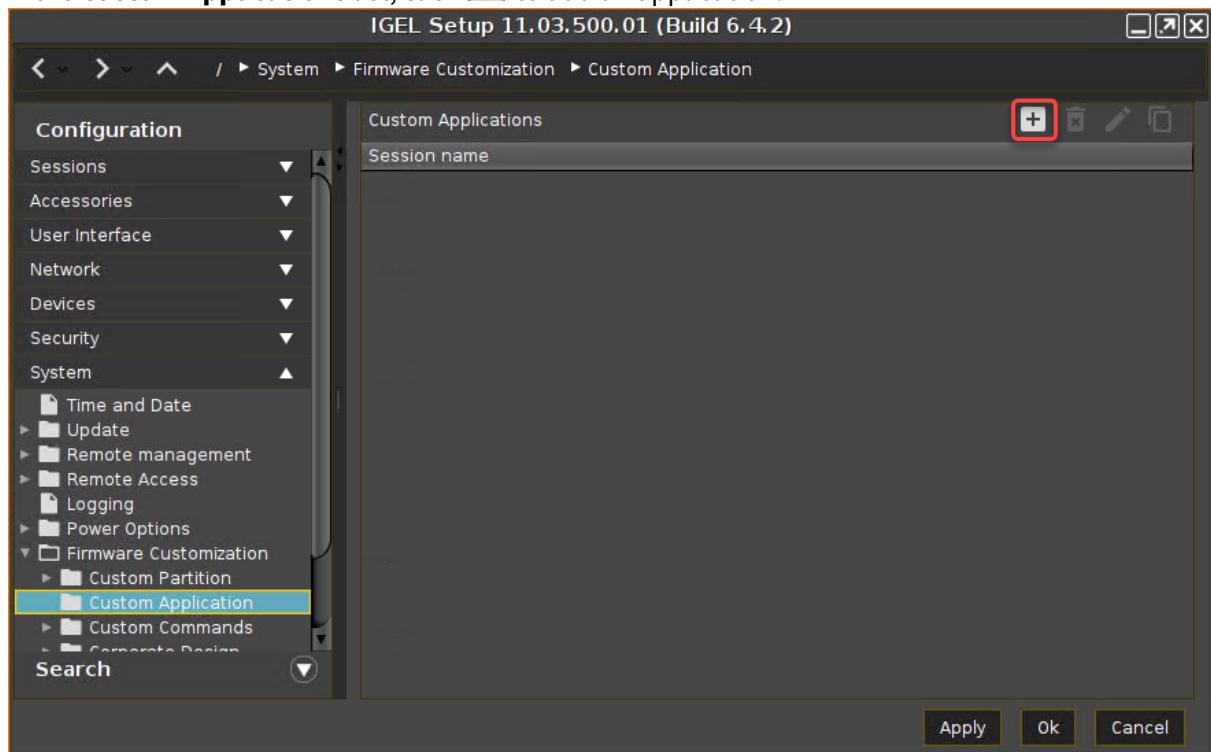
#### Configuring the Custom Application

To create a convenient starting method for the user, create a custom application that includes a starter icon on the desktop.

1. Go to **System > Firmware Customization > Custom Application**.



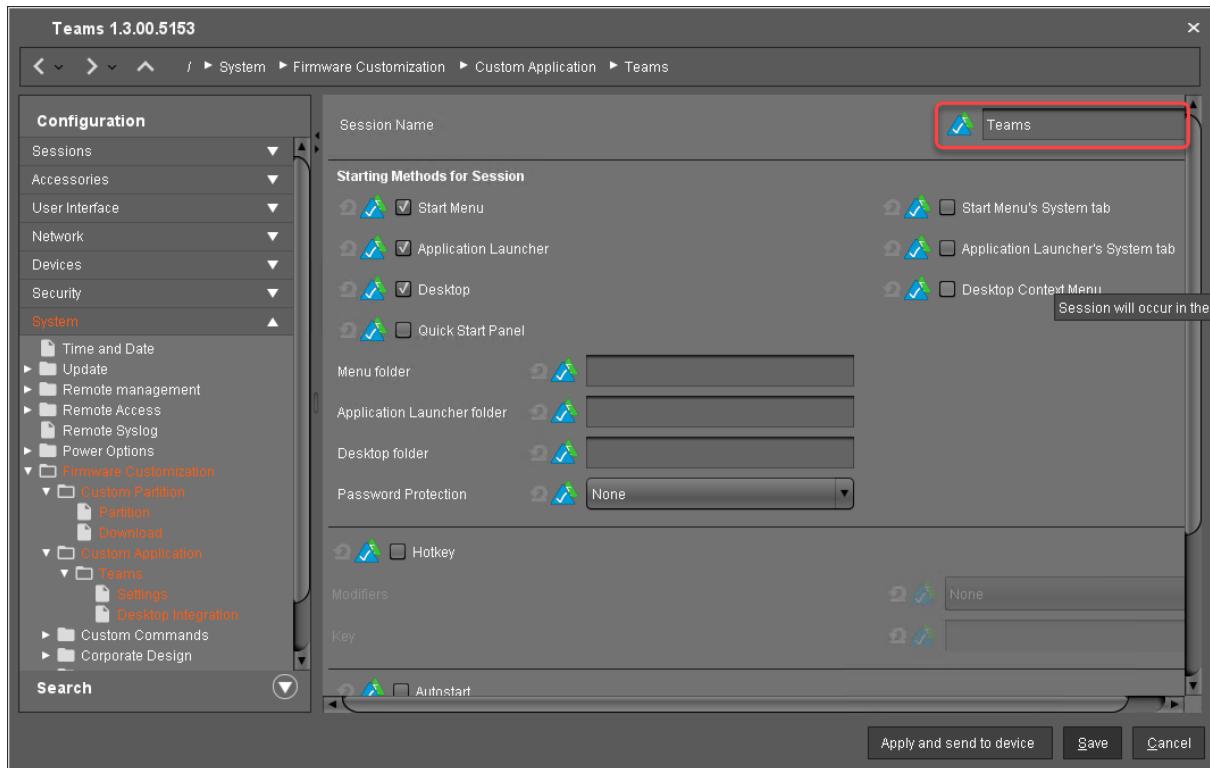
2. In the **Custom Applications** list, click to add an application.



The **Desktop Integration** page opens.



3. Enter "Teams" as the **Session name**.



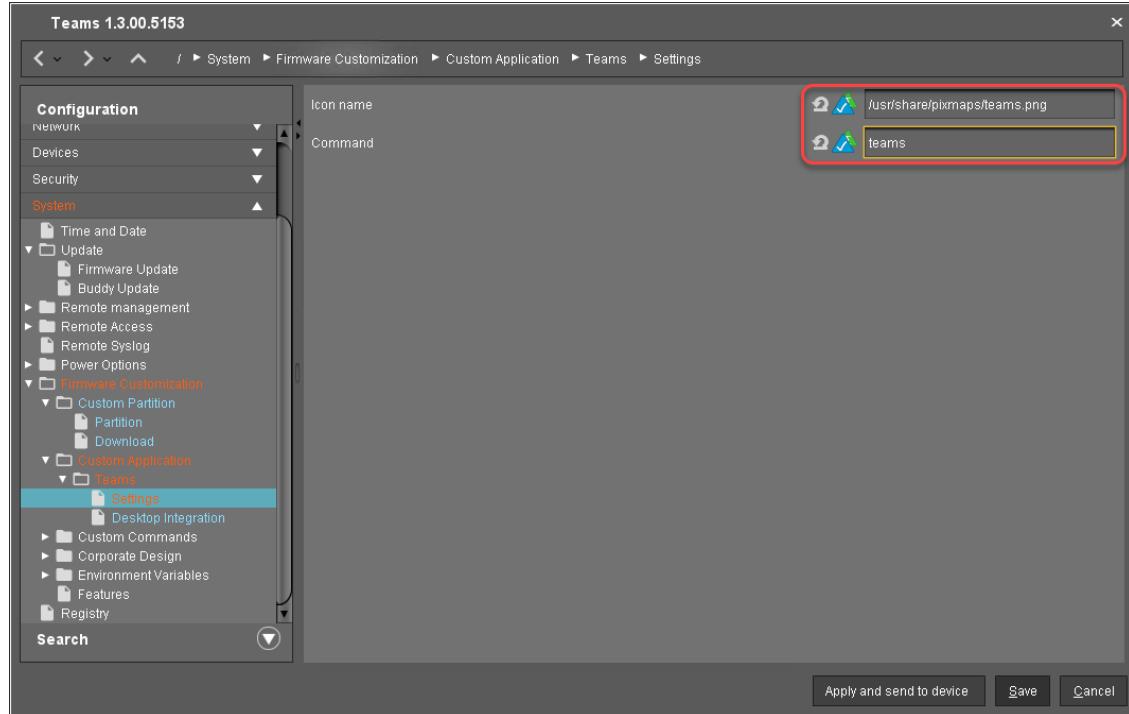
4. Go to **Settings**.

5. Edit the settings as follows:

- **Icon name:** Enter "/usr/share/pixmaps/teams.png".



- **Command:** Enter "teams".



6. Click **Save**.

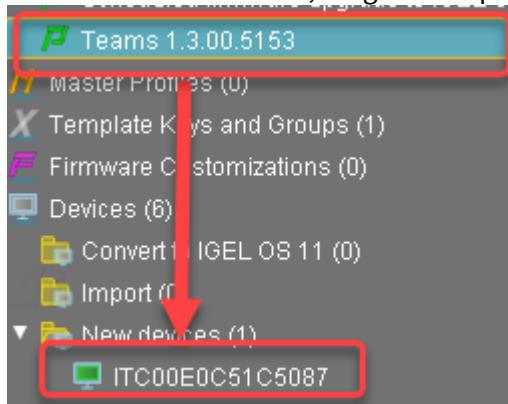
#### Next Step

>> [Assigning the Profile and Testing the Application](#)(see page 587)

#### Assigning the Profile and Testing the Application

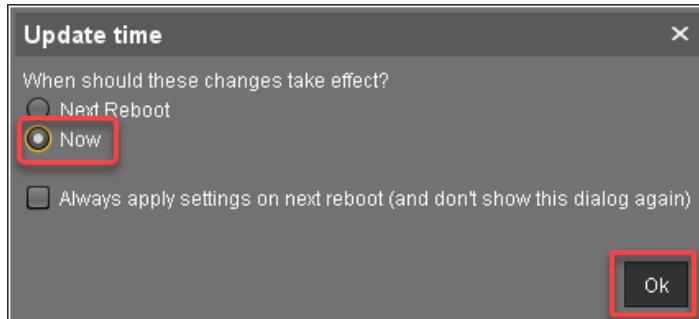
Now that you have put all the settings for installing the Custom Partition on a device into a profile, it is time to assign the profile.

1. In the UMS structure tree, drag and drop the icon of your profile onto the icon of a device.



The **Update time** dialog opens.

2. Select **Now** and click **Ok**.



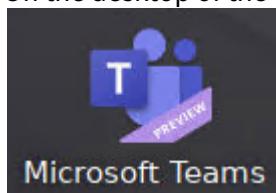
The device receives the settings of the profile, creates the Custom Partition, downloads the contents of the Custom Partition, and uncompresses them.

**Update Can Be Canceled After Timeout**

An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

On the desktop of the endpoint device, the Microsoft Teams icon should appear:



3. Click on the Microsoft Teams icon to test the application.

## 2.22.2 Using a Custom PKCS#11 Library

### Issue

You want to use your own PKCS#11 library.

### Problem

In the Setup, you cannot find how to activate a custom PKCS#11 library.



## Solution

In case of the installation of a custom PKCS#11 library, the file(s) must be placed on the endpoint device either via [UMS file transfer<sup>202</sup>](#) or [Custom Partition](#)(see page 529).

The use of the /wfs folder is NOT recommended because of its space limit.

### Using with Kerberos and/or Citrix StoreFront Logon

To use a custom PKCS#11 library with Kerberos and/or Citrix StoreFront Logon:

- In Setup, go to **Security > Smartcard > Middleware**.
- Select **Custom PKCS#11 module**.
- Under **Path to the library**, enter the path to your PKCS#11 library. Example: /usr/lib/pkcs11/[name of the library].so

### Using with VMware Horizon

To use a custom PKCS#11 library with VMware Horizon:

- In Setup, go to **System > Registry**.
- Enable the registry key vmware.view.pkcs11.use\_custom.
- Set the registry key vmware.view.pkcs11.custom\_path to the path to your PKCS#11 library.  
Example: /usr/lib/pkcs11/[name of the library].so

### Using with Firefox Browser

To use a custom PKCS#11 library with the Firefox browser:

- In Setup, go to **System > Registry**.
- Enable the registry key browserglobal.security\_device.custom.enable.
- Set the registry key browserglobal.security\_device.custom.device\_name to the name of your PKCS#11 library.
- Set the registry key browserglobal.security\_device.custom.lib\_path to the path to your PKCS#11 library. Example: /usr/lib/pkcs11/[name of the library].so

### Using with Chromium Browser

To use a custom PKCS#11 library with the Chromium browser:

- In Setup, go to **Sessions > Chromium Browser > Chromium Browser Global > Smartcard middleware**.
- Enable **Use a custom security device**.
- Under **Name of the security device**, enter an arbitrary name for the library.
- Under **Path to the library**, enter the path to your PKCS#11 library. Example: /usr/lib/pkcs11/[name of the library].so

---

<sup>202</sup> <https://kb.igel.com/display/endpointmgmt605/Files>

### 2.22.3 Adding an Icon for Browsing Removable Storage

#### Symptom

There is no obvious way of viewing files from removable media locally on the thin client.

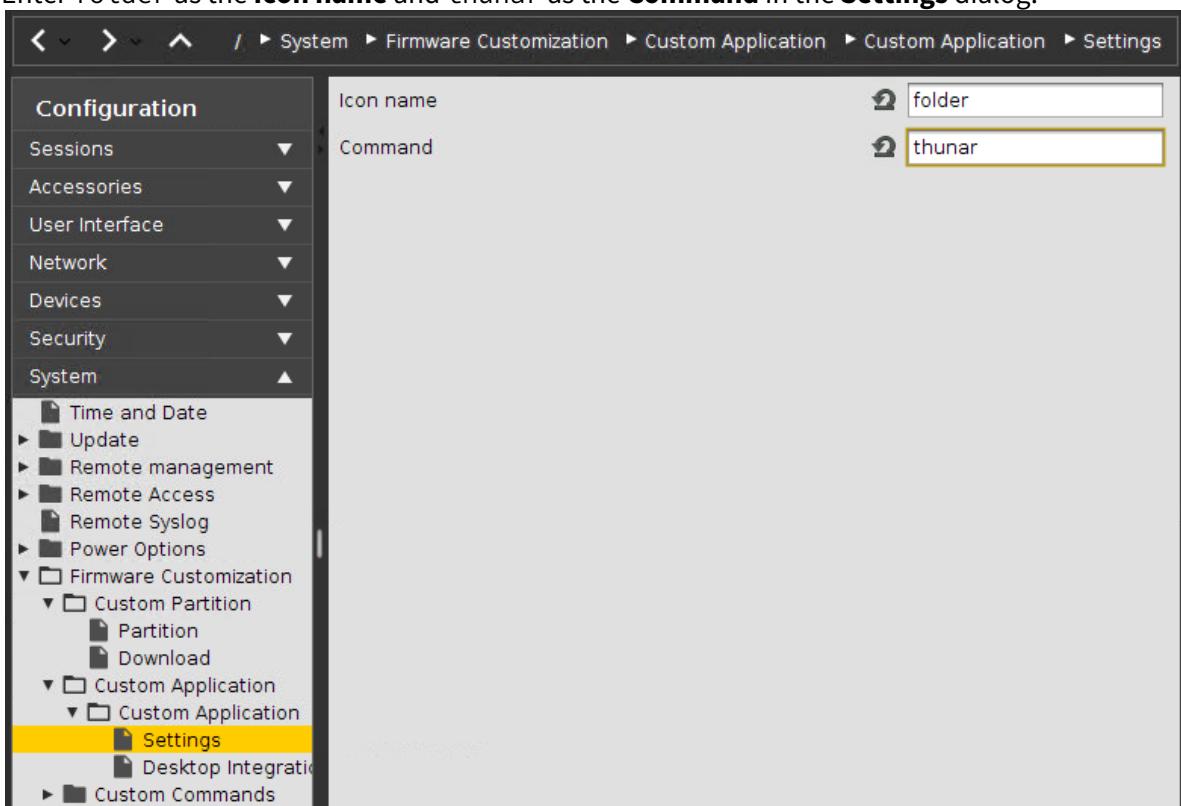
#### Problem

You want to view files from removable media locally on the thin client.

#### Solution

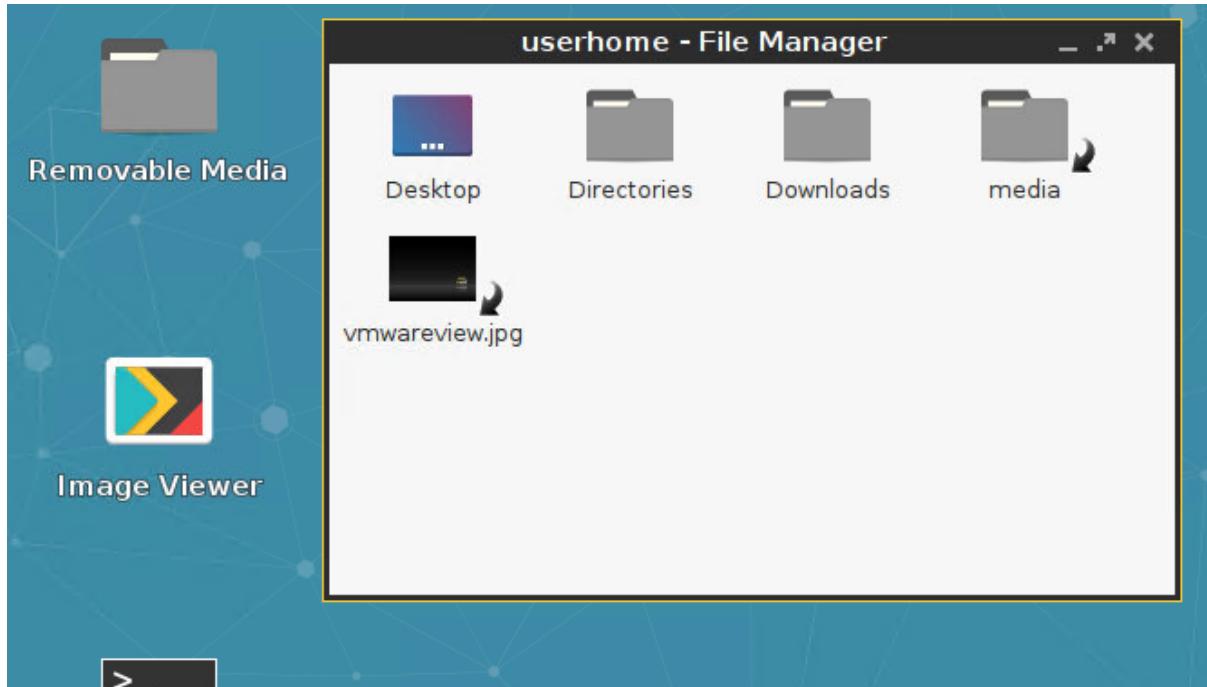
Create a custom application that opens the contents of removable media in the **File Manager**.

1. Go to **System > Firmware Customization > Custom Application** in **Setup**.
2. Click the star symbol to create a new **Custom Application**.
3. Enter a name, e.g. *Removable Media*, and choose desktop integration options for the application.
4. Enter **folder** as the **Icon name** and **thunar** as the **Command** in the **Settings** dialog:



5. Save the settings.

6. Insert a removable medium such as a USB stick into the thin client.



7. Click the new **Removable Media** icon. This opens **File Manager** and lets you browse the contents. Clicking a file will open it in the application configured by the MIME type handler (as of IGEL LINUX 5.06.100, see [FAQ](#)(see page 620)).

## 2.22.4 Adding an Icon for the Image Viewer

### Symptom

You want to view images locally on the thin client.

### Problem

The image viewer contained in *IGEL Linux* as from version 5.06.100 on has no desktop icon or menu entry.

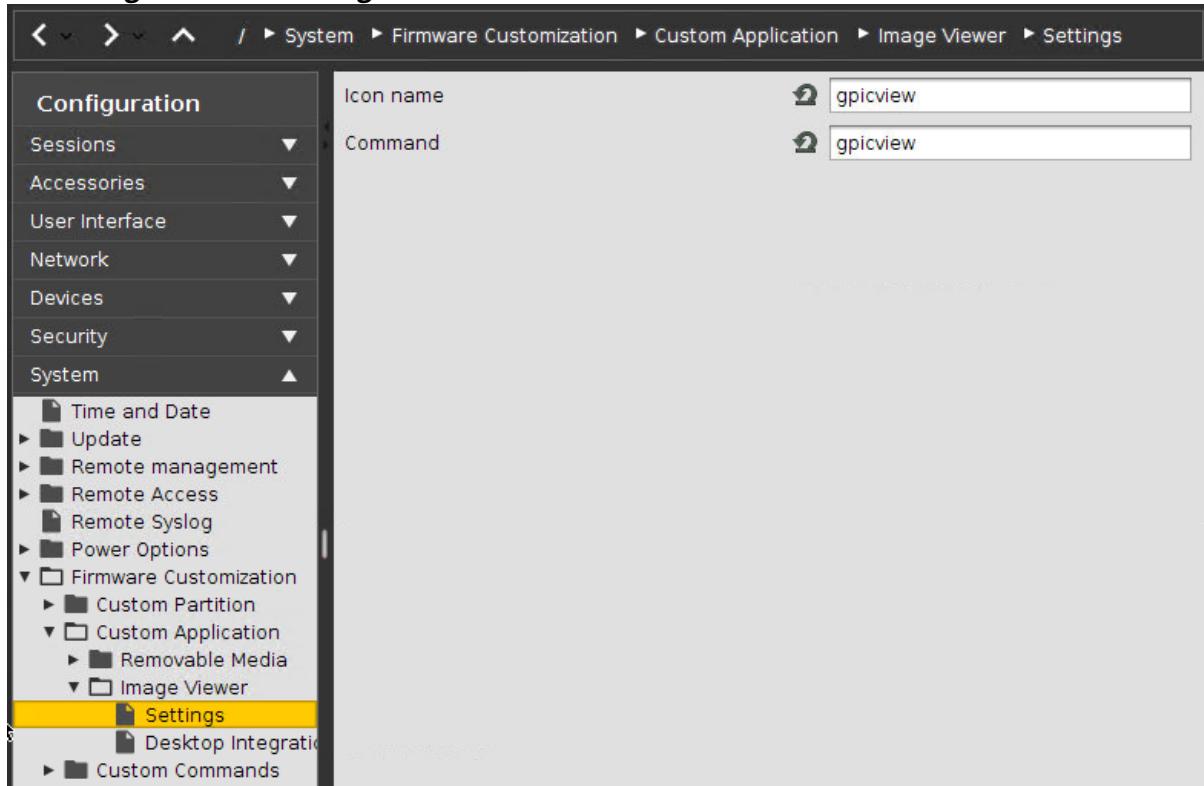
### Solution

Create a custom application that opens the Image Viewer.

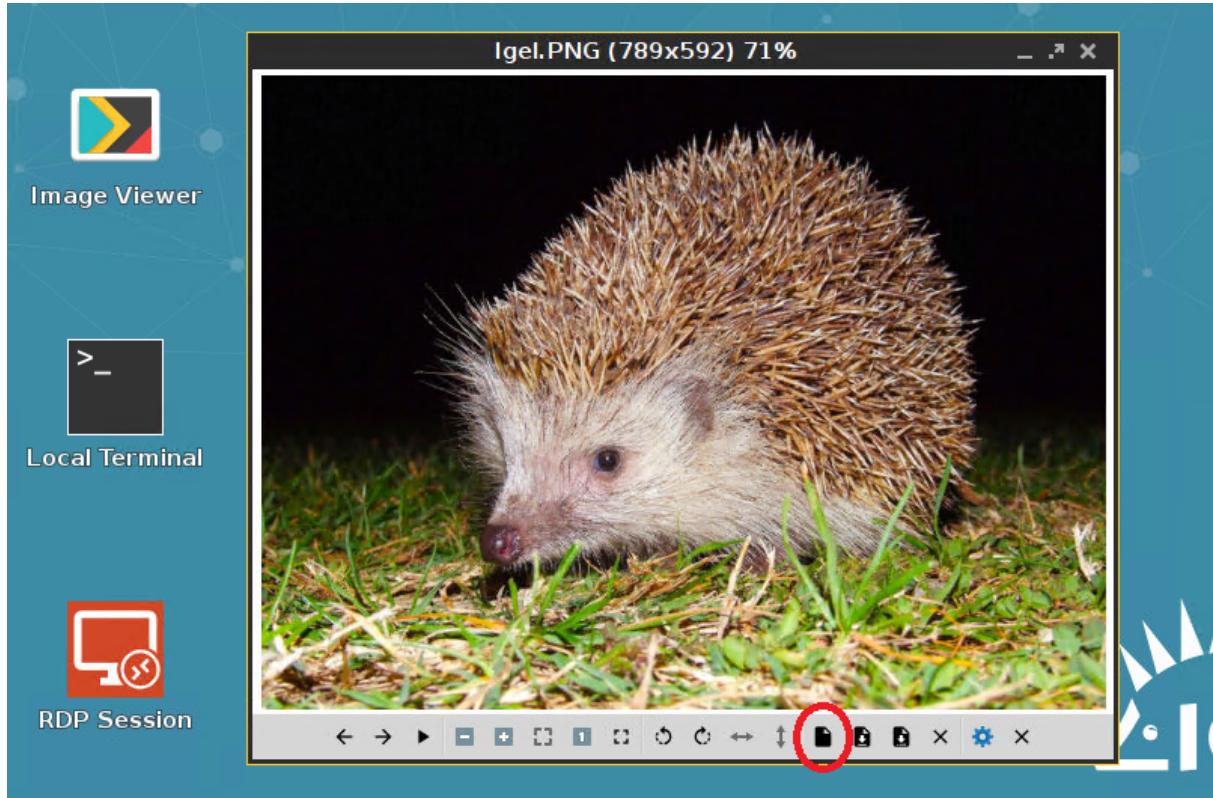
1. Go to **System > Firmware Customization > Custom Application** in Setup.
2. Click **[+]** to create a new **Custom Application**.
3. Enter a name, e.g. *Image Viewer*, and choose desktop integration options for the application.



4. Go to **Image Viewer > Settings**:



5. Enter **gpicview** as both the **Icon name** and the **Command** in the **Settings** dialog.
6. Save the settings.
7. Click the newly created icon for **Image Viewer**.
8. The **Image Viewer** opens.
9. Click the **Open File** symbol to open a file.



## 2.22.5 Creating a Timed Command (Cron Replacement)

You can define one or more commands which are executed at a defined time. The configuration is similar to that of a cron job. The implementation in IGEL OS uses systemd to execute the command.

To define a timed command:

1. In the Setup, go to **System > Registry > system > cron > cronjob%**
2. Activate **enable\_cron**.
3. If you want to define paths to executables in addition to the existing path environment variable, add them under **path**, separated by ":".
4. Click **Add Instance**.  
The instance "cronjob1" is created, which will be renamed to "cronjob0" when the device has restarted.
5. Set the parameters for your timed command according to your needs:
  - **command**: Command to be executed. Example for testing purposes: `gtkmessage -m "Here is your cron replacement"`
  - **day\_of\_month**: Day of the month  
Possible values:  
 - "1" ... "31": The command is executed on the defined day. To select a list of days for execution, enter a comma-separated list, e.g. "1,8". To enter a range of days, use a hyphen, e.g. "1-3".  
 - "\*": The command is executed every day of the month.



- **day\_of\_week:** Day of a week

Possible values:

- "1" ... "7": The command is executed on the defined day. "0" and "7" both mean Sunday. To select a list of days for execution, enter a comma-separated list, e.g. "1,3". To enter a range of days, use a hyphen, e.g. "1-3".
- "\*": The command is executed every day of the week.

- **hour**

Possible values:

- "0" ... "23": The command is executed in the defined hour. Example: "15" means 3 p.m., plus the minutes defined under **minute**. To select a list of hours for execution, enter a comma-separated list, e.g. "9,17". To enter a range of hours, use a hyphen, e.g. "9-17".
- "\*": The command is executed every hour.

- **minute**

Possible values:

- "0" ... "59": The command is executed in the defined minute. To select a list of minutes for execution, enter a comma-separated list, e.g. "15,45". To enter a range of minutes, use a hyphen, e.g. "5-10".
- "\*": The command is executed every minute.

- **month**

Possible values:

- "1" ... "12": The command is executed in the defined month. To select a list of months for execution, enter a comma-separated list, e.g. "1,4". To enter a range of months, use a hyphen, e.g. "1-3".
- "\*": The command is executed every month.

- **user:** The user under which the command is executed

Possible options:

- "root"
- "user"

- **year:** Year in 4-digit format. Example: "2019". To select a list of years for execution, enter a comma-separated list, e.g. "2019,2020". To enter a range of years, use a hyphen, e.g. "2019-2021". If the command is to be executed each year, enter "\*".

6. Click **Apply** or **Ok**.

7. Restart the device.

After the device has restarted, the command will be executed as configured.

## 2.22.6 Customizing IGEL OS Desktop

You want to give your IGEL OS desktops a more individual look and feel. This document shows how to customize your IGEL OS desktops using the Universal Management Suite (UMS). There are two ways to do it:

- via a firmware customization;
- via a profile.



With a firmware customization function, you can change your desktop design much easier and quicker than with a profile.

For an example, see [Creating Your Own Wallpaper via Firmware Customization](#)(see page 597). See also [Firmware Customizations](#)<sup>203</sup> and [Create Firmware Customization](#)<sup>204</sup> in the UMS Reference Manual.

For information on customizing IGEL OS desktops via a profile, see:

- [Introduction](#)(see page 595)
- [Creating Your Own Wallpaper](#)(see page 597)
- [Creating a New Bootsplash](#)(see page 599)
- [Creating Your Own Screensaver](#)(see page 600)
- [Assigning Your Own Company Logos](#)(see page 602)
- [Creating Your Own Taskbar](#)(see page 604)
- [Customizing Desktop Icons](#)(see page 604)

## Introduction

If you want to roll out your complete corporate design changes and apply them to multiple devices, you can create one single profile for all settings.

Before defining special profiles, you must take the following steps:

- [Uploading a Picture](#)(see page 595)
- [Creating a Profile](#)(see page 596)

### Uploading a Picture

Upload your image files to the UMS server, then assign them to the relevant profile and also to your devices.

You can choose between the following formats for your pictures : **BMP, JPG, GIF, TIF, PNG** and **SVG**. Ensure that the name of your image file has no blanks, otherwise the file will not be accepted. **25 MB** of free storage space are available for your pictures.

Upload your files:

1. Click **New file** on the context menu of the **Files** directory in the tree.
2. Browse to find your image in **Local file**.

<sup>203</sup> <https://kb.igel.com/display/endpointmgmt601/Firmware+Customization>

<sup>204</sup> <https://kb.igel.com/display/endpointmgmt601/Create+firmware+customization>



**File source**

Upload local file to UMS server

Local file

Upload location (URL)

Select file from UMS server

File location (URL)

**File target**

Classification

Thin Client file location

3. Browse to select a picture directory in **Upload location (URL)**. Since UMS version 5 you can use as upload location only /ums-filetransfer/ and its subdirectories.
4. Enter a **Thin Client file location** directory for the target device. If you enter a directory which does not yet exist, it will be created automatically. If you do not enter a specific directory, the image will be put in the root directory.
5. Click **OK**. Your image will be listed in the list of **Files**.
6. Assign the image to your devices by dragging and dropping them or by adding them under **Assigned objects**.

If you put more than one image in the **Thin Client file location** directory, all images will be alternately shown by the [screensaver](#)(see page 600), one after the other.

## Creating a Profile

You have already [uploaded your image file](#)(see page 595).

As you work with the UMS, to manage several clients, you need to create a profile to assign the new settings to your clients.

Create a **Profile** to assign your settings to the clients:

1. Click **New profile** in the context menu of the **Profiles** directory in the tree.
2. Enter a **Profile Name**.
3. Enter a **Description** and choose the firmware of your thin client under **Based on**.



4. Click **OK**.

## Creating Your Own Wallpaper

There are two ways how to create an own wallpaper:

- [Via a Firmware Customization](#)(see page 597)
- [Via a Profile](#)(see page 598)

With a Firmware Customization, setting up your own wallpaper is much easier than with a profile.

### Creating Your Own Wallpaper via Firmware Customization

This is how you can create your own wallpaper using a firmware customization function in the UMS:

1. In the UMS, right-click on **Firmware Customizations > Create New Firmware Customization**. The **Firmware Customization Details** dialog opens.
2. Enter a **Name** for your wallpaper customization.
3. As **Use Case**, select **Wallpaper**.
4. Select the image file for each monitor:
  - Click **Choose file** if you have already uploaded a file in the UMS.
  - Click **Upload file** if you want to upload a new file.



The file name must not contain any special characters such as %, §, umlauts, etc.

5. Select your image file and click **Open**.
6. Check the image file location and click **OK**.
7. Optionally, click **Next** to directly apply this new firmware customization to a device or folder of devices.
8. Click **Finish** to save your new firmware customization.

#### Creating Your Own Wallpaper via a Profile

You have already uploaded your wallpaper picture; see [Uploading a Picture](#)(see page 595).

1. Create a profile and name it, for example, **Wallpaper**; see [Creating a Profile](#)(see page 596). The **Profile Configuration** window opens.
2. Set the wallpaper server location; see below "Setting the Wallpaper Server Location".
3. Configure the background of the client desktop; see below "Configuring the Background".

#### Setting the Wallpaper Server Location

1. Click **System > Firmware Customization > Corporate Design > Background > Custom Wallpaper Server**.

**Custom Wallpaper - Server Location**

<input checked="" type="checkbox"/>	<input type="checkbox"/> Use firmware update server location
Protocol	<input type="text"/> HTTP
Server Name	<input type="text"/> 172.30.91.71
Server Path	<input type="text"/> /ums_filetransfer/
Port	<input type="text"/> 9080
User name	<input type="text"/> igel
Password	<input type="text"/> *****

2. Choose **HTTP** as **Protocol**.
3. Enter the **Server name** of your UMS Server.
4. Enter the path of your wallpaper directory as **Server path**.
5. The standard **Port** should be 9080.
6. Set your UMS administrator **User name** and **Password**.
7. Click **Save** to save the settings.

#### Configuring the Background

1. Open the profile.
2. Click **System > Firmware Customization > Corporate Design > Background (1st Monitor)**.
3. Activate **Custom wallpaper download**.



4. Enter under **Custom wallpaper file** the name of the picture you want to define as your background image.

If you use more than one monitor, you have to assign the background image to each one of them manually.

5. Assign the profile to your devices by dragging and dropping them or by adding them under **Assigned objects**.

#### Checking the Results

1. Choose the device in the UMS structure tree under **Devices**.
2. Go to **User Interface > Desktop > Background**.

You will see that the wallpaper has already been assigned by the profile; you cannot set it manually any more.

Alternatively, you can shadow your thin client and you will see the new wallpaper.

This way, you can automatically assign background images to your devices. It is very easy to maintain them because the only thing you have to do if you want to choose another image is to change it in the profile.

#### Creating a New Bootsplash

1. Upload your logo to the UMS server; see [Uploading a Picture](#)(see page 595).
2. Create a new profile named **Bootlogo**; see[Creating a Profile](#)(see page 596).
3. In the profile configuration window, click **System > Firmware Customization > Corporate Design > Custom Bootsplash** to create your own bootsplash.

**Custom Bootsplash**

<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Enable Custom Bootsplash
<hr/>	
<b>Custom Bootsplash - Server Location</b>	
<input checked="" type="checkbox"/>	<input type="checkbox"/> Use firmware update server location
Protocol	<input checked="" type="radio"/> HTTP
Server Name	<input checked="" type="text"/> dokumentation.igel.local
Server Path	<input checked="" type="text"/> ums_filetransfer/bootlogo
Port	<input checked="" type="text"/> 9080
User Name	<input checked="" type="text"/> igel
Password	<input checked="" type="text"/> ****

4. Activate **Enable Custom Bootsplash**.
5. Choose **HTTP** as **Protocol**.



6. Enter the **Server Name** of your UMS server.
7. Enter the path of your boot logo directory as **Server Path**.
8. Specify your HTTP server port under **Port**.

The default UMS HTTP server port is 9080.

9. Enter your UMS administrator **User Name** and **Password**.

#### Custom Bootsplash - Settings

Custom Bootsplash file	<input checked="" type="checkbox"/> mylogo.jpg
Horizontal position of bootsplash image	<input checked="" type="checkbox"/> 50
Vertical Position of bootsplash image	<input checked="" type="checkbox"/> 50
Horizontal position of progress indicator	<input checked="" type="checkbox"/> 90
Vertical Position of progress indicator	<input checked="" type="checkbox"/> 90

10. Enter the name of your logo image in **Custom Bootsplash file**.

The optimum size of the picture is **800 x 600 pixels**.

11. Apply **vertical and horizontal position** for the image and progress indicator. The scale goes from 0 (left) to 100 (right); the default setting is 50 (centered).
12. **Save** the settings.
13. Assign the profile to your devices by dragging and dropping them or by adding them under **Assigned objects**.

After changing the image file or any setting of an existing custom bootsplash, the bootsplash code has to be rebuilt. You can trigger this from UMS via **Jobs > New Scheduled Job** with the command **Update desktop customization**.

## Creating Your Own Screensaver

This section describes how to configure an autostart screensaver with your own picture using the UMS.

Proceed as you did for the wallpaper:

1. Upload your logo to the UMS server. For details, see [Uploading a Picture\(see page 595\)](#).

The size of the picture is irrelevant because it will be reduced automatically to 200 x 150 pixels.

2. Create a new Profile named **Screensaver**. For details, see [Creating a Profile\(see page 596\)](#).



### 3. Configure the profile settings.

There are four areas where you have to make settings in the screensaver profile:

- [Setting a Delay Time for Booting\(see page 601\)](#)
- [Setting a Timeout for Autostart\(see page 601\)](#)
- [Assigning the Custom Logo\(see page 601\)](#)
- [Assigning the Custom Clock\(see page 602\)](#)

### 4. Assign the profile to your devices by dragging and dropping them or by adding them under **Assigned objects**.

#### Setting a Delay Time for Booting

Configure **Autostart** in the screensaver profile under **User Interface > Screenlock / Screensaver**.

1. Enter a **Session name**, for example **Screensaver**.
2. Enable **Autostart**.
3. Enter the number of seconds of **Delay**.

This setting tells the system that it must launch the autostart of this session with a certain delay during booting.

#### Setting a Timeout for Autostart

1. Click **User Interface > Screenlock / Screensaver > Options**.
2. Enable **Start automatically**.
3. Enter a number of minutes for **Timeout**.

With this setting, you decide how long the system has to wait before starting the screensaver after the last input.

#### Assigning the Custom Logo

1. Go to **System > Firmware Customization > Corporate Design > Company Logos**.
2. Activate **Enable image display**.
3. Enter the **Image file/directory** you have defined under **Thin Client file location**. See [Uploading a Picture\(see page 595\)](#).

If you enter a folder instead of a single image file as the source, all images in the folder will be displayed as a slide show. The **display time** for the images can be configured.

4. Activate **One image per monitor** if you use more than one monitor and if you want to show different pictures on each screen.
5. Under **Image duration** specify the time in seconds that you want to wait before the image is to be changed.
6. Under **Image display mode** you can choose between the following different image actions:



- **Small-sized hopping:** Small pictures are shown in changing positions.
- **Medium-sized hopping:** Bigger pictures are shown in changing positions.
- **Full-screen center cut out:** The pictures will be shown in full-screen mode. They may possibly be cut at the border.
- **Full-screen letterbox:** The pictures are shown in full size as large as possible according to the screen.

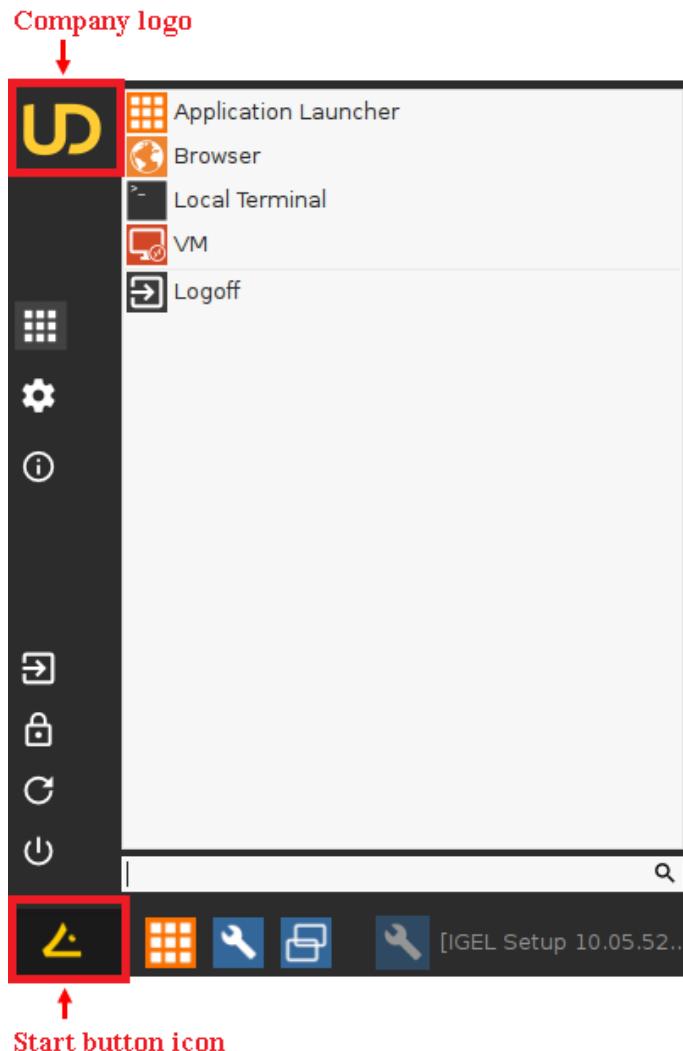
## Assigning the Custom Clock

You can also configure a digital screensaver clock independently of the screen display.

1. Click **User Interface > Screenlock / Screensaver > Screensaver**.
2. Select the **Clock display monitor** where you want to display the clock.
3. Activate **Show seconds** if you want to see the digital time display, including seconds.
4. Define the **size**, **position** and **color** settings of your screensaver clock.

## Assigning Your Own Company Logos

You can set your own images for the **start button** and the **company logo in the start menu**.



The **Start button icon** is customizable in IGEL Linux 5.08.100 and newer.

To see a start menu with a company logo, you first have to set the **Start Menu Type** on **Advanced** under **User Interface > Desktop > Start Menu**.

If you set the **Start Menu Type** on **Auto** and the device has a clock frequency of 1 GHz, the system will choose the advanced type.

To assign your own icons via UMS:

1. Upload your logos to the UMS server. For details, see [Uploading a Picture](#)(see page 595).
2. Create a new profile. For details, see [Creating a Profile](#)(see page 596).  
The profile configuration window opens.



3. Go to **System > Firmware Customization > Corporate Design > Company Logos > Start Menu**.
4. Enter the file name and the full path of the image under **Start button icon**.
5. Enter the file name and the full path of the image under **Company logo in start menu**.
6. Click **Save or Apply and send to Thin Client** to save the settings.
7. Assign the profile to your devices by dragging and dropping them or by adding them under **Assigned objects**.

An alternative to this is the chapter [Create Firmware Customization](#)<sup>205</sup> in the UMS manual. Here you will find further configuration options for adapting the UMS to your requirements.

## Creating Your Own Taskbar

You can apply your own design to a taskbar. To customize the taskbar on multiple devices, use the IGEL UMS and proceed as follows:

1. Upload the desired image to the UMS server, see [Uploading a Picture](#)(see page 595).
2. Create a new profile, see[Creating a Profile](#)(see page 596).
3. Assign the image to the profile by dragging and dropping it or by adding it under **Assigned objects**.
4. In the profile configuration window, go to **User Interface > Desktop > Taskbar Background**.
5. Select **Background image** under **Background style**.

Background Style	<input style="border: 1px solid #ccc; width: 150px; height: 25px; border-radius: 5px; background-color: #f0f0f0;" type="button" value="Background Image"/>
<hr/>	
Background Image Path	<input style="width: 150px; border: 1px solid #ccc; border-radius: 5px;" type="text" value="/wfs/user/corporate_design/igelstar"/>

6. Enter the full path of the desired image under **Background image path**.
7. Assign the profile to your devices by dragging and dropping them or by adding them under **Assigned objects**.

## Customizing Desktop Icons

You can only customize the desktop icon of a session. The taskbar icon of a session cannot be customized and will remain the default icon. Complete customization is not possible.

### Prerequisites

You can use the following graphic formats and resolutions for a custom desktop icon:

- PNG - common resolutions are 128x128, 96x96, 64x64, 48x48, 32x32, 24x24, 22x22, 16x16, but others are also accepted and scaled accordingly.

<sup>205</sup> <https://kb.igel.com/display/endpointmgmt605/Create+firmware+customization>



We recommend at least a resolution of 64x64.

- SVG - no resolutions because SVG contains freely scalable vector graphics.

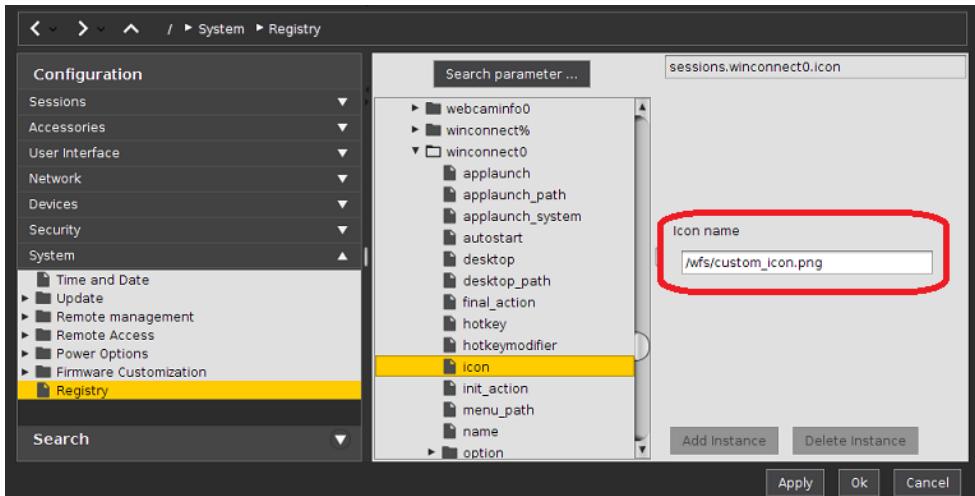
Even though other formats like BMP or JPEG are supported, only PNG and SVG are recommended because these formats support transparency.

To customize the desktop icon of a session, proceed as follows:

1. In the Setup, go to **System > Registry**.
2. In the Registry, navigate to **sessions.[session name].icon**.

For technical reasons, some registry keys do not match the session's name. For example, RDP sessions are found under the key `winconnect[0-...]`.

3. Enter under **Icon name** the absolute path to your custom icon as shown in the sample picture below.



4. Click **Ok** to save the changes.

## 2.22.7 How to Change the Font Color of the Desktop Icons

### Overview

You want to alter the font color of the desktop icons.



## Environment

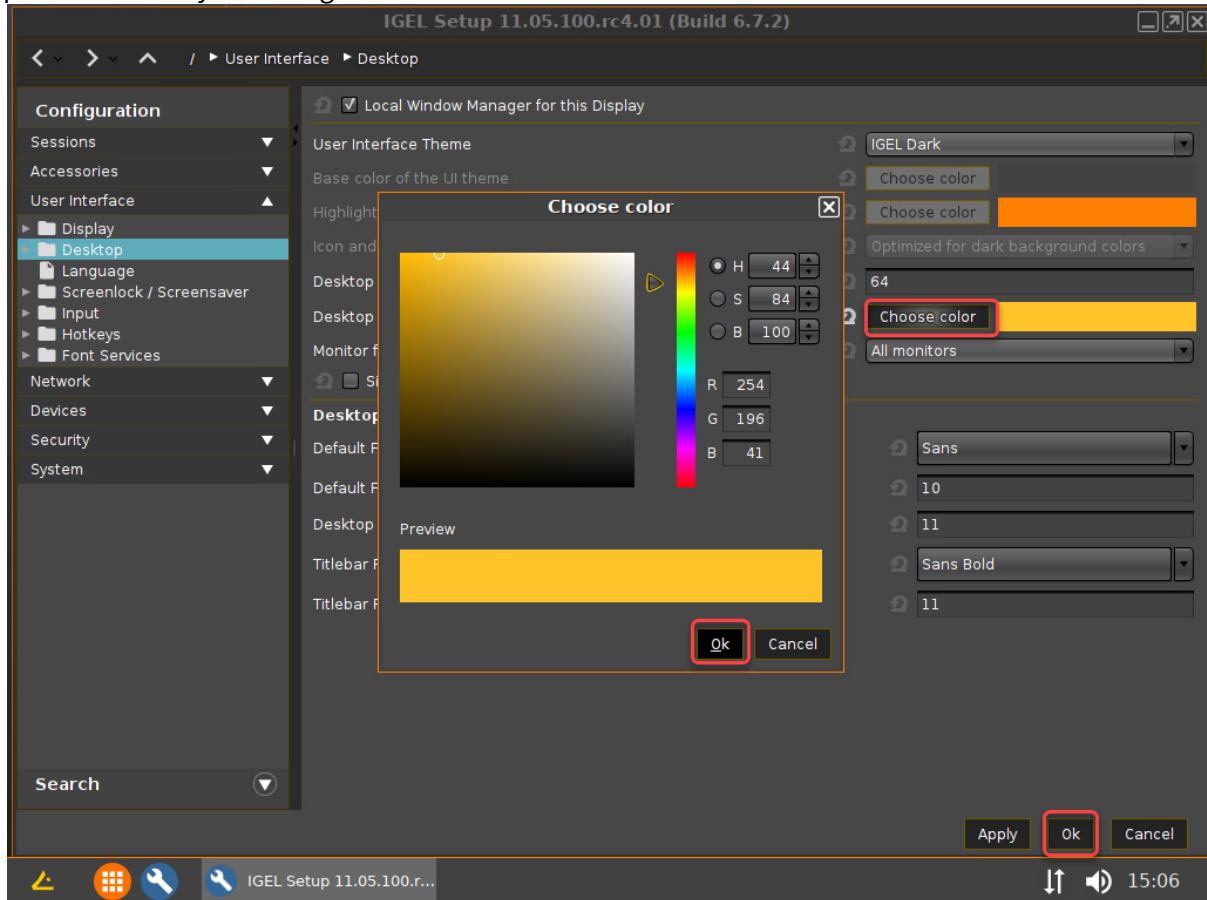
- IGEL OS 11.05.100 or higher

## Instructions

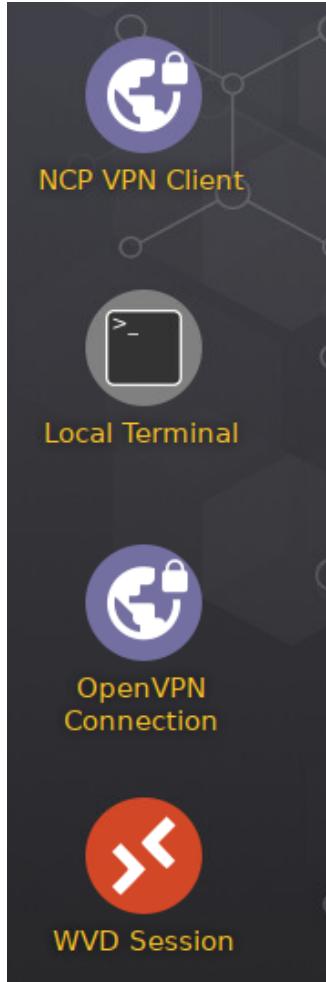
1. In the Setup, go to **User Interface > Desktop**.

As an alternative, you can enter the hexadecimal RGB hex value in **System > Registry > windowmanager > defaulttheme > desktop\_iconfont\_color** (registry key: `windowmanager.defaulttheme.desktop_iconfont_color`). Example: #FEC429

2. Beside **Desktop icon font color**, click **Choose color** and select the desired color using the color picker. Confirm your change with **Ok**.



The font color of the desktop icons is changed.



## 2.22.8 How to Set up a Screensaver Countdown

In some situations, a screenlock that comes without a warning can cause disruption. To circumvent this problem, you can set a visible countdown before the screen is locked. Additionally, you can define a shell command that is executed when the countdown reaches 0.

- [Setting up a Countdown](#)(see page 607)
- [Configuring a Conditional Countdown and Command](#)(see page 610)

### Setting up a Countdown

You can set up the countdown via the thin client's local Setup, or via the Universal Management Suite (UMS). It is recommended to use the UMS and store your settings in a profile; this allows you to apply your settings to a random number of thin clients in one go.



For more information about profiles, see the [Profiles<sup>206</sup>](#) chapter in the UMS 5 manual.

#### Defining the Countdown's Behaviour

1. In the Setup, go to **User Interface > Screenlock / Screensaver > Options**.
2. Activate **Start automatically**.
3. In the **Timeout** field, set the idle timeout in minutes after which the countdown should start.
4. Select the password to be used to unlock the screen:
  - **None**: The user can unlock the screen without a password.
  - **User password**: The user must enter the user password to unlock the screen. The user password is configured in **Security > Password**.
  - **Screenlock password**: The user must enter a special screenlock password to unlock the screen. Click **Set** to define the screenlock password.
5. Set the **Countdown duration** in seconds. The range is from 1 to 60.

Configuration example:

The screenshot shows the 'User Interface > Screenlock / Screensaver > Options' configuration page. Under the 'Behaviour' tab, the 'Start automatically' checkbox is checked. The 'Timeout' field is set to 1. In the 'Screen Lock Password' section, the 'Screen Lock Password' radio button is selected. A 'Set' button is visible next to the password selection.

6. Apply the settings to your thin clients or to your profile.

#### Defining the Countdown's Appearance

1. In the Setup, go to **User Interface > Screenlock / Screensaver > Options**.
2. If you want the current desktop as a background image during the countdown, select the visual effect:
  - **Dark screenshot**: The desktop screenshot is darkened.
  - **Gray screenshot**: The desktop screenshot is grayed out.
3. If you want a custom image as a background image during the countdown, enter a valid path and file name. Example: `/images/`. If the image is not already residing on your thin client, you can upload it using the UMS; see Uploading a Picture ([Uploading a Picture](#)(see page 595)).

Configuration example with custom image:

The screenshot shows the 'User Interface > Screenlock / Screensaver > Options' configuration page. Under the 'Appearance' tab, the 'Countdown duration in seconds' slider is set to 10. The 'Countdown visual effect' dropdown is set to 'Dark screenshot'. The 'Countdown background image' input field contains the path `/images/stopwatch.jpg`.

4. Go to **User Interface > Screenlock / Screensaver > Screensaver**.
5. Customize the countdown's appearance using the following parameters; these parameters define the appearance of both the screensaver's clock and the countdown. For further information, see the manual chapter "Screensaver" (for IGEL Linux v5) or "Screensaver" (for IGEL OS 10).

<sup>206</sup> <https://kb.igel.com/endpointmgmt-5.08/en/profiles-910377.html>



- **Image display mode:** Position and scaling for the background image

This parameter is only relevant for IGEL Linux v5. With IGEL Linux version 10.03.500 or higher, the **Image display mode** is set to "Full-screen letterbox".

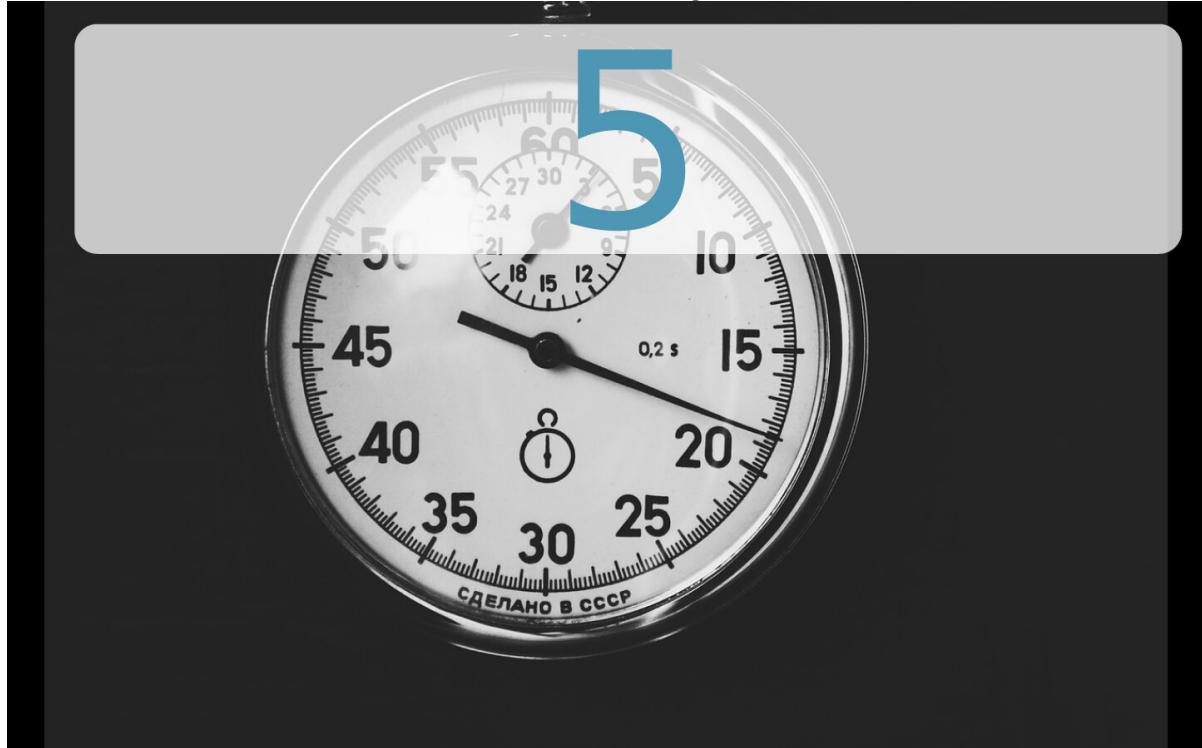
- **Clock display monitor:** Selects the monitor(s) on which the countdown is to be shown.
- **Clock display size:** Size of the countdown digits
- **Horizontal clock position:** Horizontal position of the countdown digits
- **Vertical clock position:** Vertical position of the countdown digits
- **Clock background color:** Color of the countdown background area. The countdown background area is a rectangle with rounded corners.
- **Clock foreground color:** Color of the countdown digits

Configuration example:

Image display mode	Full-screen center cut out
Clock display monitor	All
Show seconds	<input type="checkbox"/>
Clock display size	Huge
Horizontal clock position	Right
Vertical clock position	Top
Clock background color	Choose color
Clock background opacity percentage	75
Clock foreground color	Choose color

6. Apply the settings to your thin clients or to your profile.

Here is an example of the countdown with a custom image:



## Configuring a Conditional Countdown and Command

You can specify an arbitrary command that is executed when the countdown has reached 0.

Additionally, you can specify a command that determines whether the countdown is to be started.

Example use case: The countdown is running, but the user does not interact with the device in order to make the countdown stop. When the countdown has reached 0, the system checks whether a session is running, e.g. an appliance mode Citrix session. If yes, the user is logged off from this session.

If no command is set to be executed after countdown, the screen will be locked instead.

The user that issues the commands depends on the firmware version in use:

- With IGEL Linux v5, the user is root.
- With IGEL OS Linux 10, the user is user.

To specify the command that determines the condition:

1. In the Setup, go to **System > Registry** and open the registry key **sessions > xlock0 > options > countdown\_condition\_cmd** (`sessions.xlock0.options.countdown_condition_cmd`).
2. Enter the command in the field **Countdown condition command**. Example: `pgrep wfica` (determines if a Citrix session is present)



3. Click **Apply or Ok**.

If the command returns 0, the countdown or command is started.

If the command returns a non-zero value, the countdown or command is not started.

To specify the command to be executed after the countdown:

1. In the Setup, go to **System > Registry** and open the registry key **sessions > xlock0 > options > countdown\_done\_cmd** (`sessions.xlock0.options.countdown_done_cmd`).
2. Enter the command in the field **Countdown done command**. Example: `killall wfica` (terminates the Citrix ICA client)

The command is executed synchronously before the countdown goes away. If the command doesn't terminate quickly, it must be sent to the background by appending "&".

3. Open the registry key **sessions > xlock0 > options > countdown\_done\_cmd\_continue** (`sessions.xlock0.options.countdown_done_cmd_continue`) and specify whether the screensaver should be started after the command has been started.

With IGEL Linux v5, the screensaver does not start immediately. It will be started after the idle timeout defined under **User Interface > Screen Lock/Saver > Options > Timeout**.

With IGEL OS Linux 10, the screensaver is started immediately.

The screensaver is started after the command has been started.

The screensaver will not be started.

4. Click **Apply or Ok**.

## 2.22.9 Installing a Calculator on IGEL Linux

### Issue

You may want to have a desktop calculator.

### Solution

1. Download the opensource java calculator from: <http://sourceforge.net/projects/simpcalc/>

The default download location of the local Firefox browser is `/tmp/`.

2. Open a **Local Terminal** and log in as root
3. Copy the downloaded .jar file from the `/tmp/` directory to `/wfs/simplecalc.jar`:  
`cp /tmp/ /wfs/simplecalc.jar`  
 It is important to copy the file to `/wfs` because otherwise the file would be flushed with a reboot.
4. Open IGEL Setup and create a new custom application: **System > Firmware Customization > Custom Application**
5. Set **Command** to `java -jar /wfs/simplecalc.jar` in **Settings**
6. Click the newly created icon on the desktop to run the custom application.



To distribute this application to several thin clients please use the file transfer option in IGEL UMS and set up a profile with the custom application configuration.

### 2.22.10 Keyboard Shortcuts for Managing Windows

Switching back and forth between open application windows by using keyboard shortcuts is a common way of managing windows.

If you work in a fullscreen environment, you also need a way to switch to the desktop.

With IGEL Linux OS version 10.03.500, the device desktop was added to the window cycle of the window manager.

Use the following default shortcuts to switch from application windows to the desktop:

Task	Default Shortcut
Switch between active windows using Task Switcher	Ctrl + Alt + Tab
Switch between active windows using Task Switcher (backwards)	Ctrl+Alt+Shift+Tab
Switch focus to next window	Ctrl + Esc
Switch focus to next window (2)	Ctrl + Alt + UpArrow
Switch focus to next window (reverse order)	Ctrl + Alt + DownArrow

Go to [IGEL Setup > User Interface > Hotkeys > Commands](#)(see page 976) to change these shortcut combinations.

Switching to the desktop minimizes all windows. Switching back to a window right after that restores all windows.

### 2.22.11 Make Frequent User Actions Easier by Defining Hotkeys

For common actions, such as switching between different windows, or lock the screen, you can use a hotkey. Some hotkeys are preconfigured, but you can activate, deactivate, and modify them.



The following example shows how to find out or modify the hotkey for switching between windows:

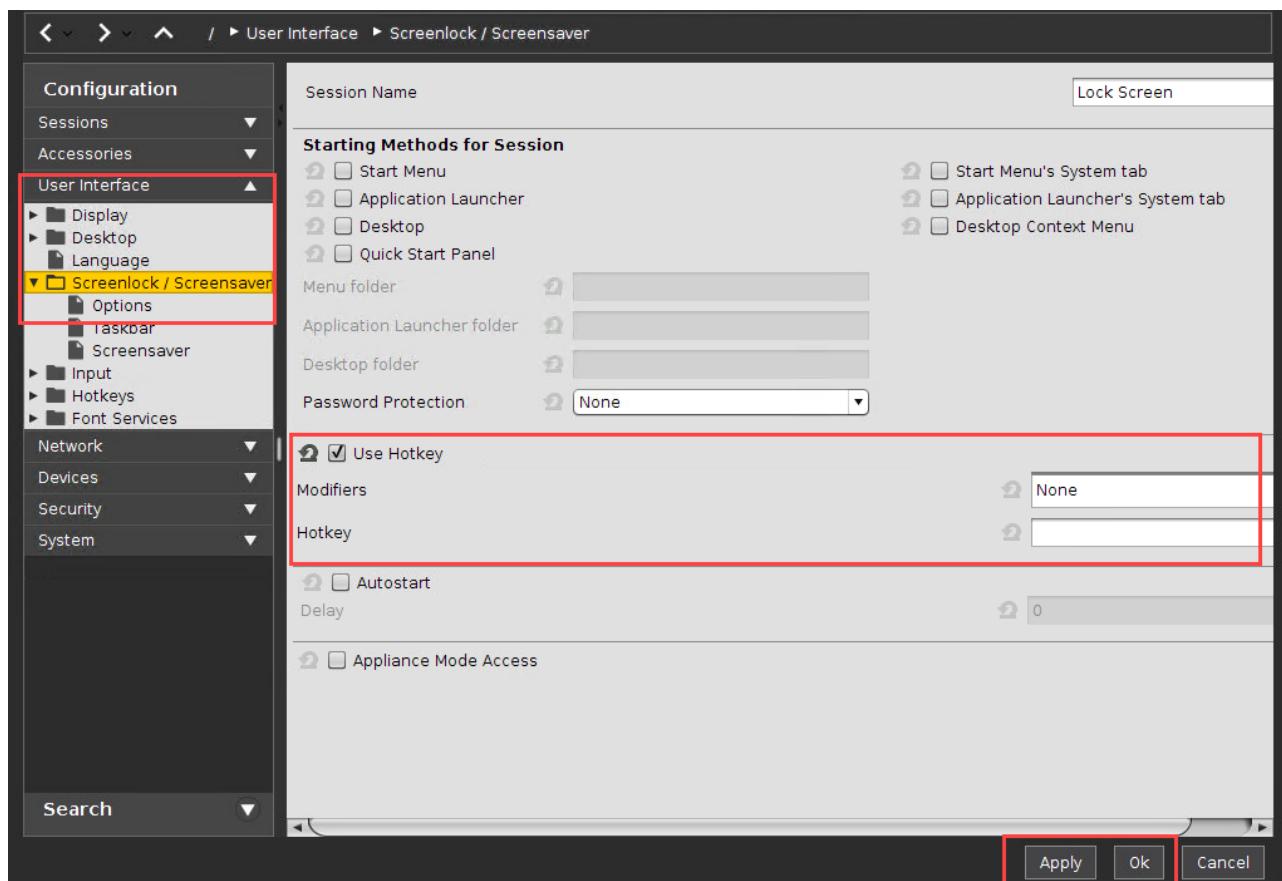
The screenshot shows the 'User Interface > Hotkeys > Commands' section of the configuration. The 'User Interface' category is selected in the left sidebar. A yellow box highlights the 'Commands' item under 'Hotkeys'. In the main list, the 'Switch between active windows using Task Switcher' command is selected, highlighted with a yellow box. A red circle with a white pencil icon is positioned over the 'Edit' button in the toolbar above the list. A red box highlights the 'Hotkey' checkbox in the dialog window titled 'Switch between active windows using'. The dialog also shows 'Modifiers: Ctrl|Alt' and 'Key: Tab'. Below the dialog, the 'Appliance Mode Access' checkbox is shown. At the bottom right of the main window, there are 'Apply', 'Ok', and 'Cancel' buttons.

1. Open the setup and go to **User Interface > Hotkeys > Commands**.
2. Select **Switch between active windows using Task Switcher**.
3. Click on **Modify**.  
A dialog window is opened.
4. Enable **Hotkey**, if not already enabled.
5. Select a modifier key or a combination of modifier keys under **Modifiers**.
6. Enter a **Key**.

If you want to enter a key that has no visible character assigned, e. g. the [Tab] key, open a terminal, logon as user and enter `xev -event keyboard`. Press the key designated for the hotkey. The text in brackets starting with `keysym` will contain the desired string for the **Key** field; example: Tab in (`keysym 0xff09, Tab`)

7. Click on **Ok**.
  8. Click on **Apply** or **Ok**.
- The hotkey is ready for use.

The following example shows how to define a hotkey to lock the screen:



1. Open the setup and go to **User Interface > Screenlock/Screensaver**.
  2. Enable **Hotkey**.
  3. Select a modifier key or a combination of modifier keys under **Modifiers**.
  4. Enter a **Key**.
  5. Click on **Apply** or **Ok**.
- The hotkey is ready for use.

## 2.22.12 Shutdown/Suspend Devices Automatically at the End of a Session

### Issue

You may want to shut down, suspend, restart or log off from the device automatically after ending a session.

### Solution

You can define an "after-logoff-action" dependent on a session type. This action is performed after ending the last instance of the defined session type.

Proceed as follows:



1. In the device's local Setup (or its UMS configuration or profile), navigate to **System > Firmware Customization > Custom Commands > Post Session**.
2. Choose a **Session type**.
3. Choose a **Post-session command**.
4. Save the changes with **Apply** or **OK**.

If the last instance of the chosen session type is ended, the post-session command will be processed.

See also IGEL OS manual: [Post Session](#)(see page 1272)

The post-session command **Shutdown/suspend** will perform the default action defined under **System > Power Options > Shutdown > Default action**. Please check this parameter before using the command.

The post-session command **Logoff** is futile unless you define a login method under **Security > Logon** (Smartcard, Active Directory/Kerberos, or IGEL Shared Workplace). The **Logoff** command also cannot be used with an appliance – in this case, only **Shutdown/suspend** or **Reboot** commands are working.

When using auto-logoff commands with an appliance, make sure to define the corresponding session type – e.g. **Horizon View** when using the *VMware Horizon View* appliance.

### 2.22.13 Suspend to RAM - Wake Up by USB Mouse

You can wake up your device by mouse click or key press.

The wake-up functionality strongly depends on the hardware and BIOS version in use. We recommend testing this function before using it. With devices converted by UDC3/OS Creator (OSC) or UD Pocket, it only works when the hardware is fully supported.

#### Setting System Suspend as the Default Action

1. In Setup, go to **System > Power Options > Shutdown**.
2. Activate **Allow system suspend**.
3. Under **Default action**, select "Suspend".
4. Save the setting by clicking **Apply** or **Ok**.

From now on, the system will be suspended to RAM whenever it is shut down.

To use the wake-up functionality, the following steps must be performed:

#### Configuring the BIOS for PS/2 Mouse and Keyboard

1. Open the BIOS of your device and check if the power management section has parameters named "PS/2 Wake up from S3" or similar.



2. If present, set the parameters to enabled.
3. Save the BIOS configuration and continue booting.

## Configuring the BIOS for USB Mouse and Keyboard

1. Open the BIOS of your device and check if the power management section has parameters named "USB Wake Up from S3" or similar.
2. If present, set the parameters to enabled.
3. Save the BIOS configuration and continue booting.

## Enabling the Wake-Up Functionality

1. In the IGEL Setup, activate **System > Registry > system > acpi\_wakeup > enabled > Wakeup from S3 by USB devices**.
2. Click **Apply** or **Ok**.



To check if the wake-up functionality works, click **L** > **Power**, wait a few minutes, and try to wake up the device using a mouse click or a key press.

### 2.22.14 Taking Screenshots on IGEL Linux

#### Issue

For support or documentation purposes, the user wants to take a screenshot in IGEL Linux without accessing the client via VNC.

#### Solution

On IGEL Linux 5.08.100 and newer or IGEL Linux 10.01.100 and newer, use the pre-installed [Screenshot Tool](#)(see page 1084).

On earlier versions:

1. Download the tool [Rapid Screenshot](#)<sup>207</sup>.

The default download location of local Firefox is /tmp/.

2. Open a **Local Terminal** and log in as root.
3. Copy the downloaded .jar file from the /tmp/ directory to /wfs/screenshot.jar:  
`cp /tmp/ /wfs/screenshot.jar`  
 It is important to copy the file to /wfs because otherwise the file would be flushed with a reboot.
4. Open IGEL setup and create a new **custom application**:  
**System > Firmware Customization > Custom Application**

<sup>207</sup> <https://sourceforge.net/projects/screenshot/?source=directory>



5. Set **Command** to `java -jar /wfs/screenshot.jar` in **Settings**.
6. Click the new icon on the desktop to run the **custom application**.

To distribute this application to several thin clients use the file transfer option in IGEL UMS and set up a profile with the custom application configuration.

1. HOW TO USE *Easy Screenshot Maker*:
  - a. Start the application.
  - b. Make a screenshot.
  - c. Save the file for example as `test.png`.
2. HOW TO USE *Rapid Screenshot*:
  - a. Start the application.
  - b. Click **Save in** to configure the path to store screenshots.
  - c. Click button **Click**.  
The screenshot will be saved automatically as `.jpg`.

Please note the licenses for both screenshot capture tools mentioned on the websites of these specific tools!

## 2.22.15 Setting the Device's System Time

### Issue

The thin client's system time is not correct.

### Solution

1. Open the thin client's configuration either locally or in UMS.
2. Go to **System > Time and Date**
3. Choose your **Continent/Area** (e.g. America).
4. Choose your **Location** (e.g. New York).
5. Set time and date
  - a. either manually by clicking **Set time and date**
  - b. or automatically by configuring an **NTP Time Server**.
6. Click **OK** or **Apply** to save your settings.

Note: If choosing **General** as **Time Zone Area** you have to set your GMT time zone (**Location**) following the POSIX standard (as usual in Linux) - which means you have to invert the offset of your common UTC time zone! (See tool tip for **Location** as well.) Therefore it is preferable to set the system's time zone by choosing the corresponding area and location instead of defining the GMT offset.

Example for America/New York: In POSIX standard **GMT+5** is the time zone **5 hours west** of Greenwich and corresponds to **UTC-5**

**Legal Note**

IGEL's [Terms & Conditions](#)<sup>208</sup> apply.

## 2.22.16 Updating Timezone Information (Daylight Saving Time, DST)

### Symptom

The device is showing an incorrect time of day for your location, although you have set the correct time zone.

### Problem

The time zone or the regulation for Daylight Saving Time (DST) for your location has changed.

### Solution

- ▶ Update the time zone information files via IGEL Universal Management Suite (UMS).

#### Retrieving Current Time Zone Information Files

##### On Windows

- Use your web browser to download the following package files:
  - <http://packages.ubuntu.com/xenial-updates/all/tzdata/download> for IGEL Linux version 10.x
- Extract the package contents using the program 7-Zip (freely available from <http://www.7-zip.org>).
- Find the file for your location in the extracted directory in `usr/share/zoneinfo/`, e.g. `usr/share/zoneinfo/Africa/Casablanca` for Morocco.

##### On Linux

- Update your system time zone information with these commands: `sudo apt-get update` `sudo apt-get install tzdata`
- Find the file for your location in the system directory `/usr/share/zoneinfo/`, e.g. `/usr/share/zoneinfo/Africa/Casablanca` for Morocco.

#### Distributing the Files from IGEL Universal Management Suite

- Select **System > New > New File** from the UMS Console menu bar or go to **Files** in the tree structure and select **New File** from the context menu.
- Select the time zone file for your location under **Local File**.
- Select **Undefined** under **Classification**.
- Specify `/wfs/zoneinfo/` as the **Devices file location**.

<sup>208</sup> <https://www.igel.com/terms-conditions/>



- Set the **Access rights** to Read and Write for the Owner, and to Read for Others.
- Select Root as the **Owner**.
- Click **OK** to confirm the settings.

**New file**

**File source**

( Upload local file to UMS server)

Local file

Upload location (URL)  https://<server:port>/ums\_filetransfer

( Select file from UMS server)

File location (URL)

**File target**

Classification  Undefined

Devices file location  /wfs/zoneinfo/

**Access rights**

	Read	Write	Execute
Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Others	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Owner	<input type="button" value="Root"/>		

**Ok**    **Cancel**

On a device, you can verify the transfer and activation of the new time zone information files:

- In the **Local Terminal**, enter grep 'timezone\_config' /var/log/messages

On IGEL Linux version 10.x, use: journalctl | grep 'timezone\_config'

- The output should look like the following:
 

```
Feb 27 11:28:13 (none) timezone_config: loading /wfs/zoneinfo/Casablanca
to /usr/share/zoneinfo/Africa/Casablanca
Feb 27 11:28:13 (none) timezone_config: loading /wfs/zoneinfo/Casablanca
to /usr/share/zoneinfo posix/Africa/Casablanca
Feb 27 11:28:13 (none) timezone_config: configure timezone Africa/Casablanca
```



## 2.22.17 Adding or Changing a MIME Type Handler

### Symptom

Files or protocols are opened with the wrong application.

### Problem

The MIME type handler for the file type or the protocol is missing or misconfigured.

### Solution

Change the MIME type handler or add a new one.

MIME type handlers are defined by \*.desktop files in the /usr/share/applications.mime/ directory.

To add a new \*.desktop file, use the following sample and edit it according to your needs:

```
[Desktop Entry]
Version=1.0
Encoding=UTF-8
Type=Application
Name=Browser//A name for the MIME type handler
Categories=Application
Exec=/usr/bin/firefox %u//The binary to execute on opening an associated file
MimeType=x-scheme-handler/http;x-scheme-handler/https;text/html;application/xhtml+xml;//A
list of MIME types separated by semicolon
Terminal=false
StartupNotify=false
NoDisplay=true
```

You can find out more about \*.desktop files in a [specification at freedesktop.org](#)(see page 620).

These are the default handlers on IGEL Linux:Images (opened via gpicview)

- image/bmp;
- image/gif;
- image/jpeg;
- image/jpg;
- image/png;
- image/x-bmp;
- image/x-pcx;
- image/x-tga;
- image/x-portable-pixmap;
- image/x-portable-bitmap;
- image/x-targa;



- image/x-portable-greymap;
- application/pcx;
- image/svg+xml;
- image/svg+xml;

Videos and Music (opened via `/services/mplr/bin/mediaplayer`)

Note that `/services/mplr/bin/mediaplayer` calls either `/config/sessions/mediaplayer0` if existent or `totem` if this is not the case

- application/mxf;
- application/ogg;
- application/ram;
- application/sdp;
- application/smil;
- application/smil+xml;
- application/vnd.ms-wpl;
- application/vnd.rn-realmedia;
- application/x-extension-m4a;
- application/x-extension-mp4;
- application/x-flac;
- application/x-flash-video;
- application/x-matroska;
- application/x-netshow-channel;
- application/x-ogg;
- application/x-quicktime-media-link;
- application/x-quicktimeplayer;
- application/x-shorten;
- application/x-smil;
- application/xspf+xml;
- audio/3gpp;
- audio/ac3;
- audio/AMR;
- audio/AMR-WB;
- audio/basic;
- audio/midi;
- audio/mp4;
- audio/mpeg;
- audio/mpegurl;
- audio/ogg;
- audio/prs.sid;
- audio/vnd.rn-realaudio;
- audio/x-ape;
- audio/x-flac;
- audio/x-gsm;
- audio/x-it;
- audio/x-m4a;



- audio/x-matroska;
- audio/x-mod;
- audio/x-mp3;
- audio/x-mpeg;
- audio/x-mpegurl;
- audio/x-ms-asf;
- audio/x-ms-asx;
- audio/x-ms-wax;
- audio/x-ms-wma;
- audio/x-musepack;
- audio/x-pn-aiff;
- audio/x-pn-au;
- audio/x-pn-realaudio;
- audio/x-pn-realaudio-plugin;
- audio/x-pn-wav;
- audio/x-pn-windows-acm;
- audio/x-realaudio;
- audio/x-real-audio;
- audio/x-sbc;
- audio/x-scpls;
- audio/x-speex;
- audio/x-tta;
- audio/x-wav;
- audio/x-wavpack;
- audio/x-vorbis;
- audio/x-vorbis+ogg;
- audio/x-xm;
- image/vnd.rn-realpix;
- image/x-pict;
- misc/ultravox;
- text/google-video-pointer;
- text/x-google-video-pointer;
- video/3gpp;
- video/dv;
- video/fli;
- video/flv;
- video/mp4;
- video/mp4v-es;
- video/mpeg;
- video/msvideo;
- video/ogg;
- video/quicktime;
- video/vivo;
- video/vnd.divx;
- video/vnd.rn-realvideo;
- video/vnd.vivo;



- video/x-anim;
- video/x-avi;
- video/x-flc;
- video/x-fli;
- video/x-flic;
- video/x-flv;
- video/x-m4v;
- video/x-matroska;
- video/x-mpeg;
- video/x-ms-asf;
- video/x-ms-asx;
- video/x-msvideo;
- video/x-ms-wm;
- video/x-ms-wmv;
- video/x-ms-wmx;
- video/x-ms-wvx;
- video/x-nsv;
- video/x-ogm+ogg;
- video/x-theora+ogg;
- video/x-totem-stream;
- x-content/video-dvd;
- x-content/video-vcd;
- x-content/video-svcd;

Documents (opened via /usr/bin/evince)

- application/pdf;
- image/tiff

Web (opened via /usr/bin/firefox -remote)

- x-scheme-handler/http;
- x-scheme-handler/https;
- text/html;
- application/xhtml+xml;

## 2.22.18 Regional Settings in Sessions

### Symptom

If you set a certain keyboard language it has no effect on the regional settings.



## Problem

In the *IGEL* setup there are several input fields for regional settings. You would like to understand which setting has what effect in the sessions.

## Solution

Defining general regional settings:

- ▶ Go to **IGEL Setup > User Interface > Language**.
  - **Language**: Select one of the languages offered for the graphical user interface.
  - **Keyboard Layout**: Select the country-specific assignment of keys, e.g. English(US).
  - **Input Language**: Set the language you are going to write in, e.g. English(Australia).
  - **Standards and Formats**: Select country-specific formats, e.g. for date and time or currency.

Defining session-specific regional settings:

- ▶ Go to the settings of your session, e.g. Citrix: **IGEL Setup > Sessions > Citrix > Citrix Global > Keyboard**.

The default settings are those you defined under **User Interface > Language**.

- ▶ Specify **Keyboard Layout** and **Input Language** for your Citrix Session.

## 2.23 Devices

- [Monitor\(see page 625\)](#)
- [Using a Cherry SECURE BOARD\(see page 640\)](#)
- [Webcam Redirection and Optimization\(see page 663\)](#)
- [Webcam Information\(see page 673\)](#)
- [Bluetooth Tool\(see page 674\)](#)
- [How to Deploy a Jabra Xpress Package\(see page 677\)](#)
- [Connecting Signature Pads\(see page 681\)](#)
- [Using a Kofax / Wacom Signature Pad\(see page 681\)](#)
- [Using a StepOver Signature Pad\(see page 682\)](#)
- [eGK/KVK - Card Reader\(see page 685\)](#)
- [Using Mobile Device Access\(see page 692\)](#)
- [Swapping Function of Mouse Buttons \(e.g. When Using an Evoluent Mouse\)\(see page 698\)](#)
- [Connecting a Serial Barcode Scanner\(see page 699\)](#)
- [Using DriveLock with IGEL Devices\(see page 701\)](#)
- [Restricting the Mounting of Hotplug Storage Devices on IGEL Linux\(see page 702\)](#)
- [When to Use USB Redirection\(see page 703\)](#)
- [How to Configure USB Access Control\(see page 706\)](#)
- [Issues with USB IDs in USB Devices Rules\(see page 708\)](#)
- [How Can I Fix Touchpad Issues?\(see page 710\)](#)



## 2.23.1 Monitor

- [Touchscreen Calibration](#)(see page 625)
- [Touchscreen in Multimonitor Environment](#)(see page 636)
- [USB-Powered ASUS Monitor and IGEL OS 11](#)(see page 636)
- [Solving Hotplugging Issues with DisplayPort Monitors](#)(see page 637)
- [No Sound When Using a DisplayPort Monitor](#)(see page 637)
- [Connecting Three DVI Monitors to UD7 with Passive DisplayPort Adapters](#)(see page 639)

### Touchscreen Calibration

For setting up a touchscreen, you have to enable the touchscreen function and select a specific touchscreen driver.

The initial configuration should take place with a mouse and keyboard connected to ensure that you can open the setup and navigate within it.

To set up a touchscreen:

1. In IGEL Setup, go to **User Interface > Input > Touchscreen**.
2. Activate **Enable touchscreen**.
3. Select your touchscreen driver under **Touchscreen type**.

Depending on the selected driver, you have different configuration options. For further information, click the appropriate link:

- [EvTouch \(USB\)](#)(see page 625)
- [eGalax](#)(see page 629)
- [Elo Multitouch \(USB\)](#)(see page 631)
- [Elo Singletouch \(USB\)](#)(see page 633)
- [TSHARC \(USB\)](#)(see page 634)

### EvTouch (USB)

#### Supported Devices

Supported touch monitors and touchscreen controllers:

Vendor	Product	Name
0x16FD	0x5453	Reakin, TS2005F USB TouchController
0x7374	0x0001	



<b>Vendor</b>	<b>Product</b>	<b>Name</b>
0x04E7	0x0020	Elo TouchSystems, Touchscreen Interface (2700)
0x1870	0x0001	Nexio Co., Ltd, iNexio Touchscreen controller
0x10F0	0x2002	Nexio Co., Ltd, iNexio Touchscreen controller
0x0664	0x0306	ET&T Technology Co., Ltd., Groovy Technology Corp. GTouch Touch Screen
0x0664	0x0309	ET&T Technology Co., Ltd. Groovy Technology Corp. GTouch Touch Screen
0x14C8	0x0003	Zytronic, Unknown device
0x1AC7	0x0001	
0x0F92	0x0001	
0x08F2	0x00F4	Gotop Information Inc., Unknown device
0x08F2	0x00CE	Gotop Information Inc., Unknown device
0x08F2	0x007F	Gotop Information Inc., Super Q2 Tablet
0x0DFC	0x0001	GeneralTouch Technology Co., Ltd, Touchscreen
0x1391	0x1000	IdealTEK, Inc., URTC-1000
0x6615	0x0001	IRTOUCHSYSTEMS Co. Ltd., Touchscreen
0x595A	0x0001	IRTOUCHSYSTEMS Co. Ltd., Touchscreen
0x0AFA	0x03E8	
0x0637	0x0001	
0x1234	0x5678	Brain Actuated Technologies, Unknown device
0x16E3	0xF9E9	



Vendor	Product	Name
0x0403	0xF9E9	Future Technology Devices International, Ltd, Unknown device
0x0596	0x0001	MicroTouch Systems, Inc., Touchscreen
0x134C	0x0004	PanJit International Inc., Touch Panel Controller
0x134C	0x0003	PanJit International Inc., Touch Panel Controller
0x134C	0x0002	PanJit International Inc., Touch Panel Controller
0x134C	0x0001	PanJit International Inc., Touch Panel Controller
0x1234	0x0002	Brain Actuated Technologies, Unknown device
0x1234	0x0001	Brain Actuated Technologies Unknown device
0x0EEF	0x0002	D-WAV Scientific Co., Ltd, Touchscreen Controller(Professional)
0x0EEF	0x0001	D-WAV Scientific Co., Ltd, eGalax TouchScreen
0x0123	0x0001	
0x3823	0x0002	
0x3823	0x0001	

#### Setup Parameters

- **Touchscreen type**  
[More](#)

**IGEL Setup > User Interface > Input > Touchscreen**

> <b>Touchscreen type</b>	userinterface.touchscreen.driver	
---------------------------	----------------------------------	--

- **Swap X and Y values**  
[More](#)



### IGEL Setup > User Interface > Input > Touchscreen

<b>&gt; Swap X and Y values</b>	userinterface.touchscreen.swapxy	enabled / <a href="#">disabled</a>
---------------------------------	----------------------------------	------------------------------------

- **Set driver specific defaults** for resetting calibration values.

Calibration / Reset

Calibrating the touchscreen:

1. Go to **IGEL Setup > User Interface > Input > Touchscreen**.
2. Set **Touchscreen already calibrated** to 'false'.

[More](#)

### IGEL Setup > User Interface > Touchscreen

<b>&gt; Touchscreen already calibrated</b>	userinterface.touchscreen.calibrat	enabled / <a href="#">disabled</a>
--	------------------------------------	------------------------------------

3. Set **Touchscreen type** to **EvTouch (USB)**.

[More](#)

### IGEL Setup > User Interface > Input > Touchscreen

<b>&gt; Touchscreen type</b>	userinterface.touchscreen.driver	
------------------------------	----------------------------------	--

4. Reboot the device or click **IGEL Setup > Accessories > Touchscreen Calibration** to use the IGEL touchscreen calibration tool.

This will call the *xinput\_calibrator* calibration tool which is located at */usr/bin/xinput\_calibrator*. The calibration parameter will be saved in IGEL setup.

Hold-to-Right-Click Feature

To activate the feature:

1. Enable the option **Emulate right button** under **User Interface > Input > Touchscreen**.

[More](#)



### IGEL Setup > User Interface > Input > Touchscreen

<b>&gt; Emulate right button</b>	userinterface.touchscreen.emulatethirdbutton	enabled / <u>disabled</u>
----------------------------------	--	---------------------------

2. Set under **Right button timeout** the time after which right-click is generated.

[More](#)

### IGEL Setup > User Interface > Input > Touchscreen

<b>&gt; Right button timeout</b>	userinterface.touchscreen.emulatethirdbuttontimeout	Default: <u>1000 msec</u>
----------------------------------	---	---------------------------

#### Multimonitor

Multimonitor configuration is not supported.

#### eGalax

##### Supported Devices

EETI eGalax eMPIA USB touchscreens.

#### Setup Parameters

- Touchscreen type**

[More](#)

### IGEL Setup > User Interface > Input > Touchscreen

<b>&gt; Touchscreen type</b>	userinterface.touchscreen.driver
------------------------------	----------------------------------

#### Calibration / Reset

Calibrating the touchscreen:

1. Go to **IGEL Setup > User Interface > Input > Touchscreen**.
2. Set **Touchscreen already calibrated** to 'false'.

[More](#)



### IGEL Setup > User Interface > Touchscreen

<b>&gt; Touchscreen already calibrated</b>	userinterface.touchscreen.calibrat ed	enabled / <u>disabled</u>
--	--	---------------------------

- Set **Touchscreen type** to **eGalax**.

[More](#)

### IGEL Setup > User Interface > Input > Touchscreen

<b>&gt; Touchscreen type</b>	userinterface.touchscreen.driver	
------------------------------	----------------------------------	--

- Reboot the device or click **IGEL Setup > Accessories > Touchscreen Calibration** to use the IGEL touchscreen calibration tool.

This will call the proprietary EETI calibration tool, which is located at `/usr/bin/eCalib`. The calibration parameter will be saved in `/wfs/egtouch.d`.

#### Hold-to-Right-Click Feature

To activate the feature:

- Enable the option **Emulate right button** under **User Interface > Input > Touchscreen**.

[More](#)

### IGEL Setup > User Interface > Input > Touchscreen

<b>&gt; Emulate right button</b>	userinterface.touchscreen.emulatethirdbutton enabled	<u>enabled</u> / <u>disabled</u>
----------------------------------	---	----------------------------------

- Set under **Right button timeout** the time after which right-click is generated.

[More](#)

### IGEL Setup > User Interface > Input > Touchscreen

<b>&gt; Right button timeout</b>	userinterface.touchscreen.emulatethirdbuttonti meout	Default: <u>1000 msec</u>
----------------------------------	---	---------------------------



## Multimonitor

Multimonitor configuration is not supported.

## Elo Multitouch (USB)

### Supported Devices

IntelliTouch Plus/iTouch Plus 2515-07(non HID), 2521 (HID), 2515-00(HID) PCAP 2 touch, 4 touch and 10 touch controllers.

### Setup Parameters

- **Touchscreen type**

[More](#)

### IGEL Setup > User Interface > Input > Touchscreen

> <b>Touchscreen type</b>	userinterface.touchscreen.driver	
---------------------------	----------------------------------	--

### Calibration / Reset

Calibrating the touchscreen:

1. Go to **IGEL Setup > User Interface > Input > Touchscreen**.
2. Set **Touchscreen already calibrated** to 'false'.

[More](#)

### IGEL Setup > User Interface > Touchscreen

> <b>Touchscreen already calibrated</b>	userinterface.touchscreen.calibrated	enabled / <u>disabled</u>
---	--------------------------------------	---------------------------

3. Set **Touchscreen type** to **Elo Multitouch (USB)**.

[More](#)

### IGEL Setup > User Interface > Input > Touchscreen



> Touchscreen type	userinterface.touchscreen.driver	
--------------------	----------------------------------	--

4. Reboot the device or click in IGEL Setup **Accessories > Touchscreen Calibration** to use the IGEL touchscreen calibration tool.

This will call the proprietary ELO Multitouch calibration tool which is located at /etc/opt/elo-  
mt-usb/elova. The calibration parameter will be saved in /wfs/elo-usb.d/MT-  
USBConfigData.

#### Hold-to-Right-Click Feature

To activate the feature:

1. Enable the option **Emulate right button** under **User Interface > Input > Touchscreen**.  
[More](#)

#### IGEL Setup > User Interface > Input > Touchscreen

> Emulate right button	userinterface.touchscreen.emulatethirdbutton	enabled / <u>disabled</u>
---------------------------	--	------------------------------

2. Set under **Right button timeout** the time after which right-click is generated.

[More](#)

#### IGEL Setup > User Interface > Input > Touchscreen

> Right button timeout	userinterface.touchscreen.emulatethirdbuttontimeout	Default: <u>1000</u> <u>msec</u>
---------------------------	---	-------------------------------------

#### Multimonitor

Multiple ELO Multitouch (USB) touchscreens on a single IGEL device are supported. Calibration of the second ELO Multitouch USB touchscreen can be done via command line by using: /etc/opt/elo-  
mt-usb/elova --videoscreen=2 where 2 is the second ELO Multitouch touchscreen connected to the IGEL device.

To view a list of video and USB touchscreen devices available for calibration, use the command: /etc/  
opt/elo-  
mt-usb/elova --viewdevices.



## Elo Singletouch (USB)

### Supported Devices

Elo Smartset USB Controllers:

- IntelliTouch(R) 2701, 2700, 2600, 2500U
- CarrollTouch(R) 4500U, 4000U
- Accutouch(R) 2216, 3000U, 2218
- Surface Capacitive 5020, 5010, 5000
- Acoustic Pulse Recognition(APR) Smartset 7010
- Other Elo Smartset USB controllers

### Setup Parameters

#### **Touchscreen type**

[More](#)

#### IGEL Setup > User Interface > Input > Touchscreen

> <b>Touchscreen type</b>	userinterface.touchscreen.driver	
---------------------------	----------------------------------	--

### Calibration / Reset

Calibrating the touchscreen:

1. Go to **IGEL Setup > User Interface > Input > Touchscreen**.
2. Set **Touchscreen already calibrated** to 'false'.

[More](#)

#### IGEL Setup > User Interface > Touchscreen

> <b>Touchscreen already calibrated</b>	userinterface.touchscreen.calibrated	enabled / <u>disabled</u>
---	--------------------------------------	---------------------------

3. Set **Touchscreen type** to **Elo Singletouch (USB)**.

[More](#)

#### IGEL Setup > User Interface > Input > Touchscreen

> <b>Touchscreen type</b>	userinterface.touchscreen.driver	
---------------------------	----------------------------------	--



4. Reboot the device or click in IGEL Setup **Accessories > Touchscreen Calibration** to use the IGEL touchscreen calibration tool.

This will call the proprietary ELO Singletouch calibration tool which is located at /etc/opt/elo-usb/elova. The calibration parameter will be saved in /wfs/elo-usb.d/USBConfigData.

#### Hold-to-Right-Click Feature

The feature is not supported.

#### Multimonitor

Multiple ELO Singletouch USB touchscreens on a single IGEL device are supported. Calibration of the second ELO Singletouch USB touchscreen can be done via command line by using: /etc/opt/elo-usb/elova --videoscreen=2 where 2 is the second ELO Singletouch USB touchscreen connected to the IGEL device.

To view a list of video and USB touchscreen devices available for calibration, use the command: /etc/opt/elo-usb/elova --viewdevices.

#### TSHARC (USB)

##### Supported Devices

Hampshire TSHARC USB touchscreens.

##### Setup Parameters

- **Touchscreen type**  
[More](#)

#### IGEL Setup > User Interface > Input > Touchscreen

> <b>Touchscreen type</b>	userinterface.touchscreen.driver	
---------------------------	----------------------------------	--

#### Calibration / Reset

Calibrating the touchscreen:

1. Go to **IGEL Setup > User Interface > Input > Touchscreen**.
2. Disable **Touchscreen already calibrated**.  
[More](#)



### IGEL Setup > User Interface > Touchscreen

> Touchscreen already calibrated	userinterface.touchscreen.calibrated	enabled / <u>disabled</u>
----------------------------------	--------------------------------------	---------------------------

3. Set **Touchscreen type** to **TSharc**.

[More](#)

### IGEL Setup > User Interface > Input > Touchscreen

> Touchscreen type	userinterface.touchscreen.driver	
--------------------	----------------------------------	--

4. Reboot the device or click **IGEL Setup > Accessories > Touchscreen Calibration** to use the IGEL touchscreen calibration tool.

This will call the proprietary Hampshire calibration tool, which is located at /usr/bin/tscal. The calibration parameter will be saved in /wfs/tsharc.d.

#### Hold-to-Right-Click Feature

To activate the feature:

1. Enable the option **Emulate right button** under **User Interface > Input > Touchscreen**.

[More](#)

### IGEL Setup > User Interface > Input > Touchscreen

> Emulate right button	userinterface.touchscreen.emulatethirdbutton	enabled / <u>disabled</u>
------------------------	--	---------------------------

2. Set under **Right button timeout** the time after which right-click is generated.

[More](#)

### IGEL Setup > User interface > Input > Touchscreen

> Right button timeout	userinterface.touchscreen.emulatethirdbuttontimeout	Default: <u>1000 msec</u>
------------------------	---	---------------------------



## Multimonitor

Multimonitor configuration is not supported.

## Touchscreen in Multimonitor Environment

### Symptom

You are using a touchscreen in a multimonitor environment. In this case, it can happen that the touchscreen coordinate matrix expands over both monitors, with the result that the monitor interprets the touch point in a wrong way.

### Problem

You touch the touchscreen in its center and the cursor moves between the two screens.

### Solution

To avoid the unrequested expansion of the touchscreen matrix you have to select the correct touchscreen connection type in the setup:

1. Click **User Interface > Input > Touchscreen** in the IGEL setup.
2. Select the correct connection type under **Multi Monitor > Touchscreen Monitor**.

## USB-Powered ASUS Monitor and IGEL OS 11

### **Solution Based on Experience from the Field**

This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

### Issue

USB-powered monitor

### Environment

- IGEL OS 11 (11.03.100)
- UMS 6.01 and higher

### Description

Recommendation for a USB-powered monitor



## Solution

In the following link, you can find the USB-powered ASUS monitor that works plug and play with IGEL OS <https://www.asus.com/us/Monitors/MB168B/>.

## Solving Hotplugging Issues with DisplayPort Monitors

### Symptom

On IGEL Linux, in a dual view configuration, the following problem occurs: If a monitor connected via DisplayPort is only switched on after booting the device, it will remain black.

### Problem

The DisplayPort standard allows for a powered-off monitor to be undetectable by the graphics card.

### Solution

The following checks whether a monitor contained in the configuration is missing (i.e. powered off) and makes it usable as soon as it appears (i.e. is powered on):

1. If you are using IGEL Linux 5, make sure you are running version 5.10.410 or newer.  
If you are using IGEL Linux 10 you do not need to upgrade.
2. In Setup, go to **System > Registry > Parameter >**  
`session.user_display%.options.enhanced_hotplug`
3. Make sure the parameter is set to true (default).

There is another setting you can use if you do not want IGEL Linux to change the display settings every time a DisplayPort monitor is switched on/off:

- Go to **System > Registry > Parameter >**  
`sessions.user_display%.options.disable_hotplug`
- Set it to **DP\_Disconnect\_Only**.

## No Sound When Using a DisplayPort Monitor

### Symptom

You do not hear any sound from your *IGEL UD5* or *UD6* device. You are using a monitor connected via DisplayPort.

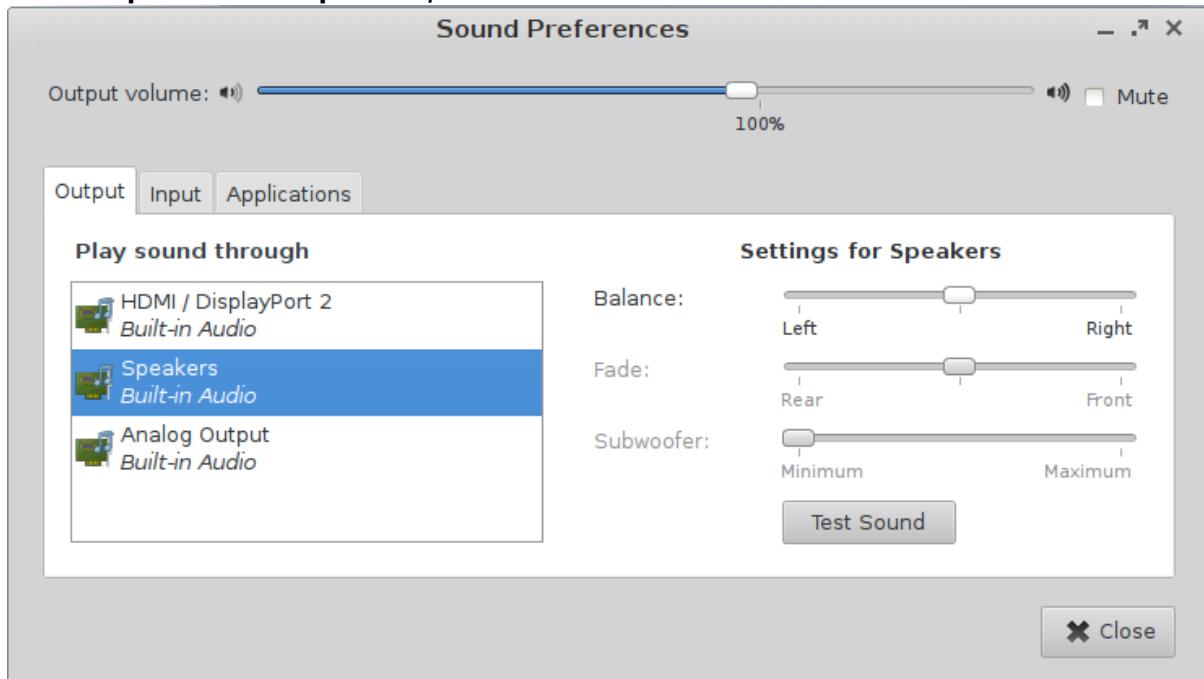
### Problem

Some DisplayPort monitors misleadingly report support for display audio although they do not have loudspeakers. Therefore *IGEL Linux* will try to play back audio via the monitor.

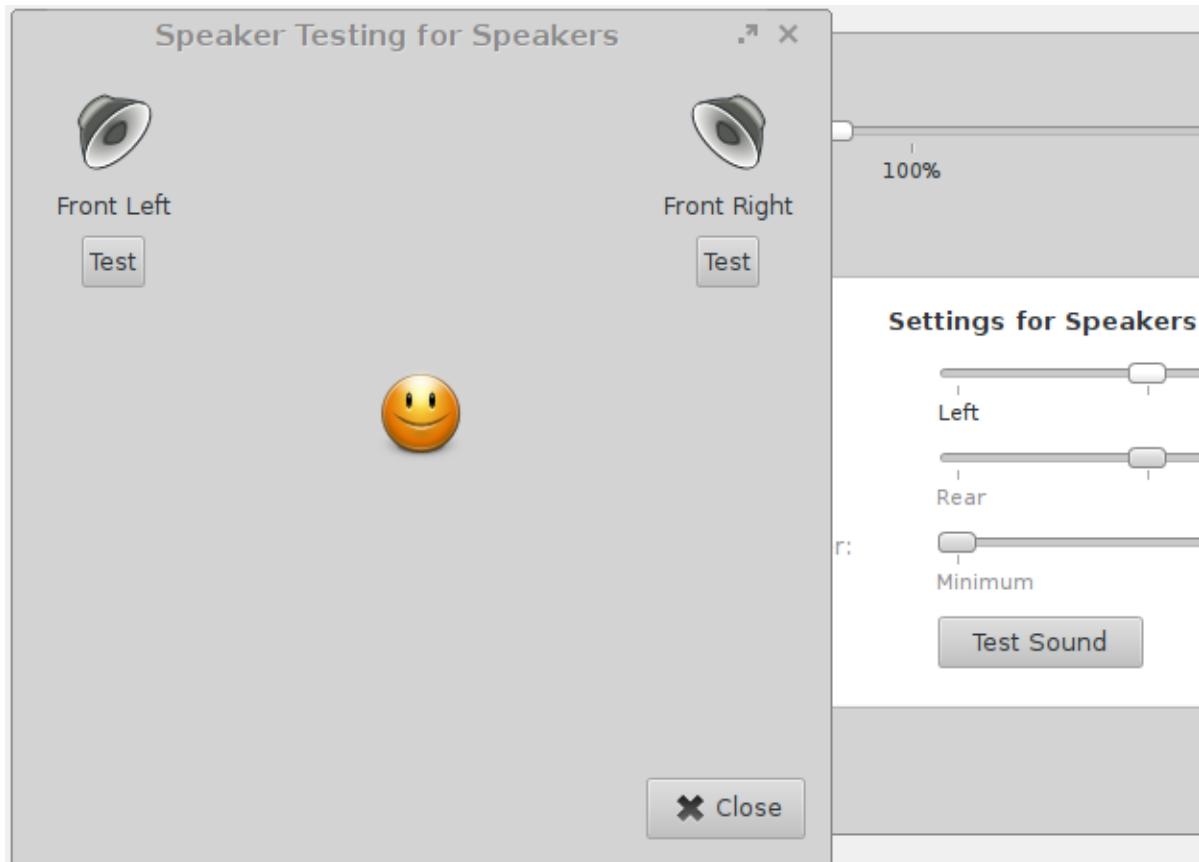


## Solution

1. Right-click on the loudspeaker icon in the panel and open **Sound Preferences**.
2. In the **Output** tab select **Speakers / Built-in Audio**.



3. Click **Test Sound** to test the new setting. Check if you hear a voice saying "Front Left" and "Front Right" on the device speakers.



## Connecting Three DVI Monitors to UD7 with Passive DisplayPort Adapters

### Problem

When three DVI monitors are connected to a UD7 thin client over passive DisplayPort adapters, only one or two monitors are detected.

### Solution

This solution is only persistent if energy saving is switched off.

1. Open the thin client's Setup.
2. Go to **System > Registry > x > xserver0 > force\_reconfig** (Registry key: `x.xserver0.force_reconfig`) and set the value to **never**.
3. Click **Ok** to save the setting and close the Setup.
4. Restart the device.  
All three monitors should be detected.



## 2.23.2 Using a Cherry SECURE BOARD

### Overview

Cherry SECURE BOARD 1.0 provides a secure keyboard input mode which safeguards against hardware keylogging and "Bad USB" attacks.

The following security features are available when an IGEL OS 11 device is connected to a Cherry SECURE BOARD 1.0 in secure mode:

- Your IGEL OS 11 devices will accept keyboard input only from a personalized Cherry SECURE BOARD with secure mode enabled.
- The keyboard traffic between the keyboard and the endpoint is transmitted over a TLS 1.3 encrypted connection.
- Optionally, the keyboard can be configured so that it will only accept endpoints that have the right certificates.

For further details on the Cherry SECURE BOARD, see <https://www.cherry-world.com/cherry-secure-board-1-0.html>.

### Prerequisites

- Devices with IGEL OS 11.03 or higher
- UMS 6.01 or higher

### Getting the Cherry SECURE BOARD to Work in Secure Mode

To set up a number of Cherry SECURE BOARD keyboards, you must first configure one endpoint that will be used for personalizing the keyboards. The personalization process implies deploying the appropriate certificates to every Cherry SECURE BOARD keyboard that will be used in secure mode.

In addition, the endpoints that are to be connected to the Cherry SECURE BOARD keyboards must be provisioned with the appropriate certificates.

To set up and use Cherry SECURE BOARD keyboards, perform the following steps:

1. [Getting the Certificates](#)(see page 640)
2. [Setting Up the Personalization Machine](#)(see page 653)
3. [Personalizing the Cherry SECURE BOARD](#)(see page 654)
4. [Setting Up the Endpoints](#)(see page 658)

If you want to put a Cherry SECURE BOARD keyboard into its original state, see [Resetting the Cherry SECURE BOARD to Its Original State](#)(see page 662).

### Getting the Certificates

Secure mode requires a set of certificates being present both on the endpoint and the keyboard. First, all required certificates are transferred to the endpoint. Then, the endpoint installs a user certificate and the corresponding key on the keyboard; optionally, the client root CA certificate is also installed. This installation of certificates is referred to as personalization.



## Downloading the Device Certificates

- ▶ Download all certificates from <https://github.com/secureboard10/secureboard-ca>:

- Device root CA certificate: SecureboardRootCA.pem
- Device intermediate CA certificates: p-20190712.pem, p-20191030 etc.

## Creating the Custom Certificates

According to "CHERRY SECUREBOARD 1.0, Software Developer's Guide", chapter 9.5, all certificate and key pairs that are sent to the keyboard must meet the following requirements:

- X509 Version 3 using ECDSA over NIST curve prime256v1 with corresponding keys
- Size: Maximum of 572 bytes resp. 475 bytes in DER format

- ▶ Create the following custom certificates:

An example how-to for OpenSSL can be found in "CHERRY SECUREBOARD 1.0, Software Developer's Guide", chapter 9.5; see [https://www.cherry.de/files/manual/SECUREBOARD\\_SwDev\\_Guide\\_en-0.4.pdf](https://www.cherry.de/files/manual/SECUREBOARD_SwDev_Guide_en-0.4.pdf).

Also, the SECURE BOARD 1.0 Quick Installation Package contains a ready-made shell script that creates example certificates. Download the package from [https://www.cherry.de/files/software/Cherry\\_Secureboard\\_1.0\\_Quick\\_Installation\\_Package\\_V1.0.zip](https://www.cherry.de/files/software/Cherry_Secureboard_1.0_Quick_Installation_Package_V1.0.zip), unzip the file, and use Cherry Secureboard 1.0 cert-package V1.0/secureboard\_linx/create\_certs.sh (Linux) or Cherry Secureboard 1.0 cert-package V1.0/secureboard\_windows/create\_certs.bat (Windows).

Certificate	Required/Optional	Requirements	Encoding	Max. Extension	File Size*	Name	Remarks
User root CA certificate	required	not specified	PEM	not specified	not specified	If this certificate is also used as the client root CA certificate for mutual authentication, it must meet the requirements for certificates that are sent to the keyboard: X509 Version 3 using ECDSA over NIST curve prime256v1 with corresponding keys; max. 475 bytes	
Intermediate CA certificates	optional (according to the certificate chain that is to be used)	not specified	PEM	not specified	not specified		

Certificate	Required/Optional	Requirements	Encoding/Max. Extension	Max. File Size*	File Name	Remarks
User certificate (keyboard)	required	X509 Version 3 using ECDSA over NIST curve prime256v1 with corresponding keys	DER (binary)	572 bytes	user-cert.der	
Corresponding user key (keyboard)	required	X509 Version 3 using ECDSA over NIST curve prime256v1 with corresponding keys	PEM (without a passphrase)	not specified	user-key.pem	
Client root CA for certificate mutual authentication** (see page 642)	optional; mutual authentication** (see page 642)	X509 Version 3 using ECDSA over NIST curve prime256v1 with corresponding keys	PEM	475 bytes	not specified	Can be identical with the user root CA certificate
Client certificate for mutual authentication (endpoint) (int)	optional; mutual authentication** (see page 642)	X509 Version 3 using ECDSA over NIST curve prime256v1 with corresponding keys	PEM	475 bytes	client-cert.pem	
Client key for mutual authentication (endpoint) (int)	optional; mutual authentication** (see page 642)	X509 Version 3 using ECDSA over NIST curve prime256v1 with corresponding keys	PEM (without a passphrase)	not specified	client-key.pem	

\* The relevant value is the file size that the certificate has when it is stored in binary format.

\*\* When these certificates are installed, the keyboard can verify if the endpoint is authentic. Without the optional certificates, only the verification of the keyboard's authenticity by the endpoint will be carried out.

## Provisioning the Personalization Machine

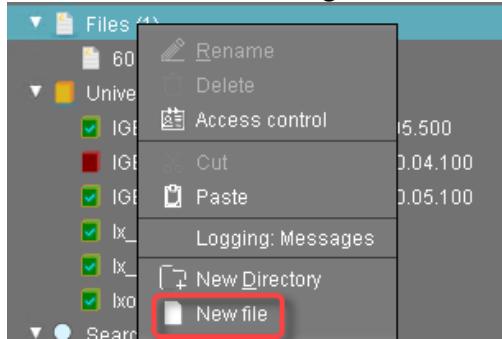
The following instructions describe how to transfer the required certificates to the personalization machine. The personalization machine will deploy the certificates to the keyboard. The UMS will be used for this purpose.

First, a file object is created for each certificate or key file so that the files can be handled by the UMS.

Second, the file objects are assigned to the personalization machine, which results in the files being transferred to that machine.

#### Creating the File Object for the Device Root CA Certificate

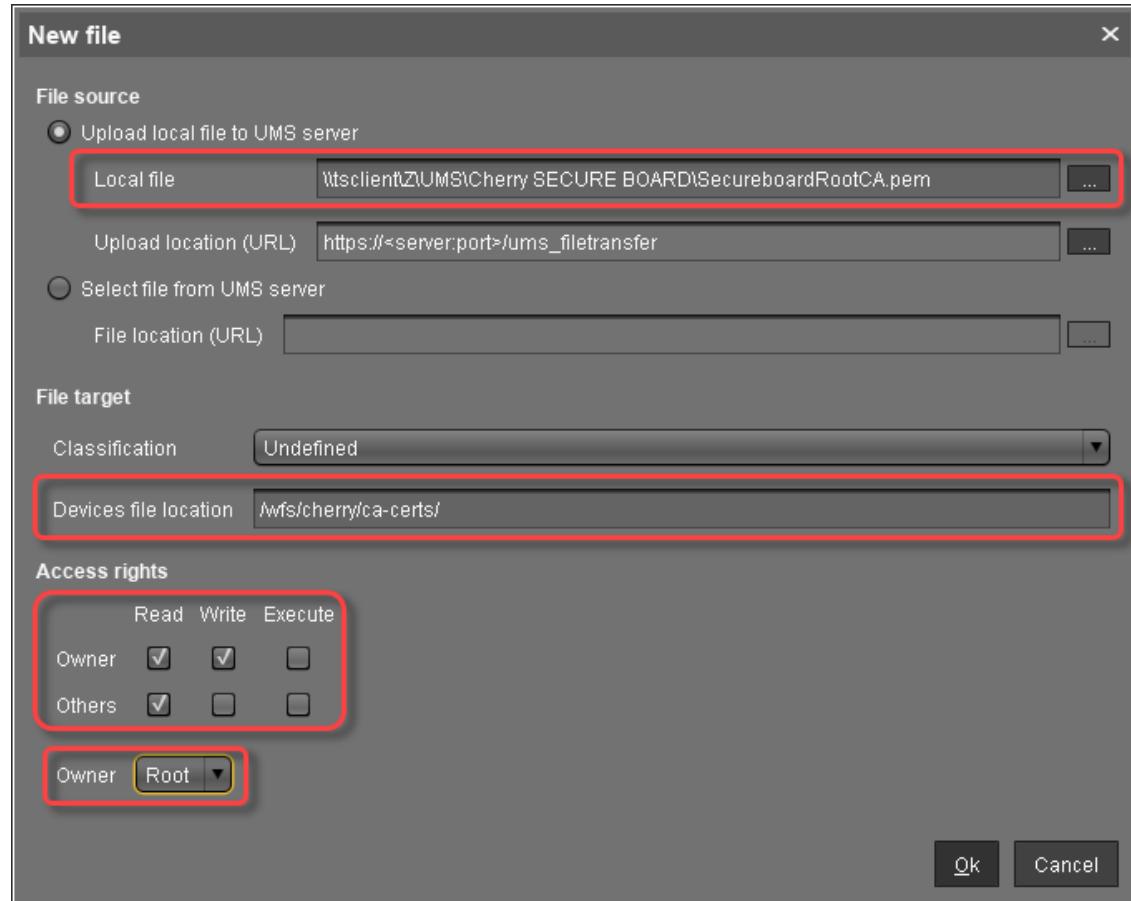
1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



2. In the **New file** dialog, configure the settings as follows:

- **Local file:** Local file path of SecureboardRootCA.pem. Use the file chooser by clicking .
- **Device file location:** /wfs/cherry/ca-certs/
- **Access rights - Owner:** Read, Write
- **Access rights - Others:** Read

- **Owner:** Root

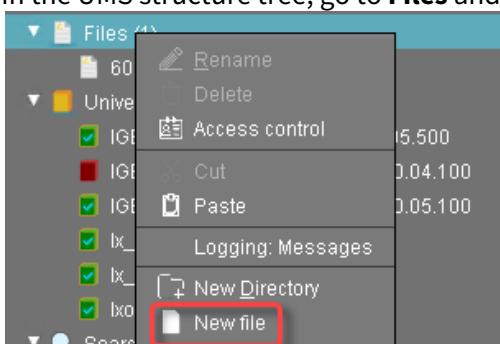


3. Click **Ok**.

In the UMS, the file object **SecureBoardRootCA.pem** is created.

#### Creating the File Object for the Device Intermediate CA Certificate

1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.

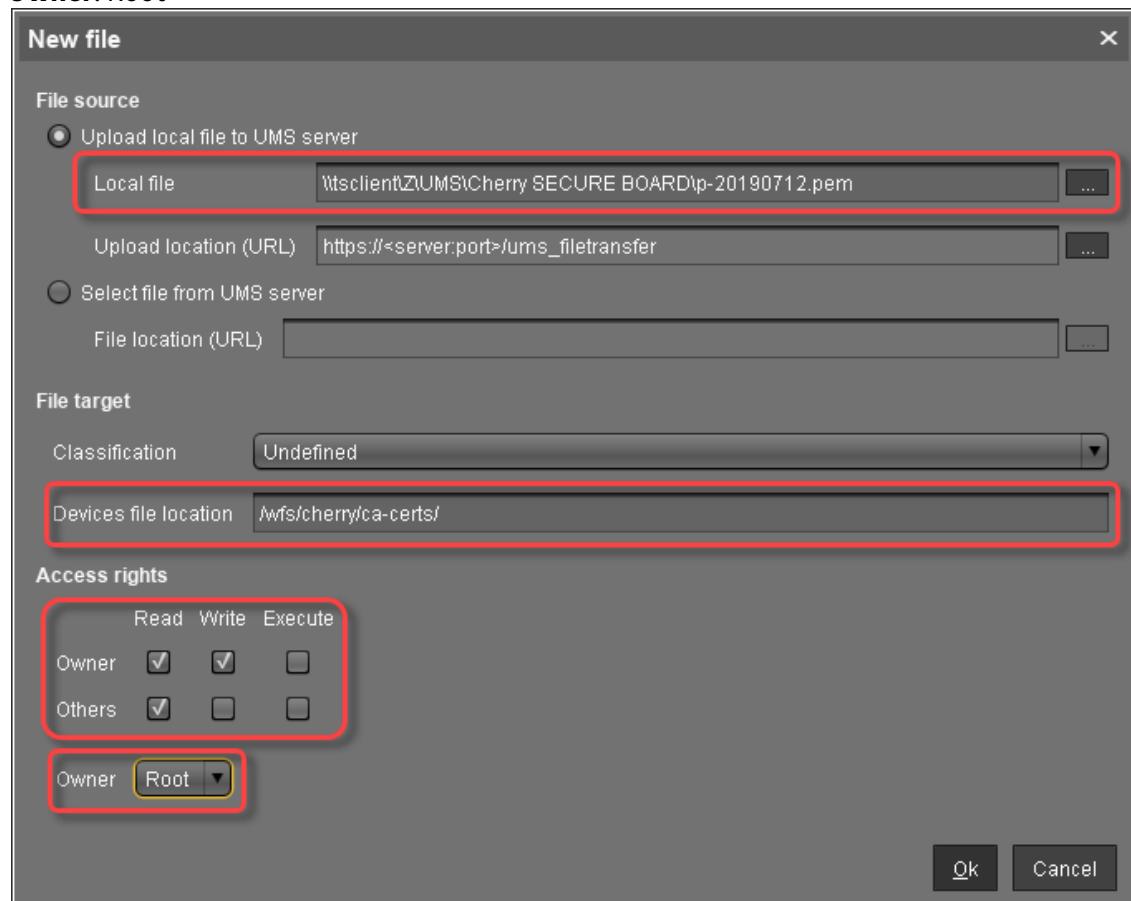


2. In the **New file** dialog, configure the settings as follows:

- **Local file:** Local file path of p-20190712.pem. Use the file chooser by clicking .
- **Device file location:** /wfs/cherry/ca-certs/
- **Access rights - Owner:** Read, Write



- **Access rights - Others:** Read
- **Owner:** Root

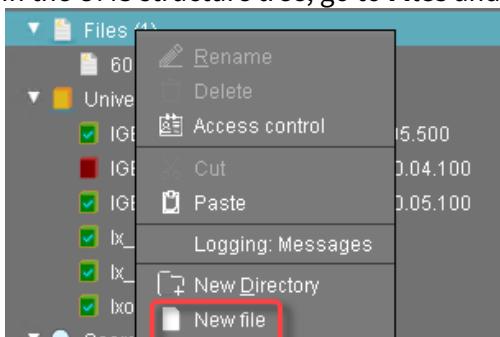


3. Click **Ok**.

In the UMS, the file object **p-20190712.pem** is created.

#### Creating the File Object for the Device Client CA Certificate (Optional)

1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.

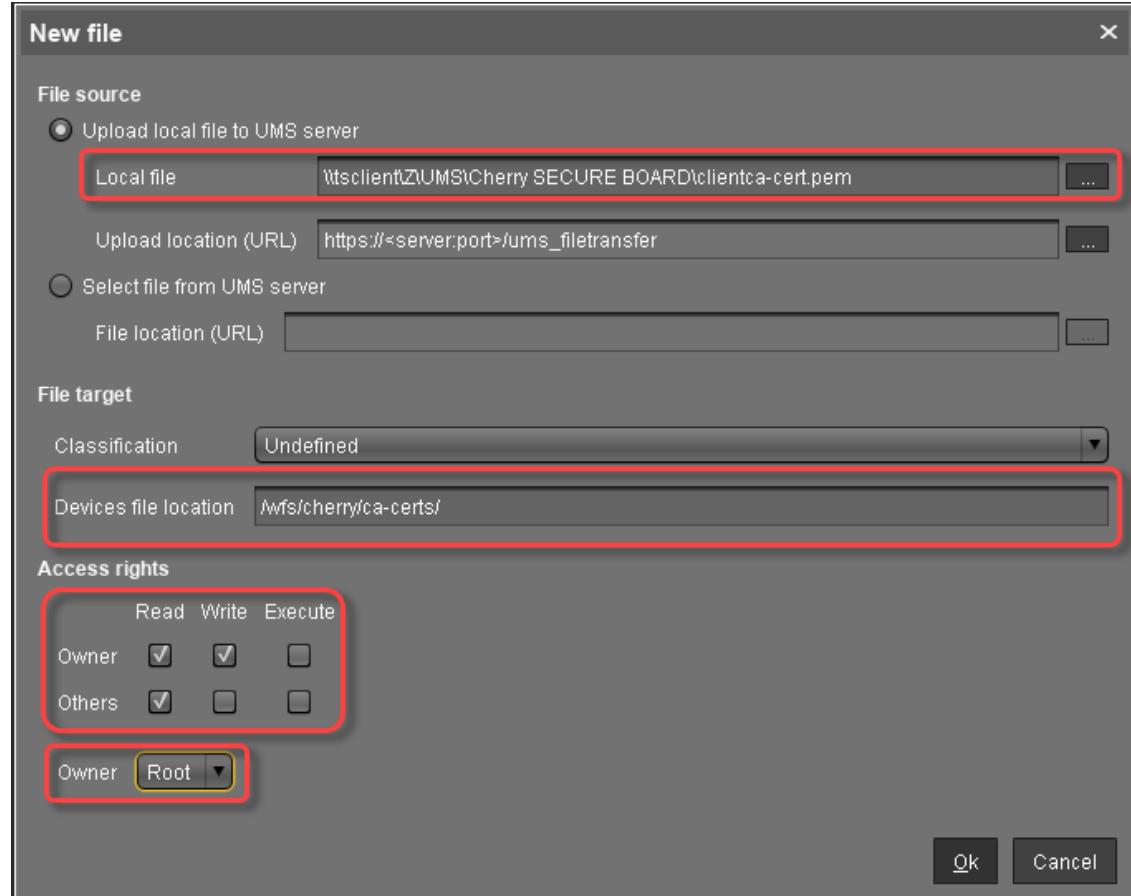


2. In the **New file** dialog, configure the settings as follows:

- **Local file:** Local file path of `clientca-cert.pem`. Use the file chooser by clicking .
- **Device file location:** `/wfs/cherry/ca-certs/`



- **Access rights - Owner:** Read, Write
- **Access rights - Others:** Read
- **Owner:** Root



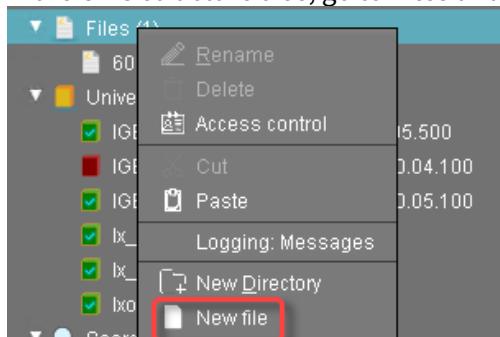
### 3. Click **Ok**.

In the UMS, the file object **clientca-cert.pem** is created.

Creating the File Object for the User Certificate (Keyboard)

To transfer the certificate file user-cert.der to the directory /wfs/cherry/client-certs/ on the personalization machine, proceed as follows:

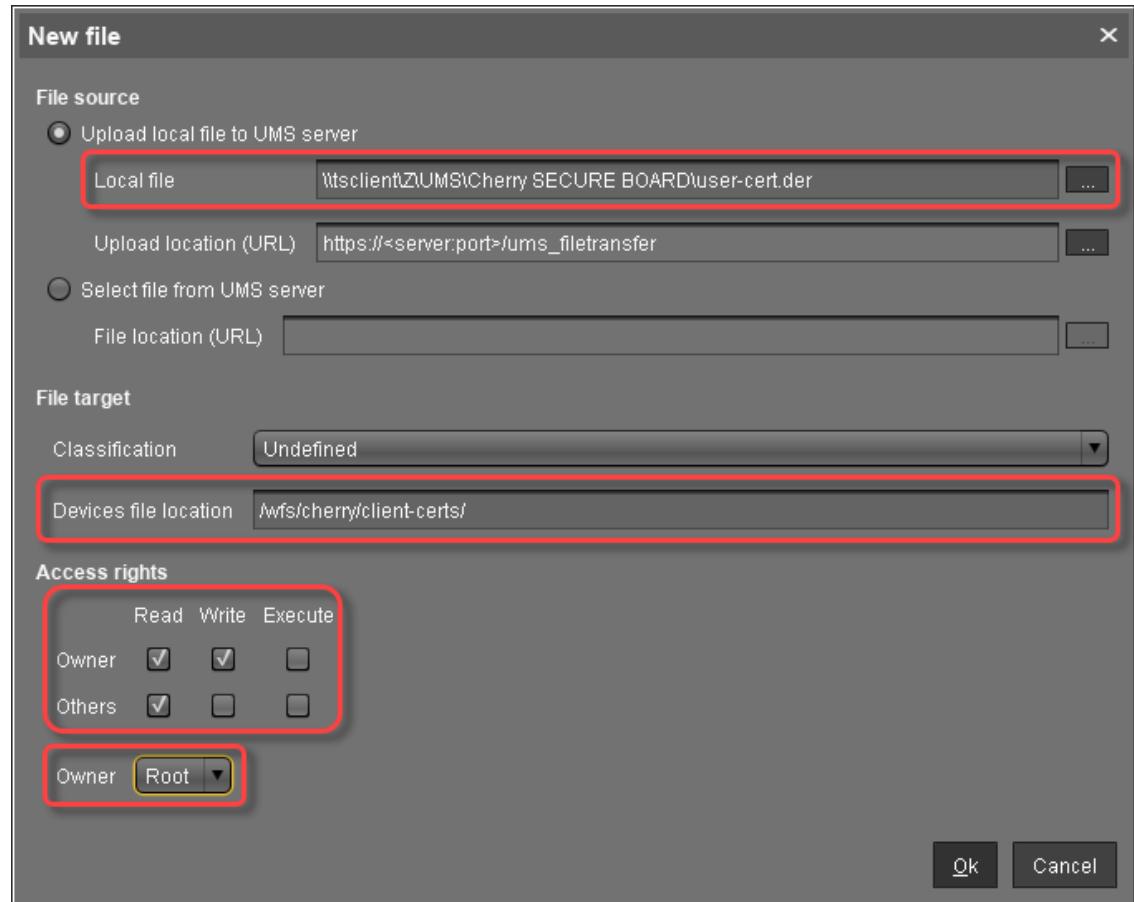
1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.





2. In the **New file** dialog, configure the settings as follows:

- **Local file:** Local file path of user-cert.der. Use the file chooser by clicking .
- **Device file location:** /wfs/cherry/client-certs/
- **Access rights - Owner:** Read, Write
- **Access rights - Others:** Read
- **Owner:** Root



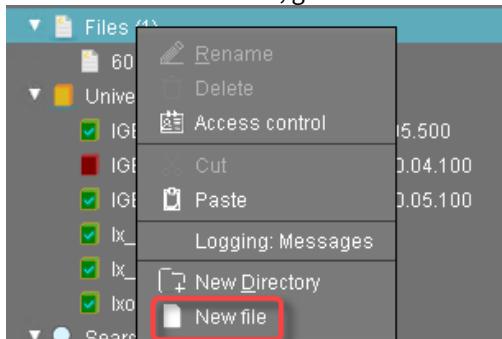
3. Click **Ok**.

In the UMS, the file object **user-cert.der** is created.



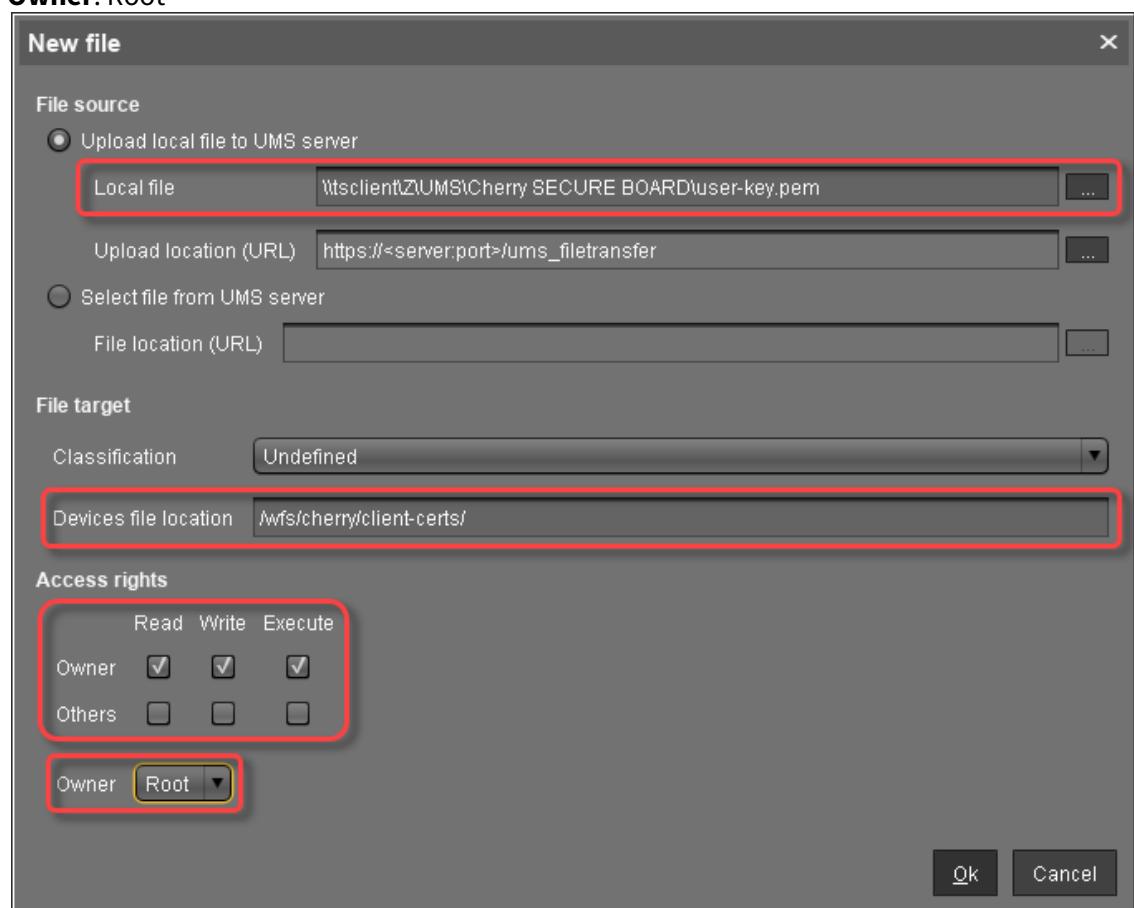
## Creating the File Object for the User Key (Keyboard)

In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



1. In the **New file** dialog, configure the settings as follows:

- **Local file:** Local file path of user-key.pem. Use the file chooser by clicking .
- **Device file location:** /wfs/cherry/client-certs/
- **Access rights - Owner:** Read, Write
- **Access rights - Others:** -
- **Owner:** Root



2. Click **Ok**.

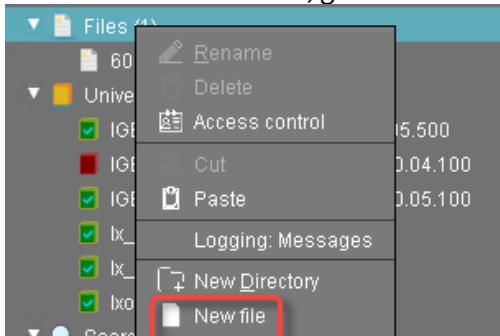
In the UMS, the file object **user-key.pem** is created.

#### Provisioning the Endpoints for Using the SECURE BOARD

The following instructions describe how to transfer the required certificates to the endpoints which will be connected to the SECURE BOARD in secure mode.

#### Creating the File Object for the User Root CA Certificate

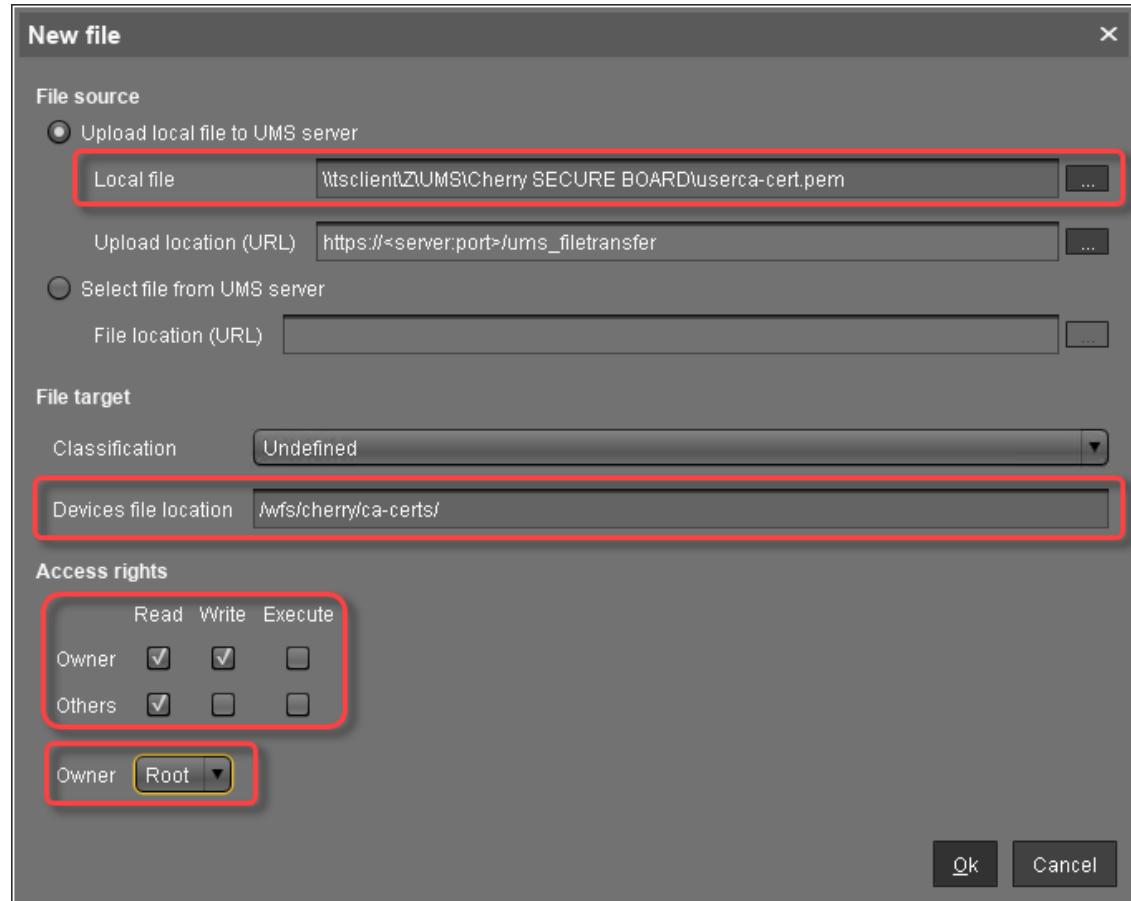
1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



2. In the **New file** dialog, configure the settings as follows:

- **Local file:** Local file path of the certificate file. Use the file chooser by clicking .
- **Device file location:** /wfs/cherry/ca-certs/
- **Access rights - Owner:** Read, Write
- **Access rights - Others:** Read

- **Owner:** Root

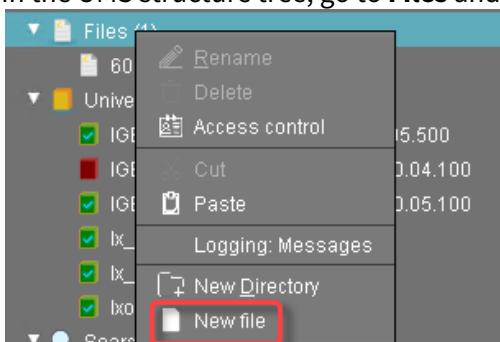


3. Click **Ok**.

In the UMS, the file object is created. The name of the file object is derived from the file name.

#### Creating the File Object for the Client Root CA Certificate (Optional)

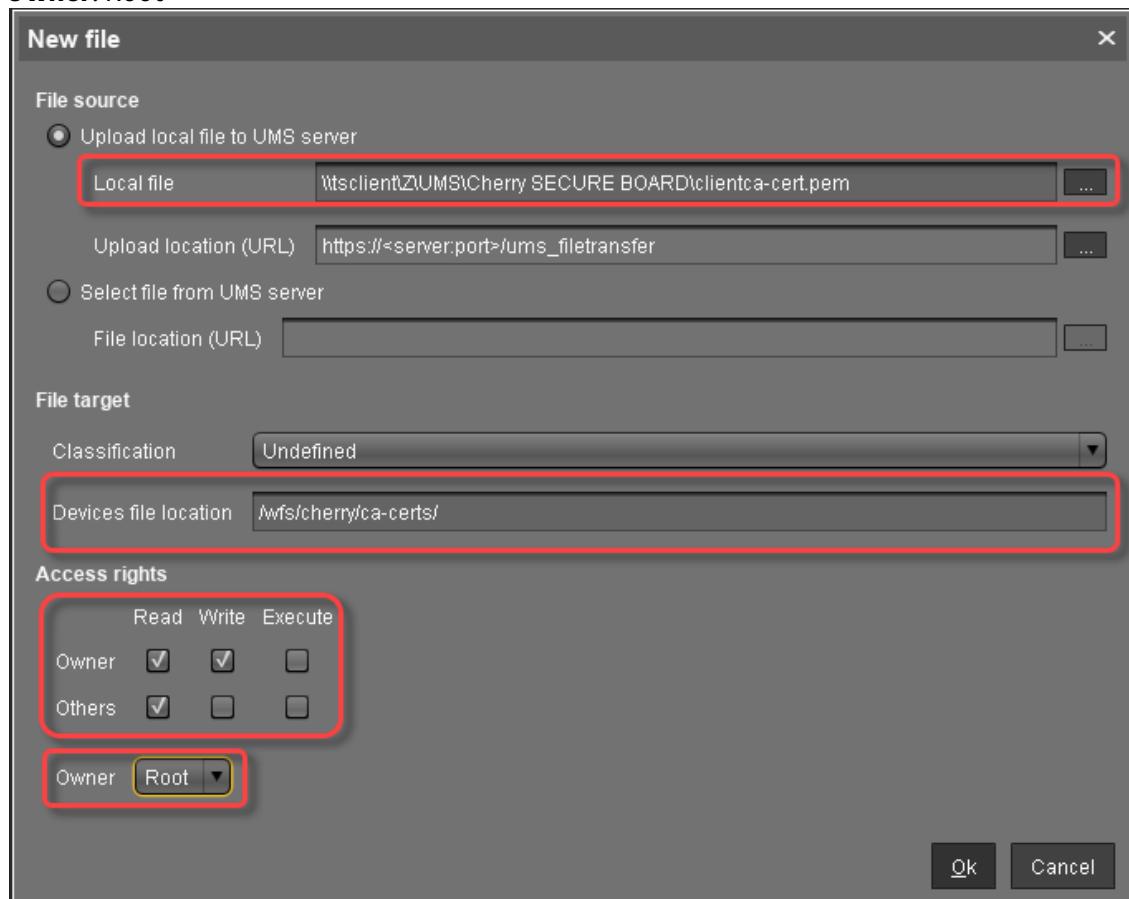
1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



2. In the **New file** dialog, configure the settings as follows:

- **Local file:** Local file path of the certificate file. Use the file chooser by clicking .
- **Device file location:** /wfs/cherry/ca-certs/
- **Access rights - Owner:** Read, Write

- **Access rights - Others:** Read
- **Owner:** Root

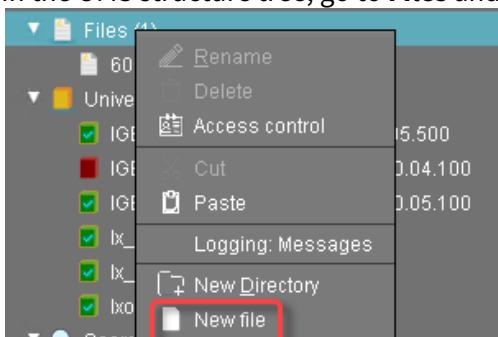


3. Click **Ok**.

In the UMS, the file object is created. The name of the file object is derived from the file name.

#### Creating the File Object for the Client Certificate (Endpoint) (Optional)

1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.

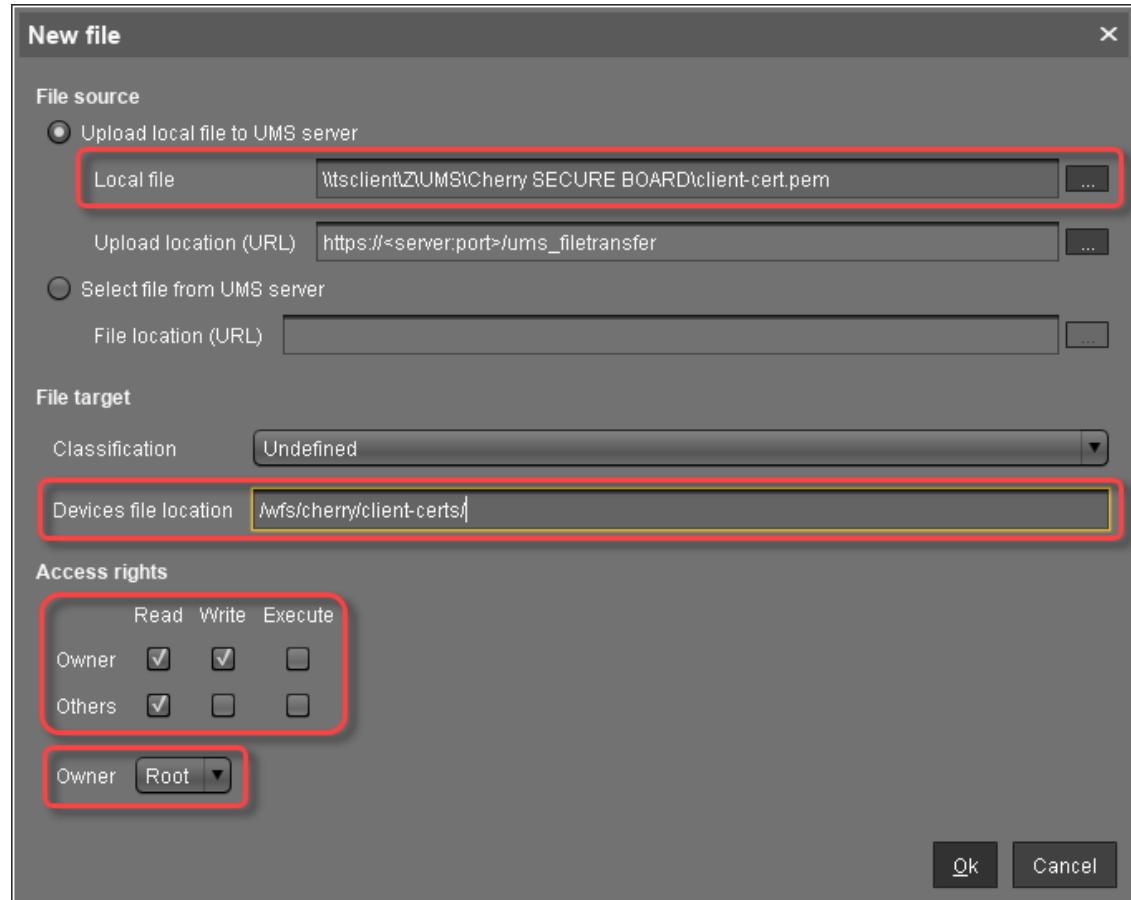


2. In the **New file** dialog, configure the settings as follows:

- **Local file:** Local file path of `client-cert.pem`. Use the file chooser by clicking .
- **Device file location:** `/wfs/cherry/client-certs/`



- **Access rights - Owner:** Read, Write
- **Access rights - Others:** Read
- **Owner:** Root

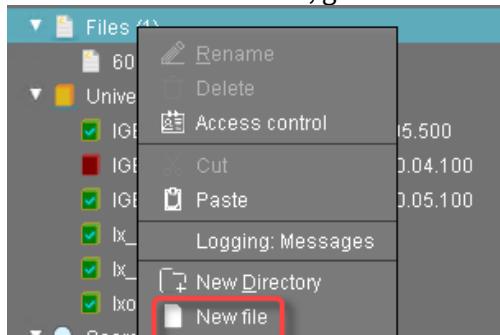


3. Click **Ok**.

In the UMS, the file object is created. The name of the file object is derived from the file name.

#### Creating the File Object for the Client Key (Endpoint) (Optional)

1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



2. In the **New file** dialog, configure the settings as follows:

- **Local file:** Local file path of client-key.pem. Use the file chooser by clicking .



- **Device file location:** /wfs/cherry/client-certs/
- **Access rights - Owner:** Read, Write
- **Access rights - Others:** -
- **Owner:** Root

**New file**

**File source**

Upload local file to UMS server

Local file

Upload location (URL)

Select file from UMS server

File location (URL)

**File target**

Classification

Devices file location

**Access rights**

	Read	Write	Execute
Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Others	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Owner

**Ok** **Cancel**

### 3. Click **Ok**.

In the UMS, the file object is created. The name of the file object is derived from the file name.

## Setting Up the Personalization Machine

### Setting Up the Local Terminal

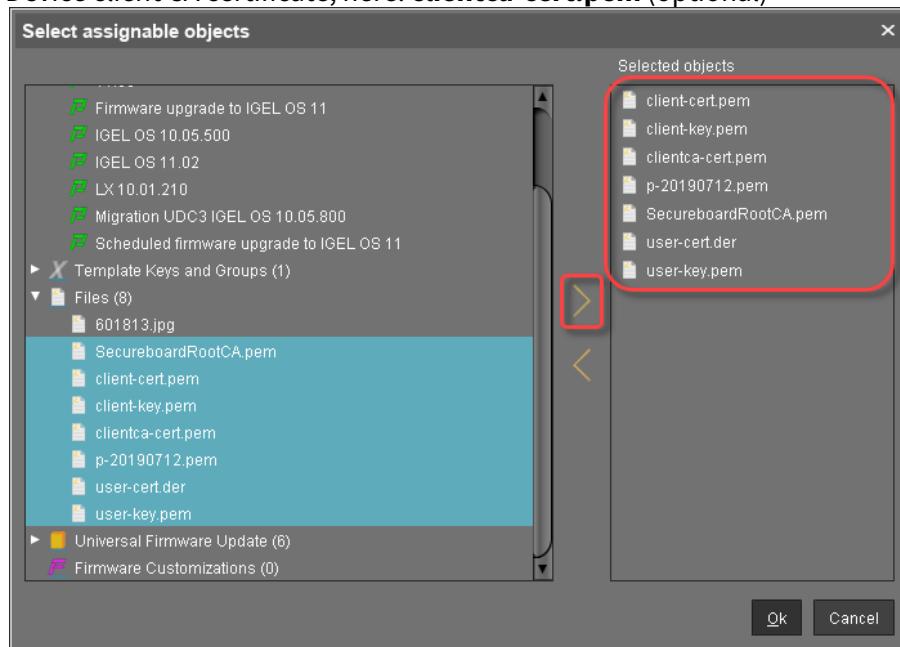
If a local terminal session has already been configured on the designated personalization machine, you can skip this step.

1. Open the device's Setup and go to **Accessories >Terminals**.
  2. Select .
  3. Click **Ok**.
- On the desktop and in the Application Starter, a starter for the terminal session is created.



## Assigning the File Objects to the Personalization Machine

1. In the UMS structure tree, select the endpoint that will act as the personalization machine.
2. In the **Assigned objects** area, click
3. Under **Files**, select the file objects using the button:
  - **SecureboardRootCA.pem**
  - Device intermediate CA certificates; here: **p-20190712.pem**
  - **user-cert.der**
  - **user-key.pem**
  - **client-cert.pem** (optional)
  - **client-key.pem** (optional)
  - Device client CA certificate; here: **clientca-cert.pem** (optional)

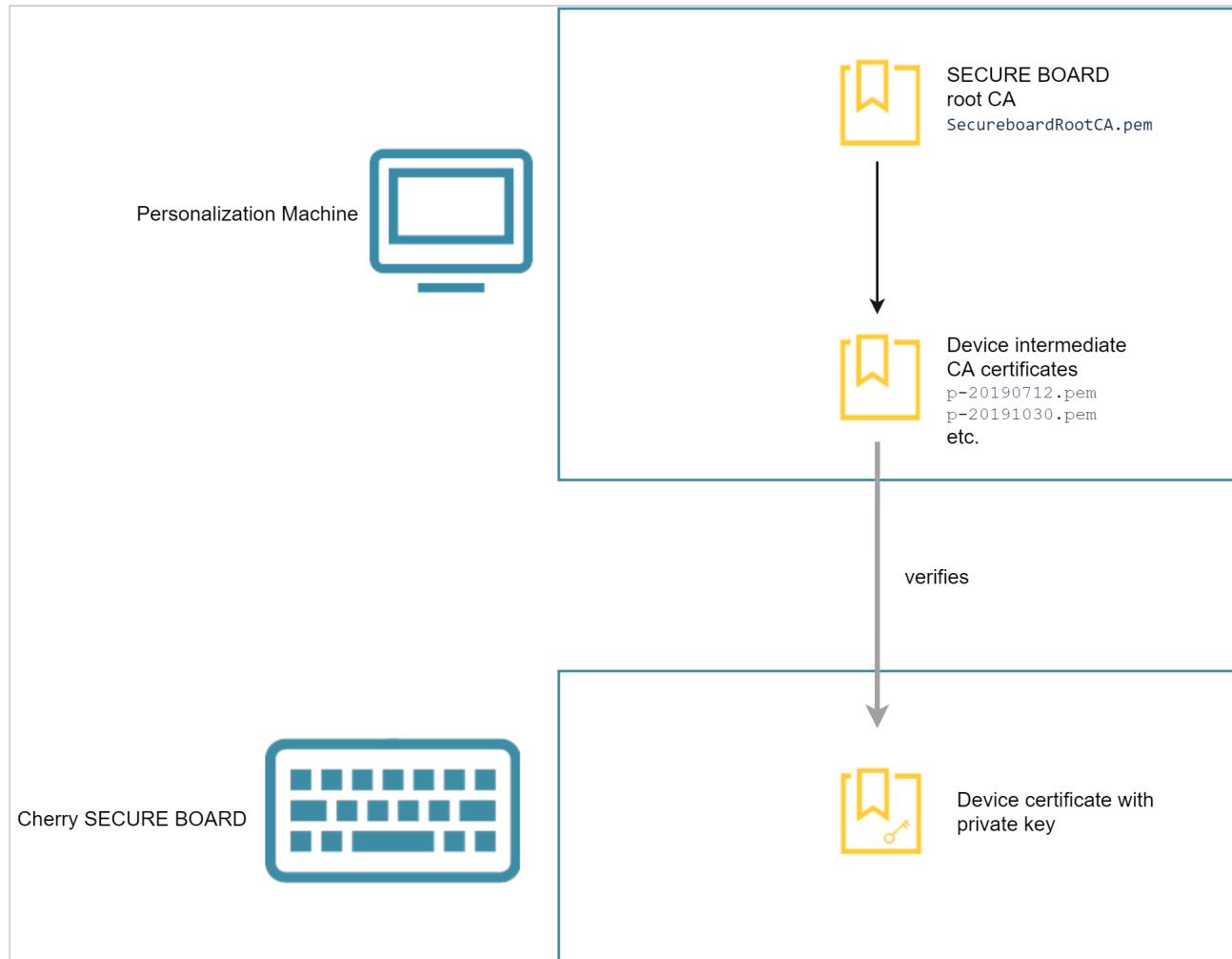


4. Click **Ok**.
5. In the **Update time** dialog, select **Now** and click **Ok**.  
The certificate and key files are transferred to the personalization machine. The personalization machine is ready for operation.

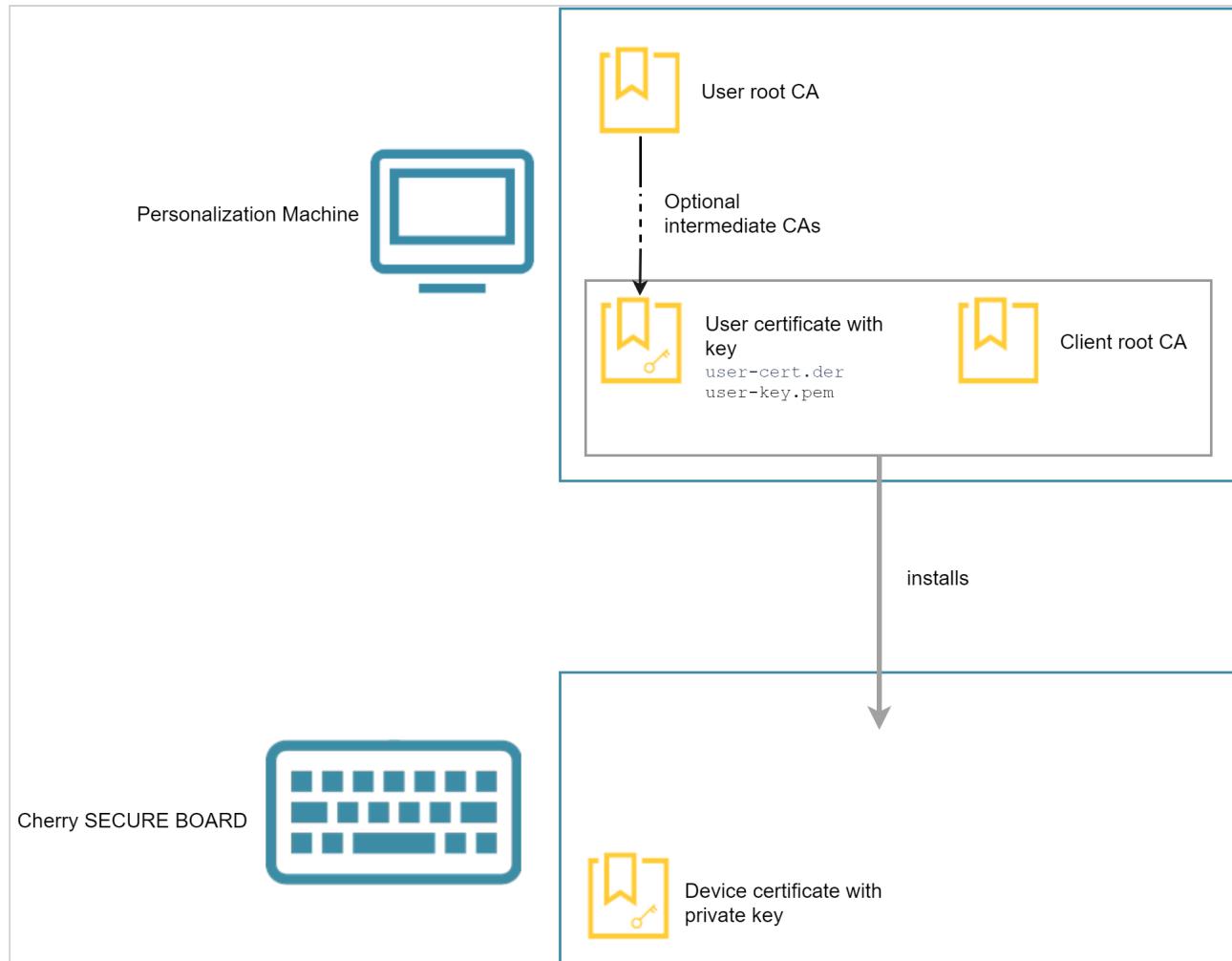
## Personalizing the Cherry SECURE BOARD

### Overview

Personalization Machine Verifies if the Keyboard Is a Genuine Cherry SECURE BOARD



Personalization Machine Installs the Certificates on the Keyboard



### Prerequisites

- The machine has been prepared as described under [Setting Up the Personalization Machine](#)(see page 653).
- The Cherry SECURE BOARD keyboards are in factory state or have been reset (see [Resetting the Cherry SECURE BOARD to Its Original State](#)(see page 662)).

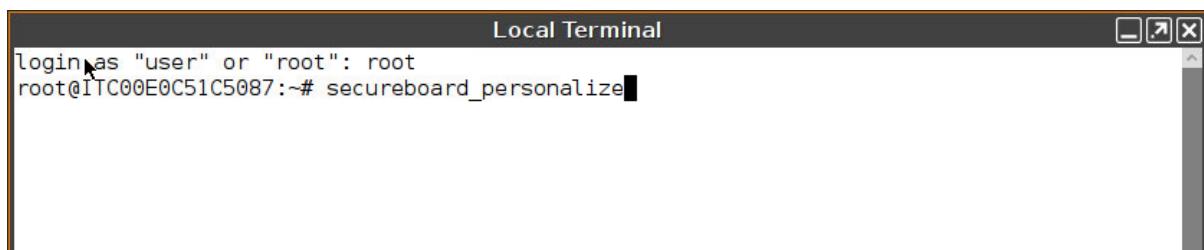
### Instructions

1. Start the local terminal and log in as root.



A screenshot of a "Local Terminal" window. The title bar says "Local Terminal". The command line shows "login as "user" or "root": root" followed by a cursor. The window has standard Linux-style window controls at the top right.

2. Enter the command `secureboard_personalize`



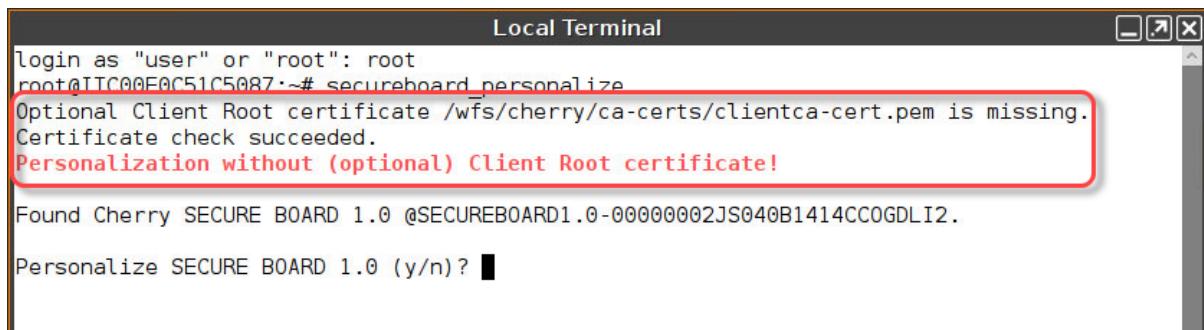
A screenshot of a "Local Terminal" window. The title bar says "Local Terminal". The command line shows "login as "user" or "root": root" followed by "root@ITC00E0C51C5087:~# secureboard\_personalize" and a cursor. The window has standard Linux-style window controls at the top right.

If all required certificates and the optional certificates for mutual authentication are present, the personalization facility is ready.



A screenshot of a "Local Terminal" window. The title bar says "Local Terminal". The command line shows "login as "user" or "root": root" followed by "root@ITC00E0C51C5087:~# ls /wfs/cherry/client-certs/" and a list of files: "client-cert.pem", "client-key.pem", "user-cert.der", and "user-key.pem". Below that, "root@ITC00E0C51C5087:~# ls /wfs/cherry/ca-certs/" and a list of files: "311625f3.0", "570b05fc.0", "d81e5d09.0", "ece45aca.0", "SecureboardRootCA.pem", "46c284d6.0", "clientca-cert.pem", "dce0a93b.0", and "p-20190712.pem". Then "root@ITC00E0C51C5087:~# secureboard\_personalize" and "Certificate check succeeded." The last line is highlighted with a red box.

In case only the required certificates are present, the personalization facility is ready, but a message stating the absence of the optional certificates for mutual authentication is shown:



A screenshot of a "Local Terminal" window. The title bar says "Local Terminal". The command line shows "login as "user" or "root": root" followed by "root@ITC00E0C51C5087:~# secureboard\_personalize". A message follows: "Optional Client Root certificate /wfs/cherry/ca-certs/clientca-cert.pem is missing." Below it, "Certificate check succeeded." and "Personalization without (optional) Client Root certificate!" are displayed in red text, also enclosed in a red box. At the bottom, "Found Cherry SECURE BOARD 1.0 @SECUREBOARD1.0-00000002JS040B1414CC0GDLI2." and "Personalize SECURE BOARD 1.0 (y/n)?" are shown.



### 3. Plug in a Cherry SECURE BOARD.

A message confirms that the keyboard has been detected; you are prompted to start the personalization.

The screenshot shows a terminal window titled "Local Terminal". The terminal output includes several file listing commands and a command to personalize a secure board. A red box highlights the final command and its response:

```

Local Terminal
login as "user" or "root": root
root@ITC00E0C51C5087:~# ls /wfs/cherry/client-certs/
client-cert.pem client-key.pem user-cert.der user-key.pem
root@ITC00E0C51C5087:~# ls /wfs/cherry/ca-certs/
311625f3.0 570b05fc.0 d81e5d09.0 ece45aca.0 SecureboardRootCA.pem
46c284d6.0 clientca-cert.pem dce0a93b.0 p-20190712.pem
root@ITC00E0C51C5087:~# secureboard_personalize
Certificate check succeeded.

Found Cherry SECURE BOARD 1.0 @SECUREBOARD1.0-00000002JS040B1414CC0GDLI2.

Personalize SECURE BOARD 1.0 (y/n)? █
  
```

### 4. Enter y to start the personalization process.

During the personalization process, a few messages are shown. If everything has gone well, a message about the successful personalization appears.

The screenshot shows a terminal window titled "Local Terminal". The terminal output is identical to the previous one, but the final command and its response are highlighted in green:

```

Local Terminal
login as "user" or "root": root
root@ITC00E0C51C5087:~# ls /wfs/cherry/client-certs/
client-cert.pem client-key.pem user-cert.der user-key.pem
root@ITC00E0C51C5087:~# ls /wfs/cherry/ca-certs/
311625f3.0 570b05fc.0 d81e5d09.0 ece45aca.0 SecureboardRootCA.pem
46c284d6.0 clientca-cert.pem dce0a93b.0 p-20190712.pem
root@ITC00E0C51C5087:~# secureboard_personalize
Certificate check succeeded.

Found Cherry SECURE BOARD 1.0 @SECUREBOARD1.0-00000002JS040B1414CC0GDLI2.

Personalize SECURE BOARD 1.0 (y/n)? y

libsecureboard version 0.1.3.2
Updating User Private Key

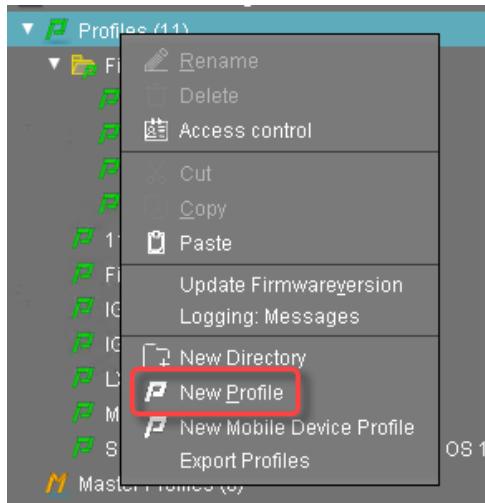
SECURE BOARD 1.0 successfully personalized.
  
```

### 5. Unplug the personalized Cherry SECURE BOARD and proceed with the next Cherry SECURE BOARD.

## Setting Up the Endpoints

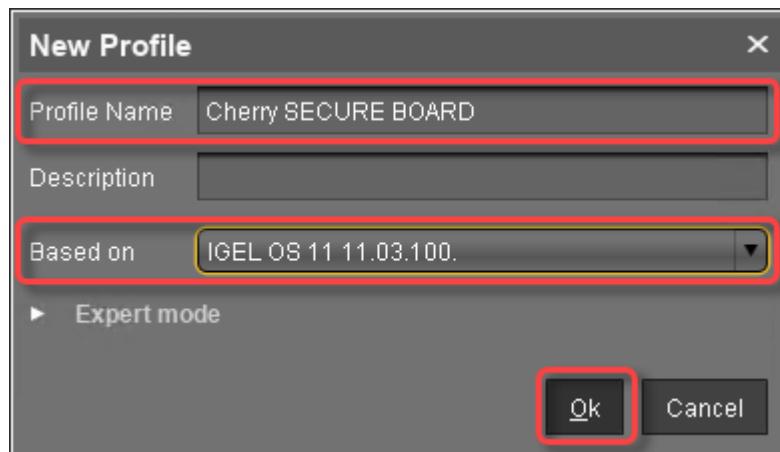
### Creating a Profile for the Endpoints

- In the UMS structure tree, open the context menu for **Profiles** and select **New Profile**.



2. In the **New Profile** dialog, enter the required data and click **Ok**:

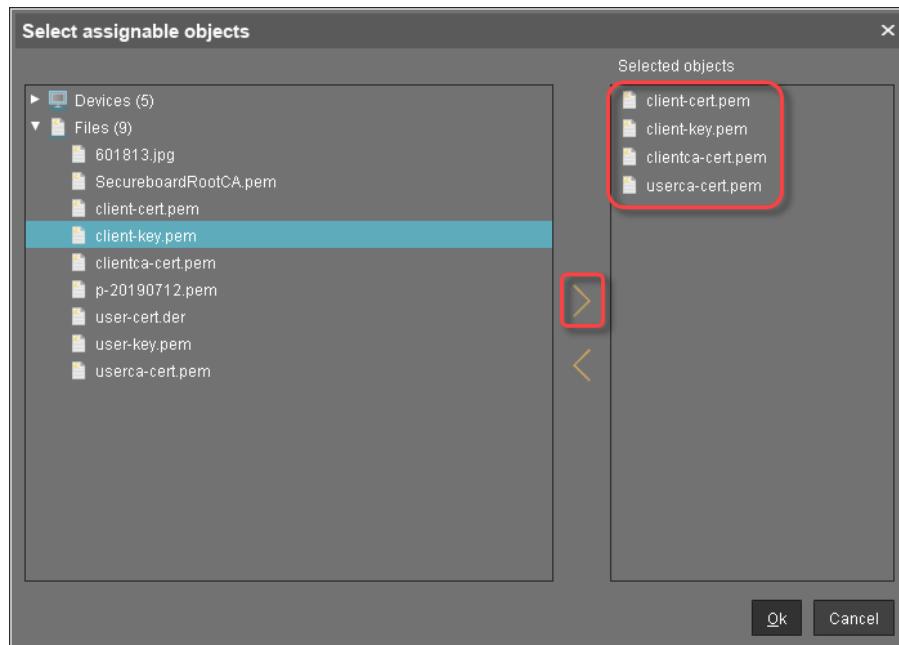
- **Profile Name:** Name for the profile
- **Based on:** Select the version of IGEL OS that is installed on your devices (IGEL OS 11.03.100 or higher).



3. In the configuration dialog of the profile, go to **System > Registry > devices > cherry\_secureboard > enable** and activate **Secure keyboard input with Cherry SECURE BOARD** (registry key: `devices.cherry_secureboard.enable`). (From UMS 6.03.130 or higher, the parameter can be found under **User Interface > Input > Keyboard**)



4. Click **Ok** to save and close the profile.
5. Make sure that the profile is selected in the UMS structure tree.
6. In the **Assigned objects** area, click
7. Under **Files**, select the file objects using the button:
  - User root CA certificate; here: **userca-cert.pem**
  - Client root CA certificate; here: **clientca-cert.pem** (optional)
  - Client certificate; here: **client-cert.pem**
  - Client key; here: **client-key.pem**

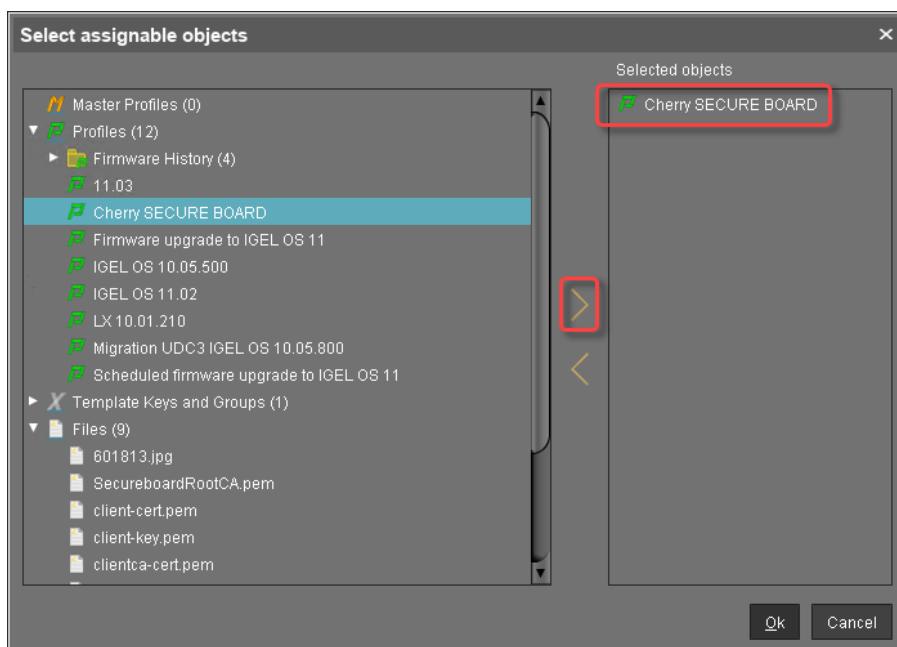




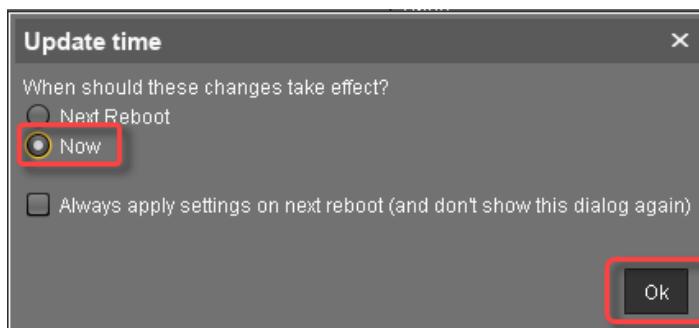
8. Click **Ok**.
9. In the **Update time** dialog, select **Now** and click **Ok**.  
The certificate and key files are assigned to the profile.

#### Assigning the Profile to the Endpoints

1. In the UMS structure tree, select the devices that are to be connected to the Cherry SECURE Board keyboards.
2. In the **Assigned objects** area, click .
3. Under **Profiles**, select the appropriate profile using the button.



4. Click **Ok**.
5. In the **Update time** dialog, select **Now** and click **Ok**.



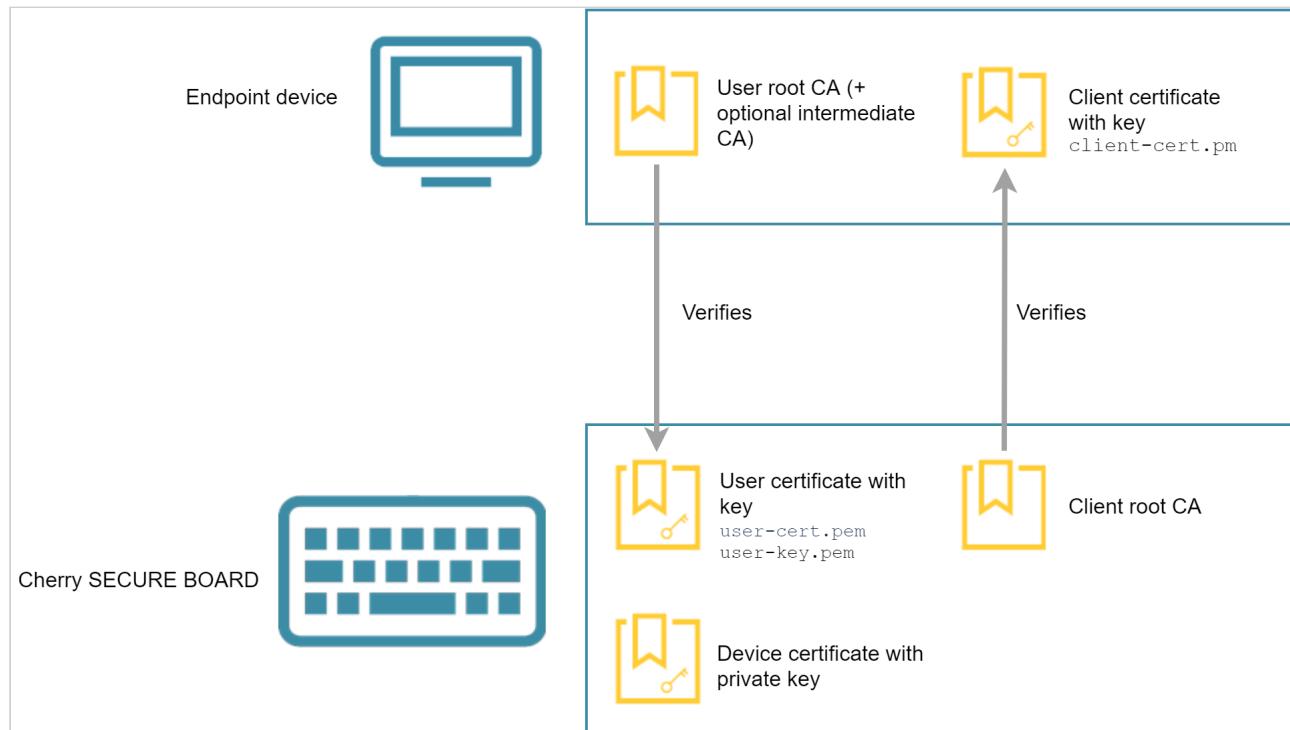


The settings and certificate and key files are transferred to the endpoints. The endpoints are ready for connecting to the Cherry SECURE BOARD keyboards.

## Operation

The endpoint verifies if the Cherry SECURE BOARD has the right certificates. When the optional client certificates have been installed, too, the Cherry SECURE BOARD verifies if the endpoint has the right certificates. When everything went well, the endpoint and the Cherry SECURE BOARD work in secure mode.

On the keyboard side, the secure mode is indicated by the red light next to the lock symbol. On the endpoint side, the secure mode is indicated by an icon on the system tray.



## Resetting the Cherry SECURE BOARD to Its Original State

To reset the Cherry SECURE BOARD to its factory settings:

1. Disconnect the keyboard from the endpoint.
2. Hold the keys [D], [J] and [RGUI] (right Windows key) and, at the same time, connect the keyboard to the endpoint.

When the reset has been successful, all LEDs flash for about 1 second. After that, the keyboard starts normally, and the certificate store is emptied. The keyboard can be personalized again.



### 2.23.3 Webcam Redirection and Optimization

#### Overview

This article provides an overview and best-practice recommendations for the use of webcams on IGEL OS within remote sessions such as Citrix, VMware Horizon, and RDP.

In general, webcam support on IGEL OS can be divided into three categories:

Unoptimized	<p>The raw data from the webcam is sent over the network via USB redirection. The raw data from the webcam is highly affected by network latency between the client and the server and takes up a lot of bandwidth, requires the correct drivers on the server-side, increases the server's CPU and RAM load.</p> <p>Example: <b>Native USB Redirection</b> for RDP sessions</p>
Optimization type 1	<p>In this case, the video and audio data is compressed on the client side. This optimization type makes the webcam stream far more efficient and reliable, although the data stream must still pass via the VDI server in addition to the cloud servers of the particular communication software (Teams, Zoom, etc.).</p> <p>Examples: <b>HDX RealTime Webcam redirection</b> for Citrix sessions, <b>Real Time Audio Video (RTAV)</b> for VMware Horizon sessions</p>
Optimization type 2	<p>In this case, the video and audio data is also compressed on the client side. However, unlike type 1, this optimization type offloads the data stream from the VDI server and sends it <i>directly</i> to Teams/Zoom/etc. in the cloud, i.e. "single-hop". This allows for the best performance and also removes the server load, but relies on the correct optimization pack being present on the client and is specific to each communication suite. It may also require a more complex network configuration because the endpoint has to be able to communicate directly with the communication cloud server and not only the VDI server.</p> <p>Examples: <b>Microsoft Teams optimization</b> and <b>Zoom Media plugin</b> for Citrix sessions</p>



In the case of optimization type 1 or type 2, it is important to ensure that the agent/component on the server side is installed and is compatible with the client-side version. For details on the latter, see the "Component Versions" section of the [IGEL OS release notes](#)(see page 1422).

## General Recommendations

For optimal performance of webcams on IGEL OS, the correct optimization pack has to be enabled for the specific application, e.g. **Microsoft Teams optimization**, **Zoom Media plugin**, **Cisco Webex Teams VDI**, etc. However, optimization packs are not available for all session types.

### USB Redirection

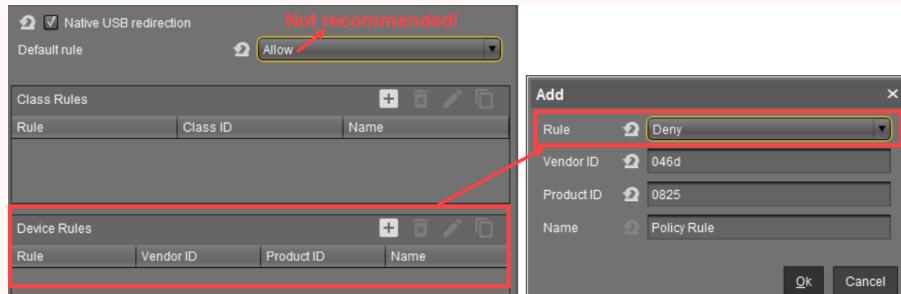
If no optimization pack exists for your session type or the optimization pack available does not function correctly, you can try to use USB redirection – either the **Native USB Redirection** or the less frequently used **Fabulotech USB Redirection** (not both together), – but ONLY as a LAST RESORT, when no other solution is possible.

In general, where USB redirection is available as an option inside the VDI session options, it should be disabled for the webcam devices.

- Set **Default rule** to **Deny**
- OR, if the **Default rule** is **Allow** (NOT recommended), go to **Device Rules** and add **Deny** rules for the specific Vendor ID and Product ID of the webcam.

### How to Find Out Vendor and Product IDs

To get Vendor/Product IDs, use the command `lsusb` in the terminal. You can also use the **System Information** tool, see [Using “System Information” Function](#)(see page 1108).



This is necessary because USB redirection will block the webcam from being correctly optimized (if optimization is possible).

Always check the [IGEL OS release notes](#)(see page 1422) for specific remarks, especially in the case of [private builds](#)<sup>209</sup>. Always try to use the latest firmware, see [IGEL download server](#)<sup>210</sup>.

<sup>209</sup> <https://kb.igel.com/display/licensesmoreigelos11/What+is+the+Meaning+of+IGEL+Release+Names>

<sup>210</sup> <https://www.igel.com/software-downloads/workspace-edition/>



In certain cases, some of the settings described later on in this article may not be visible even though you have selected the correct firmware version for the profile in the UMS. In this case, update the UMS to the latest version.

## Citrix

### Option 1: **Unified Communications** (Best Choice)

<b>Microsoft Teams Optimization</b>	<p>Path: <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; VDI Solutions &gt; Microsoft Teams optimization</b>(see page 795) (enabled by default)</p> <ul style="list-style-type: none"> <li>Available as of IGEL OS version 11.04.100.</li> <li>Depends on the version of Citrix Workspace App used. For best results, the latest version should be preferred. For the Citrix Workspace App versions included, see <a href="#">IGEL OS release notes</a>(see page 1422).</li> </ul> <p>For server-side requirements for Microsoft Teams optimization, see <a href="#">Microsoft Teams installation</a><sup>211</sup>.</p> <p>To troubleshoot Microsoft Teams optimization in Citrix, see:</p> <ul style="list-style-type: none"> <li><a href="#">Troubleshooting HDX Optimization for Microsoft Teams</a><sup>212</sup></li> <li><a href="#">Peripherals in Microsoft Teams</a><sup>213</sup></li> </ul>
<b>Zoom Media Plugin</b>	<p>Path: <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; VDI Solutions &gt; Zoom Media Plugin</b>(see page 795)</p> <ul style="list-style-type: none"> <li>Available as of IGEL OS version 11.04.100</li> <li>For the Zoom Media Plugin versions included, see <a href="#">IGEL OS release notes</a>(see page 1422).</li> </ul> <p>For more information about Zoom Media Plugin, including server-side requirements, see <a href="#">Getting started with VDI</a><sup>214</sup>.</p>

<sup>211</sup> <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/multimedia/opt-ms-teams.html#microsoft-teams-installation>

<sup>212</sup> <https://support.citrix.com/article/CTX253754>

<sup>213</sup> <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/multimedia/opt-ms-teams.html#peripherals-in-microsoft-teams>

<sup>214</sup> <https://support.zoom.us/hc/en-us/articles/360031096531-Getting-Started-with-VDI>



<b>Cisco Webex Meetings / Teams VDI</b>	<p>Path: <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; Cisco &gt; Cisco Webex Meetings VDI</b> or <b>Cisco Webex Teams VDI</b>(see page 796)</p> <ul style="list-style-type: none"> <li>• Available as of IGEL OS version 11.04.100</li> <li>• For the Cisco Webex Meetings / Teams VDI versions included, see <a href="#">IGEL OS release notes</a>(see page 1422).</li> </ul> <p>For more information about Cisco Webex products for VDI, including supported environments, see:</p> <ul style="list-style-type: none"> <li>• <a href="#">Cisco Webex Meetings Virtual Desktop Software</a><sup>215</sup></li> <li>• <a href="#">Overview of Webex Teams for VDI</a><sup>216</sup></li> </ul>
<b>Cisco JVDI Client</b>	<p>Path: <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; Cisco &gt; Cisco JVDI client</b>(see page 796)</p> <ul style="list-style-type: none"> <li>• For the Cisco JVDI client versions included, see <a href="#">IGEL OS release notes</a>(see page 1422).</li> </ul> <p>For more information about Cisco JVDI client, see <a href="#">Deployment and Installation Guide for Cisco Jabber Softphone for VDI</a><sup>217</sup>.</p>
<b>Skype for Business</b>	<p>Path: <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; Skype for Business &gt; HDX RealTime Media Engine</b>(see page 796) (enabled by default)</p> <ul style="list-style-type: none"> <li>• Skype for Business webcam redirection relies on the <b>Citrix HDX Realtime Media Engine</b> (client-side counterpart to the Lync Optimization Pack).</li> <li>• This setting is the same as <b>Sessions &gt; Citrix &gt; Citrix Global &gt; HDX Multimedia &gt; HDX RealTime Media Engine</b>.</li> </ul> <div style="border: 1px solid red; padding: 10px; margin-top: 20px;"> <p><b>IMPORTANT:</b> <a href="#">Skype for Business Online will be retired by Microsoft on July 31, 2021</a><sup>218</sup>. After this,</p> </div>

<sup>215</sup> <https://help.webex.com/en-us/nfjsqzbb/Cisco-Webex-Meetings-Virtual-Desktop-Software>

<sup>216</sup> [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/wbxt/vdi/wbx-teams-vdi-deployment-guide/wbx-teams-vdi-deployment-wbx-calling-EFT\\_chapter\\_00.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/vdi/wbx-teams-vdi-deployment-guide/wbx-teams-vdi-deployment-wbx-calling-EFT_chapter_00.html)

<sup>217</sup> [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/jvdi/12\\_9/dig/jvdi\\_b\\_deploy-install-jvdi-12-9/jvdi\\_b\\_deploy-install-jvdi-12-9\\_chapter\\_01.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jvdi/12_9/dig/jvdi_b_deploy-install-jvdi-12-9/jvdi_b_deploy-install-jvdi-12-9_chapter_01.html)

<sup>218</sup> <https://techcommunity.microsoft.com/t5/microsoft-teams-blog/skype-for-business-online-to-be-retired-in-2021/ba-p/777833>



it will no longer be available, and Microsoft Teams must be used instead.

## Option 2: HDX RealTime Webcam Redirection (Should Only Be Used If Optimization Packs under Option 1 Are Not Applicable)

For other VDI programs which require the use of a webcam (e.g. the browser), [HDX RealTime Webcam redirection](#)(see page 792) can be used. This option enables the compression of audio and video on the client side, which is redirected to an HDX virtual webcam on the server side. It also allows for the resolution of the webcam to be defined manually.

### Only One Option at a Time for a Particular Device

- **HDX RealTime Webcam redirection** and **HDX RealTime Media Engine** should not be enabled at the same time.
- If you use HDX or an application-specific optimization pack (e.g. **Zoom Media plugin**), **Native USB Redirection / Fabulotech USB Redirection** should be disabled.

### Settings on the Server Side

The following policy settings must be enabled:

- Multimedia conferencing (enabled by default)
- Windows Media Redirection (enabled by default)

For details, see <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/multimedia/webcam-compression.html>.

### Settings on the Client Side

1. Go to **Sessions > Citrix > Citrix Global > HDX Multimedia**.
2. Enable **Multimedia redirection** (enabled by default).
3. Enable **HDX RealTime Webcam redirection**.
4. Configure the webcam resolution, 352 x 288 by default, and other settings if required.

Certain webcam models may only support specific resolutions. For more information, see [How to Configure Webcam settings When Webcams are Not Redirected Through HDX Real-Time](#)<sup>219</sup>.

5. If the USB redirection is enabled (not recommended), use **Device Rules** to forbid the forwarding of the webcam via USB redirection. See [the section above](#)(see page 664).

### Dependencies

- **HDX RealTime Webcam Redirection** is only supported for 32-bit applications on the server side (limitation of Citrix Receiver/Workspace App for Linux). Deploy a 32-bit browser to verify the



webcam redirection online, e.g. [www.webcamtests.com](http://www.webcamtests.com)<sup>220</sup>. See also <https://support.citrix.com/article/CTX223199>.

- Webcam redirection generally works with or without **HDX RealTime Media Engine (RTME)**. However, to avoid conflicts and for the better performance of webcam redirection, disabling **RTME** (enabled by default) is highly recommended.
- Webcam usage is limited to one application. For instance, when Skype is running with a webcam and GoToMeeting is started, you have to exit Skype to use the webcam with GoToMeeting.

### Supported Video Conferencing Applications

- Adobe Connect
- Cisco Webex and Webex for Teams (Give preference to the optimization pack for Cisco Webex Meetings / Teams VDI instead, [see above\(see page 665\)](#))
- GoToMeeting
- Google Hangouts and Hangouts Meet
- IBM Sametime
- Microsoft Skype for Business 2015, 2016, and 2019 (Give preference to the optimization pack for Skype for Business instead, [see above\(see page 665\)](#))
- Microsoft Lync 2010 and 2013
- Microsoft Skype 7 or higher
- Media Foundation-based video applications on Windows 8.x or higher and Windows Server 2012 R2 and higher

**HDX RealTime Webcam Redirection** is NOT supported for Microsoft Teams. Use **Microsoft Teams optimization** instead, [see above\(see page 665\)](#).

### Does Webcam Audio Work but Video Doesn't?

- ▶ Try to increase the graphics memory in the BIOS to 512 MB.

For more detailed information about HDX RealTime Webcam, see:

- <https://support.citrix.com/article/CTX132764>
- <https://docs.citrix.com/en-us/citrix-workspace-app-for-linux/configure-xenapp.html#webcams>

<sup>220</sup> <http://www.webcamtests.com>



## VMware Horizon

### Option 1 (Best Choice)

<b>Zoom Media Plugin</b>	<p>Path: <b>System &gt; Registry &gt; vmware &gt; view &gt; vdzoom &gt; enable</b></p> <ul style="list-style-type: none"> <li>• Available as of IGEL OS version 11.04.200</li> <li>• For the Zoom Media Plugin versions included, see <a href="#">IGEL OS release notes</a>(see page 1422).</li> </ul>
	<div style="border: 1px solid #f0e68c; padding: 10px;"> <p>Zoom Media Plugin will NOT function if you enable <b>HTML5 multimedia redirection</b> (<b>System &gt; Registry &gt; vmware &gt; view &gt; html5mmr</b>, disabled by default).</p> </div>
	<p>For more information about Zoom Media Plugin, including server-side requirements, see <a href="#">Getting started with VDI</a><sup>221</sup>.</p>
<b>Cisco Webex Teams VDI</b>	<p>Path: <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Unified Communications &gt; Cisco &gt; Cisco Webex Teams VDI</b>(see page 859)</p>
	<ul style="list-style-type: none"> <li>• Available as of IGEL OS version 11.04.100</li> <li>• For the Cisco Webex Teams VDI versions included, see <a href="#">IGEL OS release notes</a>(see page 1422).</li> </ul>
	<p>For more information, see <a href="#">Overview of Webex Teams for VDI</a><sup>222</sup>.</p>

<sup>221</sup> <https://support.zoom.us/hc/en-us/articles/360031096531-Getting-Started-with-VDI>

<sup>222</sup> [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/wbxt/vdi/wbx-teams-vdi-deployment-guide/wbx-teams-vdi-deployment-wbx-calling-EFT\\_chapter\\_00.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/vdi/wbx-teams-vdi-deployment-guide/wbx-teams-vdi-deployment-wbx-calling-EFT_chapter_00.html)



<b>Cisco JVDI Client</b>	<p>Path: <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Unified Communications &gt; Cisco &gt; Cisco JVDI client</b>(see page 859)</p> <ul style="list-style-type: none"> <li>For the Cisco JVDI client versions included, see <a href="#">IGEL OS release notes</a>(see page 1422).</li> </ul> <p>For more information about Cisco JVDI client, see <a href="#">Deployment and Installation Guide for Cisco Jabber Softphone for VDI</a><sup>223</sup>.</p>
<b>Skype for Business</b>	<p>Path: <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Unified Communications &gt; Skype for Business &gt; Virtualization Pack Skype for Business</b>(see page 859) (enabled by default)</p> <div style="border: 1px solid red; padding: 10px;"> <p><b>IMPORTANT:</b> <a href="#">Skype for Business Online will be retired by Microsoft on July 31, 2021</a><sup>224</sup>. After this, it will no longer be available, and Microsoft Teams must be used instead.</p> </div>

#### Option 2: Real-Time Audio-Video (RTAV)

Real-time Audio-Video (RTAV) is the optimization pack for audio and video calls inside VMware Horizon sessions. RTAV compresses audio and video on the client side and sends it to the Horizon server, where a VMware Virtual Webcam instance is created.

Like for Citrix sessions, USB redirection should be disabled if RTAV is to be used.

► Enable **Sessions > Horizon Client > Horizon Client Global > Multimedia > Real Time Audio Video (RTAV)**(see page 856).

RTAV is only available when connecting via PCoIP or VMware Blast.

Note that only one webcam will be redirected (limitation of Horizon client for Linux). If multiple webcams are available on the client, the preferred webcam can be defined in the IGEL Setup under **System >**

<sup>22</sup> [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/jvdi/12\\_9/dig/jvdi\\_b\\_deploy-install-jvdi-12-9/jvdi\\_b\\_deploy-install-jvdi-12-9\\_chapter\\_01.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jvdi/12_9/dig/jvdi_b_deploy-install-jvdi-12-9/jvdi_b_deploy-install-jvdi-12-9_chapter_01.html)

<sup>224</sup> <https://techcommunity.microsoft.com/t5/microsoft-teams-blog/skype-for-business-online-to-be-retired-in-2021/ba-p/777833>



**Registry > vmware.view.rtav-webcam-id.** For details, see [Select a Preferred Webcam or Microphone on a Linux Client System](#)<sup>225</sup>.

For more information about RTAV, see [Configuring Real-Time Audio-Video](#)<sup>226</sup>.

### Microsoft Teams

Microsoft Teams can be used with RTAV in "Fallback Mode". This configuration is not an optimal solution as the data makes multiple hops between the Horizon client, server, and Microsoft Teams server. For more information, see [Configuring Microsoft Teams with Real-Time Audio-Video](#)<sup>227</sup>.

Microsoft Teams media optimization (single-hop or "Optimized Mode") in Horizon sessions is currently only supported with the Horizon client for Windows 10 in conjunction with Horizon 8 (2006). For more information, see [Microsoft Teams Optimization with VMware Horizon](#)<sup>228</sup>.

## RDP

There is currently no optimization available for webcam redirection in RDP sessions. It may be possible to redirect webcams via USB redirection, e.g. **Native USB Redirection**. However, each webcam has to be individually tested for if it functions with this method. It often depends on the webcam itself and its Windows driver whether they can cope with the higher latencies that occur with USB redirections compared to the real USB bus.

In some situations, webcams may not be redirected correctly due to network latency, bandwidth limitations, or the lack of compatible drivers on the server.

### Unoptimized Webcam Support

- Note that because USB redirection is not designed for redirecting video devices, the bandwidth usage and server CPU load may increase significantly.
- For this reason, it is recommended to use webcams that output directly H.264 or H.265 streams, and not MJPEG, in order to reduce the data volume.

## Native USB Redirection

1. Enable **Sessions > RDP > RDP Global > Native USB Redirection > Enable native USB redirection**.
2. Set the **Default rule** to **Deny**.
3. Under **Device Rules**, add the specific **Vendor ID** and **Product ID** of the device to be redirected.

<sup>225</sup><https://docs.vmware.com/en/VMware-Horizon-7/7.9/horizon-remote-desktop-features/GUID-C8C17975-AA1E-4378-A305-00E02FF93201.html>

<sup>226</sup><https://docs.vmware.com/en/VMware-Horizon-7/7.6/horizon-remote-desktop-features/GUID-D6FD6AD1-D326-4387-A6F0-152C7D844AA0.html>

<sup>227</sup><https://docs.vmware.com/en/VMware-Horizon/2006/horizon-remote-desktop-features/GUID-E64B3E85-BA1E-4FB7-9DB4-FF9B7B7A892C.html>

<sup>228</sup><https://techzone.vmware.com/resource/microsoft-teams-optimization-vmware-horizon>



To find out the **Vendor ID** and **Product ID** of the connected USB device, use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal. You can also use the **System Information** tool, see [Using “System Information” Function](#)(see page 1108).

On RDS servers, the following may be helpful:

- ▶ Disable the setting **Do not allow supported Plug and Play device redirection** under **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection**.

#### For Microphone (e.g. Headset)

- ▶ Enable **Sessions > RDP > RDP Global > Mapping > Audio > Audio recording**.

#### Custom Partition as a Local Alternative

You can also use [Custom Partitions](#)(see page 529) for Microsoft Teams or Zoom, e.g. in order to save backend resources, which may be a good choice in slow RDP backends. The Custom Partition is locally installed but is easy to access in the remote session.

- For details, see [Microsoft Teams as a Custom Partition](#)(see page 573), [Zoom as a Custom Partition](#)(see page 558).
- Contact the IGEL Support Team to get support for the deployment of Custom Partitions.

For how to open up the webcam in Windows 10, see [Open the Camera in Windows 10](#)<sup>229</sup>.

For a video overview on using webcams and other USB devices in remote sessions, see:  
**English**



Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:

<https://www.youtube.com/watch?v=PYCU1AEfS-g&feature=youtu.be>

#### German

---

<sup>229</sup> <https://support.microsoft.com/en-us/windows/open-the-camera-in-windows-10-8da044ed-c4a8-2fb4-da51-232362e4126d#:~:text>To%20open%20up%20your%20webcam,Let%20apps%20use%20my%20camera.>



Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:  
<https://www.youtube.com/watch?v=caNhFib5cuA&feature=youtu.be>

## 2.23.4 Webcam Information

If you are running a device with *IGEL Linux* version 5.3.100 or higher, you can configure and test a webcam using a built-in tool. This tool is called **Webcam Information**.

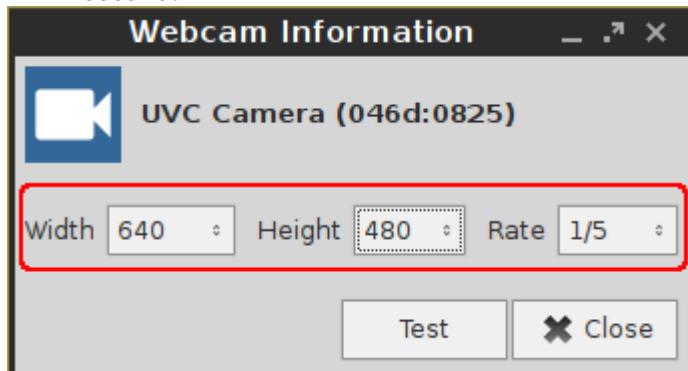
- ▶ To configure a starter for **Webcam Information**, open the IGEL Setup and go to **Accessories > Webcam Information**.

To determine and change the width, height, and frame rate of your webcam:

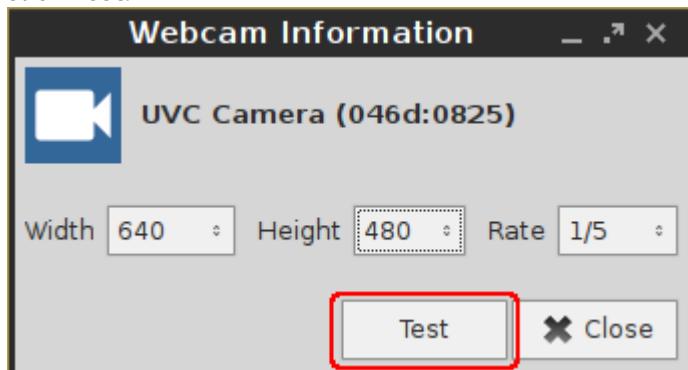
1. Start the **Webcam Information** tool.

The following values are shown:

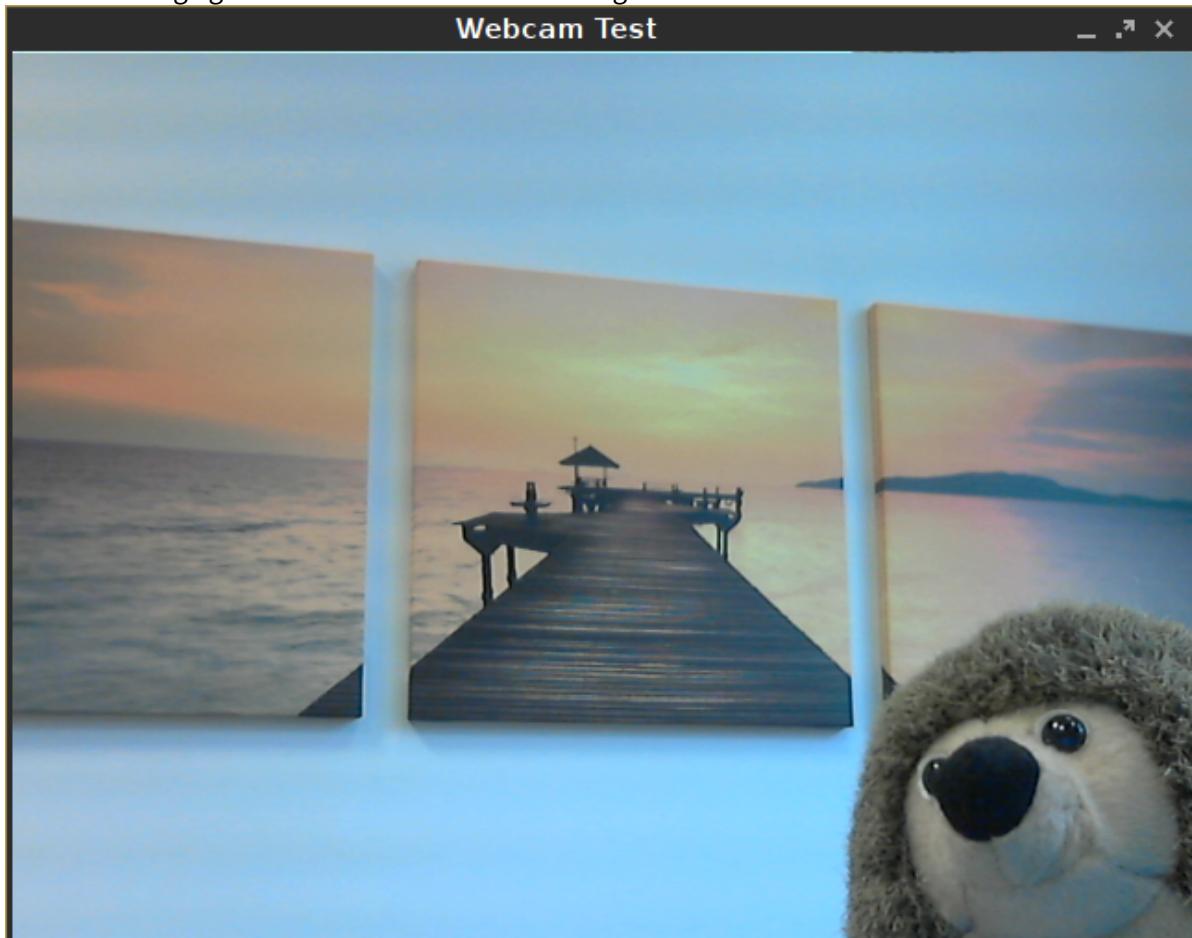
- **Width:** Width of the image in pixels
- **Height:** Height of the image in pixels
- **Rate:** Frame rate in fps (frames per second). Example: **1/30** means 30 single images per second.



2. Click on one of the fields to change the value. In doing so, the supported values are shown.
3. Click **Test**.



The video image generated with the current settings is shown.



To check if the webcam is working in a session (e.g. via Citrix HDX webcam redirection), open a browser in the session and go to <https://www.onlinemictest.com/webcam-test/>.

### 2.23.5 Bluetooth Tool

You can connect or disconnect Bluetooth devices conveniently using the Bluetooth tool. The Bluetooth tool supports the following pairing methods:

- **Automatic PIN selection:** Pairing with automatic PIN allocation
- **0000, 1111, 1234:** Pairing with a fixed PIN (for most headsets, mice, or GPS devices)
- **Custom PIN:** Pairing with a fixed PIN entered by the user.

For further information, refer to the manual chapters [Using Bluetooth Tool](#)(see page 1102) and [Bluetooth Tool](#)(see page 1100).

In the following example, we will connect a Bluetooth keyboard with **Automatic PIN selection**:

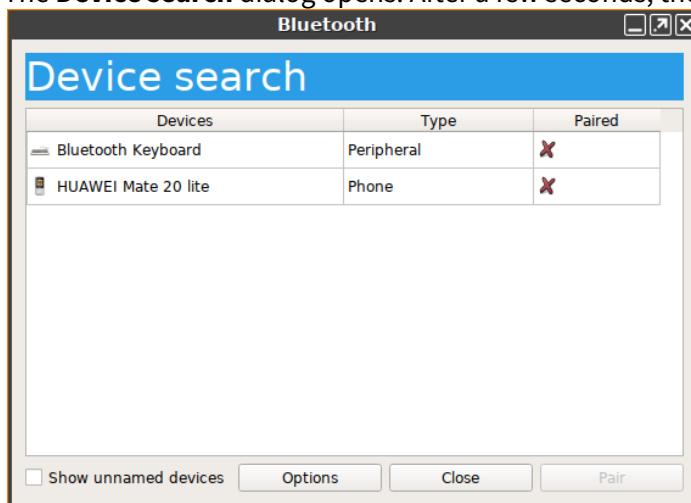
1. Make sure that the following preconditions are met:
  - The options **Devices > Bluetooth > Bluetooth** and **Tray Icon** are enabled in the IGEL Setup.
  - The Bluetooth device is ready.



If your endpoint device (e.g. UD2 D220) does not support Bluetooth, it is necessary to connect a Bluetooth USB adapter to it.

2. Launch the **Bluetooth Tool** from the IGEL menu  via **System > Bluetooth Tool** or another launch option, if available.

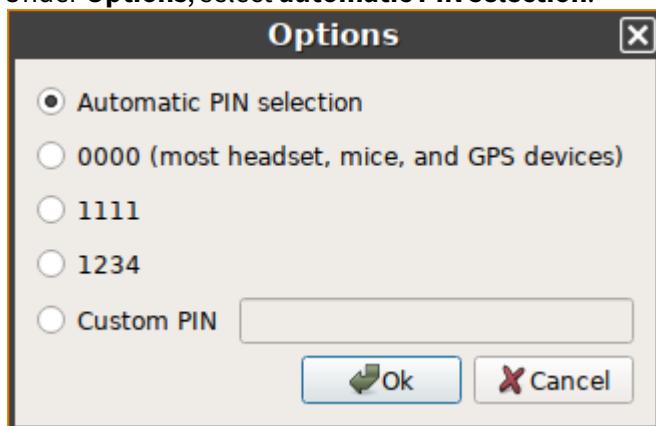
The **Device search** dialog opens. After a few seconds, the Bluetooth devices found are displayed.



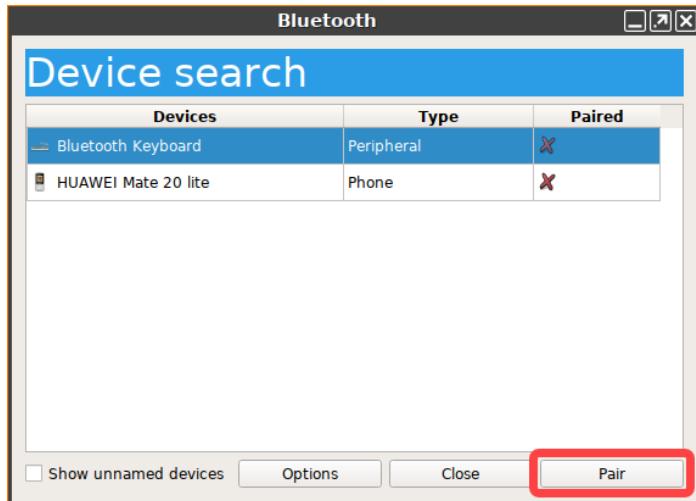
#### Tip

If no devices are found, turn the Bluetooth device off and on again or press the Bluetooth pairing button, in our case **Connect** on the back side of the keyboard.

3. Highlight the desired Bluetooth device.
4. Under **Options**, select **automatic PIN selection**.



5. Click on **Pair**.



A PIN to be entered will be shown.



**Tip**

If no PIN is displayed, click the **Pair** button again.

6. Enter the PIN into your Bluetooth device.

If everything went well, the status of the connection will be shown.



7. Close the dialog.



Your Bluetooth device is ready for use. By right-clicking the icon in the system tray, you can start the Bluetooth tool again, e.g. to pair another Bluetooth device or to unpair a device.

### 2.23.6 How to Deploy a Jabra Xpress Package

Jabra Xpress is a solution for the remote mass-deployment of Jabra USB headsets that enables creating and deploying packages containing settings, firmware updates, etc. for Jabra devices. For more information, see <https://www.jabra.com/supportpages/jabra-xpress#/>.

Deployment of a Jabra Xpress package involves the following steps:

1. Making the package available for download over the FTP(S) or HTTP(S) protocol(see page 677)
2. Configuring the source URL in the IGEL Setup(see page 678)
3. Triggering the deployment process in the UMS(see page 679)

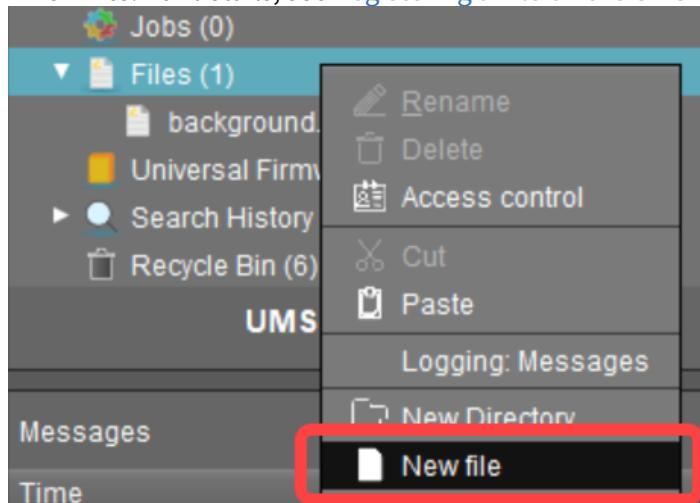
#### Making the Jabra Xpress Package Available for Download

1. Create a package on the Jabra Xpress portal and download it.
2. Place the ZIP archive onto your FTP(S) or HTTP(S) server.

If you want to use the UMS as a source location, register the ZIP archive in the UMS under **Files**



> New file. For details, see Registering a File on the UMS Server<sup>230</sup>.



## Configuring the Source URL

Now you have to configure the download location:

1. In the IGEL Setup or in the configuration dialog in the UMS, go to **Devices > Unified Communications > Jabra > Jabra Xpress**.
2. Under **Device Dashboard URL**, you can optionally specify the URL of the dashboard server of the Jabra device.
3. Under **Package**, enter the file name of the Jabra Xpress package.  
Example: `xpress_package_20190109_144111.zip`.
4. Under **Source URL**, specify the URL to the directory containing the Xpress package.  
Example: `https://172.30.92.5:8443/ums_filetransfer/` if you use the UMS as the source location.
5. Disable **Check SSL certificate** if your HTTPS or FTPS server uses a self-signed certificate.
6. Under **User name**, specify the user name for accessing the Xpress package that resides under the **Source URL**.

---

<sup>230</sup> <https://kb.igel.com/display/endpointmgmt606/Registering+a+file+on+the+UMS+server>



7. Under **Password**, specify the password for accessing the Xpress package that resides under the **Source URL**.

The screenshot shows the UMS (Unified Management System) configuration interface. The left sidebar navigation tree is expanded to show the path: Devices > Unified Communications > Jabra > Jabra Xpress. The main configuration panel is titled 'Jabra Xpress' and contains the following fields:

Setting	Value
Device Dashboard URL	(empty)
Xpress Package	
Package	xpress_package_20190109_144111.zip
Source URL	https://172.30.92.5:8443/ums_filetransfer/
<input checked="" type="checkbox"/> Check SSL certificate	(unchecked)
User name	techdoc_user
Password	***** (redacted)

At the bottom of the configuration panel are three buttons: 'Apply and send to device', 'Save', and 'Cancel'. A red box highlights the 'Source URL', 'User name', and 'Password' fields.

8. Save the settings.

## Triggering the Deployment Process

Finally, you have to trigger the deployment process. There are two possibilities:

- In the UMS, go to **Devices** > [context menu of the device] > **Specific Device Command** and select **Deploy Jabra Xpress Package**.



The screenshot shows the UMS interface with a device named 'techdoc\_RD1' selected. A context menu is open, and the 'Specific Device Command' option is highlighted with a red box. A secondary window titled 'Specific Device Command' is displayed, showing a list of commands. The 'Deploy Jabra Xpress package' option is selected and highlighted with a red box. The 'Execute' button at the bottom of this window is also highlighted with a red box.

OR

- In the UMS, go to **Jobs > New Scheduled Job** and select **Deploy Jabra Xpress package** as **Command**. Assign the job to the necessary devices, see [Assignment](#)<sup>231</sup>.

The screenshot shows the UMS interface with the 'New Scheduled Job' dialog open. In the 'Details' tab, the 'Command' dropdown is set to 'Deploy Jabra Xpress package', which is highlighted with a red box. The 'New Scheduled Job' button in the left sidebar is also highlighted with a red box.

<sup>231</sup> <https://kb.igel.com/display/endpointmgmt606/Assignment>



Note that it is not possible to reverse the deployment process, e.g. to remove an Xpress package from the Jabra device. If you require the previous settings, you have to configure and deploy a new Jabra Xpress package with the old headset firmware and configuration.

See also [Jabra Xpress\(see page 1233\)](#) in the IGEL OS reference manual.

### 2.23.7 Connecting Signature Pads

You can connect signature pads from the following manufacturers:

- StepOver;
- signotec.

- ▶ To enable them, go to Setup > **User Interface > Input > Signature Pad**.
- ▶ To configure a serial connection in order to be able to use USB signature pads from these manufacturers, proceed as follows:
  1. Enable **COM port mapping** under:
    - Setup > **Sessions > Citrix > Citrix Global > Mapping > COM Ports** for Citrix sessions;
    - Setup > **Sessions > RDP > RDP Global > Mapping > COM Ports** for RDP sessions.
  2. Click on **Add**
  3. Click **Detect Devices....**
  4. Select your device.  
Your signature pad can now be used.

### 2.23.8 Using a Kofax / Wacom Signature Pad

You can use a Kofax / Wacom signature pad in Citrix sessions using the Kofax SPVC signature pad channel. The Virtual Serial Sign Pad method is no longer supported.

#### On the Device

1. Connect the signature pad to one of the device's USB ports.
2. Go to **Sessions > Citrix > Citrix Global > Mapping > Device Support**.



### 3. Enable Kofax SPVC signature pad channel.

The screenshot shows the 'Configuration' menu on the left with the following tree structure:

- Sessions
- Citrix
- Citrix Client Selection
- ▼ Citrix Global
  - StoreFront Login
  - Window
  - Keyboard
  - ▼ Mapping
    - Drive Mapping
    - COM Ports
    - Printer
    - Device Support**
  - Firewall
  - Options
  - Native USB Redirection

To the right of the tree view is a list of available channels, each preceded by a checkbox. The 'Kofax SPVC signature pad channel' checkbox is checked. Below this list are two dropdown menus labeled 'P' and 'S'.

#### On the VDI Server (Windows)

- ▶ Install the required software from Kofax / Wacom.  
The driver contained in this software will listen for signature pads on a virtual channel. Applications such as SignDoc will be able to use the signature pad.

#### 2.23.9 Using a StepOver Signature Pad

You can use a StepOver signature pad in Citrix and RDP sessions. There are two different means to achieve this:

- [With StepOver TCP Client](#)(see page 682)
- [With StepOver Signature Pad Channel](#)(see page 685)

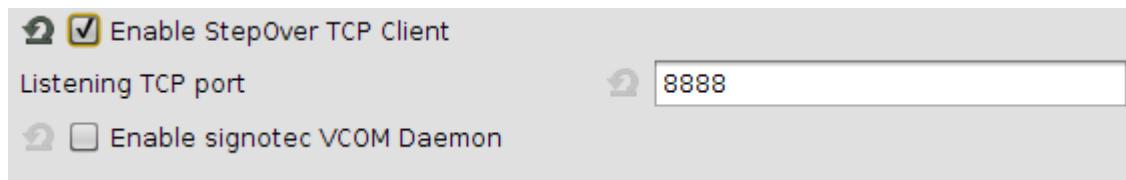
Only one of the methods can be used at a given time. Which of the two you need is determined by your applications on the server side.

See also [StepOver Signature Pads Compatibility](#)(see page 63).

#### With StepOver TCP Client

##### On the Device

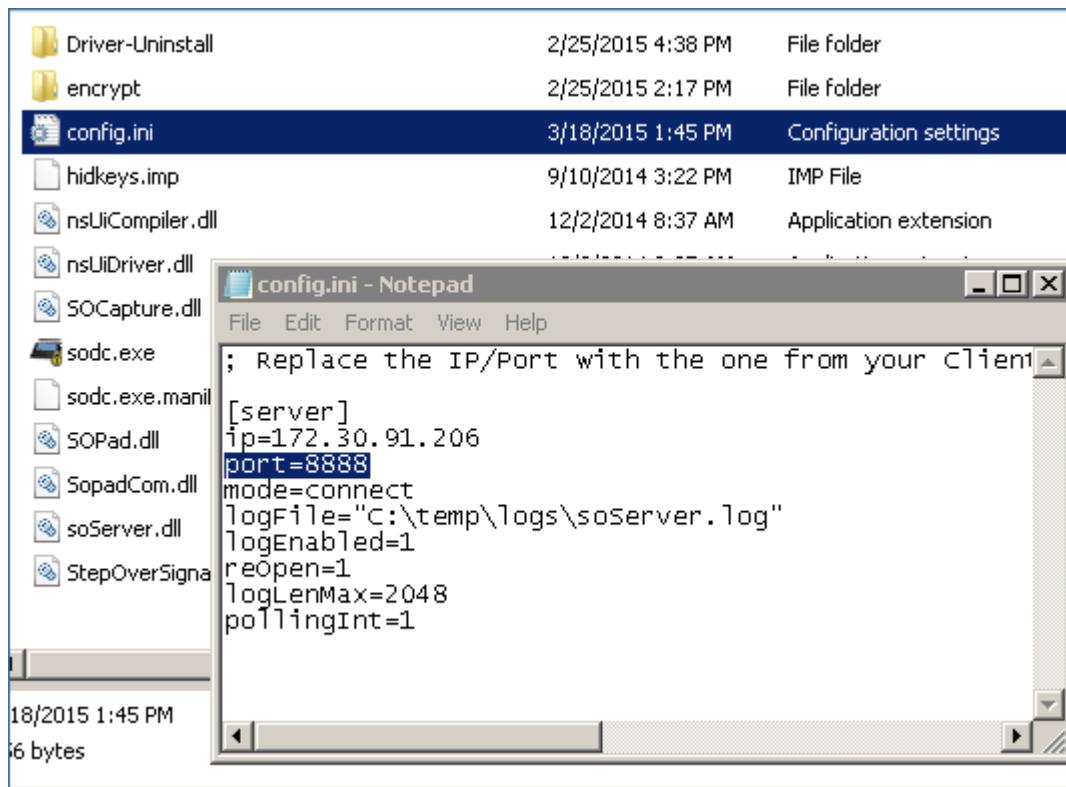
- ▶ Connect the signature pad to one of the device's USB ports.
- ▶ Go to **User Interface > Input > Signature Pad** in IGEL Setup.
- ▶ Enable **StepOver TCP Client**.
- ▶ Modify **Listening TCP Port** if needed. (Default: 8888)



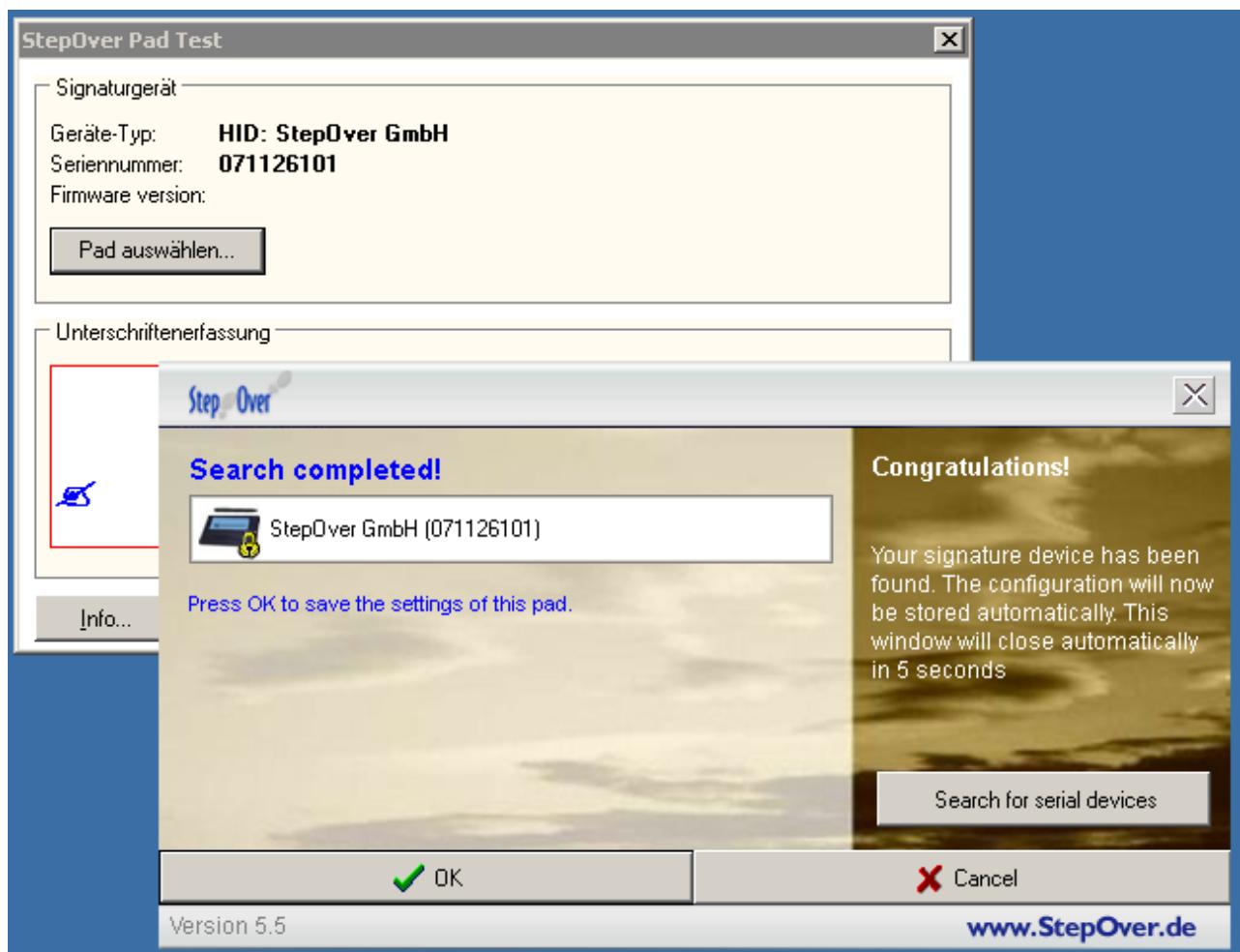
You can check whether the **StepOver TCP Client** is running on the device by entering the following in a local terminal: `ps waux | grep sotcp`. The result should contain an `sotcp` process.

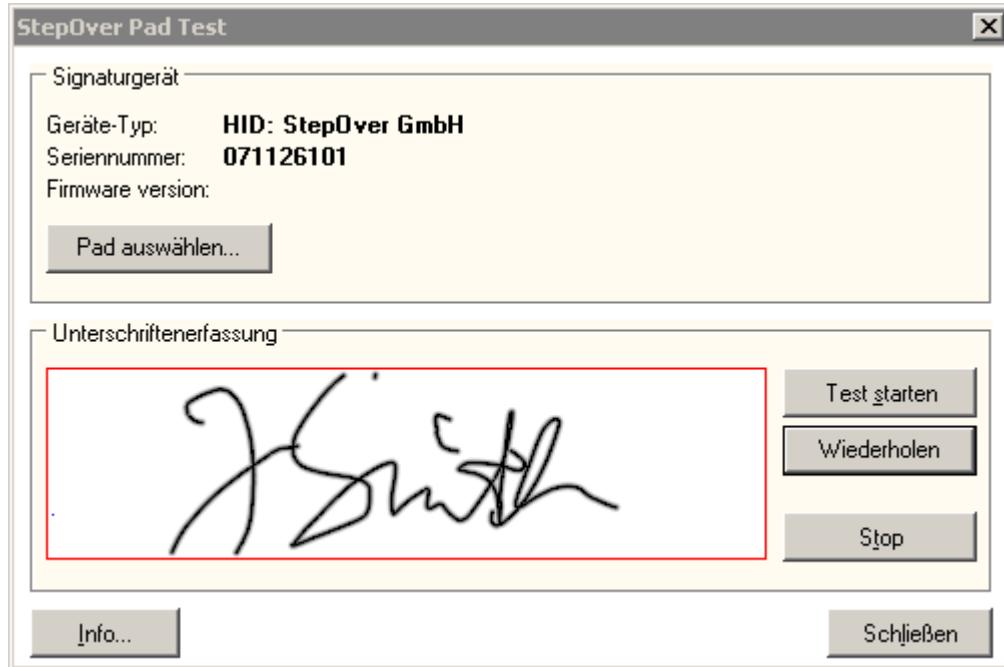
#### On the VDI Server (Windows)

- ▶ Locate the `sodc.exe` program on the server. It is the part of StepOver eSignature Office and can be found in `[Your Program Files Directory]\StepOver\esignatureOffice [version]\driver\`.
- ▶ If you are using a non-standard TCP port, change it in the `config.ini` file located in the same directory.



- ▶ Execute `sodc.exe`. The **StepOver Pad Test** window will open. Use its buttons to search and select your signature pad and try writing into the provided field.





The status LED of the pad will turn to green when the connection is successful. The signature pad is now ready to be used with enabled applications such as StepOver eSignature Office.

### With StepOver Signature Pad Channel

**StepOver signature pad channel** is applicable to Citrix sessions only. It activates StepOver Citrix Client and enables the redirection via Citrix virtual channel.

#### On the Device

- ▶ In the IGEL Setup, go to **Sessions > Citrix > Citrix Global > Mapping > Device Support**.
- ▶ Enable **StepOver signature pad channel** and save the changes.

#### On the Server

- ▶ During the installation of the StepOver software, select the option "Citrix".

### 2.23.10 eGK/KVK - Card Reader

The IGEL Linux thin clients support the reading of German electronic health cards (eGK), health insurance cards (KVK) and the German card for allied health professions (HBA) by a variety of readers connected via RDP or ICA. Configuration and functionality vary according to the reader type.

The following tested solutions are available:



Reader	Port	Client/server connection
Cherry G80-1502	Serial	COM port mapping
Cherry ST-2052	USB	Smartcard mapping
Cherry ST-1503 and Cherry G87-1504	USB	Cherry Virtual Channel (IGEL Linux v5 only)
SICCT via LAN provided by the Cherry USB2LAN proxy (IGEL Linux version 5.12.100 and IGEL Linux version 10.03.100 onwards)		
ORGA 910/920 M	USB	COM port mapping
ORGA 6041 L eGK eHealth-BCS	USB	COM port mapping
SCM Microsystems eHealth200	USB	Smartcard mapping
SCM Microsystems eHealth500	USB	COM port mapping
celectronic CARD STAR /medic2	Serial	COM port mapping
celectronic CARD STAR /memo3	USB	COM port mapping

- [Cherry G80-1502 at the Serial Port](#)(see page 686)
- [Cherry ST-2052](#)(see page 687)
- [Cherry ST-1503 und G87-1504 \(USB\)](#)(see page 688)
- [Orga 910/920 M](#)(see page 689)
- [Orga 6041 L eGK eHealth-BC S](#)(see page 690)
- [celectronic CARD STAR / medic2](#)(see page 691)
- [celectronic CARD STAR/ memo3](#)(see page 692)

## Cherry G80-1502 at the Serial Port

### Connecting the keyboard

- Connect the keyboard to both the PS/2 port and the serial port of the thin client.

Firmware version 1.19 of the keyboard must be present and the keyboard must be in mode S1. Refer to [http://www.cherry.de/files/manual/Cherry\\_G80-1502\\_mit\\_eGK.pdf](http://www.cherry.de/files/manual/Cherry_G80-1502_mit_eGK.pdf).



Functionality	
Software:	Cherry eHealth eGK/KVK software
Device/server connection:	COM port mapping

#### Configuring the device

In IGEL Setup, add the COM port device to which the keyboard is connected:

1. Click **Sessions > RDP > RDP Global > Mapping > COM Ports**
2. Click
3. Select a **COM port device** (COM1, COM2,... ).

#### Configuring the server

1. Install the eGK-KVK software by *Cherry*.  
See also [http://www.cherry.de/files/manual/eHealth\\_Client-Server\\_Einbindung.pdf](http://www.cherry.de/files/manual/eHealth_Client-Server_Einbindung.pdf)
2. Start the program CT-API configuration.
3. Select the appropriate port number for the G80-1502.

#### Cherry ST-2052

Functionality	
USB ID:	046a:003e
Software:	Cherry eHealth eGK/KVK software
Device/server connection:	Smartcard (PC/SC) mapping

#### Configuring the device

- Select **Activate PC/SC Daemon** in Setup under **Security > Smartcard > Services**:



The screenshot shows the 'Configuration' screen of the IGEL OS software. On the left, there is a navigation tree with sections like 'Configuration', 'Accessories', 'User Interface', 'Network', 'Devices', and 'Security'. Under 'Configuration', several client types are listed: NoMachine NX Client, X Sessions, Parallels Client, PowerTerm WebConnector, PowerTerm Terminal Emulator, IBM iSeriesAccess, IBM iAccess Client, ThinLinc, SSH, VNC Viewer, VERDE Sessions, Browser, Media Player, JWS Sessions, and VoIP Client. The 'Services' item under 'Configuration' is currently selected. On the right, there are configuration options for 'Activate PC/SC Daemon' (checked), 'Currently active PC/SC devices' (listing 'OMNIKEY CardMan 3x21 00 00'), a 'Refresh device list' button, 'Cherry USB2LAN Proxy' (checked), 'Network Interface' (set to 'auto'), and a 'Services' dropdown menu.

### Configuring the server

1. Install the eGK-KVK software by *Cherry*.  
See also [http://www.cherry.de/files/manual/eHealth\\_Client-Server\\_Einbindung.pdf](http://www.cherry.de/files/manual/eHealth_Client-Server_Einbindung.pdf)
2. Start the program *CT-API configuration*.
3. Select port number 1 for the ST-2052.

### Cherry ST-1503 und G87-1504 (USB)

Functionality	
USB ID:	046a:0080 for ST-1503 046a:0081 for G87-1504
Software:	Cherry eHealth eGK/KVK software
Client/server connection:	SICCT via LAN provided by the Cherry USB2LAN proxy

Cherry USB2LAN proxy: Makes Cherry electronic health card devices available in the network via SICCT. The communication between card reader and server takes place independently of the VDI connections.



## Configuring the Thin Client for Using the Cherry USB2LAN Proxy

1. Activate **Security > Smartcard > Services > Cherry USB2LAN Proxy:**



## Configuring the Server for the Cherry USB2LAN Proxy

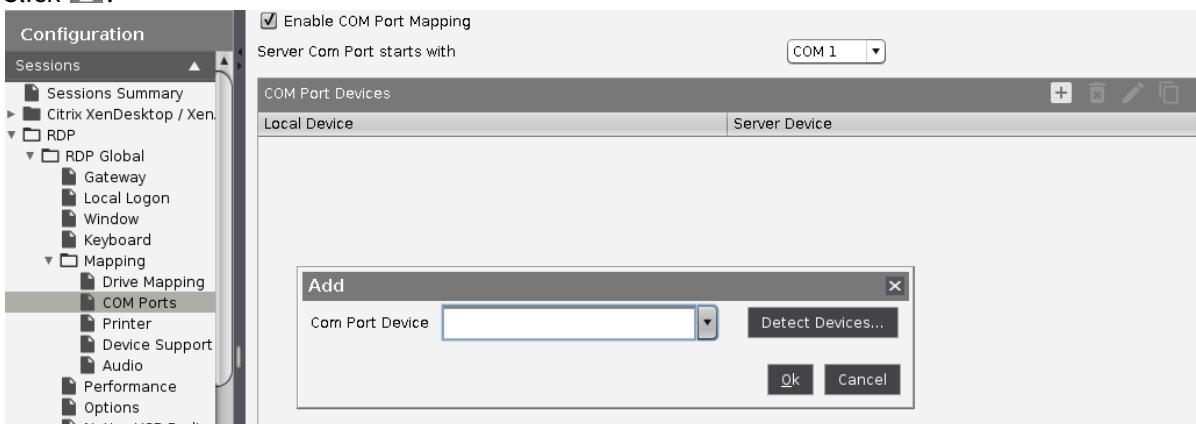
1. Install the eGK-KVK software by Cherry.
2. Configuration according to chapter 6 in [http://www.cherry.de/files/manual/eHealth\\_Client-Server\\_Einbindung.pdf](http://www.cherry.de/files/manual/eHealth_Client-Server_Einbindung.pdf).

## Orga 910/920 M

Functionality	
USB ID:	0780:1202
Software:	CT-API by Orga
Device/server connection:	COM port mapping

## Configuring the device

1. Click **Sessions > RDP > RDP Global > Mapping > COM Ports** for RDP
2. Select **Enable Com Port Mapping:**
3. Click **(+)**.



4. Select USB COM 1 as a new COM port device (/dev/ttysUB0).

## Configuring the server

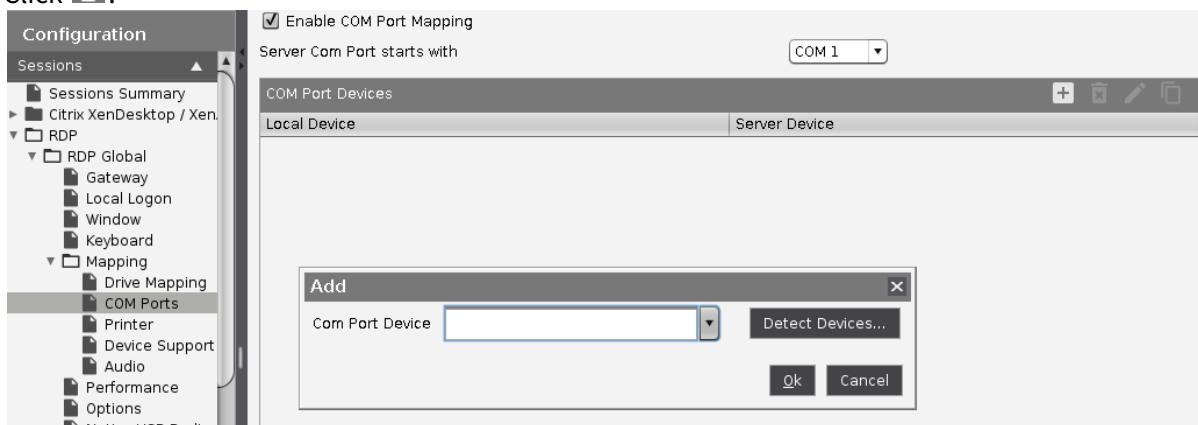
1. Download the appropriate driver for *Orga 910/920 M* from the download page:  
[http://healthcare-eid.ingenico.com/de/treiber\\_anleitungen.aspx](http://healthcare-eid.ingenico.com/de/treiber_anleitungen.aspx)<sup>232</sup>
2. Install the driver.

## Orga 6041 L eGK eHealth-BC S

Functionality	
USB ID:	0780:1302
Software:	CT-API by Orga
Device/server connection:	COM port mapping

## Configuring the device

1. Click **Sessions > RDP > RDP Global > Mapping > COM Ports** for RDP.
2. Select **Enable Com Port Mapping**:
3. Click .



4. Select USB COM 1 as a new COM port device (/dev/ttyUSB0).

## Configuring the server

1. Download the appropriate driver for *Orga 6041 L eGK eHealth-BC S* from the download page:  
[http://healthcare-eid.ingenico.com/de/treiber\\_anleitungen.aspx](http://healthcare-eid.ingenico.com/de/treiber_anleitungen.aspx)<sup>233</sup>
2. Install the driver.

<sup>232</sup> <https://ingenico.de/healthcare/downloads>

<sup>233</sup> <https://ingenico.de/healthcare/downloads>

## cematic CARD STAR / medic2

### Connecting the reader

- Connect the reader to the COM port of the thin client.

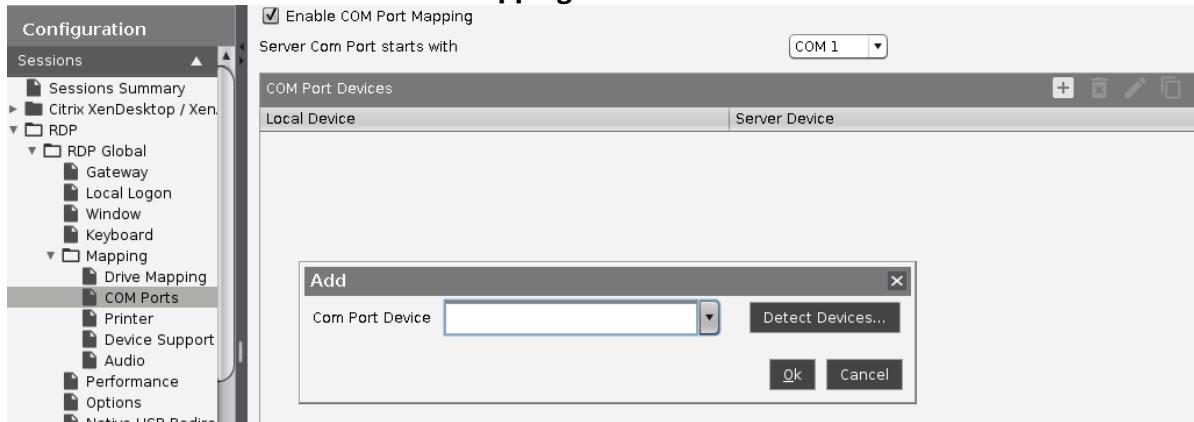
The reader must be set to host/PC serial interface.

Functionality	
Software:	CT-API by cematic
Device/server connection:	COM port mapping

### Configuring the device

In IGEL Setup, add the COM port device to which the keyboard is connected:

1. Click **Sessions > RDP > RDP Global > Mapping > COM Ports** for RDP.



2. Click .
3. Select a **COM port device** (COM1, COM2, ...).

### Configuring the server

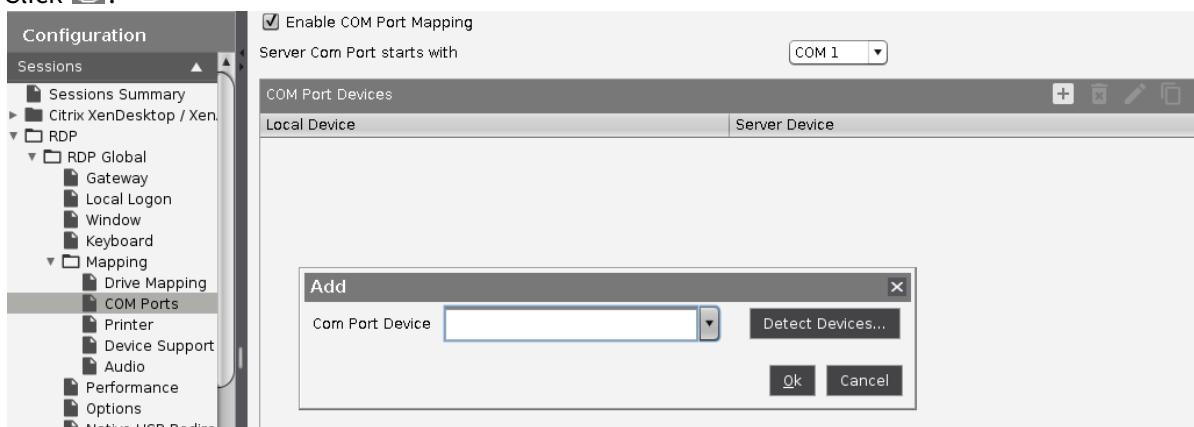
1. Download the appropriate driver for *cematic CARD STAR / medic2* from the download page:  
<https://www.ccv.eu/de/>
2. Install the driver.

## celectronic CARD STAR/ memo3

Functionality	
USB ID:	152a:8180
Software:	CT-API by celectronic
Device/server connection:	COM port mapping

### Configuring the device

1. Click **Sessions > RDP > RDP Global > Mapping > COM Ports** for RDP.
2. Select **Enable Com Port Mapping**:
3. Click .



4. Select USB COM 1 as a new COM port device (/dev/ttyUSB0).

### Configuring the server

1. Download the appropriate driver for *celectronic CARD STAR memo3* from the download page: <https://www.ccv.eu/><sup>234</sup>
2. Install the driver.

### 2.23.11 Using Mobile Device Access

You can access your mobile device file structure via USB, e.g. to make it available in a session.

**Feature with limited support!** The mobile device access feature comes with “limited support”. This feature is offered ‘as is’ without any warranty. Any support for this feature is provided on a non-binding, “best effort” basis.

<sup>234</sup> <https://www.ccv.eu/de/>



The following device types can be used:

- Smartphones with Android (via MTP / PTP) or iOS
- Tablets with Android via MTP / PTP) or iOS
- Digital cameras

The functionality may differ according to the specific device and operating system version.

## Environment

- IGEL Universal Desktop (UD) with IGEL OS10.04.100 or higher

IZ devices are not supported!

- IGEL Universal Desktop Converter 3 (UDC3) with IGEL Linux 10.04.100 or higher
- UD Pocket with IGEL Linux 10.04.100 or higher
- To configure the feature via UMS, UMS version 5.08.110 is required.

- 
- [Enabling Mobile Device Access](#)(see page 693)
  - [Disabling Mobile Device Access](#)(see page 694)
  - [Mapping a Mobile Device for a Session](#)(see page 694)
  - [Connecting Your Mobile Device](#)(see page 695)
  - [Accessing the Mobile Device USB Window from a Session](#)(see page 695)
  - [Viewing the Files and Directories Locally](#)(see page 696)
  - [Safely Removing the Mobile Device](#)(see page 697)

## Enabling Mobile Device Access

1. Ensure that the settings under **System > Update > Firmware Update** are correct. The **Server Path** must point to the firmware version that is currently installed. This is required because the software package for mobile device access must be downloaded in order to deploy the feature.
2. Go to **System > Firmware Customization > Features** and activate **Mobile Device Access USB**.
3. Confirm the warning dialog with **Ok**.
4. Click **Ok** in the main window.
5. Reboot the device.  
On reboot, the device downloads and installs the software package for the mobile device access feature.
6. If mobile device access should be available permanently, make sure that **Autostart** is activated under **Accessories > Mobile Device Access**. The other start options are described in the manual under [Mobile Device Access](#)(see page 1114).



If you want to use mobile device access in appliance mode, you must enable autostart or configure a hotkey. Autostart is recommended.

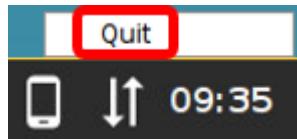
7. Configure the start options for mobile device access according to your requirements.
8. If you have activated **Autostart** as the only start option, restart the device.

When the mobile device access is activated, the smartphone symbol is shown in the task bar. For appliance mode sessions, the in-session control bar is available; see [Accessing the Mobile Device USB Window from a Session](#)(see page 695).

## Disabling Mobile Device Access

### Disabling Mobile Device Access

- In the context menu of the tray icon, click **Quit**.



## Mapping a Mobile Device for a Session

There are two alternative options to map a mobile device to a drive in a session:

- Automatic Drive Mapping
- Manual Mapping to a Specific Drive

### Automatic Drive Mapping

You can use dynamic client drive mapping to have a drive automatically mapped to your mobile device. The directories and files on your mobile device will be accessible under this drive.

1. In the IGEL Setup, go to **Devices > Storage Devices > Storage Hotplug** and enable **Storage hotplug**.
2. Set **Client drive mapping** to "**Dynamic**".
3. Click **OK**.

You can access the directories and files on your mobile device like with a regular hotplug storage device.

For further information, see the manual chapter [Storage Hotplug](#)(see page 1228).

### Manual Mapping to a Specific Drive

You can specify a drive letter under which the directories and files on your mobile device will be accessible.

1. If the session will run in fullscreen mode, open the IGEL Setup, go to **User Interface > Desktop** and activate **In-Session Control Bar**.



2. If the session will run in fullscreen mode or appliance mode, ensure that **Autostart** under **Accessories > Mobile Device Access** is enabled. See here also [Enabling Mobile Device Access](#)(see page 693).
3. Go to the **Drive Mapping** page for your session type. Example: With RDP sessions, the setup path is **Sessions > RDP > RDP Global > Mapping > Drive Mapping**.
4. Activate **Enable drive mapping**.
5. Click **Add** to bring up the mapping window.
6. Click **Enabled** to enable the drive connection.
7. Select a **Drive to map** from the list under which the local device or the folder is to be mapped.
8. Enter `/media` as the **Local Drive Path**.
9. Click **OK**.

You can access the directories and files on your mobile device like with a regular hotplug storage device.

## Connecting Your Mobile Device

1. If mobile device access is not started already, use one of the start options configured under **Accessories > Mobile Devices Access**.
2. Connect your mobile device with your thin client.
3. Allow file transfer on your phone, e. g. **Transfer Files** (Android smartphones) or **Trust The Computer** (Apple iPhone).

The directories of your mobile device are mounted.

You can view the contents; see [Viewing the Files and Directories Locally](#)(see page 696).

You can remove the mobile device securely; see [Safely Removing the Mobile Device](#)(see page 697).

## Accessing the Mobile Device USB Window from a Session

### Non-Fullscreen Session

- ▶ Click **Mobile Device Access USB** to open the **Mobile Device Access USB** window.

The **Mobile Device Access USB** window appears.

You can view the directories and files on your mobile device or safely remove the device; see [Safely Removing the Mobile Device](#)(see page 697).

### Fullscreen Session

In a session that is running in fullscreen mode or appliance in a fullscreen session, you can use the in-session control bar to open the **Mobile Device Access USB** window.

1. Move the mouse pointer to the upper edge of the screen.  
The in-session control bar appears.



2. Click the smartphone symbol.  
The **Mobile Device Access USB** window appears.  
You can view the directories and files on your mobile device or safely remove the device.

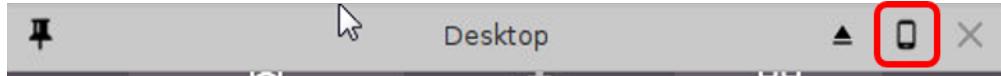


## Appliance Mode Session

In a session that is running in appliance mode, you can use the in-session control bar to open the **Mobile Device Access USB** window.

1. Move the mouse pointer to the upper edge of the screen.

The in-session control bar appears.



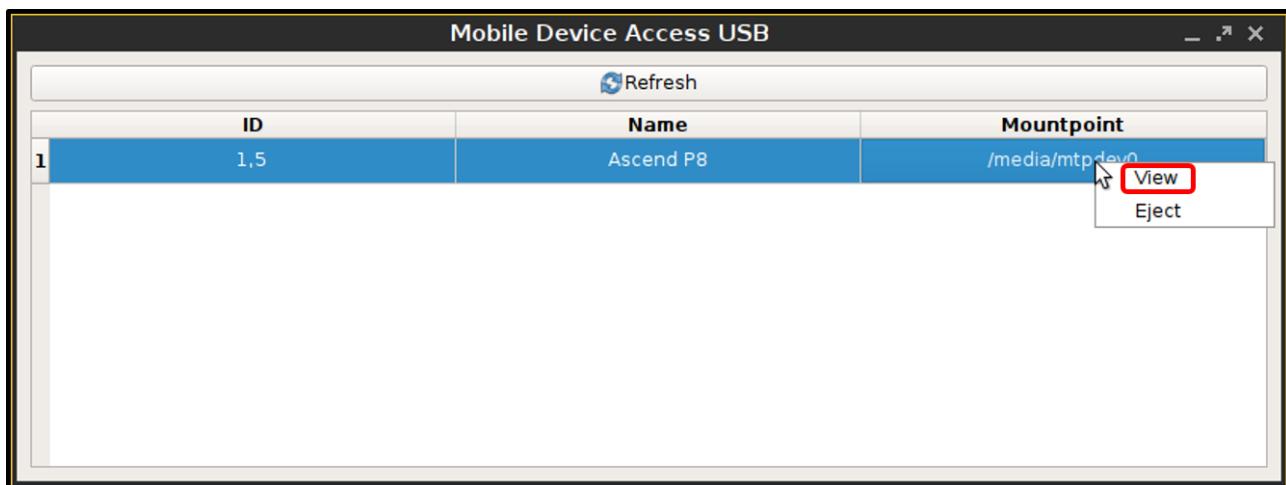
2. Click the smartphone symbol.

The **Mobile Device Access USB** window appears.

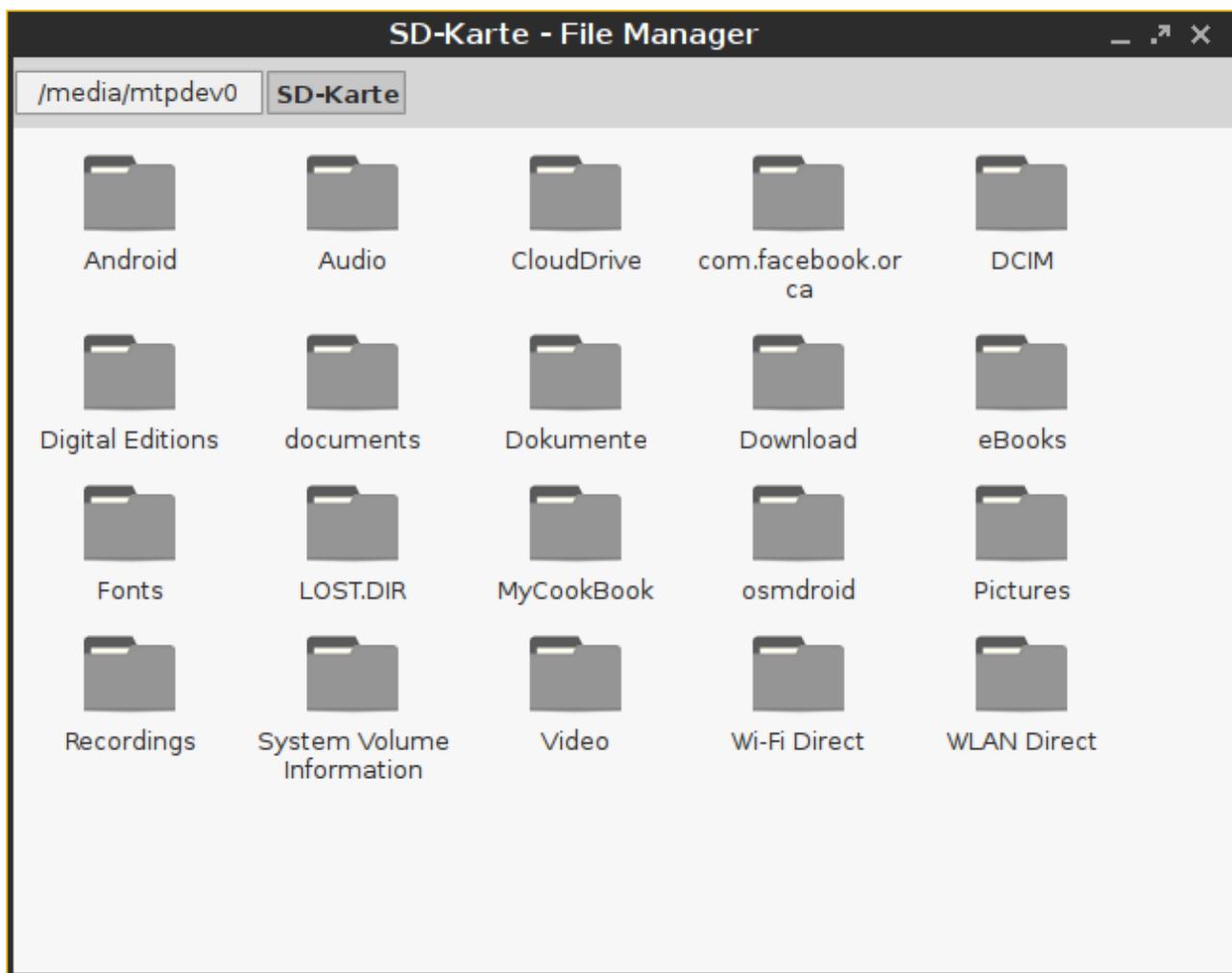
You can view the directories and files on your mobile device or safely remove the device.

## Viewing the Files and Directories Locally

- Select **View** in the context menu.

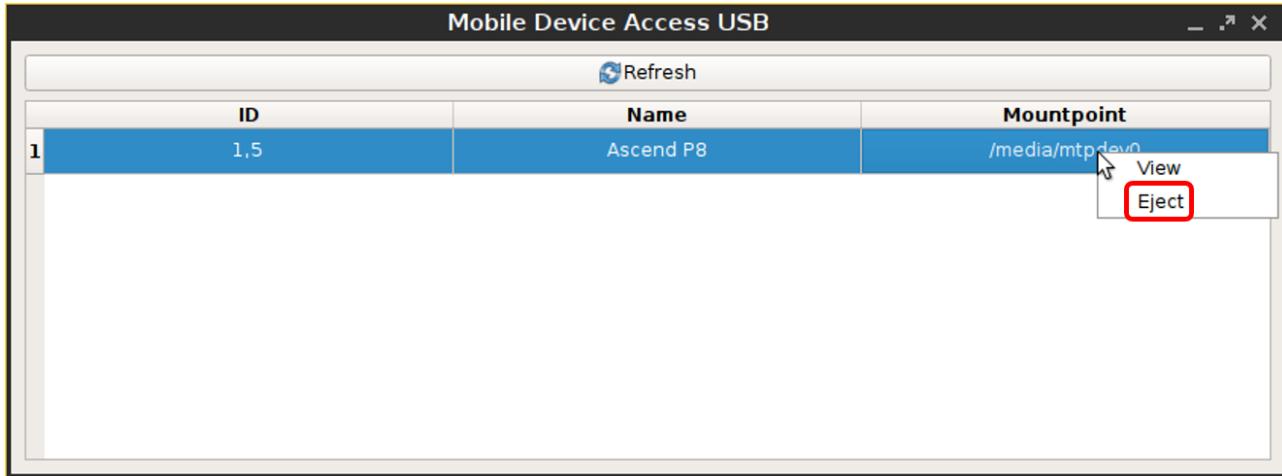


The directories on your smartphone are displayed. Access is read-only, i. e. you can only view the directories and files.



## Safely Removing the Mobile Device

- ▶ Click **Eject** in the context menu for the device in question.



### 2.23.12 Swapping Function of Mouse Buttons (e.g. When Using an Evoluent Mouse)

The assignment of mouse buttons for *Evoluent Mouse 3* changed between firmware versions 5.04.130 and 5.05.100.

#### Problem

Users have become used to the assignment as it was up to 5.04.130, so you want to reproduce the same assignment in 5.05.100.0.

#### Solution

A. To manually analyze the assignment and determine how it needs to be adjusted:

1. Open a local terminal.
2. Find the mouse ID: `xinput list`  
The output should look something like this:  
`| Virtual core pointerid=2[master pointer (3)] |- Virtual core XTEST pointer id=4[slave pointer (2)] |- Logitech USB Optical Mouse id=10[slave pointer (2)] - Virtual core keyboardid=3[master keyboard (2)] - Virtual core XTEST keyboard id=5[slave keyboard (3)] - Power Buttonid=6[slave keyboard (3)] - Video Busid=7[slave keyboard (3)] - Power Buttonid=8[slave keyboard (3)] - Sleep Buttonid=9[slave keyboard (3)] - Logitech USB Keyboardid=11[slave keyboard (3)] - Logitech USB Keyboardid=12[slave keyboard (3)]`
3. Find your mouse and its ID in the output (here: Logitech USB Optical Mouse, id=10 ).
4. Check the number of buttons in the button map: `xinput get-button-map [ID]` (where ID is the ID of your mouse device).
5. Now check which button number is set for the buttons in question: `xev`  
A test window will appear.
6. Click into the window using the buttons that you want to swap. Look for the button numbers in the terminal output: `ButtonPress event, serial 39, synthetic NO, window 0x3200001, root 0xae, subw 0x0, time 25542794, (114,113), root:(2884,634), state 0x10, button 1, same_screen YES ButtonRelease event, serial 39, synthetic NO,`



```
window 0x3200001, root 0xae, subw 0x0, time 25542898, (114,113), root:  
(2884,634), state 0x10, button 1, same_screen YES ButtonPress event, serial  
39, synthetic NO, window 0x3200001, root 0xae, subw 0x0, time 25543218,  
(114,113), root:(2884,634), state 0x10, button 3, same_screen YES  
ButtonRelease event, serial 39, synthetic NO, window 0x3200001, root 0xae,  
subw 0x0, time 25543330, (114,113), root:(2884,634), state 0x410, button 3,  
same_screen YES
```

In the above example the buttons number 1 and 3 were used.

B. To change the assignment of the mouse buttons on the local thin client:

1. Set a new button map for the mouse in **Setup > System > Firmware Customization > Custom Commands > Desktop Commands > Final**.
2. Swap the buttons in the map. To swap e.g. the buttons 1 and 3, change the setting from `xinput set-button-map [ID] 1 2 3 4 5 6 7` to `xinput set-button-map [ID] 3 2 1 4 5 6 7`

C. To automatically change the assignment using a UMS profile:

As the ID of the mouse may be different on each client, you cannot use the command as shown in B2 but need to use a script that will automatically map the correct input device.

1. Run the following command in a local terminal: `xinput --list`
2. Make a note of the complete name of the mouse.
3. Create a profile in **Setup > System > Firmware Customization > Custom Commands > Desktop Commands > Final** with a custom command: `MouseID=$(xinput --list --id-only 'NAME OF MOUSE') xinput set-button-map $MouseID 3 2 1 4 5 6 7`
4. Replace NAME OF MOUSE with the name of the mouse as determined in step C1.

## 2.23.13 Connecting a Serial Barcode Scanner

### Connecting Barcode Scanner via COM Port

1. Determine to which COM port of the device the barcode reader is physically connected.
2. Open the IGEL Setup, go to **System > Registry > devices > serial > inputattach** and enable the relevant key, according to the COM port in use:
  - COM1 (/dev/ttys0): **devices.serial.inputattach.com0.enabled**
  - COM2 (/dev/ttys1): **devices.serial.inputattach.com1.enabled**
  - COM3, COM4 ...: Add a new instance by clicking **devices.serial.inputattach.com% > Add Instance** and define the port appropriately, e.g. /dev/ttys2 for COM3.
3. If the device's baud differs from 9600 (default), enter the correct baud under **devices.serial.inputattach.com0.baud**.

With most barcode readers, you can change the baud by scanning a specific bar code.



4. In the Setup, click **Apply** or **Ok** to submit the new settings. To make absolutely sure that the new settings are effective, you can reboot the device.
5. Check if the barcode scanner is working.

## Connecting Barcode Scanner via USB

If the barcode scanner is connected over USB, the challenge is to identify the device which is assigned to it. Depending on your specific device and environment, your mileage may vary. Start with the [simple procedure](#)(see page 700). If you are lucky, this will do it. If not, continue with the [extended procedure](#)(see page 700).

### Simple Procedure

1. Connect the barcode to a USB port. This will trigger an event which will be logged and reported by dmesg.
2. Open a terminal on your endpoint device. For further information on the device's terminal, see [Terminals](#)(see page 1042).
3. To find the right device file, enter `dmesg | grep tty` in the terminal.  
If you are lucky, the relevant device file is listed. Its name is either `ttyUSB<NUM>` or `ttyACM<NUM>`.  
Example: `ttyUSB0`  
If the relevant device file is not listed, try the [extended procedure](#)(see page 700) below.
4. Open the IGEL Setup, go to **System > Registry > devices > serial > inputattach**.
5. Set the **devices.serial.inputattach.com0.port** to the device file you have found. Example: If the device file is `ttyUSB0`, enter `/dev/ttyUSB0`
6. Activate **devices.serial.inputattach.com0.enabled**.
7. If the device's baud differs from 9600 (default), enter the correct baud under **devices.serial.inputattach.com0.baud**.

With most barcode readers, you can change the baud by scanning a specific bar code.

8. Click **Apply** or **Ok** to submit the new settings. To make absolutely sure that the new settings are effective, you can reboot the endpoint device.
9. Check if the barcode scanner is working.

### Extended Procedure: Device File Was Not Found on the First Go

If the device file could not be found using the simple procedure, try loading the device driver manually. As the explicit loading of the driver must be executed with every system start, a custom command must be added.

1. In the terminal, enter the following commands, one after the other:  
`modprobe cdc-acm`  
`dmesg | grep tty`  
 The relevant device file is listed. Its name is either `ttyUSB<NUM>` or `ttyACM<NUM>`.  
 Example: `ttyACM0`
2. Open the IGEL Setup, go to **System > Registry > devices > serial > inputattach**.
3. Set the **devices.serial.inputattach.com0.port** to the device file you have found. Example: If the device file is `ttyUSB0`, enter `/dev/ttyACM0`
4. Activate **devices.serial.inputattach.com0.enabled**.



5. If the device's baud differs from 9600 (default), enter the correct rate under **devices.serial.inputattach.com0.baud**.

With most barcode readers, you can change the baud by scanning a specific barcode.

6. Go to **System > Firmware Customization > Custom Commands > Base** and under **Initialization**, enter `modprobe cdc-acm`
7. Click **Apply** or **Ok** to submit the new settings. Reboot the device.
8. Check if the barcode scanner is working.

## 2.23.14 Using DriveLock with IGEL Devices

### Issue

DriveLock allows the system administrator to control access to removable devices within Citrix or RDP sessions. This is possible for USB devices; as of IGEL OS version 10.04.100, SATA devices are also supported.

### Problem

How to integrate DriveLock solution with IGEL OS devices?

### Solution

After configuring the Citrix or RDP server according to the original documentation, you have to activate the DriveLock virtual channel in the Setup.

See the original [DriveLock documentation](#)<sup>235</sup>.

#### Using DriveLock with RDP:

1. In **Devices > Storage Devices > Storage Hotplug**, change the settings as follows:
  - Deactivate **Enable dynamic client drive mapping**.
  - Set **Number of storage hotplug devices** to 1 or higher.
  - Activate **Private drive letter for each storage drive**.
2. In **Sessions > RDP > RDP Global > Mapping > Drive Mapping**, change the settings as follows:
  - Activate **Enable Drive Mapping**.
3. In **Sessions > RDP > RDP Global > Mapping > Device Support**, change the settings as follows:
  - Activate **DriveLock channel**.

#### Using DriveLock with Citrix:

1. In **Devices > Storage Devices > Storage Hotplug**, change the settings as follows:
  - Deactivate **Enable dynamic client drive mapping**.

---

<sup>235</sup> <https://kb.igel.com/download/attachments/49588383/TA%20-%20How%20to%20use%20DriveLock%20with%20Igel%20Thin-Clients.pdf?api=v2&modificationDate=1598964656522&version=1>



- Set **Number of storage hotplug devices** to 1 or higher.
  - Activate **Private drive letter for each storage drive**.
2. In **Sessions > Citrix > Citrix Global > Mapping > Drive Mapping**, change the settings as follows:
    - Enable **Activate Drive Mapping**.
  3. In **Sessions > Citrix > Citrix Global > Mapping > Device Support**, change the settings as follows:
    - Activate **DriveLock channel**.

## 2.23.15 Restricting the Mounting of Hotplug Storage Devices on IGEL Linux

### Goal:

You want to restrict the mounting of hotplug storage devices.

### Solution:

As of *IGEL Linux version 5.10.100*, the following registry keys let you disable the mounting of hotplug storage devices based on the device class (floppy, optical, harddisk, flash, other).

- `devices.hotplug.enable_floppy`
- `devices.hotplug.enable_optical`
- `devices.hotplug.enable_harddisk`
- `devices.hotplug.enable_flash`
- `devices.hotplug.enable_other`

These are all of type **bool**. Their default value is **true**. If true, mounting volumes on floppies, optical media, harddisks, flash memory devices, and others is enabled respectively.

Even if the above settings allow mounting hotplug storage devices, the following settings may still restrict it:

- **Devices > USB access control**
- **Devices > Storage Devices > Storage Hotplug**

In order to disable mounting of a device class system-wide:

1. In setup, go to **System > Registry**.
2. In the **Parameter** tree, open **Devices > hotplug**.
3. To disable the mounting of a device class, uncheck its **Enable hotplug [...]** parameter.



## 2.23.16 When to Use USB Redirection

### Solution Based on Experience from the Field

This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

### Document Purpose

In general, USB redirection is not needed for standard functionality such as; audio, video, HID input, etc. However, in some special circumstances, a device may need to be redirected into a VDI session for full functionality, or if it requires a specific driver to function.

For webcams, see [Webcam Redirection and Optimization](#)(see page 663).

Use USB redirection ONLY WHEN ABSOLUTELY REQUIRED.

In this document, we will define the best practices for using USB redirection in a VDI environment, and go through the process with an example.

The example described here is for VMWare Horizon, but it is similar for Citrix, RDS, and most other VDI technologies as well.

### Best Practices for USB Redirection

Below are some general rules that, if followed, will provide the best performance and reliability when using USB redirection.

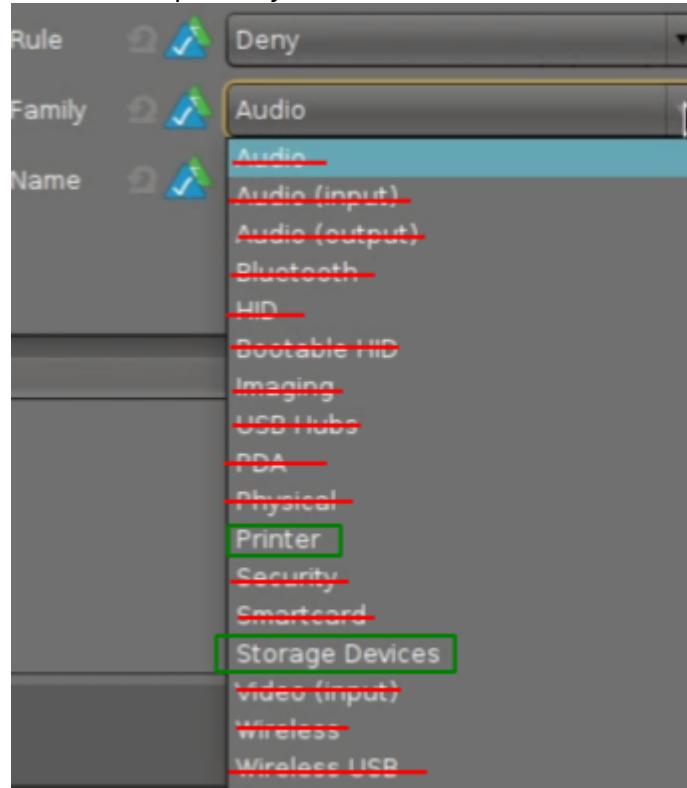
- ALWAYS set the default rule to "Deny".
- DO use VID and PID to redirect devices whenever possible. This is the best way to make sure that a device is redirected and that the USB virtual channels are not flooded with excess redirection.
- Enable USB redirection for the minimal amount of devices required to support user workflows
- As a rule, the USB classes below should NEVER be redirected. Instead, redirect individual devices in these classes using **Device Rules**.

Audio	Audio (input)	Audio (output)	Bluetooth
HID	Bootable HID	Imaging	USB Hubs
PDA	Physical	Security	Smart Card
Video (input)	Wireless	Wireless USB	

- The following classes may be redirected in specific circumstances:
  - **Printers**
    - Only if CUPS configurations or a third party does not fill this requirement
  - **Storage**



- Only if mass storage options do not meet the requirements for user workflows or software compatibility



Rules are meant to be broken, right? If redirecting these classes is the only way things work, take a deeper look and see if there is a better way. If there is no obvious better way, then test thoroughly before moving into production.

### Example: Redirecting a Nuance Powermic (Dictaphone)

Below we will run through the basic process of redirecting a single device into a Horizon VDI session from an IGEL device.

Some devices, including the Nuance Powermic, require custom split rules in Horizon, which will not be covered in this article. The splitting can be done with Horizon Group Policy on the VM, or as additional settings on IGEL. Please contact your vendor for their best practice for the devices.

#### Prerequisites

- Make sure that **Devices > USB Access Control** is disabled on the IGEL devices, or make sure there are no USB access control rules restricting access to the USB device. More information about IGEL USB access can be found under [USB Access Control](#)(see page 1231).
- USB redirection policies for Horizon/Citrix/RDS must be configured to allow redirection to happen



3. The VDI image must have compatible drivers installed for the devices being redirected into the session

### Getting Device Information from IGEL

The first step that needs to be done, is to identify the device's vendor ID and product ID which will be used to create our redirection rule.

1. Plug in the USB device to an IGEL terminal.
2. Connect to the IGEL device using SSH or **IGEL Secure Terminal**.
3. Log in as **user** with the user password set by the IGEL profile.
4. Type su to switch to the root account and provide the root password when prompted.
5. Run lsusb to display a list of devices and locate the device.
6. Note the **ID numbers** separated by a colon ":"
  - a. In the Dictaphone example, this is 0554 and 1001.
  - b. The first number is the vendor ID (VID) and the second is the product ID (PID).

```
root@HW-UD3-2020:/userhome# lsusb
Bus 002 Device 002: ID 174c:3074 ASMedia Technology Inc. ASM1074 SuperSpeed hub
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 005: ID 076b:3031 OmniKey AG
Bus 001 Device 004: ID 067b:23a3 Prolific Technology, Inc.
Bus 001 Device 008: ID df04:0004
Bus 001 Device 007: ID 0554:1001 Dictaphone Corp.
Bus 001 Device 006: ID 0451:2036 Texas Instruments, Inc. TUSB2036 Hub
```

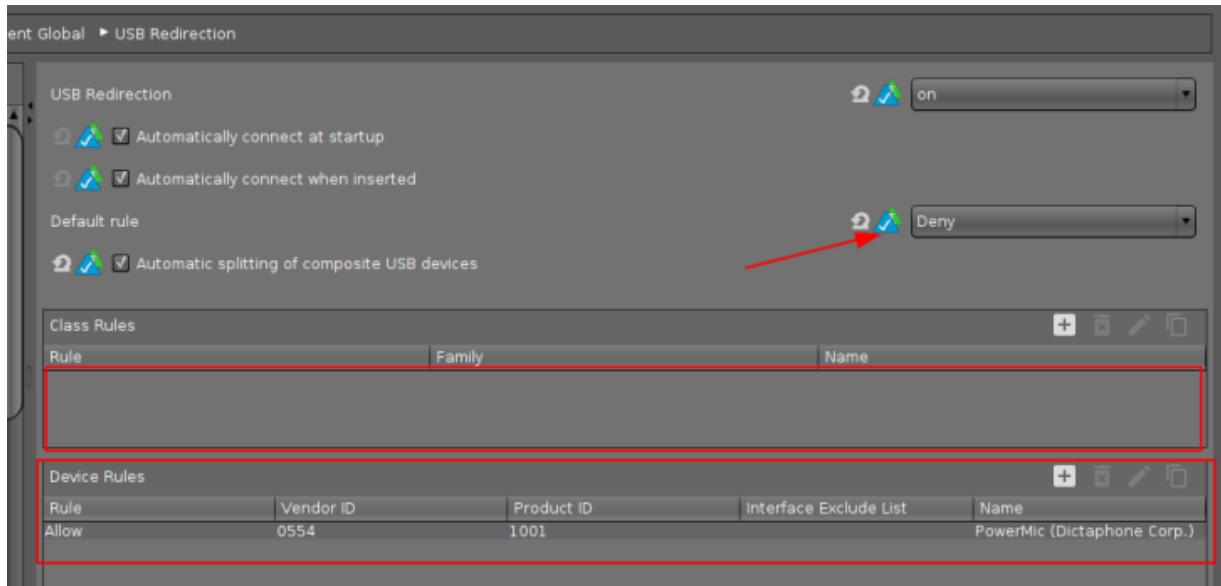
If the device cannot be easily identified by name, then disconnect the device and run lsusb again to see which one disappeared.

### Configuring the IGEL Profile

1. Create a new profile in UMS called "USB Redirection".
2. Go to the **USB Redirection** page for your session.
3. Set **USB Redirection** to "on" and set the **Default rule** to "Deny".
4. Make sure that both **Automatically connect at startup** and **Automatically connect when inserted** are both **enabled**.
5. Clear out any existing **Class Rules** that may have previously existed (if using an existing profile).
6. Add a **Device Rule** using the **Vendor ID** and **Product ID** collected in the previous section, and set it to "Allow".

To make it easy, set the name of the rule to match the device name.

7. Apply the new profile to the device, and reboot for safe measures.  
The device should now be reflected in the Windows Device manager in the VDI session. If so, then the redirection rule is correct and working as expected.



If the device shows up as **unknown** then most likely a driver will need to be installed in the OS to support the device.

### 2.23.17 How to Configure USB Access Control

You can allow and prohibit the use of USB devices on your endpoint device. Specific rules for individual devices or device classes are possible.

The activation of **USB Access Control** and setting the **Default rule** to **Deny** will block the use of USB devices locally and in the session and, thus, might disable devices needed for the users. Therefore, activate the USB access control only if your security policy requires that. In this case, set **Default rule** to **Deny** and configure **Allow** rules for the required USB devices and USB device classes.

It is recommended to make settings for **USB Access Control** as the last step in the device configuration. Before activating the USB access control, check that all your other settings for printers, Unified Communication, USB redirections, mapping settings for USB devices are working as expected.

Note that the USB access control is completely separate than USB redirection for remote sessions, see [When to Use USB Redirection](#)(see page 703).

Take also notice that the feature does not disable a USB port physically, i.e. power delivery will still work.

#### Enable USB Access Control

1. Open the Setup and go to **Devices > USB Access Control**.
2. Enable the option **Enable**.



3. Select the **Default Rule**. The default rule specifies whether the use of USB devices is generally allowed or prohibited.
4. Create one or more rules for classes of devices or individual devices.

## Create a Class Rule

1. To create a new rule, click **[+]** in the **Class Rules** area.
2. Choose a **rule**. The rule specifies whether use of the device class defined here is allowed or prohibited.
3. Under **Class ID**, select the class of device for which the rule should apply. Examples: **Audio, Printer, Mass Storage**.
4. Under **Name**, give a name for the rule.
5. Click **OK**.
6. Save the changes.  
The rule is active.

## Create a Device Rule

When a rule is defined, at least one of the properties **Vendor ID** or **Product ID** or **UUID** must be given.

1. To create a new rule, click **[+]** in the **Device Rules** area.
2. Choose a **rule**. The rule specifies whether use of the device defined here is allowed or prohibited.
3. Give the **Vendor ID** of the device as a hexadecimal value.
4. Give the **Product ID** of the device as a hexadecimal value.

To find out the **Vendor ID** and **Product ID** of the connected USB device, use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal. You can also use the **System Information** tool, see [Using “System Information” Function](#)(see page 1108).

5. Give the **Device UUID** (Universal Unique Identifier) of the device.
6. Specify **Permissions** for the device.

Possible values:

- Global setting: The default setting for hotplug storage devices is used; see **Default permission** parameter under **Devices > Storage Devices > Storage Hotplug**.
- Read only
- Read/Write

7. Under **Name**, give a name for the rule.
8. Click **OK**.
9. Save the changes.  
The rule is active.

## Example

- The set rule prohibits the use of USB devices on the device.



- A class rule allows the use of all entry devices (HID = Human Interface Devices).
- A device rule allows the use of the USB storage device with the UUID 67FC-FDC6.
- The use of all other USB devices, for example, storage devices or printers, is prohibited.

The screenshot shows the configuration interface for USB Devices Rules. It includes two main sections: 'Class Rules' and 'Device Rules'.

**Class Rules:**

Rule	Class ID	Name
Allow	HID (Human Interface Device)	Allow HID

**Device Rules:**

Rule	Vendor ID	Product ID	Device uuid	Permission	Name
Allow			67FC-FDC6	Read/Write	Storage Device

In both tables, the 'Allow' column is highlighted with a red box. In the 'Device Rules' table, the 'Device uuid' column also has a red box around its value '67FC-FDC6'.

## 2.23.18 Issues with USB IDs in USB Devices Rules

### Symptom

USB Device Rules you configured do not take effect.

### Problem

The [System Information](#)(see page 1105) tool in IGEL OS up to version 11.04.100 omits leading zeros in USB vendor and product IDs. These are shown only three hexadecimal digits long.



USB Devices - System Information

Information View Help

Refresh Copy to Clipboard

Computer

- Summary
- Operating System
- Kernel Modules
- Languages
- Display
- Environment Variables
- Users

Devices

- Processor
- Memory

Done.

xHCI Host Controller

xHCI Host Controller

xHCI Host Controller

USB Optical Mouse

USB Keyboard

Misc

USB Version	2.00
Class	0x0
Vendor	0x46d
Product ID	0xc05a
Bus	1

## Solution

If you see three-digit USB IDs in **System Information**, use the `lsusb` command:

1. Open **Local Terminal**.
2. Enter the `lsusb` command.
3. Look for the device in question, possibly using `grep` to search in the `lsusb` output:  
`lsusb | grep -i [search term]`

Local Terminal

```
user@Mathias:~$ lsusb | grep -i Mouse
Bus 001 Device 003: ID 046d:c05a Logitech, Inc. M90/M100 Optical Mouse
user@Mathias:~$
```

4. Use the four-digit IDs that `lsusb` reports.



## 2.23.19 How Can I Fix Touchpad Issues?

### Overview

On some notebooks, the touchpad does not work properly with IGEL OS. Some of these issues can be solved by adding or modifying parameters for the device driver. For usability, the parameter modifications are accessible via the Registry of the IGEL Setup.

If your changes do not seem to be effective after you confirmed them, reboot the device.

### Issues and Solutions

#### Issues with the i2c-i801 Driver

The Registry parameter: `system.module_params.i2c_i801.blacklist` defines whether the i2c-i801 driver is to be blacklisted. The driver is blacklisted by default because it might cause system freezes. If the driver is blacklisted, some functions are not available.

1. In the Setup or the UMS configuration dialog, go to **System > Registry > system > module\_params > i2c\_i801 > blacklist**. and select the desired option:
  - "Default": The decision of whether the i2c-i801 driver is blacklisted or not may change dependent on the hardware you are using.
  - "Yes": The i2c-i801 driver is blacklisted.
  - "No": The i2c-i801 driver is not blacklisted.
2. Click **Apply** or **Ok**.

#### Touchpad Is a Synaptics Intertouch Device

If your notebook has a Synaptics Intertouch touchpad, the Registry parameter `system.module_params.psmouse.synaptics_intertouch` should be enabled.

1. In the Setup or the UMS configuration dialog, go to **System > Registry > system > module\_params > psmouse >synaptics\_intertouch** and activate **Set this if touchpad is a synaptics intertouch device**.
2. Click **Apply** or **Ok**.

#### Touchpad Needs the A4tech Workaround

If your touchpad needs the A4tech workaround, enable it with the Registry parameter `system.module_params.psmouse.a4tech_workaround`. If you are unsure whether you need the A4tech workaround, ask your hardware vendor.

1. In the Setup or the UMS configuration dialog, go to **System > Registry > system > module\_params > psmouse >a4tech\_workaround** and activate **Set this if touchpad needs the a4tech workaround**.
2. Click **Apply** or **Ok**.



## Changing the Compat Protocol

A solution for touchpad issues might lie in changing the communication protocol; this is done with the Registry parameter `system.module_params.psmouse.protocol`.

1. In the Setup or the UMS configuration dialog, go to **System > Registry > system > module\_params > psmouse > protocol** and select the desired option:
  - "Default": The system will detect the protocol automatically.
  - "PS/2"
  - "ImPS/2"
  - "ImExPS/2"
2. Click **Apply** or **Ok**.

## Changing the Resolution

You can change the resolution for your touchpad via the Registry parameter `system.module_params.psmouse.resolution`.

1. In the Setup or the UMS configuration dialog, go to **System > Registry > system > module\_params > psmouse > resolution**, parameter **Resolution in dpi (0 means use default)**, and enter the desired resolution in dpi as an integer.
2. Click **Apply** or **Ok**.

## Changing the Report Rate / Polling Rate

You can change the report rate resp. polling rate for your touchpad via the Registry parameter `system.module_params.psmouse.rate`.

1. In the Setup or the UMS configuration dialog, go to **System > Registry > system > module\_params > psmouse > rate**, parameter **Report rate in reports per second (0 means use default)**, and enter the desired report rate as an integer.
2. Click **Apply** or **Ok**.

## Reset the Touchpad after a Defined Number of Lost Packages

You can force a reset of the touchpad after a defined number of data packages has been lost; the Registry parameter is `system.module_params.psmouse.resetafter`.

1. In the Setup or the UMS configuration dialog, go to **System > Registry > system > module\_params > psmouse > resetafter**, parameter **Reset device after so many packages (0 means never)**, and enter the desired number of packages as an integer.
2. Click **Apply** or **Ok**.

## Forcing a Resync after a Defined Idle Time

1. In the Setup or the UMS configuration dialog, go to **System > Registry > system > module\_params > psmouse > resync\_time**, parameter **Mouse idle time before forcing resync in seconds (0 means never)**, and enter the desired number of seconds as an integer.
2. Click **Apply** or **Ok**.



## 2.24 Printer

- CUPS: Mapping Local Printer to Citrix or RDP Sessions(see page 712)
- Print Server Configuration(see page 712)
- Installing a Custom CUPS Driver(see page 714)

### 2.24.1 CUPS: Mapping Local Printer to Citrix or RDP Sessions

#### Issue

How to map a locally connected PCL/PS-based printer to a Citrix or RDP session?

#### Problem

The CUPS driver does not support all printer functions such as duplex, color profiles, etc.

#### Solution

1. Open local IGEL Setup or UMS configuration or profile.
2. Go to **Devices > Printer > CUPS > Printers**.
3. Create a new printer and define a **Printer Name**.
4. Select the **Printer Port** your printer is connected to.
5. Set **Manufacturer = Generic**.
6. Set **Printer names = Raw Queue**.
7. Switch to the tab **Mapping in sessions**.
8. Enable **Map Printer in ICA Sessions** or **Map Printer in RDP Sessions**.
9. Enable the radio button **Use Custom Windows Driver Name**.
10. Enter the exact name of the Windows driver installed on the server.
11. Check if **Sessions > Citrix > Citrix Global > Mapping > Printer > Client printer mapping** or **Sessions > RDP > RDP Global > Mapping > Printer > Enable Client Printer Mapping** is enabled.
12. Start the ICA or RDP session and install the printer driver with the redirected port named TS00x/ClientPort.

### 2.24.2 Print Server Configuration

#### Prerequisites

- IGEL OS version 10 or higher
- Printer with the integrated PCL/PS controller.



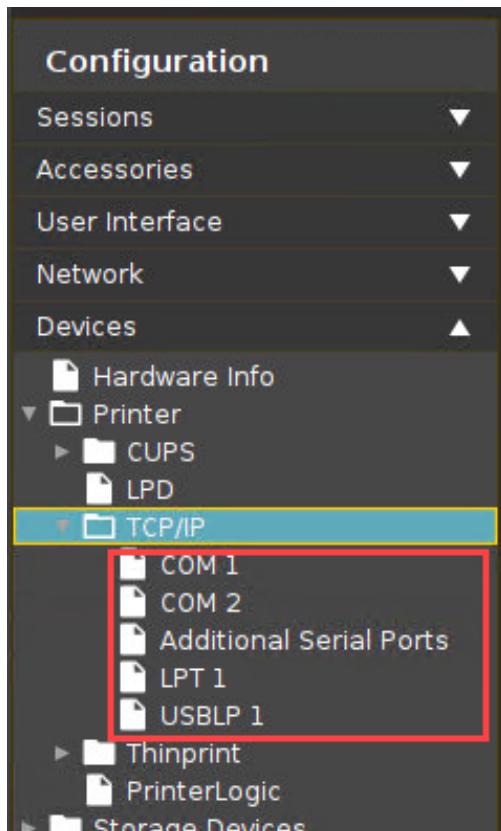
## Recommendation

Assign a fixed IP address to the IGEL device or reserve one for it via DHCP.

## Instructions

To use the IGEL device as a print server for locally connected printers, follow the steps below:

1. In the IGEL Setup, go to **Devices > Printer > TCP/IP**.
2. Select the port to which the printer is connected.
  - COM 1
  - COM 2
  - Additional Serial Ports
  - LPT 1
  - USBLP 1



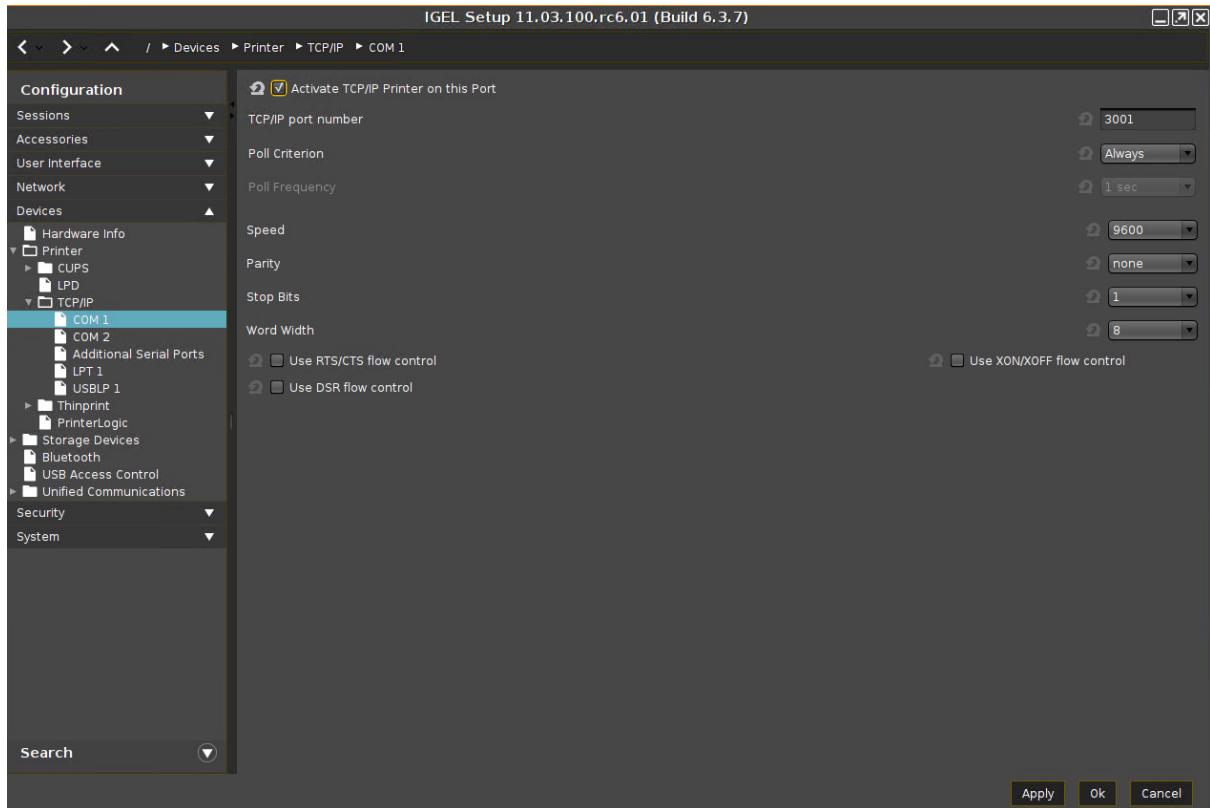
3. Enable **Activate TCP/IP Printer on this Port**.

Enter the **TCP/IP port number** on which the print server service is listening. (Windows default: 9100)

**Poll Criterion** and **Poll Frequency** must only be adjusted if required by the environment.



4. Click **Apply** or **Ok** to save the settings.



The printer can be installed and used by other systems like a regular network printer.

### 2.24.3 Installing a Custom CUPS Driver

#### Environment

IGEL Linux v5 and higher.

#### Issue

Your printer is not included in the CUPS default configuration.

#### Solution

You can install a custom driver from your manufacturer.



## Copying the PPD Driver File to the Device

- ▶ Copy the driver file (PPD file) to the folder /wfs using the UMS file transfer mechanism, see [Files<sup>236</sup>](#).

## Adding a New CUPS Driver

Now that you have copied the driver file to the device, you have to add a new printer and set the PPD file as the driver definition. To do so, proceed as follows:

For a detailed description of the CUPS configuration options, see [CUPS\(see page 1216\)](#).

1. In Setup, go to **Devices > Printer > CUPS > Printer**.
2. Click  to get to **Add** dialogue.
3. Define the following settings:
  - **Printer name:** Name of the printer.
  - **Printer port:** Port to which the printer is connected. Depending on which type you select, you will have to provide additional information, e.g. server and port in the case of **TCP Printer Port**.
  - **Manufacturer:** Choose **Custom**, which will bring up the **Driver definition** field.
  - **Driver definition:** Enter the absolute path to the PPD file.
4. Click **Ok** to save the settings.
5. Restart your device.

## 2.25 UD Pocket

- Running IGEL OS from UD Pocket on a Dell WYSE ZX0D (aka 7010) Device([see page 715](#))
- Running UD Pocket on an Acer Chromebook C910([see page 716](#))
- UD Pocket Seems to Break Microsoft Surface([see page 717](#))
- How to Boot from the UD Pocket on Mac mini, MacBook Air 2018, MacBook Pro([see page 719](#))

### 2.25.1 Running IGEL OS from UD Pocket on a Dell WYSE ZX0D (aka 7010) Device

Here you can learn which settings you have to make on the Dell WYSE ZX0D (aka 7010) to be able to start the device with a UD pocket.

1. Boot up the Dell device.
2. In the BIOS go to the **Advanced** tab.
3. Enable **Boot From USB**.
4. Change to the **Boot** tab.
5. Change the boot priority to make **USB HDD** the default by moving it to the top.
6. Save the settings
7. Put in the UD Pocket

See this video:

---

<sup>236</sup> <https://kb.igel.com/display/endpointmgmt605/Files>



Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:  
<https://www.youtube.com/watch?v=C0NWdjVE1RI>

## 2.25.2 Running UD Pocket on an Acer Chromebook C910

You can use the IGEL UD Pocket with the Acer Chromebook C910. This requires installation of a BIOS extension which enables the device to boot into an alternative operating system.

The procedures described here have been tested with the Acer Chromebook C910; the procedures may differ for other Chromebook types.

For further information, refer to [MrChromebox.tech](https://mrchromebox.tech)<sup>237</sup>.

### Enabling Your Device to Boot from UD Pocket

1. Ensure that you have a WiFi connection; this is required for downloading the SeaBIOS extension.
2. Boot into recovery mode by pressing [ESC] + (Refresh) + (Power) simultaneously.  
The recovery mode screen is shown, which states that the OS is broken.
3. Press [Ctrl] + [D] to enter developer mode.  
The developer mode screen is shown, confirming that OS verification is off.
4. Open a root-capable shell by pressing [Ctrl] + [Alt] + (F2).
5. Login as chronos; no password is required unless one has been set.
6. Change to /tmp: cd /tmp.
7. Download the ChromeOS firmware utility script: curl -LO https://mrchromebox.tech/firmware-util.sh
8. Start the script with root permissions: sudo bash firmware-util.sh
9. Enter 1 to select the first option.
10. Enter y to confirm.  
The RW\_Legacy firmware is downloaded to your device.
11. When the download has completed, press [Enter].
12. Enter r to reboot.  
The device reboots into developer mode.
13. To boot from UD Pocket, press [Ctrl] + [L].

<sup>237</sup> <https://mrchromebox.tech>



### Booting from UD Pocket

1. Ensure that the device is in developer mode. This should be the case if the device has been configured according to the procedures described above, and if since then no changes were made that have affected the developer mode.
2. Press [Ctrl] + [L] to boot from UD Pocket.

### 2.25.3 UD Pocket Seems to Break Microsoft Surface

Please note that this device is not officially supported. Therefore, we can not offer any guarantee or support for the procedures described in this article.

#### Tested Environment

The following information describes the exact environment on which the issue and the troubleshooting method have been tested. However, the method will probably work on similar versions.

- Microsoft Surface Book 1
- Windows 10 build 1903 4/25/2019 18362.267
- IGEL UD Pocket with IGEL OS 11.02.100

#### Issue

After having booted successfully into UD Pocket once, the Microsoft Surface notebook is not able to boot into Windows anymore.

#### Solution

With the following procedures, you can set your Microsoft Surface to boot from USB storage permanently or, alternatively, on-demand.

For detailed information, see [How do I use the BIOS/UEFI?](#)<sup>238</sup> by Microsoft.

##### Enabling Boot from USB Storage Permanently

1. Ensure that your Microsoft Surface has shut down.
2. Press and hold down the volume + (up) button and at the same time, power up the Microsoft Surface.
3. When the Surface logo appears, release the volume + (up) button.  
The UEFI menu is displayed.
4. Under **Configure boot device order**, move **USB Storage** to the top using drag & drop.
5. Under **Advanced options**, change the settings as follows:
  - **Enable alternate boot sequence: On**

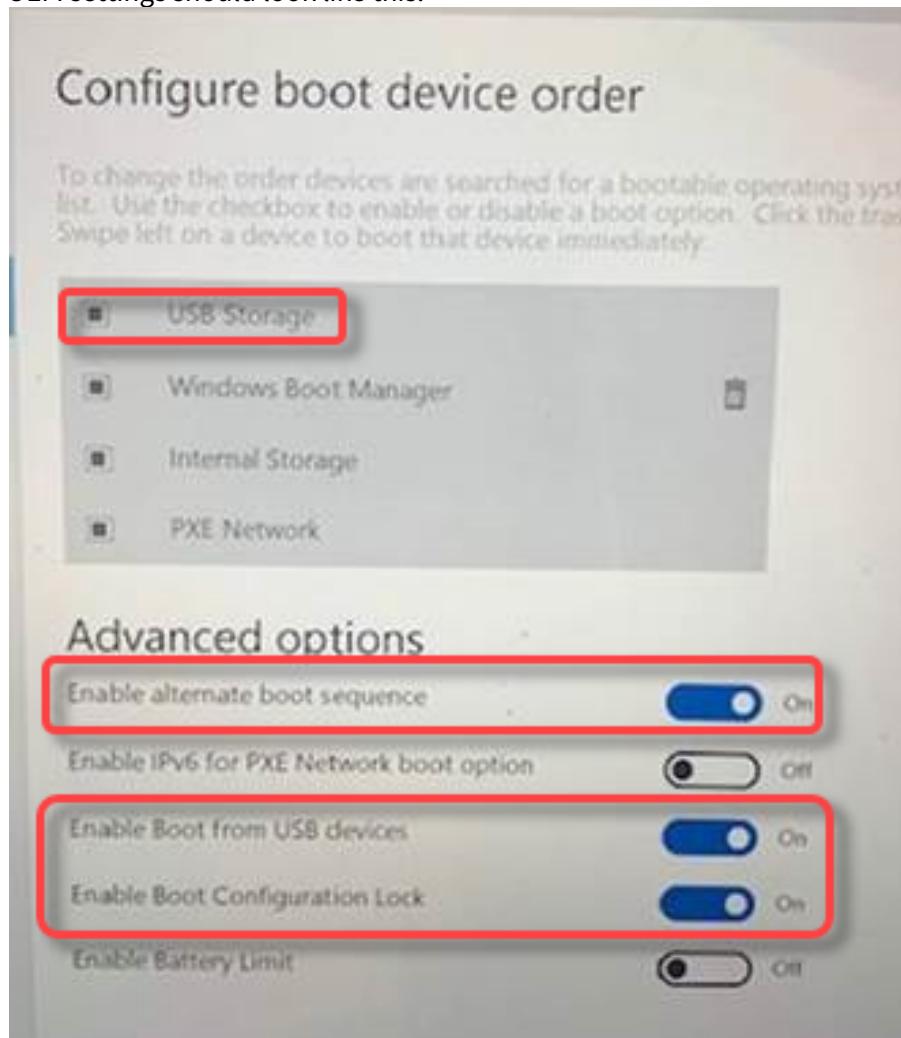
---

<sup>238</sup> <https://support.microsoft.com/en-ae/help/4023532/surface-how-do-i-use-the-bios-uefi>



- **Enable Boot from USB devices:** On
- **Enable Boot Configuration Lock:** On

Your UEFI settings should look like this:



6. Exit the UEFI settings.
7. Insert the UD Pocket into the USB port of your Microsoft Surface.
8. Reboot your Microsoft Surface.

Your Microsoft Surface boots from your UD Pocket.

#### Booting from USB Storage On-Demand

1. Ensure that your Microsoft Surface has shut down.
2. Insert the UD Pocket into the USB port of your Microsoft Surface.
3. Press and hold down the volume + (up) button and at the same time, power up the Microsoft Surface.
4. When spinning dots appear beneath the Surface logo, release the volume + (up) button.

Your Microsoft Surface boots from your UD Pocket.



## 2.25.4 How to Boot from the UD Pocket on Mac mini, MacBook Air 2018, MacBook Pro

### Solution Based on Experience from the Field

This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

### Environment

- Mac devices with an Apple T2 Security Chip, e.g. Mac mini, MacBook Pro, MacBook Air 2018, iMac Pro

### Problem

The secure boot implemented with the Apple T2 Security Chip does not allow to boot Linux on the above-mentioned devices. For details, see the German overview <https://www.computerbase.de/2018-11/apple-t2-linux-installation-umgehung/>. Therefore, some configuration changes on these devices are required to boot from the UD Pocket.

### Solution

Via the recovery menu, it is possible to disable the secure boot option. To do this, proceed as follows:

1. To get into the macOS recovery menu, press and hold the command key [⌘] + [R] during the boot process as soon as the Apple logo appears.
2. Under **Utilities**, select the **Startup Security Utility**.
3. Use an administrator account to deactivate the secure boot option under **Secure Boot > No Security**.

For more information about the Startup Security Utility on Mac devices, see <https://support.apple.com/en-us/HT208198>.

## 2.26 Miscellaneous

- [Sending Device Log Files to IGEL Support](#)(see page 720)
- [Exporting the Local Device Configuration](#)(see page 727)
- [Which Unified Communication Solutions Does IGEL OS Support?](#)(see page 729)
- [Passthrough Authentication](#)(see page 730)
- [Hardware Video Acceleration on IGEL OS](#)(see page 736)
- [Running Commands before or after a Session](#)(see page 739)
- [Copy Sessions in Setup or UMS](#)(see page 741)
- [IZ1 and UD2-MM Usage of RAM](#)(see page 742)
- [Using Symantec Ghost to Deploy IGEL OS](#)(see page 742)



- Starting UMS Console Crashes NX Session(see page 744)
- Accessing IGEL Setup within Appliance Mode(see page 744)
- Application Is Terminated with Message "Low memory! Killing process ..." (see page 745)
- An Application Window Cannot Be Repositioned(see page 745)
- Updating IGEL UMD: Error "not compatible with System5"(see page 747)
- Using Natural Scrolling (reverse Scrolling Direction)(see page 748)
- IGEL Third-party Endpoint Partners: Ensuring Image Integrity with a Checksum(see page 749)

## 2.26.1 Sending Device Log Files to IGEL Support

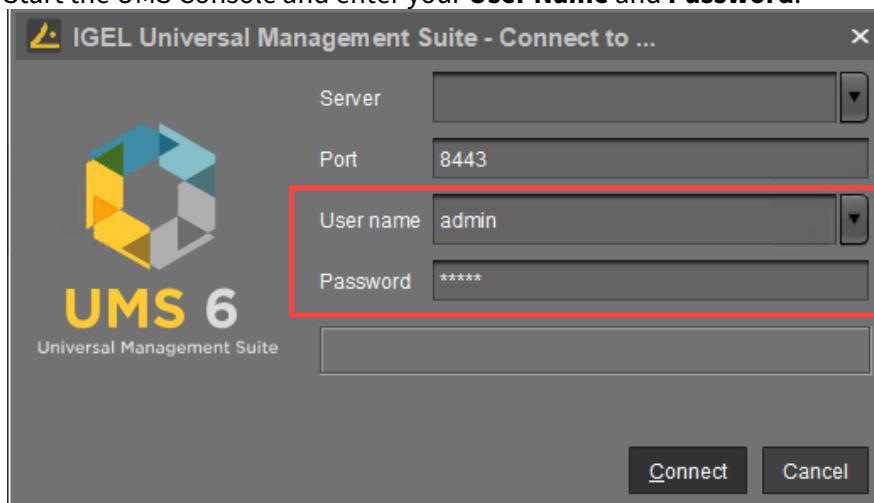
When the IGEL support team asks you to provide your device's log files, follow the instructions below.

There are two opportunities to send log files to the support team:

- With UMS(see page 720)
- Without UMS(see page 725)

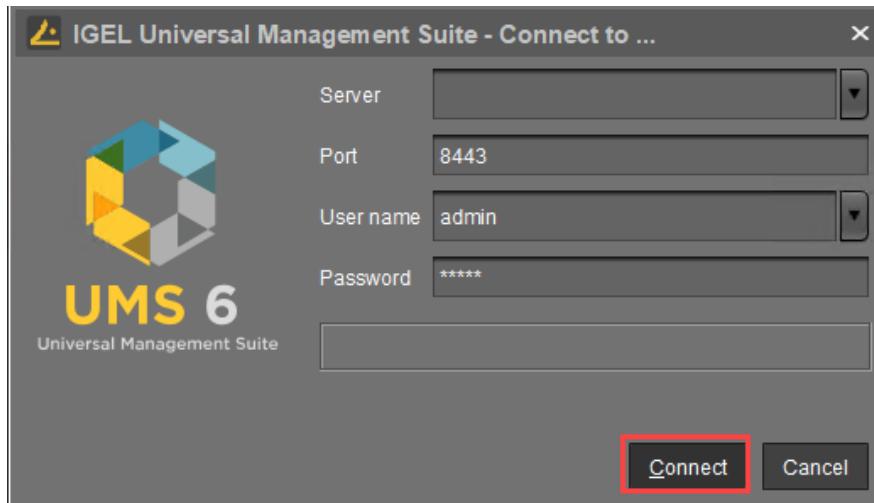
### With UMS

1. Start the UMS Console and enter your **User Name** and **Password**.



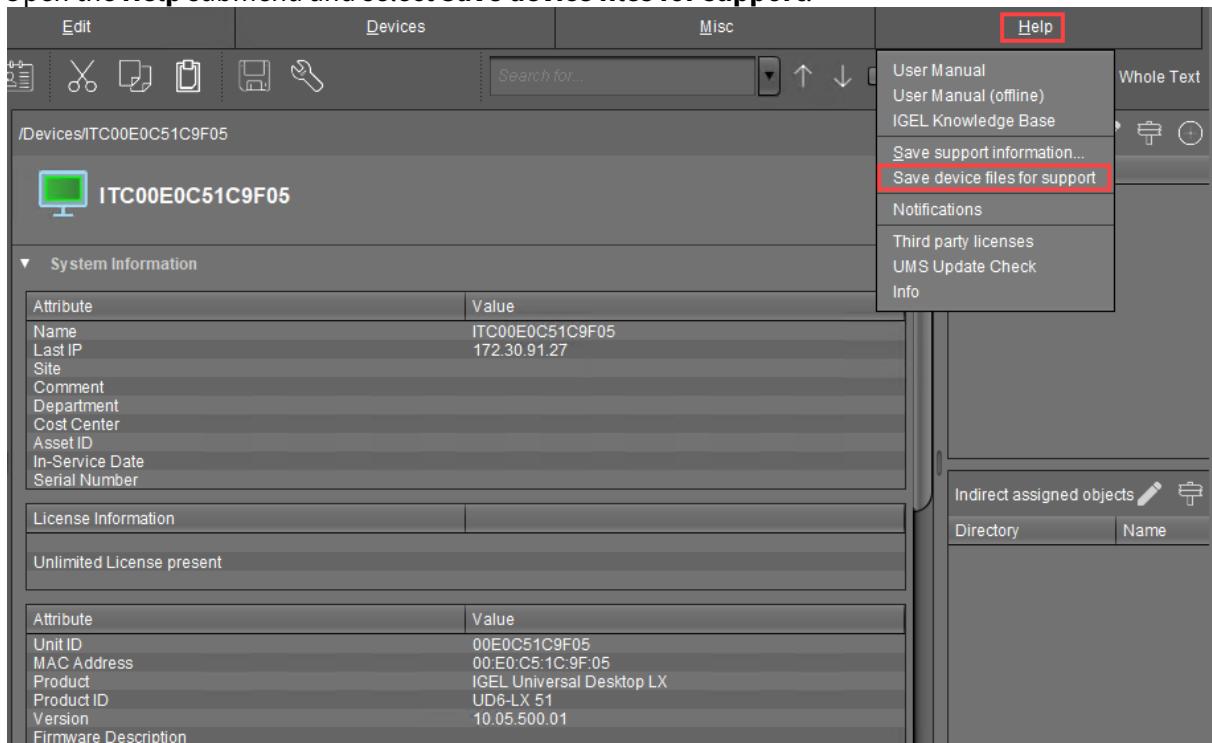


2. Click **Connect**.



The UMS Console window opens.

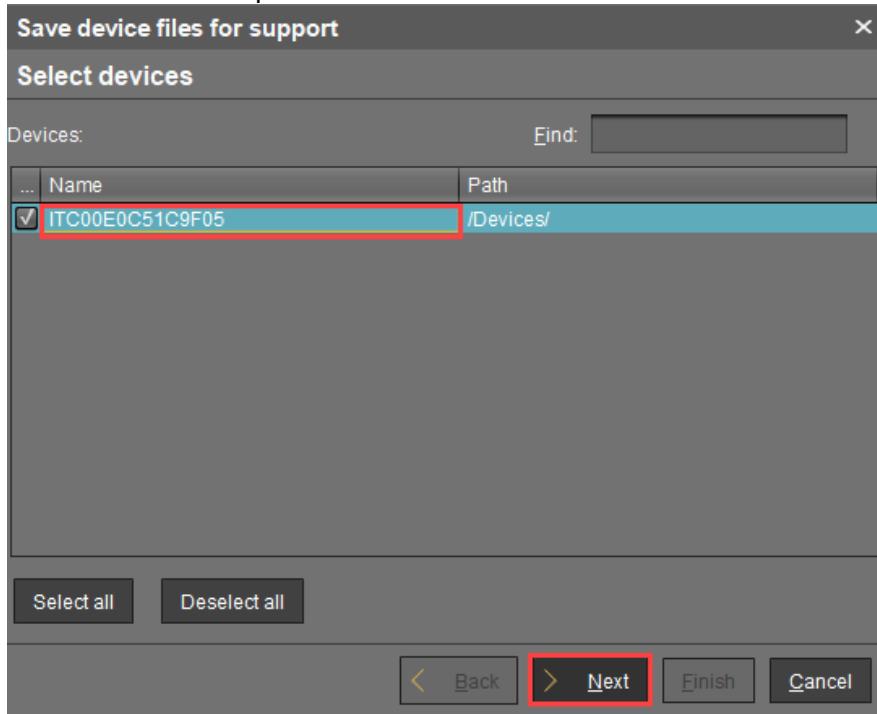
3. Open the **Help** submenu and select **Save device files for support**.



The dialog **Save device files for support** opens.

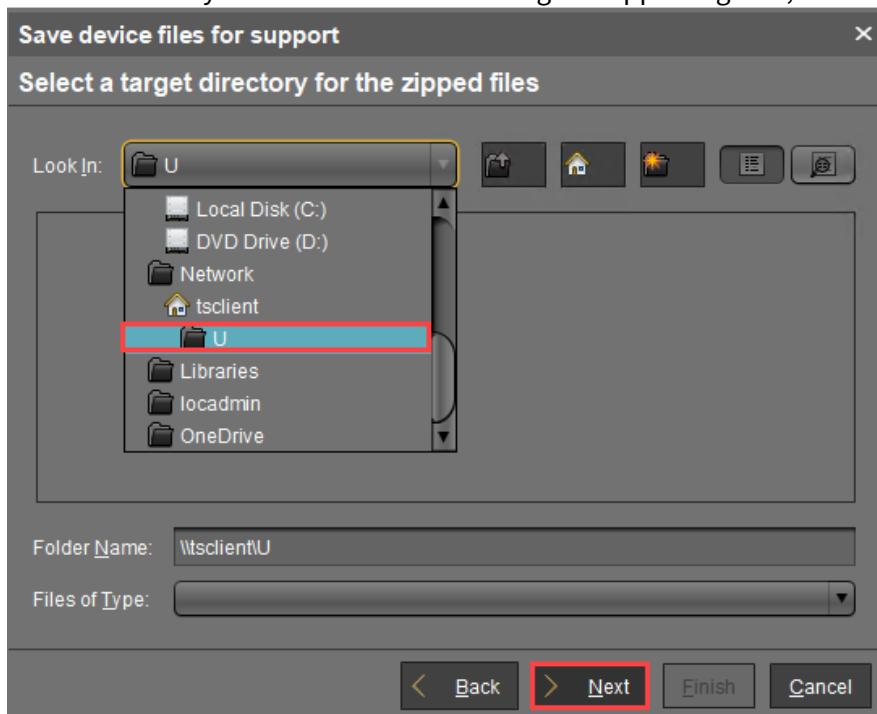


4. Select the device in question and click **Next**.



The dialog **Select a target directory for the zipped files** opens.

5. Select a directory which is suitable for saving the zipped log files, and click **Next**.



A confirmation dialog shows the path and file name under which the log files are stored.



Depending on your system, you can copy the path using [Ctrl] + [C] and paste it into the File Explorer's address bar.

**Save device files for support** ×

**Finished zipping of the device files**

The archive with the device files was stored as

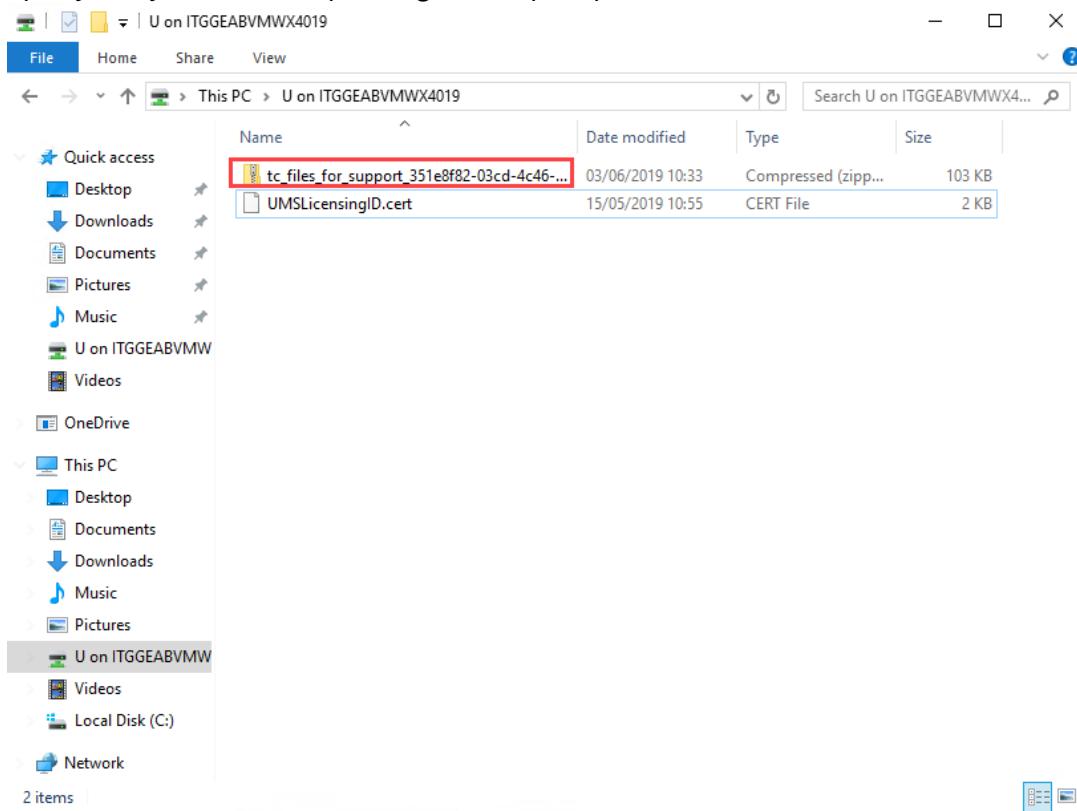
`\!tsclient\Utc_files_for_support_3d542c0d-4899-4bd3-829a-471b8921593b.zip`

Please attach the archive to your support ticket for this issue.

< Back Next > Finish Cancel



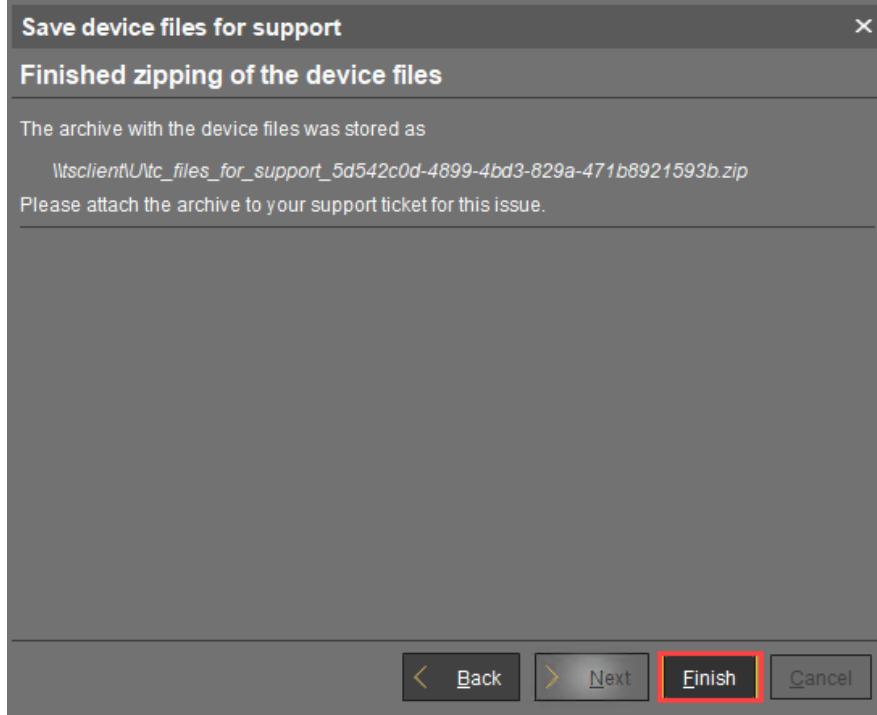
6. Open your system's File Explorer, go to the path portion of the file location.



7. Send the ZIP file to the IGEL support team.



8. Close the confirmation dialog by clicking **Finish**.



The above procedure collects only those logs that have been written since the last system start. To allow persistent logs, you can configure a dedicated partition for debug logs. For more information, also on adding additional logs, see [Extended Logging With Syslog, Tcpdump and Netlog](#)(see page 403).

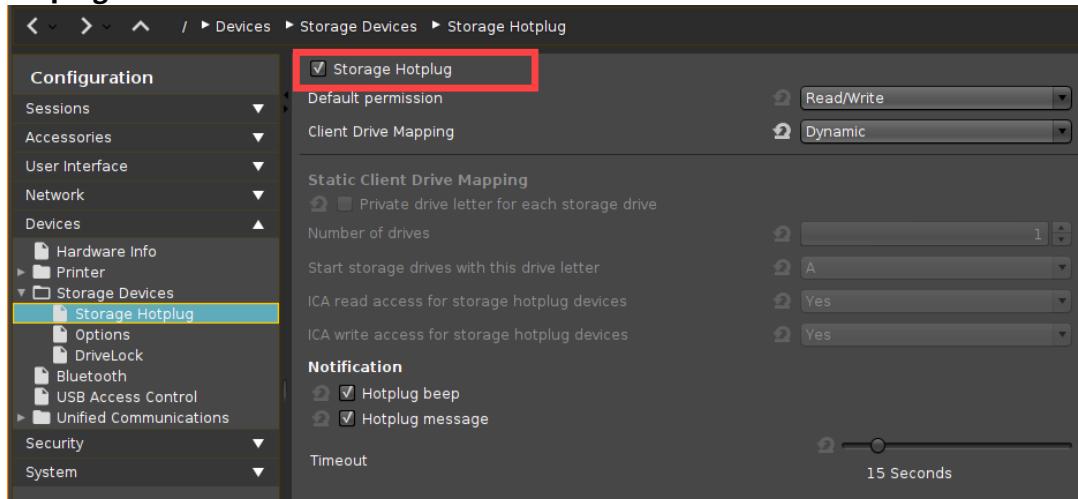
## Without UMS

When the UMS is not accessible or there is an issue with network connectivity, you can still extract system logs from a device and send them to support. You will need a USB stick, preferably formatted to NTFS format, to transfer the logs to.

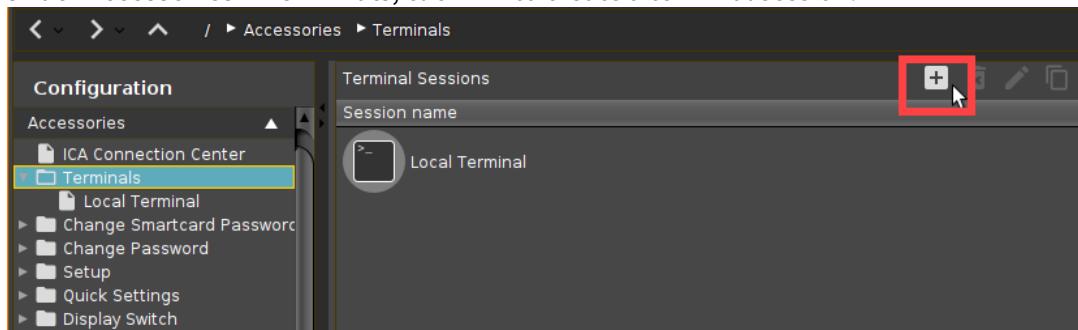


## Setting Up the Device

- In the IGEL Setup, go to **Devices > Storage Devices > Storage Hotplug** and enable **Storage Hotplug**.

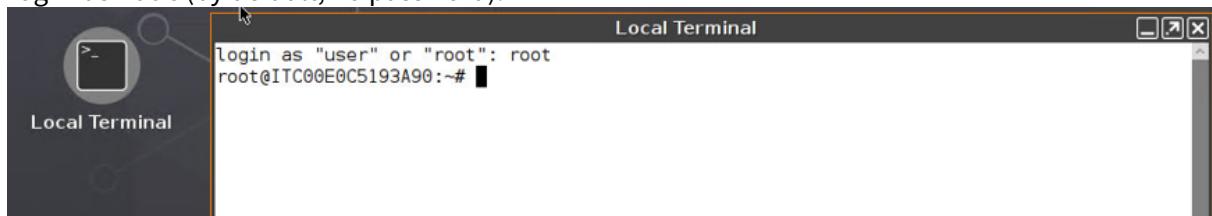


- Under **Accessories > Terminals**, click **+** to create a terminal session.



## Identifying the USB Stick

- Plug the USB stick into the IGEL OS device and start the terminal session.
- Log in as root (by default, no password).



- Enter the following commands:
- ```
cd /userhome/media
ls -l
```



4. Note the name of the USB stick:

```
Local Terminal
login as "user" or "root": root
root@ITC00E0C5193A90:~# cd /userhome/media
root@ITC00E0C5193A90:/userhome/media# ls -l
total 4
drwxr-xr-x 1 user users 4096 Nov 10 12:01 NEW VOLUME
root@ITC00E0C5193A90:/userhome/media#
```

#### Writing the Log File

1. In the terminal, run the command `cd /userhome/media/[Name of your USB stick]`. If there are spaces in the device name, use quotation marks "" Example: `cd /userhome/media/"NEW VOLUME"`  
If there are no spaces in the device name, quotation marks are not required.
2. Run the command `journalctl > logfile.txt`. This will create the system log files on the USB stick with the file name `logfile.txt`.

```
Local Terminal
root@ITC00E0C5193A90:~# cd /userhome/media/"NEW VOLUME"
root@ITC00E0C5193A90:/userhome/media/NEW VOLUME# journalctl > logfile.txt
root@ITC00E0C5193A90:/userhome/media/NEW VOLUME#
```

3. Safely eject the USB stick from the IGEL OS device.  
You can now examine this log file yourself or send it to IGEL support for analysis.

### 2.26.2 Exporting the Local Device Configuration

#### Issue

There is a specific support case and you need to read out the current local configuration of the device.

#### Solution

If you need to read out the current local configuration of the device (e.g. during a support case), you can copy the two local files `setup.ini` and `group.ini` either locally or via the IGEL UMS.

##### Option 1: Via UMS Console > Help > Save device files for support

You can transfer the `setup.ini` and `group.ini` files together with the device's log files as described in the section "With UMS" under [Sending Device Log Files to IGEL Support](#)(see page 720).

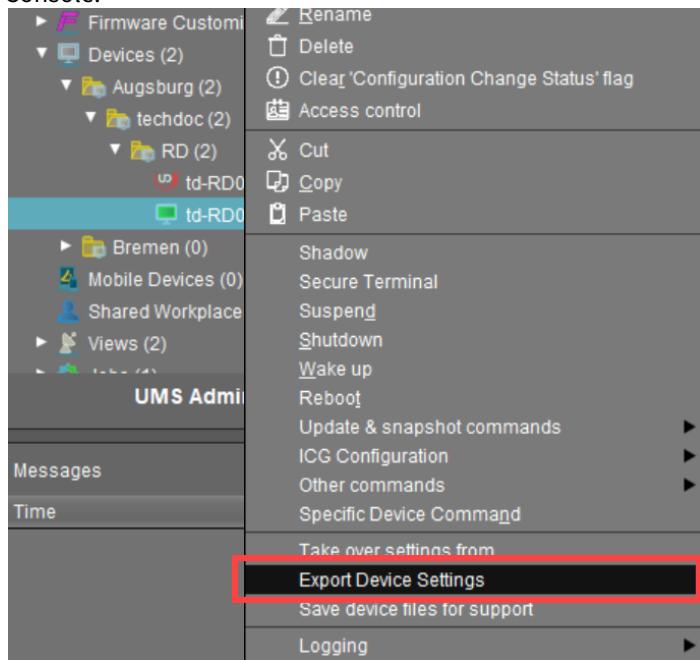
##### Option 2: Via UMS Console > [device's context menu] > Export Device Settings

Alternatively, you can export the effective settings that affect the device (i.e. the interaction of local settings and all profiles) as an XML file: **UMS Console > [device's context menu] > Export Device Settings**.

The IGEL Support can import this file into the UMS as a profile and view the effective settings directly in the UMS



## Console.



Option 3: Via UMS Console > [device's context menu] > Other commands > Device File->UMS

You can also transmit the setup.ini and group.ini files from the device to the UMS as follows:

1. In the UMS Console, select **Other commands > Device File->UMS** from the device's context menu or under **Devices** in the menu bar.
2. Under **Device file location**, specify /wfs/ as the source.  
Example: /wfs/setup.ini
3. Under **Target URL**, select the destination on the UMS Server and enter the name of the transferred file under **File Name**.  
Example: https://umsserver.domain:8443/ums\_filetransfer/setup.ini
4. Click **Device File->UMS**.  
The file will be transferred to /rmguiserver/webapps/ums\_filetransfer.

Option 4: Via copying to a USB storage device

You can also save the files locally on a FAT32-formatted USB stick:

1. In the IGEL Setup, go to **Devices > Storage Devices > Storage Hotplug** and enable **Storage Hotplug**.  
If you use static client drive mapping, make sure that the **Number of drives** is greater than zero.  
See [Storage Hotplug](#)(see page 1228).
2. Create a terminal session under **Accessories > Terminals**.
3. Connect your USB stick.
4. Open the terminal and log in as root.



To find out the name of the USB stick, you can use the commands:

```
cd /userhome/media
ls -l
```

If there are spaces in the device name, you'll have to include it later in the quotation marks "".

If there are no spaces in the device name, quotation marks will not be required.

5. Type `cp /wfs/*.ini /media/[name of USB storage device]/` and press [Return] to copy all .ini files from your endpoint device, incl. `setup.ini` and `group.ini`, to the USB stick.
6. Type `sync` and press [Return]. Wait a few seconds before safely ejecting the USB stick from the endpoint device.

 A screenshot of a terminal window titled "Local Terminal". The window has standard window controls (minimize, maximize, close) at the top right. The terminal content shows a root shell session on an IGEL endpoint. The user runs several commands: navigating to the media directory, listing files (-l), copying configuration files from the wfs directory to the media directory, and finally running sync. The output includes file permissions and names like 'NEW VOLUME'.
 

```
login as "user" or "root": root
root@TD-RD03:~# cd /userhome/media
root@TD-RD03:/userhome/media# ls -l
total 16
drwxr-xr-x 4 user users 16384 Jan  1 1970 'NEW VOLUME'
root@TD-RD03:/userhome/media# cd
root@TD-RD03:~# cp /wfs/*.ini /media/"NEW VOLUME"/
root@TD-RD03:~# sync
root@TD-RD03:~#
```

### 2.26.3 Which Unified Communication Solutions Does IGEL OS Support?

This article provides an overview of the Unified Communication software and hardware solutions that are supported by IGEL OS.

#### Hardware

- [Jabra Handsets / Headsets](#)(see page 58)
- [Poly Headsets](#)(see page 61)
- [EPOS/Sennheiser](#)(see page 61)

#### Virtual Desktop Optimizations

The virtual desktop optimizations provide the endpoint device with a media engine and redirect the audio and video streams so that they are exchanged directly between the endpoint devices. This results in higher performance and a lower server load.

#### For Citrix Sessions

- Skype for Business; for configuration, see the chapter [Skype for Business](#)(see page 796) in the [IGEL OS Reference Manual](#)(see page 750).
- Cisco Jabber (JVDI Client); for configuration, see the chapter [Cisco](#)(see page 796) in the [IGEL OS Reference Manual](#)(see page 750).



- Cisco WebEx Teams and Cisco WebEx Meetings; for configuration, see the chapter [Cisco](#)(see page 796) in the [IGEL OS Reference Manual](#)(see page 750).
- Microsoft Teams; for configuration, see the chapter [VDI Solutions](#)(see page 795) in the [IGEL OS Reference Manual](#)(see page 750).
- Zoom Media Plugin; for configuration, see the chapter [VDI Solutions](#)(see page 795) in the [IGEL OS Reference Manual](#)(see page 750).

#### For Horizon Sessions

- Skype for Business; for configuration, see the chapter [Skype for Business](#)(see page 859) in the [IGEL OS Reference Manual](#)(see page 750).
- Cisco Jabber (JVDI Client); for configuration, see the chapter [Cisco](#)(see page 859) in the [IGEL OS Reference Manual](#)(see page 750).
- Cisco Teams

#### Local Installation on the Endpoint Device with a Custom Partition

In contrast to the virtual desktop optimizations, where the Unified Communication apps are installed on the VDI server, this approach involves installing the apps on the endpoint device. This is achieved by using the Custom Partition mechanism of IGEL OS.

For building a Custom Partition by yourself, see the [Custom Partition Tutorial](#)(see page 529).

You can acquire any of the following Custom Partitions free of cost; ask contact your IGEL contact:

- TeamViewer
- Zoom (see also [Zoom as a Custom Partition](#)(see page 558) in the [Custom Partition Tutorial](#)(see page 529))

#### 2.26.4 Passthrough Authentication

Passthrough authentication is a convenient single sign-on method. With this function, an IGEL user logs in once and gains access to all sessions without having to explicitly authenticate themselves again for each of them.

This document explains what basic settings are necessary for passthrough authentication and where you can enable the single sign-on method in the relevant sessions.

- [Introduction](#)(see page 730)
- [Basic configuration](#)(see page 732)
- [Session Configuration](#)(see page 735)

#### Introduction

Two methods of single sign-on for a session are available:

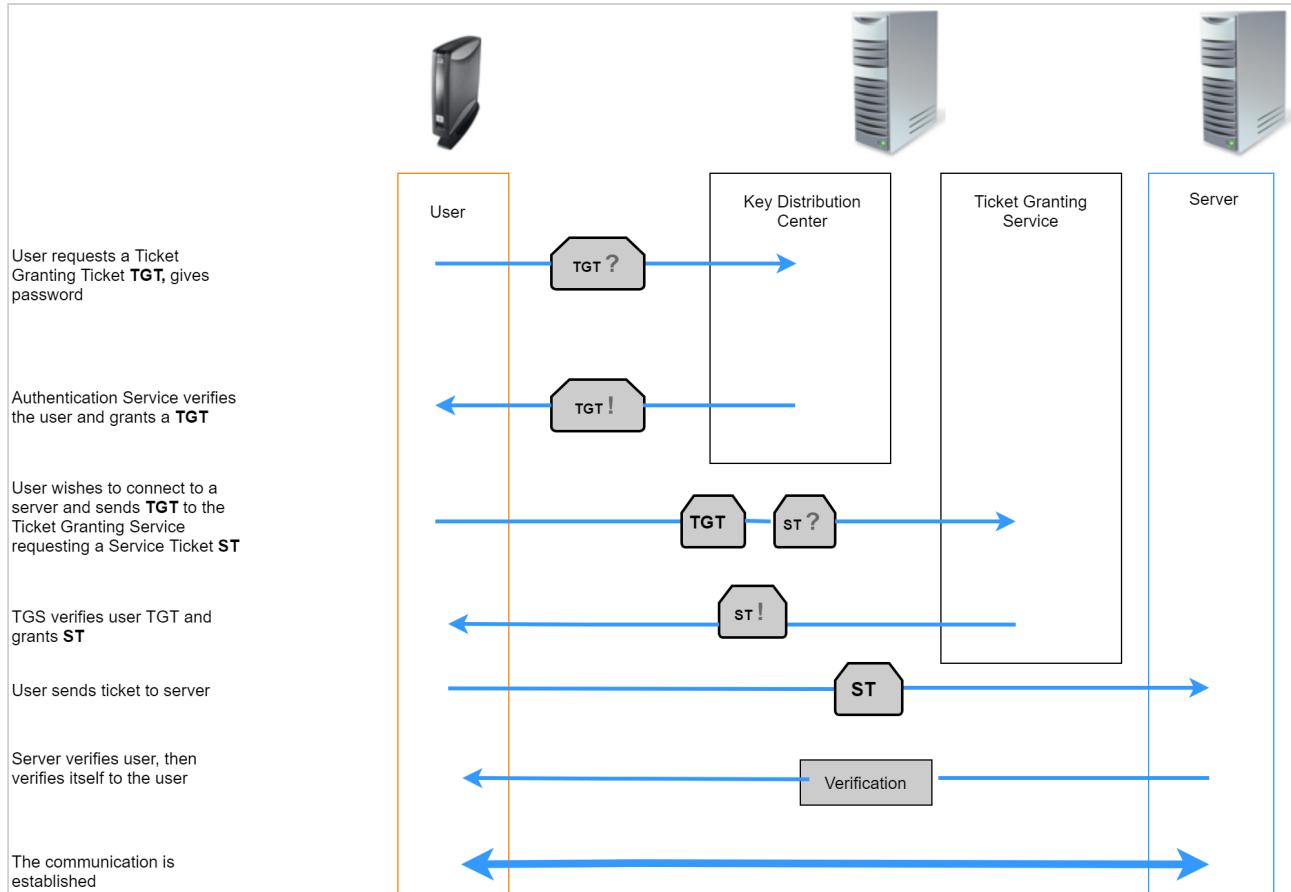


|                      |                                                                                                                                                                                                                                             |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kerberos Passthrough | <p>Real Kerberos authentication with clients that support Kerberos.</p> <p>Within a session, you can access network resources, e.g. file servers, without having to authenticate yourself again; this works automatically via Kerberos.</p> |
| Passthrough          | <p>Uses cached credentials (user name and password) from local log-on for authentication.</p> <p>For access to network resources within sessions, you have to enter your credentials again.</p>                                             |

Kerberos is an authentication service. It operates with user, service and computer entities which are known as **principals**. These principals all belong to a **realm**, an administrative unit. Each principal has a unique **principal name** within the realm. To provide the authentication system, a service known as **key distribution center** is used.

As an example, Microsoft Windows Domains form a realm. The Windows Domain name is the realm name (in upper case letters), e.g. EXAMPLE.COM. A user principal would be for example user@EXAMPLE.COM. The domain controllers take on the role of the key distribution centers.

When logging in, a user obtains a **ticket granting ticket** from the key distribution center. This ticket expires after a certain time (usually 1 day). When the user starts an ICA session for example, the client can obtain a so-called **service ticket** from the key distribution center with the aid of the ticket granting ticket. With this service ticket, authentication for the ICA server is accomplished.



To enable passthrough authentication you have to make certain settings:

1. [Modify certain basic settings which are necessary to fulfill the conditions for Kerberos passthrough authentication.\(see page 732\)](#)
2. [Enable passthrough authentication in the relevant session.\(see page 735\)](#)

## Basic configuration

Your client configuration must fulfill certain conditions before you can enable passthrough authentication.

- [Set the time correctly on all involved hosts and clients.\(see page 732\)](#)
- [Configure the domain.\(see page 733\)](#)
- [Activate login to the Active Directory domain.\(see page 734\)](#)

When activating the **Smartcard** login method, [some additional configuration may be necessary\(see page 734\).](#)

## Time

The time must be set correctly on all involved hosts and clients.



The best practice procedure is as follows:

1. Activate **Use NTP Time Server** under **System > Time and Date** in the setup.
2. Specify the **NTP Time Server**.

A Windows domain controller can be used for this, if applicable.

## Domains/Realms

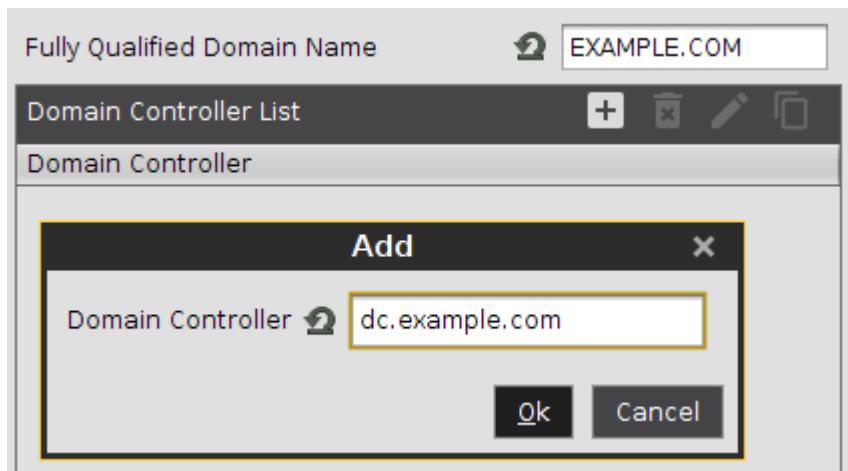
To configure the domain(s) proceed as follows:

1. Click **Security > Active Directory/Kerberos**.
2. Activate **enable** to enable Kerberos.
3. Enter the fully qualified domain name under **Default Domain**, e.g. EXAMPLE.COM (upper case letters).
4. Enable **DNS Lookup for Domain Controller** and **DNS Lookup for Domain**.

These settings are sufficient for the domain setup when the DNS servers, e.g. the domain integrated MS DNS servers, are aware of the Active Directory.

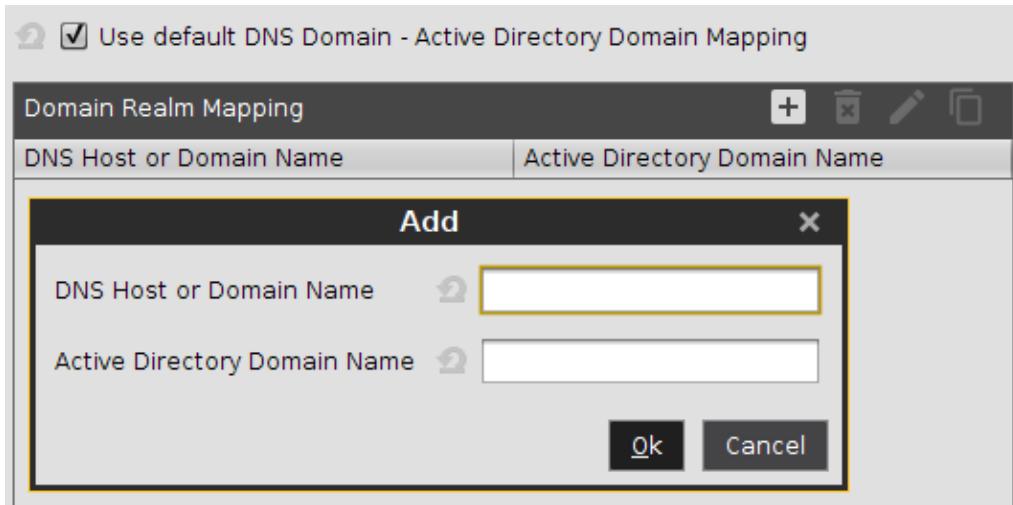
Otherwise you may configure up to 4 domains/realms:

1. Click **Security > Active Directory/Kerberos > Domain1...4**.
2. Enter the **fully qualified domain name**, e.g. EXAMPLE.COM (upper case letters).
3. Specify at least one Windows domain controller (Kerberos key distribution center) in the **Domain Controller List**.  
It can be a DNS name or an IP address.



4. Click **Security > Active Directory/Kerberos > Domain Realm Mapping** to define the mapping between Active Directory domain names and DNS names.

## 5. Activate **Use default DNS Domain - Active Directory Domain Mapping**.



If both names match, i.e. if a host in the domain EXAMPLE.COM has the DNS name host.example.com, nothing needs to be done here and the default setting is sufficient. Otherwise an appropriate entry in the **Domain Realm Mapping** list has to be created.

### Login

1. Click **Security > Logon > Active Directory/Kerberos**.
2. Activate **Login to Active Directory Domain**.
3. Choose one or more of the following login options:
  - **Explicit**: A login dialog is presented to the user.
  - **Remember last user name**: The login dialog will be prepopulated with the last user name that logged in. This option can be checked for convenience if **Explicit Login** is selected.
  - **Smartcard**: Login with smartcard and related smartcard PIN.
4. Underneath **Logout Shortcut Locations**, specify where a log-out button will appear.

### Smartcard

For using the **Smartcard** login method, some additional configuration is necessary:

1. Under **Security > Login > Active Directory/Kerberos**, activate **Smartcard**.
2. Under **Smartcard removal action**, define what should happen when the smartcard is removed:
  - **Log out**: Performs a disconnect or log out of running sessions, removes all user related data from the device and prepares the device for the next user login.
  - **Lock device**: Locks the screen during sessions. Only the user who is already logged in can unlock the device with his smartcard and PIN. Additionally, select **User password** under **User Interface > Screenlock / Screensaver > Options**, to make the setting effective.
3. Choose an appropriate PKCS#11 module under **Security > Smartcard > Middleware > Custom PKCS#11 module**.



The smartcards for this login must be supported by a PKCS#11 module which can access the certificates on the smartcard.

Kerberos login with a smartcard involves certificates. The root certificate of the certificate used by the key distribution center (domain controller) must therefore be available on the device. Either the root certificate is one of the public trusted certificate authorities or it must be deployed to the device, see [Deploying Trusted Root Certificates](#)(see page 470).

When using Windows 2000 or Windows Server 2003-based domain controllers in combination with smartcard login, the parameter auth.krb5.realms.pkinit.pkinit\_win2k has to be activated in the registry. This enables the use of an earlier protocol version of PKINIT preauthentication.

## Kerberos Ports

The following Kerberos ports are relevant for Linux environments:

|                                           | UDP Port | TCP Port |
|-------------------------------------------|----------|----------|
| Getting tickets including the initial TGT | 88       | 88       |
| Changing password from UNIX/Linux         |          | 749      |

## Session Configuration

For single sign-on with sessions, two methods are available:

- **Kerberos Passthrough:** Uses real Kerberos authentication with clients that support Kerberos.
- **Passthrough:** Uses cached user name and password from local logon for authentication.

Currently, real Kerberos authentication is only available in Citrix sessions.

In the following sections, you can find how to activate passthrough authentication in sessions that support it:

- [Citrix StoreFront/Web Interface](#)(see page 735)
- [RDP](#)(see page 736)
- [Horizon Client](#)(see page 736)
- [Parallels Client](#)(see page 736)

### Citrix StoreFront/Web Interface

1. Go to **Sessions > Citrix > Citrix Global > StoreFront Login.**



## 2. Select the **Authentication type**:

- **Password authentication:** To enable passthrough, this option must be selected, and **Use Passthrough authentication** must be activated.
- **Kerberos passthrough authentication:** This will only work with Web Interface, not with StoreFront.
- **Smartcard authentication (StoreFront only, not Web Interface):** Authentication via smartcard will only work with StoreFront, not with Web Interface.
- **Citrix authentication mechanism (instead of IGEL), Smartcard disabled**
- **Citrix authentication mechanism (instead of IGEL), Smartcard enabled**

See also [StoreFront Login\(see page 777\)](#).

### RDP

For RDP sessions, passthrough is supported. Kerberos passthrough is not yet supported.

1. Go to **Sessions > RDP > RDP Sessions > [session name] > Logon**.
2. Enable **Use passthrough authentication for this session**.

### Horizon Client

For Horizon sessions, passthrough is supported. Kerberos passthrough is not yet supported.

1. Go to **Sessions > Horizon Client > Horizon Client Sessions > [session name] > Connection settings**.
2. Enable **Use passthrough authentication for this session**.

### Parallels Client

For Parallels Client sessions, passthrough is supported. Kerberos passthrough is not yet supported.

1. Go to **Sessions > Parallels Client > Parallels Client Sessions > [session name] > Connection**.
2. Enable **Use system credentials** to use the passthrough authentication.

## 2.26.5 Hardware Video Acceleration on IGEL OS

### Question

Does my hardware with IGEL OS offer video acceleration?

### Answer

Open **Application Launcher > About** to look up your product ID and device type:



**Application Launcher**

**IGEL WORKSPACE**

**Product**

|                       |                                                         |
|-----------------------|---------------------------------------------------------|
| Copyright             | IGEL Technology GmbH                                    |
| Firmware Release Date | Mittwoch, 5. August 2020                                |
| Firmware Version      | 11.04.100.01                                            |
| Product ID            | UD3-LX 51                                               |
| Product Name          | IGEL OS 11                                              |
| Website               | <a href="https://www.igel.com">https://www.igel.com</a> |

**License Information**

|                                                   |                                 |
|---------------------------------------------------|---------------------------------|
| Workspace Edition Maintenance Expiration Date     | ✓ Freitag, 12. März 2021        |
| Enterprise Management Pack Expiration Date        | ✓ Freitag, 12. März 2021        |
| Workspace Edition Add-on Teradici Expiration Date | ✓ Donnerstag, 3. September 2020 |

**Network**

|                            |                 |
|----------------------------|-----------------|
| Local Name                 | ITC00E0C520986A |
| Default gateway            | ✓               |
| DNS Server 1               | ✓               |
| DNS Server 2               | ✓               |
| Universal Management Suite | ✓               |

**Interface 1 (eth0)**

|                  |                                                           |
|------------------|-----------------------------------------------------------|
| Description      | Realtek Semiconductor Co., Ltd.                           |
| Hardware Address | RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller |
| IP Address       | 00:E0:C5:20:98:6A                                         |

**Hardware**

|                  |                                                        |
|------------------|--------------------------------------------------------|
| Boot Mode        | EFI                                                    |
| CPU Model        | AMD GX-424CC SOC with Radeon(TM) R5E Graphics (4 CPUs) |
| Device Type      | IGEL M340C                                             |
| Flash Size       | 3761 MB                                                |
| Graphics Chipset | ATI MULLINS                                            |

In version 5.07.100 and newer and version 10.01.100 and newer, IGEL OS offers hardware video acceleration for

- Media Player
- Citrix Multimedia Redirection
- RDP Multimedia Redirection (TSMF and EVOR)
- VMware Horizon Multimedia Redirection

on selected devices. This allows playing back HD video with a maximum of 20% CPU usage.

The Multimedia Codec Pack (MMCP) is required for this feature if your IGEL OS version is lower than 11.01.100.



Hardware video acceleration is supported on the following IGEL devices:

| <b>Product ID</b>                            | <b>Device Type</b>                 | <b>Chipset</b>             | <b>IGEL Linux &gt;= v5.07.100</b> | <b>IGEL Linux &gt;= v5.09.100</b> | <b>IGEL OS 10</b> | <b>IGEL OS 11</b> |
|----------------------------------------------|------------------------------------|----------------------------|-----------------------------------|-----------------------------------|-------------------|-------------------|
| IZ2-HDX/RFX/<br>HORIZON<br>40*(see page 739) | IGEL D220                          | Intel Bay Trail            | ✓                                 | ✓                                 | ✓                 | ✓*(see page 739)  |
| IZ3-HDX/RFX/<br>HORIZON 41,<br>42            | IGEL M330C                         | VIA VX900                  | ✓                                 |                                   |                   |                   |
| IZ3-HDX/RFX/<br>HORIZON<br>50*(see page 739) | IGEL M340C                         | ATI Mullins                |                                   | ✓                                 | ✓                 | ✓*(see page 739)  |
| IZ3-HDX/RFX/<br>HORIZON<br>51*(see page 739) | IGEL M340C                         | ATI Mullins                |                                   |                                   | ✓                 | ✓*(see page 739)  |
| UD2-LX 40                                    | IGEL D220                          | Intel Bay Trail            | ✓                                 | ✓                                 | ✓                 | ✓                 |
| UD2-LX 50, 51                                | IGEL M250C                         | Intel HD Graphics          |                                   |                                   |                   | ✓                 |
| UD3-LX 40                                    | IGEL M320C                         | VIA VX900                  | ✓                                 | ✓                                 |                   |                   |
| UD3-LX 41, 42                                | IGEL M330C                         | VIA VX900                  | ✓                                 | ✓                                 |                   |                   |
| UD3-LX 50                                    | IGEL M340C                         | ATI Mullins                |                                   | ✓                                 | ✓                 | ✓                 |
| UD3-LX 51                                    | IGEL M340C                         | ATI Mullins                |                                   |                                   | ✓                 | ✓                 |
| UD3-LX 60                                    | IGEL M350C                         | AMD Radeon Vega 3 Graphics |                                   |                                   |                   | ✓                 |
| UD5-LX 40                                    | IGEL H820C                         | Intel Sandy Bridge         | ✓                                 | ✓                                 | ✓                 |                   |
| UD5-LX 50                                    | IGEL H830C<br>(Dualcore CPU Model) | Intel Bay Trail            | ✓                                 | ✓                                 | ✓                 | ✓                 |
| UD6-LX 51                                    | IGEL H830C<br>(Quadcore CPU Model) | Intel Bay Trail            | ✓                                 | ✓                                 | ✓                 | ✓                 |



| Product ID                       | Device Type        | Chipset                    | IGEL Linux >= v5.07.100 | IGEL Linux >= v5.09.100 | IGEL OS 10 | IGEL OS 11 |
|----------------------------------|--------------------|----------------------------|-------------------------|-------------------------|------------|------------|
| UD7-LX 10                        | IGEL H850C         | AMD Radeon Graphics        |                         |                         | ✓          | ✓          |
| UD7-LX 11                        | IGEL H850C         | AMD Radeon Graphics        |                         |                         |            | ✓          |
| UD7-LX 20                        | IGEL H860C         | AMD Radeon Vega 8 Graphics |                         |                         |            | ✓          |
| UD9-LX 40,<br>UD9-LX 41<br>Touch | IGEL UD9 BT        | Intel Bay Trail            |                         | ✓                       | ✓          | ✓          |
| UD10-LX                          | IGEL UD10<br>TC236 | VIA VX900                  | ✓                       | ✓                       |            |            |

On 3rd-party hardware with UDC3, IGEL OS Creator (OSC), and UD Pocket, hardware video acceleration depends on the graphics chipset of the device.

## Codecs

The following codecs are supported:

- MPEG-2 (simple and main profiles)
- H.264 (baseline, main and high profiles)
- WVC1/WMV3 (simple, main and advanced profiles)
- MPEG-4 (DivX/Xvid): only on VIA VX900 and ATI Mullins

\* To upgrade your IZ device to IGEL OS 11, please contact your IGEL sales representative. See also <https://www.igel.com/tradeup/> and [The IGEL OS 11 Trade-Up](#)<sup>239</sup>.

## 2.26.6 Running Commands before or after a Session

### Symptom

You want to run shell commands before a specific session is started or after it has terminated.

### Problem

You need hooks which will call your shell commands.

### Solution

---

<sup>239</sup> <https://kb.igel.com/display/licensesmoreigelos11/The+IGEL+OS+11+Trade+up>



As of *IGEL Universal Desktop Linux 5.06.100* there is a generic mechanism for calling shell commands before and after a session. It works with Citrix ICA, RDP and VNC Viewer sessions.

This feature is accessible only through the **Registry**.

Open **Setup** at **System > Registry**. Use either the Registry tree or the **Search parameter ...** function to locate the following Registry keys:

for VNCviewer:

```
sessions.vncviewer*.init_action  
sessions.vncviewer*.final_action
```

for RDP:

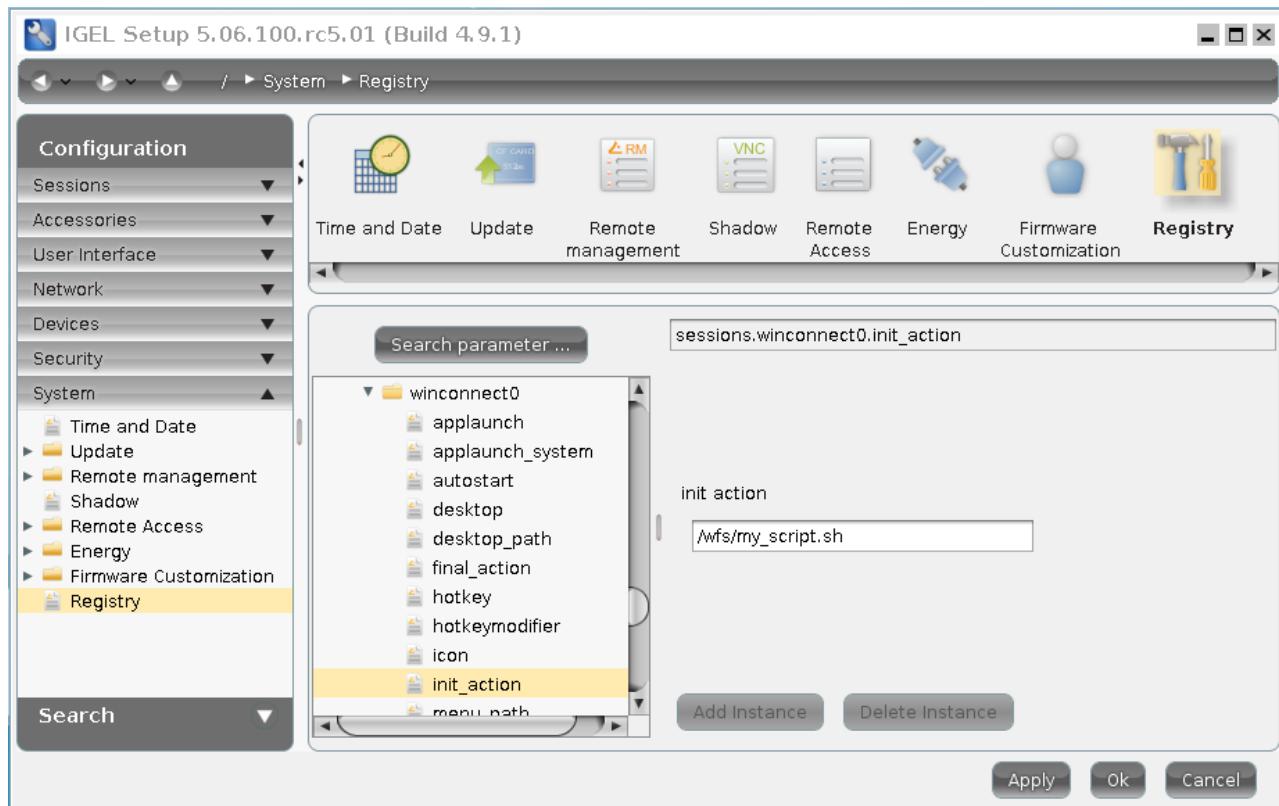
```
sessions.winconnect*.init_action  
sessions.winconnect*.final_action
```

for Citrix/ICA:

```
sessions.ica*.init_action  
sessions.ica*.final_action
```

(where \* is the related session number, e.g. 0,1,2,3,...)

The **init\_action** is executed before the session is started. The **final\_action** is executed after the session has been terminated. Enter shell commands or the path to a custom script or executable:



The Registry keys for newly created sessions only appear after a restart of **Setup**.

Your `init_action` scripts or executables have to return before the session will start. Alternatively, background your command by adding '`&`' to the end of the commandline.

## 2.26.7 Copy Sessions in Setup or UMS

Sometimes you want to create a session that differs from another only in a few details. *IGEL Linux version 5.10.100* or newer and *UMS version 5.02.100* or newer let you copy complete sessions. Once the session is copied, you can easily adapt the required settings.

Copying is available in the **Sessions** section of *IGEL Setup* (and occasionally in some other sections) as well as in the **Edit Configuration** function in *UMS*.

To copy a session, proceed as follows:

1. In the setup, open the menu path **Sessions > [Session Type] > [Session Type] Sessions**.  
Example: **Sessions > RDP > RDP Sessions**  
The existing sessions are shown.
2. Highlight the session that you want to copy.



3. Click .

A copy of the session will be created within the same folder.

## 2.26.8 IZ1 and UD2-MM Usage of RAM

How is RAM used by processes in UD2-MM and IZ1 (also known as ARM or SoC devices)?

A total of 1024 MB main memory is divided as follows:

- ~128 MB is used for graphics
- ~362 MB is used for internal processes such as communication between DSP and ARM processor
- ~534 MB is available for user processes

## 2.26.9 Using Symantec Ghost to Deploy IGEL OS

### **Solution Based on Experience from the Field**

This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

**Topic of discussion/Issue**

Using Symantec Ghost to Deploy IGEL OS

**Firmware version**

OS10 and OS11 (11.02.100)

**UMS version**

6.01

**Description**

This is in lieu of SCCM and our Deployment Appliance

**Solution**

We are deploying and capturing our IGEL base installation to/from a virtual machine using:

**vSphere Client 6.0, version 11 VM:**



- 8 GB RAM
- 4 CPUs (1 socket, 4 cores)
- Video: 1 display, 4 MB memory
- SCSI Controller Type: LSI Logic SAS
- CD/DVD Drive 1: IGEL\_UDC\_10.05.500.ISO
- CD/DVD Drive 2: Symantec WinPE
- HDD: SCSI, Thick Provision Lazy Zeroed, 20 GB
- Network Adapter: VMXNET 3
- Boot Options/Firmware: EFI

**Boot to CD/DVD drive 1 and navigate through the UDC installation options:**

- UDC Installation
- Language: English
- EULA: I Agree
- Force Legacy Installation: Not selected
- Force MS-DOS partitioning during installation: Selected
- Migrate old settings: Not selected
- Install Firmware
- Shutdown (do NOT reboot)

**Boot to CD/DVD drive 2:**

- Boot to WinPE
- Capture HDD image using Ghost command: `ghost64.exe -sure -clone,mode=create,src=1,dst=s:\igel\igel 10.05.500-YYYYMMDD_HHMMSS-0.gho -ial -ibg -nolilo`
  - -ial = Forces a sector-by-sector copy of Linux partitions. Other partitions are copied normally.
  - -ibg = Ignore Ghost Boot partition.
  - -nolilo = Does not attempt to patch the LILO or GRUB boot loader after a clone. If you use the -NOLILO switch, you can restart your computer from a storage device after a clone and then run /sbin/lilo or GRUB install script as the root user to reinstall the boot loader.

**To deploy to a physical client:**

- Boot to WinPE
- Execute Diskpart:
  - select Disk 0
  - clean
  - exit
- Deploy HDD image using Ghost command: `ghost64.exe -sure -clone,mode=restore,dst=1,src=s:\igel\igel 10.05.500-20190510_185741-0.gho -ial -ibg -nolilo`
  - -ial = Forces a sector-by-sector copy of Linux partitions. Other partitions are copied normally.
  - -ibg = Ignore Ghost Boot partition.
  - -nolilo = Does not attempt to patch the LILO or GRUB boot loader after a clone. If you use the -NOLILO switch, you can restart your computer from a storage device after a clone and



then run `/sbin/lilo` or the GRUB install script as the root user to reinstall the boot loader.

- `-szee` = Forces Norton Ghost to keep the sizes of all destination partitions the same as in the source partition (no resizing).

We don't do any image prep other than the `diskpart clean` command.

### 2.26.10 Starting UMS Console Crashes NX Session

#### Symptom:

When you are connected to an Ubuntu host via NX, starting UMS console on the Ubuntu host crashes the NX session.

#### Solution:

1. Become **Root** on the Ubuntu host.
2. Open the configuration file `/opt/IGEL/RemoteManager/rmclient/RemoteManager.bin.config` in a text editor.
3. Add the line `vmparam -Dsun.java2d.xrender=false` to the file.
4. Save the file.
5. Become a regular user.
6. Start UMS Console.

### 2.26.11 Accessing IGEL Setup within Appliance Mode

#### Symptom

When using the appliance mode, IGEL Setup is not accessible directly.

#### Problem

Within the appliance mode, all other local applications are hidden; the system's hotkey [Ctrl+Alt+s] does not work either.

#### Solution

To start the IGEL Setup within the appliance mode, press hotkey [Ctrl+Alt+F2].

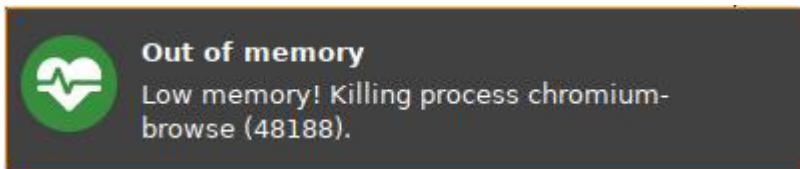


## 2.26.12 Application Is Terminated with Message "Low memory! Killing process ..."

### Symptom

A local application or session is killed, and a message that reads **Low memory! Killing process [...]** is shown.

Example:



### Environment

- IGEL OS 11.04 or higher

### Problem

The system is running out of memory. As a countermeasure, the system has terminated the application.

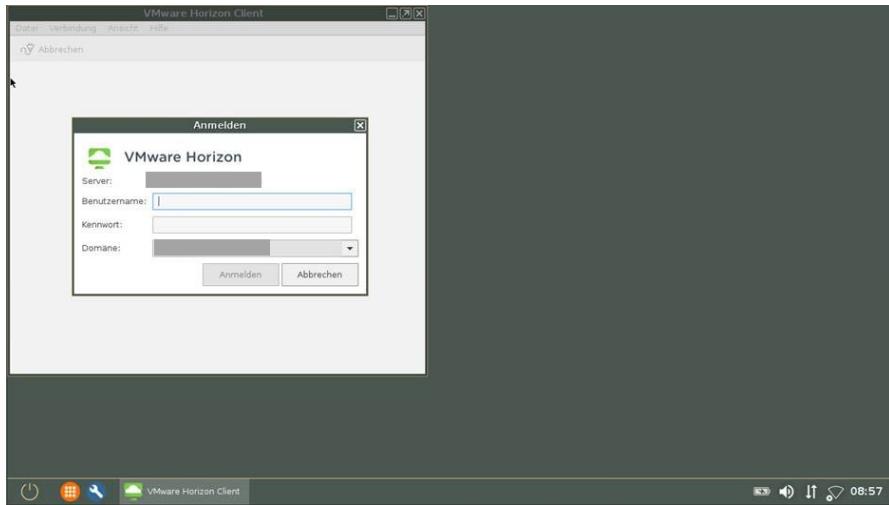
### Solution

- ▶ Close other applications that are not needed and restart the application.
- ▶ If the terminated application is Chromium or Firefox, restart it and try using fewer open tabs.
- ▶ If the issue occurs often, consider extending the memory size of the devices.

## 2.26.13 An Application Window Cannot Be Repositioned

### Symptom

Some application windows, e.g. VMware Horizon windows, are placed at startup in the upper left corner instead of being displayed in the middle. In case of frameless applications, the window cannot then be moved and may conceal the icons.



## Problem

Either the screen is too small or the selected resolution is too low.

## Solution

1. Go to **System > Registry**.
2. Select the registry key `windowmanager.wm0.variables.placement_ratio`.
3. Specify a higher percentage value under **Maximum window size for which the preferred placement should apply**. This entry refers to the total work area.

The preferred placement is defined with the registry key `windowmanager.wm0.variables.placement_mode`.



The screenshot shows the IGEL Configuration software interface. The left sidebar has a tree view with 'Configuration' expanded, showing 'Sessions', 'Accessories', 'User Interface', 'Network', 'Devices', 'Security', 'System' (with 'Time and Date', 'Update', 'Remote management', 'Remote Access', 'Remote Syslog', 'Power Options', 'Firmware Customization', and 'Registry' listed), and a 'Search' field. The main area shows a registry key 'windowmanager.wm0.variables.placement\_ratio' selected in the search bar. Below it, a dropdown menu titled 'Maximum window size for which the preferred placement should apply.' lists percentage values from 20% to 100%, with '20%' highlighted. At the bottom right are 'Apply', 'Ok', and 'Cancel' buttons.

## Example

Session: VMware Horizon Client

Screen resolution: 1366x768

Value for **Maximum window size for which the preferred placement should apply:** at least 40%

## 2.26.14 Updating IGEL UMD: Error "not compatible with System5"

### Symptom

Universal Multi Display firmware (IGEL UMD) can't be updated to version 4.13.100.

Error Message:

```
Firmware not compatible.
dmx_networkd: Slave #0 (MAC) not compatible with System5
```



Fehler: Die neue Firmware ist nicht mit diesem Gerät kompatibel.

▽ Mehr Details

Fehler: Die neue Firmware ist nicht mit diesem Gerät kompatibel.

dmx\_networkd: Slave #0 (00:E0:C5:3E:C5:5D) not compatible with System 5  
Error: Firmware update failed.

Fehler: Die neue Firmware ist nicht mit diesem Gerät kompatibel.

## Solution

Delete file /tmp/NOT\_SYS\_5\_COMPATIBLE from UMD master client and update again without rebooting.

### 2.26.15 Using Natural Scrolling (reverse Scrolling Direction)

#### Issue

You are using a touchpad instead of a mouse and you want to reverse the scrolling direction to have natural scrolling – with the screen content moving synchronously to the fingers' movement on the touchpad.

#### Problem

There is no "reverse scrolling" parameter in IGEL Setup.

#### Solution

1. Open the device's configuration either locally or in the UMS.
2. Go to **System > Firmware Customization > Custom Commands > Desktop > Final desktop command.**
3. Enter the following command:  

```
echo "pointer = 1 2 3 5 4 6 7 8 9 10 11 12" > ~/.Xmodmap && xmodmap  
~/.Xmodmap
```
4. Save the settings and restart your device.

This will reverse the scrolling direction of a mouse wheel as well. Swapping 4 and 5 will reverse vertical scrolling, swapping 6 and 7 will reverse horizontal scrolling as well (if supported).



## 2.26.16 IGEL Third-party Endpoint Partners: Ensuring Image Integrity with a Checksum

### Overview

To ensure the integrity of your master image, it is recommended to create checksums and compare them between the original image and the images derived from it. This article describes how to create checksums for IGEL OS images that have been created using the IGEL OS Creator (OSC).

### Requirements

- IGEL OS Creator (OSC) with IGEL OS 11.05.120 or higher

### Instructions

For IGEL OS images that have been created with IGEL OSC Creator (OSC), partition 4 of the main device must be checked with the checksum method.

In the following example, the main device is /dev/sda:

1. Open a terminal on the device that contains the image. For more information, see [Terminals\(see page 1042\)](#).
2. In the terminal, enter `sha512sum /dev/sda4`  
The result should look like this:  
`7d5a25fac1756ef81ac78398d49db197904f60a0cf6594eac92071a5f6a8d6d4562fd3c8dc12  
7cf22f89f6894000ca94918703c7143fb11f1dd2ec052eaa52d /dev/sda4`
3. Repeat this process for all IGEL OS image copies you want to check and compare their checksums.  
If the checksums are identical, the images can be deployed.



## 3 IGEL OS Reference Manual

- [What Is New in 11.06.100?\(see page 750\)](#)
- [IGEL Workspace Edition\(see page 753\)](#)
- [Bluetooth Assistant\(see page 756\)](#)
- [Setup Assistant\(see page 757\)](#)
- [Boot Procedure\(see page 762\)](#)
- [The IGEL OS Desktop\(see page 765\)](#)
- [Setup\(see page 772\)](#)
- [Sessions\(see page 774\)](#)
- [Accessories\(see page 1038\)](#)
- [User Interface\(see page 1142\)](#)
- [Network\(see page 1171\)](#)
- [Devices\(see page 1215\)](#)
- [Security\(see page 1235\)](#)
- [System\(see page 1251\)](#)

### 3.1 What Is New in 11.06.100?

The release notes for the latest release of IGEL OS 11.06.100 can be found on our download server at [www.igel.com/software-downloads/workspace-edition/](https://www.igel.com/software-downloads/workspace-edition/)<sup>240</sup> as well as in the Knowledge Base under [Notes for Release 11.06.100\(see page 1422\)](#).

#### 3.1.1 Login with Local User Password

Authentication with a local user password upon device startup can now be activated in the Setup under **Security > Logon > Local User**, see [Local User\(see page 1246\)](#). The feature can also be activated during the initial configuration via the Setup Assistant, see [Local Logon\(see page 759\)](#).

#### 3.1.2 Names of Ethernet and WLAN Interfaces Changed

Names of Ethernet and WLAN interfaces have been changed. Apart from some symbolic occurrences, "eth0", "eth1", and "wlan0" have been replaced by so-called predictable network interface names. See "Predictable Network Interface Names (PNINs)" under [LAN Interfaces\(see page 1172\)](#).

#### 3.1.3 Automatic Switch between LAN/Wi-Fi

If you have to frequently switch between LAN and WLAN networks, it is now possible to activate **Enable Wi-Fi automatic switch** under **Network > LAN Interfaces > Wireless**, see [Wireless\(see page 1178\)](#).

---

<sup>240</sup> <https://www.igel.com/software-downloads/workspace-edition/>



### 3.1.4 Support for EAP-FAST

You can now select "FAST" as EAP type and specify an anonymous identity and the way the PAC (Protected Access Credential) is delivered to the client. For details, see [Authentication](#)(see page 1175) and [Default Wi-Fi Network](#)(see page 1182).

### 3.1.5 Proxy Settings

It is now possible to set up automatic proxy configuration and activate client-side NTLM authenticating proxy, see [Proxy](#)(see page 1214).

### 3.1.6 A Post-Session Command for Multiple Sessions

You can now define a post-session command for multiple session types, see [Post Session](#)(see page 1272).

### 3.1.7 Remote Management

The timeout for the "Apply changes" dialog is now 20 seconds by default. If the timeout is exceeded, the received settings will be automatically applied. The behavior is configurable under **System > Remote management > Timeout**, see [Remote Management](#)(see page 1254).

### 3.1.8 AVD: CUPS Printer Redirection

CUPS printers configured under **Devices > Printer > CUPS > Printers** can now be redirected to the AVD (former "WVD") session. See [CUPS Printer Redirection](#)(see page 1023).

### 3.1.9 TLS Encryption for Remote Syslog

For remote syslog, you can now activate the TLS encryption and configure the CA root certificate, see [Logging](#)(see page 1259). See also [Logging and Log Evaluation](#)<sup>241</sup>.

### 3.1.10 AppliDis Sessions

The AppliDis Client has been integrated, see [AppliDis](#)(see page 875).

### 3.1.11 Amazon WorkSpaces Sessions

The Amazon WorkSpaces Client has been integrated, see [Amazon WorkSpaces](#)(see page 1026).

---

<sup>241</sup> <https://kb.igel.com/display/securitysafety/Logging+and+Log+Evaluation>



### 3.1.12 Parallels Client

Some configuration options for Parallels Client sessions have been added or updated, see [Display](#)(see page 912), [Local Resources](#)(see page 913), and [Experience](#)(see page 914).

### 3.1.13 Imprivata

- It is now possible to ignore the VMware protocol selected by the Imprivata appliance and to use the local selection, instead. See [Imprivata: Session Customization](#)(see page 323).
- There is now a registry key for setting a default AD domain for PIE agent, see "Useful Registry Keys" under [Imprivata](#)(see page 872).

### 3.1.14 RD Web Access

It is now possible to save the username and domain from the last login, see [Authentication](#)(see page 842).

### 3.1.15 Chromium Browser

- The Chromium browser can now be configured to wait for a network connection before it starts automatically. See [Desktop Integration](#)(see page 992).
- The redundant **Incognito mode** switch has been removed; see [Privacy](#)(see page 985).
- File access (download and upload) has been optimized; see [Security](#)(see page 987).

### 3.1.16 Device Encryption

IGEL OS 11.06 or higher offers strong device encryption that is derived from a user password. For details, see [How to Deploy Device Encryption](#)(see page 452) and the manual chapter [Device Encryption](#)(see page 1235).

### 3.1.17 Security: Timeout for Port 30022 (Secure Shadowing and Secure Terminal)

To avoid a denial of service attack by blocking port 30022, which is used for secure shadowing (secure VNC) and secure terminal connections, a timeout can be configured. For details, see [Security: Timeout for Secure Shadowing and Secure Terminal](#)(see page 456).

### 3.1.18 Configurable Default Web Browser

You can define which browser will be chosen by the system, e.g. for opening Citrix Storefront. See [Chromium Browser Global](#)(see page 982) and [Firefox Browser Global](#)(see page 957).

### 3.1.19 Conky System Monitor Added

The Conky system monitor displays current system data such as uptime, CPU frequency, RAM usage, and process-specific data. For details, see [Conky System Monitor](#)(see page 1136).



### 3.1.20 Suppressing Enterprise Management Pack Expiration Warnings

To prevent your users from being distracted by warnings about Enterprise Management Pack license expiry, you can suppress these warnings. For details, see [How Can I Suppress Enterprise Management Pack Expiration Warnings?](#)<sup>242</sup>

### 3.1.21 Zoom Client Selection

You can select the Zoom client version to be used for the Zoom VDI Media Plugin. For details, see [Zoom Client Selection](#)(see page 1037).

### 3.1.22 Cisco WebEx Meetings VDI Client Selection

You can select the desired client version to be used for Cisco WebEx Meetings VDI. For details, see [Cisco WebEx Meetings VDI Selection](#)(see page 1037).

### 3.1.23 Wildcard in Horizon Client USB Redirection Rules

You can use a wildcard symbol in device rules. For details, see [USB Redirection](#)(see page 851).

### 3.1.24 Registry Parameters for Fixing Touchpad Issues

Some touchpad issues can be solved by adding or modifying parameters for the device driver. For usability, the parameter modifications are now accessible via the Registry of the IGEL Setup; see [How Can I Fix Touchpad Issues?](#)(see page 710)

### 3.1.25 Automatic Update Service for Evaluation Purposes

The automatic update service checks for available firmware updates periodically. The service is available for devices with an evaluation license. For details, see [IGEL OS Automatic Update Service for Device Evaluation](#)(see page 237).

## 3.2 IGEL Workspace Edition

IGEL devices comprise the latest hardware and an embedded operating system based on IGEL Linux.

The firmware included with every IGEL Workspace product is multifunctional and contains a wide range of protocols allowing access to server-based services.

Management software: Universal Management Suite

For optimum management of your IGEL devices, the IGEL Universal Management Suite (UMS) is available on our [download page](#)<sup>243</sup>.

---

<sup>242</sup> <https://kb.igel.com/pages/viewpage.action?pageId=45415669>

<sup>243</sup> <https://www.igel.com/software-downloads/igel-universal-management-suite/>



With the IGEL Universal Management Suite, you can configure devices in the same way as in the devices' local setup.

- [Supported Formats and Codecs](#)(see page 754)
- [IGEL Devices Supported by IGEL OS 11](#)(see page 755)

### 3.2.1 Supported Formats and Codecs

As supplied, *IGEL Linux* supports the following multimedia formats and codecs:

- Ogg/Vorbis
- Ogg/Theora
- WAV
- FLAC

The following codecs can be added with the optional [Multimedia Codec Pack](#)<sup>244</sup>:

| Supported formats:           | Supported codecs: |
|------------------------------|-------------------|
| AVI                          | MP3               |
| MPEG                         | AAC               |
| ASF (restricted under Linux) | WMA stereo        |
| WMA                          | WMV 7/8/9         |
| WMV (restricted under Linux) | MPEG 1/2          |
| MP3                          | MPEG4             |
| OGG                          | H.264             |

AC3 is not licensed.

IGEL zero clients in the IZ range feature the Multimedia Codec Pack as standard.

<sup>244</sup> <https://www.igel.com/multimedia-codec-pack/>



### 3.2.2 IGEL Devices Supported by IGEL OS 11

IGEL UD (Universal Desktop)

| <b>Product Line</b> | <b>Device Type</b> | <b>Hardware ID</b> | <b>64 Bit</b> | <b>Memory</b> | <b>Storage</b> | <b>HW Video Acceleration</b> |
|---------------------|--------------------|--------------------|---------------|---------------|----------------|------------------------------|
| UD2                 | D220               | 40                 | Yes           | 2 GB          | 4 GB           | Yes                          |
| UD2                 | M250C              | 50                 | Yes           | 2 GB          | 4 GB           | Yes                          |
| UD2                 | M250C              | 51/52              | Yes           | 2 GB          | 8 GB           | Yes                          |
| UD3*(see page 755)  | M340C              | 50                 | Yes           | 2 GB          | 4 GB           | Yes                          |
| UD3                 | M340C              | 51                 | Yes           | 2 GB          | 4 GB           | Yes                          |
| UD3                 | M350C              | 60                 | Yes           | 4 GB          | 8 GB           | Yes                          |
| UD5                 | H830C              | 50                 | Yes           | 2 GB          | 4 GB           | Yes                          |
| UD6                 | H830C              | 51                 | Yes           | 2 GB          | 4 GB           | Yes                          |
| UD7                 | H850C              | 10                 | Yes           | 4 GB          | 4 GB           | Yes                          |
| UD7**(see page 755) | H850C              | 11                 | Yes           | 4 GB          | 4 GB           | Yes                          |
| UD7                 | H860C              | 20                 | Yes           | 8 GB          | 8 GB           | Yes                          |
| UD9                 | TC215B             | 40 / 41 (Touch)    | Yes           | 2 GB          | 4 GB           | Yes                          |

\* IGEL UD3-LX 50 is officially supported up to IGEL OS 11.05, incl. private builds.

\*\*As of December 2019, IGEL UD7 model H850C is equipped with the AMD Secure Processor<sup>245</sup>; for further information, see UD7 Model H850C<sup>246</sup>.

### IGEL Zero

#### Note on IZ Devices

The IZ devices listed below can be upgraded to IGEL OS 11. To upgrade your IZ devices to IGEL OS 11, please contact your IGEL sales representative. See also <https://www.igel.com/tradeup/> and [The IGEL OS 11 Trade-Up](#)<sup>247</sup>.

<sup>245</sup> <https://kb.igel.com/display/securitysafety/AMD+Secure+Processor>

<sup>246</sup> <https://kb.igel.com/display/securitysafety/UD7+Model+H850C>

<sup>247</sup> <https://kb.igel.com/display/licensesmoreigelos11/The+IGEL+OS+11+Trade+up>



| Product Line | Device Type | Hardware ID | 64 Bit | Memory | Storage | UEFI Secure Boot Support | HW Video Acceleration |
|--------------|-------------|-------------|--------|--------|---------|--------------------------|-----------------------|
| IZ2          | D220        | 40          | Yes    | 2 GB   | 4 GB    | Yes                      | Yes                   |
| IZ3          | M340C       | 50          | Yes    | 2 GB   | 4 GB    | Yes                      | Yes                   |
| IZ3          | M340C       | 51          | Yes    | 2 GB   | 4 GB    | Yes                      | Yes                   |

### 3.3 Bluetooth Assistant

A Bluetooth Assistant starts before the actual Setup Assistant. This tests whether a USB mouse and/or a USB keyboard are available. If not, it searches for unconnected Bluetooth devices and helps you connect them.

The assistant starts with a window in which a timeout expires for a few seconds. During this time you can still cancel the wizard.

On the following setup pages you can make settings related to Bluetooth:

#### 3.3.1 Bluetooth Tool:

Path: [Accessories > Bluetooth Tool](#)(see page 1100)

Here you define the start options for the **Bluetooth Tool** session.

#### 3.3.2 USB Access Control:

Path: [Devices > USB Access Control](#)(see page 1231)

If you have USB access control enabled, you should make sure that you explicitly allow the connection to your Bluetooth devices via a class rule or device rule.

#### 3.3.3 Bluetooth

Path: [Devices > Bluetooth](#)(see page 1231)

**Bluetooth** must be activated here so that you can work with Bluetooth devices.

If you activate **Tray Icon**, you can start the Bluetooth tool via an icon in the system bar.

If you want to disable the Bluetooth Assistant in general, put the file `.igel_skip_bt-autopairing` in the directory `/wfs/user/`

The assistant will be skipped.

For more information about enabling Bluetooth services, see [Bluetooth](#)(see page 1231).



## 3.4 Setup Assistant

### 3.4.1 Overview

When you start an unconfigured device, you will be welcomed by the **Setup Assistant**. This assistant takes you through the most important initial configuration steps.

The Setup Assistant starts automatically after booting IGEL OS if all of the following requirements are met:

- The device is not yet configured.
- No IP address for the Universal Management Suite (UMS) was transferred using the DHCP option 224.
- No UMS can be accessed under the DNS name `igelrmserver`.

### 3.4.2 Buttons

**Next:** Go to the next configuration step

**Skip:** This button is shown if the current configuration step can be omitted. If you click on **Skip**, nothing will change during the configuration step. If the configuration is edited, the button will switch to **Next**.

**Back:** Go back to the previous step

**Cancel:** Exit the setup assistant without saving changes to the configuration. Changes to the time and date will however remain effective.

- 
- [Language](#)(see page 757)
  - [Keyboard Layout](#)(see page 758)
  - [Time Zone Continent/Area](#)(see page 758)
  - [Time and Date](#)(see page 758)
  - [Mobile Broadband](#)(see page 758)
  - [Wireless](#)(see page 759)
  - [Connectivity](#)(see page 759)
  - [Local Logon](#)(see page 759)
  - [Activate Your IGEL OS](#)(see page 760)
  - [ICG Agent Setup](#)(see page 761)
  - [Finish](#)(see page 762)

### 3.4.3 Language

**Language:** Select the language for the user interface.



### 3.4.4 Keyboard Layout

**Keyboard layout:** Select the keyboard layout. The selected layout applies for all parts of the system including emulations, window sessions and X11 applications.

### 3.4.5 Time Zone Continent/Area

**Timezone continent/area:** Select the continent/area for your location.

Possible values:

- **General:** Under **Location**, you can select a GMT time zone.
- Africa ... Pacific: Under **Location**, you can select a city for the selected continent/area.

**Location:** Select your location or time zone.

Location: Summer time adjustment is taken into account here. Example: If you select "Berlin", the device will switch between summer time and normal time in accordance with the German adjustment rules. Time zone: The GMT time zones specify by how many hours the time zone for a particular location differs from the Greenwich time zone. The preceding symbol is used in accordance with the POSIX format. Examples: For New York City, select "GMT+5" which means "5 hours west of Greenwich". For Moscow, select "GMT-3" which means "3 hours east of Greenwich".

### 3.4.6 Time and Date

**Date:** Select the current date.

**Time:** Set the current local time.

#### Use NTP time server

The device uses the NTP time server that is entered in the field. You can specify multiple NTP time servers separated by spaces. Example: 0.de.pool.ntp.org 1.de.pool.ntp.org

To configure an NTP server via a UMS profile, edit **Use NTP time server** and **NTP time server** under **System > Time and Date**. For details on profiles, see [Using Profiles<sup>248</sup>](#).

**Next:** Sets the system clock according to what is entered above.

### 3.4.7 Mobile Broadband

In the basic mode (default), you can make the following settings:

**Country:** The country of your provider.

**Provider:** Provider (the possible options depend on what you choose for **Country**)

**APN/Plan:** APN/Plan (the possible options depend on what you choose for **Provider**)

---

<sup>248</sup> <https://kb.igel.com/display/endpointmgmt606/Using+Profiles>



For more configuration options, click the **Expert Mode** button.

In the expert mode, you can make the following settings:

- **Enabled:** Determines if the settings made in the expert mode are used. (Default: Enabled)
- **APN:** APN (Access Point Name) for your network connection. If you do not know the APN, ask your mobile communications operator for it.
- **Network ID:** Network ID for your network connection. If you do not know the network ID, ask your mobile communications operator for it.
- **Number:** Access number for your network connection. If you do not know the access number, ask your mobile communications operator for it.
- **User name:** User name for your network connection. If you do not know the user name, ask your mobile communications operator for it.
- **Password:** Password for your network connection. If you do not know the password, ask your mobile communications operator for it.
- **PIN:** PIN for the SIM card used.

### 3.4.8 Wireless

This configuration step is available if a WLAN adapter was found when starting the device. The device will search for available WLAN access points as soon as the configuration step is opened. The WLAN access points found will be listed. You can then connect to your desired WLAN access point.

If you carry out the WLAN configuration and exit the Setup Assistant by selecting **Finish**, the connection will be saved and WLAN will be permanently enabled. If you skip this configuration step or cancel the configuration, WLAN will not be permanently enabled.

**Wireless regulatory domain:** In the first selection menu, select the world region (example: **Europe**) in which you are situated and in the second one the country (example: **United Kingdom**).

: Searches again for WLAN access points.

: Opens a dialog which allows you to enter the WLAN name (SSID) of a hidden WLAN access point.

(Name of a WLAN access point in the list): Click on your desired WLAN access point and enter your access data in the dialog.

Once the connection is established, the symbol will be shown in the **Connected** column.

### 3.4.9 Connectivity

This page is shown if for any reason no network connectivity is available.

Follow the instructions on the screen.

### 3.4.10 Local Logon

This step is optional. If you want to configure a local user password later, see [Local User](#)(see page 1246).

**Login with local user password**



A login screen is shown upon the start of the device, and a local user password set under **Password** is used to log in.

**Password:** Enter the desired password. The checker shown below assesses the strength of the password.

**Password (repeated):** Repeat the password.

### 3.4.11 Activate Your IGEL OS

In this step, you select the method for licensing the device.

If the device has no license yet, the following options are available:

- **Install license via UMS/ICG**
- **Manual license deployment**
- **Register for demo license**

If the device already has a license, the following options are available:

- **Keep using the current license:** You can continue with **Next**.
- **Manual license update:** The procedure is the same as that for **Manual license deployment**.

The options are described in detail further below.

#### Install License via UMS/ICG

The device will request a license from the UMS. If the device is outside the company network, the IGEL Cloud Gateway (ICG) will be used for connecting the device to the UMS. In this case, ICG access must be set up; see [ICG Agent Setup](#)(see page 761).

#### Manual License Deployment

You can deploy a license via HTTP download from a specific URL, via FTP, or from a USB memory stick.

To deploy a license from a URL:

1. Enter the complete URL of the license file in the text field, including the protocol.
2. Click **Install**.

To deploy a license via FTP:

1. Click **FTP**.
2. Define the access data for your FTP server:
  - **Host/Port:** URL of the FTP server on which the license file is located
  - **User:** User for accessing the FTP server
  - **Password:** Password associated with the **User**
3. Click **Browse**.
4. In the dialog, go to the license file and select it.
5. Click **Install**.

To deploy a license from a USB memory stick:

1. Click **File**.
2. Connect the USB flash drive that contains the license to the device.



3. Under **Storage Device**, select the USB flash drive that contains the license.
4. Click **Browse**.
5. In the dialog, go to the license file, select it and click **Open**.
6. Click **Install**.

### Register for Demo License

With this evaluation license, all features of IGEL OS 11 are available for a fixed period. This period starts when the device has received the demo license.

For a demo license, you must accept the EULA to continue with setting up and using your device.

1. Make your choice as required and fill in all fields.
2. Activate the checkbox near **I agree to the terms + conditions and privacy policy**.
3. Click **ACTIVATE YOUR OS 11**.  
Your device fetches a demo license from IGEL.

### Troubleshooting: Proxy Configuration

If you get an error at this stage of the wizard, you may need to configure a proxy.

1. Click **Proxy configuration** in the upper right of the wizard to get to the proxy configuration dialog.
2. Edit the proxy settings as required:
  - **Use proxy server**: Activate this if a proxy is required.
  - **HTTP Proxy**: Address of the HTTP proxy
  - **Port**: Port of the HTTP proxy
  - **SSL Proxy**: Address of the SSL proxy
  - **Port**: Port of the SSL Proxy
  - **SOCKS Host**: Address of the SOCKS Host
  - **Port**: Port of the SOCKS host
  - **User name**: User name for authentication
  - **Password**: Password for authentication

**User name** and **Password** are the credentials for all proxy types configurable here (HTTP, SSL and SOCKS).

### 3.4.12 ICG Agent Setup

If your system administrator has given you access data for IGEL Cloud Gateway, you can connect the device to the gateway here.

You will find instructions for this under [Using ICG Agent Setup](#)<sup>249</sup>.

Otherwise, do not touch this page and click on **Skip** or **Next**.

---

<sup>249</sup> <https://kb.igel.com/display/igelos/Using+ICG+Agent+Setup>



### 3.4.13 Finish

**Finish:** Saves all settings and closes the Setup Assistant. If you have changed the language, the X11 graphics system will restart; the screen will go black for a short time. If you have a UD Pocket Demo, a restart is required to finish the activation.

## 3.5 Boot Procedure

The quick installation procedure is complete.

- ▶ Restart the system in order to start the boot procedure.
- 

- [Boot Menu](#)(see page 762)
- [Network Integration](#)(see page 765)
- [X-Server](#)(see page 765)

### 3.5.1 Boot Menu

During the boot procedure, a boot menu is available on request. Via this menu, you can access system parameters or reset the device to the factory defaults if the device is configured incorrectly or you experience problems when booting.

- ▶ During the boot procedure, press the [Esc] key repeatedly in rapid succession in the second stage loader when the "loading kernel" message is shown on the screen.

A menu with four boot options as well as an option for resetting the device to the default factory settings will appear:

- **Quiet boot:** Normal start (default)
- **Verbose boot:** Start with system messages and an interactive root shell
- **Emergency boot (setup only):** Setup only
- **Failsafe boot with CRC check:** Start with an integrity check of the operating system
- **Reset to factory defaults:** Reset the client to factory defaults
- **Custom boot command:** Boot with configurable command line options

#### Quiet Boot

**Quiet boot** is the default boot mode. In this mode, all kernel messages are disabled and the graphical user interface is started.

#### Verbose Boot

Unlike in **Quiet boot** mode, the boot messages are shown in **Verbose boot** mode. The boot procedure also pauses before the graphics system and the user session start.

This gives you an opportunity to open a root shell and interactively execute debugging commands (such as `ifconfig` etc.).



Use the root shell only if you have adequate knowledge of Linux or if you are instructed to do so by the IGEL Helpdesk and are given appropriate guidance. Incorrect use can destroy the operating system.

Proceed as follows:

1. Select **Verbose boot** from the boot menu.
2. Wait until the boot messages stop at Reached target IGEL Network Online.
3. Open a virtual console with the key combination [Ctrl ]+ [Alt ]+ [F11 ]or [Ctrl ]+ [Alt ]+ [F12].
4. Log in by pressing [Return ]and enter the root password if necessary.
5. Go through the desired individual commands.
6. Now enter the following command to continue the normal boot procedure:  
`systemctl default`  
The graphical user session will start.

## Emergency Boot

During an **Emergency Boot**, the device is started without network drivers and with a resolution of 640 x 480 - 60 Hz. The setup is then opened directly.

This option is useful if, for example, you have selected an excessively high screen resolution or a wrong mouse type and these settings can no longer be changed in the normal setup.

- ▶ Close the setup window to shut down the system or restart it.  
Unlike with a reset, the setup will open with the actual settings.

## Failsafe Boot - CRC Check

During a **Failsafe boot**, a check of the file system is carried out first. The device then starts in **Verbose mode**.

This option is helpful if you no longer have a bootable system after a firmware update. The **Failsafe boot** checks where the problem is. If need be, an old version will be booted and you will need to repeat the firmware update.

## Reset to Factory Defaults

If you select **Reset to factory defaults**, all personal settings on the device (including your password and the sessions you have configured) will be lost.

A warning message will appear on the screen before the procedure is carried out. If the device is protected by an administrator password, you will be prompted to enter this password.

Do you know the password?

1. Confirm the warning message.
2. Enter the password. You have three attempts.



Do you not know the password?

1. Confirm the warning message.
2. When you are prompted to enter the password, press the Enter key three times.
3. Press [c].  
The Terminal Key will appear.
4. Contact us using [license@igel.com](mailto:license@igel.com)<sup>250</sup>.
5. Enter the Terminal Key shown, the firmware version, and your contact details.  
IGEL will send you a so-called Reset to Factory Defaults Key specially for your device. To ensure that the process is as straightforward and yet as secure as possible, each key is valid for just one device.

See also [Resetting a Device with Unknown Administrator Password](#)(see page 368).

You can also reset your device to factory defaults in the UMS Console under **Devices > Other commands > Reset to Factory Defaults**, see [Devices](#)<sup>251</sup>.

## Custom Boot Command

If you select **Custom boot command**, preconfigured options will be placed on the kernel command line. This allows you for example to investigate and rectify problems with specific hardware components.

The Custom boot command is merely a temporary solution – it is not an everyday booting method. It must therefore be selected manually in the boot menu.

To configure the options for the Custom boot command, proceed as follows:

1. Open a **local terminal** and log in as root.
2. Enter the following command to bring up the current options:  
`bootreg get /dev/igfdisk boot_cmd`
3. Save your desired options with the following command:  
`bootreg set /dev/igfdisk boot_cmd "<Your Options>"`
4. Check the options that you have entered:  
`bootreg get /dev/igfdisk boot_cmd`

If you would like to delete options for the Custom boot command, leave an empty string of characters in their place: `bootreg set /dev/igfdisk boot_cmd ""`

<sup>250</sup> <mailto:license@igel.com>

<sup>251</sup> <https://kb.igel.com/display/endpointmgmt604/Devices>



### 3.5.2 Network Integration

Once the kernel has been loaded, the network can be configured.

There are three possible ways of integrating the terminal into the network environment.

Depending on the terminal settings, choose between

- **DHCP**,
- **BOOTP**,
- **manually configured IP address**.

The network interface can be stopped and restarted on the Linux Console (accessible via [Ctrl]+[Alt]+[F11]) with this command: `/etc/init.d/network stop /etc/init.d/network start`

### 3.5.3 X-Server

The final step in the boot procedure involves starting the **X-Server** and the local **windowmanager**.

## 3.6 The IGEL OS Desktop

You can operate the device via the taskbar and the *IGEL* menu.



The following items can be found in the taskbar at the bottom of the screen:

|   |                   |                                                                              |
|---|-------------------|------------------------------------------------------------------------------|
| 1 |                   | Opens the <i>IGEL</i> menu.                                                  |
| 2 | Quick Start Panel |                                                                              |
|   |                   | Application Launcher: Opens a dialog window with start symbols for sessions. |
|   |                   | Setup: Opens the <i>IGEL</i> setup.                                          |



|   |                |                                                    |
|---|----------------|----------------------------------------------------|
|   |                | Symbol for sessions: Launches a session.           |
|   |                |                                                    |
|   |                |                                                    |
| ③ | Window bar     |                                                    |
|   | Window buttons | Allows you to switch between open windows.         |
| ④ | System tray    |                                                    |
|   |                | CPU power plan: Changes the power saving settings. |
|   |                | Volume control                                     |
|   |                | Allows you to remove a USB stick safely            |
|   |                | Local network connection                           |
|   |                | Time / date                                        |

The *IGEL* menu offers the following areas and functions:

- **Sessions:** Allows you to launch sessions
- **System:** Allows you to launch system programs
- **About:** Shows all relevant system information
- **Search window:** Allows you to find sessions and functions in the start menu
- Allows you to shut down the device
- Allows you to restart the device

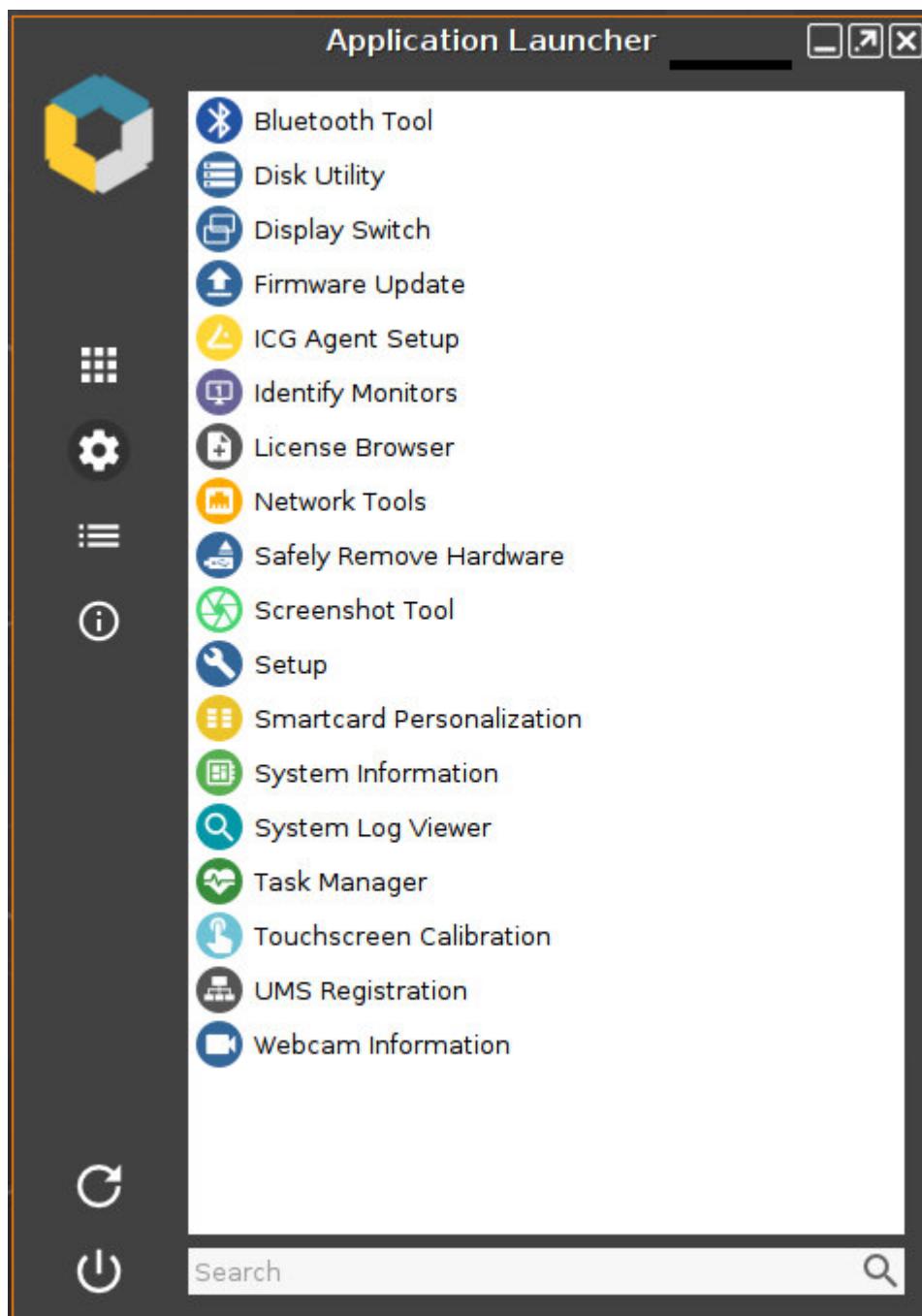


- 
- Application Launcher(see page 768)
  - Sessions(see page 770)
  - System(see page 770)
  - License(see page 771)
  - About Window(see page 771)
  - Restart and Shutdown(see page 772)

### 3.6.1 Application Launcher

To launch the **Application Launcher**, proceed as follows:

- ▶ Click on  in the Quick Start Panel or in the start menu.



The sub-areas of the Launcher provide access to:

|  |                                                              |
|--|--------------------------------------------------------------|
|  | Listing of the sessions (see page 770) that have been set up |
|--|--------------------------------------------------------------|



|  |                                                                   |
|--|-------------------------------------------------------------------|
|  | Listing of the most important tools (see page 770)                |
|  | License declarations (see page 771) for the components used       |
|  | The About Window (see page 771) with information about the system |
|  | Restart                                                           |
|  | Shut down                                                         |
|  | Search field for fast access to the components                    |

You will find information regarding the configuration under [Application Launcher](#) (see page 1063).

### 3.6.2 Sessions

All sessions created are shown in a list of applications if they are enabled for the main session page.

- ▶ To open an application, double-click on it or click on **Run**. Alternatively, you can launch sessions via icons on the desktop, in the quick launch bar or from the Start menu and context menu. Applications can also be launched automatically and a key combination (hotkey) can be defined. It is also possible, to build a file structure for the sessions in the application launcher. Therefor, in the setup page **Desktop Integration** of the relevant application you have to define a folder in the application launcher.

The available options for launching a session can be defined under **Desktop Integration** in the session configuration.

### 3.6.3 System

Under **System** , you can execute various tools including the firmware updating tool with the pre-set update information.

The following tools are available:

- **Identify Monitors:** Shows the screen's number and manufacturer details.
- **Screenshot Tool:** Takes photos of the screen content.
- **Bluetooth Tool:** Starts the Bluetooth tool.
- **Firmware Update:** Carries out the update with the settings made during the setup.



- **Safely Remove Hardware:** Removes external storage devices without a risk of losing data.
- **Disk Utility:** Shows information regarding connected USB drives.
- **Network Tools:** Provides detailed information on the network connection and offers a number of problem analysis tools such as ping or traceroute.
- **Setup:** Launches the IGEL Setup.
- **System Information:** Shows information regarding hardware, the network and connected devices.
- **System Log Viewer:** Shows system log files "live" and allows you to add your own logs.
- **Task Manager:** Manages all processes.
- **Touchscreen Calibration:** Allows a connected touchscreen monitor to be calibrated.
- **UMS Registration:** Logs the device on to a UMS server (access data for the server are required).
- **Webcam Information:** Shows data relating to a connected webcam and allows the camera to be tested.

### 3.6.4 License

Under **License** you will find the following:

- The licenses for the components used in the UD system
- Information on the provision of source code, e.g. under GPL

### 3.6.5 About Window

In the **About** window, accessible via the icon, you will find the following data:

- **Product:** Information regarding the installed firmware
  - Copyright
  - Firmware Release Date
  - Firmware Version
  - Product ID
  - Product Name
  - Website
- **License Information:** Expiration dates of available licenses
- **Network:** Computer name, hardware address, and IP address of the device
  - Local Name
  - Default Gateway (only with valid network connection)
  - DNS Server (only with valid network connection)
  - Universal Management Suite
- **Interface [number name]:**
  - Description
  - Hardware Address
  - IP Address



If the network status changes, the details will automatically be updated. To force an update, click on .

- **Hardware:**

- Boot Mode
- CPU Model
- Device Type
- Flash Size
- Graphic Chipset
- Memory Size
- Total Operating Time
- Unit ID (equal to MAC address (UD, UDC) or serial number (UD Pocket))

- **Licensed Features:** List with all firmware features for which a license is available

You can copy individual entries via the context menu (right mouse button).

### 3.6.6 Restart and Shutdown



Within the **Application Launcher** you will find two buttons for **rebooting** or **shutting down** the device. Both actions can be disabled for the user and will then be available to the administrator only.

You can change the default action when shutting down the device using the button on the screen or the on/off button on the device itself in the setup under **System > Power Options > Shutdown**.

## 3.7 Setup

With the help of the setup, you can change the system configuration and session settings.

Any changes you have made in the UMS take precedence and may no longer be able to be changed. A lock symbol before a setting indicates that it cannot be changed.

- 
- [Starting the Setup](#)(see page 772)
  - [End the Setup](#)(see page 773)
  - [Quick Setup](#)(see page 773)
  - [Setup Search](#)(see page 774)

### 3.7.1 Starting the Setup

You can open the setup in the following ways:



- Double-click in the **Application Launcher**
- or click on **Run**.
- Double-click on the desktop (if available based on the settings).
- Select **Setup** in the desktop context menu (if available based on the settings).
- Select **System > Setup** in the start menu.
- Click on in the Quick Start Panel.
- Launch the setup using the keyboard command [Ctrl]+[Alt]+[s], or in the Appliance Mode using [Ctrl]+[Alt]+[F2].

You can configure how the setup can be launched under **Accessories**. The options described above as well as combinations thereof are available.

### 3.7.2 End the Setup

In order to end the setup again, you have the following options:

- ▶ Click on **Apply** if you have finished configuring a setup area and would like to save your settings without closing the setup program.
- ▶ Click on **Cancel** if you have not made any changes and would like to abort the setup.
- ▶ Click on **OK** to save your changes and exit the setup.

### 3.7.3 Quick Setup

As administrator, you prepare the setup for the user. If you want to give the user the option of defining their own settings in certain areas of the setup, you can prepare a quick setup. A quick setup is a slimmed down version of the setup. It only displays areas the user is allowed to change.

To create a quick setup session, proceed as follows:

1. Enable the password for the administrator in IGEL Setup under **Security > Password**.<sup>252</sup>

If users are to be allowed to edit parts of the setup only with a password, enable the password for the setup user too.

2. Under **Accessories > Quick Settings**(see page 1053), define the name and options for calling up the quick setup.
3. Under **Accessories > Quick Settings > Page Authorizations**,(see page 1055) enable those areas to which the user is to have access.

<sup>252</sup> <https://kb.igel.com/display/igelos/Password>



You can set up a hotkey to start quick setup in appliance mode. Instructions for setting up the hotkey can be found under [Quick Settings](#)(see page 1053).

### 3.7.4 Setup Search

The **Search** function enables you to find parameter fields or parameter values within the setup.

1. To start a **search**, click on the button below the tree structure.
2. Enter the text to be searched for and the search details.
3. Select one of the hits.
4. Click on **Show result** and you will be taken to the relevant setup page.

The parameter or value found will be highlighted as shown below.

## 3.8 Sessions

Menu path: **Sessions > Sessions Summary**

In this area, you will find an overview of all available sessions.

**Add:** Adds a session from the selection of available session types.

**Filter:** Filters sessions shown in the list according to the string of characters entered.

- [Copy Session](#)(see page 775)
- [Global Session Options](#)(see page 775)
- [Citrix](#)(see page 776)
- [RDP Global](#)(see page 811)
- [RDP Session](#)(see page 828)
- [Remote Desktop Web Access](#)(see page 837)
- [Horizon Client Global](#)(see page 847)
- [Horizon Client Session](#)(see page 860)
- [Appliance Mode](#)(see page 869)
- [AppliDis](#)(see page 875)
- [Evidian AuthMgr](#)(see page 880)



- [NoMachine NX Client](#)(see page 887)
- [X Sessions](#)(see page 901)
- [Parallels Client Global](#)(see page 907)
- [Parallels Client Session](#)(see page 908)
- [PowerTerm Selection](#)(see page 918)
- [PowerTerm Session](#)(see page 919)
- [IBM iAccess Client](#)(see page 921)
- [ThinLinc Global](#)(see page 933)
- [ThinLinc Session](#)(see page 936)
- [SSH Session](#)(see page 946)
- [VNC Viewer Sessions](#)(see page 951)
- [Firefox Browser Global](#)(see page 957)
- [Firefox Browser Session](#)(see page 978)
- [Chromium Browser Global](#)(see page 982)
- [Chromium Sessions](#)(see page 990)
- [Media Player Global](#)(see page 994)
- [Media Player Session](#)(see page 997)
- [VoIP Client](#)(see page 1002)
- [Teradici PCoIP Session](#)(see page 1011)
- [AVD Global](#)(see page 1015)
- [AVD Session](#)(see page 1018)
- [Amazon WorkSpaces](#)(see page 1026)
- [deskMate Session](#)(see page 1032)
- [Unified Communications](#)(see page 1037)

### 3.8.1 Copy Session

You can copy a session in the setup. The copy of the session has all the properties of the original session and is located in the same folder as the original session.

To copy a session, proceed as follows:

1. In the setup, open the menu path **Sessions > [Session Type] > [Session Type] Sessions**.  
Example: **Sessions > RDP > RDP Sessions**  
The existing sessions are shown.
2. Highlight the session that you want to copy.
3. In the **[Session Type] Sessions** area, click Alternative: Open the context menu of the session by right-click and select **Copy**.  
A copy of the session will be created.

### 3.8.2 Global Session Options

Menu path: **Setup > Sessions > Global Session Options**

- **Network notification on session start:** If when launching sessions no network is available, a notification will be shown.  
 Network notification is enabled (default)



- Network notification is disabled
- **Notification delay:** Time in seconds after which the notification is shown. (default: 15)
  - Possible values:
    - 1 ... 120 seconds
- **Delay session start at boot time to apply new UMS settings:** If new settings were made in the UMS, the device may receive them during the boot procedure.
  - The session start will be delayed until the settings have been transferred or the time limit has been exceeded.
- **Timeout:** Delay in seconds. (default: 10)
  - Possible values:
    - 1 ... 120 seconds

### 3.8.3 Citrix

Menu path: **Setup > Sessions > Citrix**

- [Citrix Client Selection](#)(see page 776)
- [Citrix Global](#)(see page 776)
- [Citrix StoreFront](#)(see page 798)
- [Citrix Self-Service](#)(see page 807)

#### Citrix Client Selection

Menu path: **Sessions > Citrix > Citrix Client Selection**

Select which of the installed Citrix client versions is to be used for Citrix sessions.

**Citrix client version** (IGEL OS 11.06.100)

- Default (21.06.0)
- 20.10.0
- 21.04.0
- 21.06.0

After changing the **Citrix client version**, check the settings under:

- **Citrix > Citrix StoreFront > Server**
- **Citrix > Citrix StoreFront > Login**

#### Citrix Global

Menu path: **Sessions > Citrix > Citrix Global**

This section describes global Citrix settings which apply for all Citrix sessions. Most of these settings can be either carried over or overwritten in the individual sessions.



Please note that a number of configuration options depend on the version of the Citrix Receiver selected.

If there are problems with the logging in to a Citrix Storefront session because of the expired password, see [Login Failed because of the Expired AD Password](#)(see page 257).

- [StoreFront Login](#)(see page 777)
- [Window](#)(see page 778)
- [Keyboard](#)(see page 780)
- [Mapping](#)(see page 781)
- [Firewall](#)(see page 786)
- [Options](#)(see page 787)
- [Native USB Redirection](#)(see page 788)
- [Fabulotech USB Redirection](#)(see page 790)
- [Fabulotech Scanner Redirection](#)(see page 792)
- [HDX Multimedia](#)(see page 792)
- [Codec](#)(see page 794)
- [Unified Communications](#)(see page 795)

## StoreFront Login

Menu path: **Sessions > Citrix > Citrix StoreFront > Login**

In this area, you can define session-specific login options.

**Authentication type:** Depending on the Citrix client version, the following types are available:

- Password authentication: Suitable for on-premises connections; connections via Citrix NetScaler or to a cloud environment may cause problems.
- Kerberos passthrough authentication: Uses local login data for listing and launching applications. The option enables single sign-on if login with AD/Kerberos is configured on the device.
- Smartcard authentication (StoreFront only, not Web Interface)
- Citrix authentication mechanism (instead of IGEL), Smartcard disabled
- Citrix authentication mechanism (instead of IGEL), Smartcard enabled

If you have set an authentication type with smartcard, select the type of card on the [Smartcard](#)(see page 1249) page.

Additional options include the following:

### Use passthrough authentication

- Cached login data are used for listing and starting applications.  
 No passthrough authentication (default)

### Auto login

- Uses the login data preset on this page when connecting to the server.  
 Do not log on automatically (default)

**User name:** Can only be filled in with password authentication



**Password:** Can only be filled in with password authentication

Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

**Domain:** Can only be filled in with password authentication

**Remember username and domain:**

- Saves the user name and domain from the last login. (default)
- The user name and domain will not be saved.

**Synchronize Citrix password with screen lock:**

- Synchronizes the screen lock password with that of the Citrix application.
- No synchronization (default)

**Relaunch Citrix login after logout:**

- Automatically shows the login dialog again after logging off.
- Does not start the login procedure again. (default)

**Start a single published application automatically:** This parameter is relevant if exactly 1 published application is provided for the user whose login is configured here.

- The published application is started when the user has logged in.
- The published application is not started on login. (default)

**Start following applications automatically after server connection is established:** A list of applications to be started in the session.

To edit the list, proceed as follows:

- Click on to create a new entry. In the Add dialog, give the name of the application.

You can also enter part of the name followed by an asterisk (\*).

- Click on to remove the selected entry.
- Click on to move the entry upwards.
- Click on to move the entry downwards.

After a successful login, the associated desktop icon for each available application will be placed on the device desktop. All applications whose name matches one of the names given in the **Start following applications automatically after server connection is established** area will then be launched.

## Window

Menu path: **Sessions > Citrix > Citrix Global > Window**

Under **Window**, you can configure the following settings:

**Multimonitor full-screen mode**



Possible options:

- Restrict full-screen session to one monitor
- [Expand full-screen session across all monitors](#)
- Expand the session over a self-selected number of monitors

Select this setting if you do not want to span the session across all monitors, but only across a certain number of monitors. Under **Monitor selection**, specify the relevant monitors.

**StoreFront start monitor:** This setting is available if you selected **Restrict full-screen session to one monitor** for **Multimonitor full-screen mode**.

**Monitor selection:** This setting is available if you selected **Expand the session over a self-selected number of monitors** for **Multimonitor full-screen mode**.

#### Example

Sample configuration: If you have 4 monitors and want to expand your session across monitor 2, 3, and 4 you have to insert 2,3,4 or 2,4.

**Embed systray icons into window manager taskbar:** Specifies if an application icon is shown in the local taskbar.

- On
- Off

#### Citrix connection bar

Possible options:

- Off
- On
- Factory default is "": The Citrix connection bar is enabled or disabled by the server.

#### Control bar for Citrix sessions

The in-session control bar is present in Citrix sessions. For details, see [In-Session Control Bar\(see page 1154\)](#).

#### Screen Pinning

You can run multiple Citrix desktop sessions simultaneously on different monitors. In this section, you assign one or more monitors to each session.

If a desktop session is not assigned to monitors, the default settings in the general section of this Setup page apply to it.

This feature works only with desktop sessions; published applications cannot be controlled.

► For each Citrix desktop session, click to configure a corresponding monitor setup. The following parameters must be set:



**Citrix session name:** Name of the desktop session as displayed in the browser, desktop, or Self-Service. The session name is provided by the server. The wildcards "\*" (any number of any characters) and "?" (any single character) can be used.

#### Example

With three desktop sessions that are named "Desktop2019", "DesktopW10", and "DesktopD10", you can assign settings like so, for instance:

"Desktop\*": The settings are assigned to all three desktops.

"Desktop?10": The settings are assigned to "DesktopW10" and "DesktopD10".

"DesktopW10": The settings are assigned to "DesktopW10".

**Multimonitor full-screen mode:** Defines how the desktop sessions are distributed over the monitors. For the arrangement of the monitors and their numbering, go to **User Interface > Display** (see [Display](#)(see page 1142)).

Possible options:

- Restrict full-screen session to one monitor: The desktop session is displayed on the monitor that is selected under **Desktop session start monitor**.
- Expand full-screen session across all monitors: The desktop session uses all monitors.
- Expand the session over a self-selected number of monitors: The monitors can be selected with **Monitor selection**.

**Desktop session start monitor:** The desktop session is displayed on the selected monitor.

**Monitor selection:** Selects one or several monitors on which this desktop session is to be displayed. This setting is available if you selected **Expand the session over a self-selected number of monitors**.

#### Example

Sample configuration: If you have 4 monitors and want to expand your session across monitor 2, 3, and 4 you have to insert 2, 3, 4 or 2, 4.

## Keyboard

Menu path: **Setup > Sessions > Citrix > Citrix Global > Keyboard**

On the **Keyboard** page, you can define alternative key combinations for hotkeys commonly used during ICA sessions. In *Windows* for example, the key combination [Alt]+[F4] closes the current window. This key combination works in ICA sessions too. All key combinations with [Alt] which are not used by the *X Window Manager* function in the familiar way during an ICA session.

The following settings can be configured:

- **Keyboard layout**
  - default: The local keyboard setting will be used in ICA too.
  - Other Countries
- **Input language:**
  - default: The local keyboard setting will be used in ICA too.
  - Other Countries



- **Mapping Ctrl+Alt+End to Ctrl+Alt+Del for Citrix sessions**
  - The user can use the combination [Ctrl]+[Alt]+[End] to change the password instead of [Ctrl]+[Alt]+[Del] when the corresponding prompt message appears.
  - No mapping (default)
- **Keyboard mapping file:** You can choose between two alternatives.
  - generic: Sends language-independent scancodes from the keyboard to the computer.
  - Linux: Sends language-specific scancodes.

The key alternatives are restricted to [Ctrl]+[Shift]+[Key] by default. However, you can change the settings by clicking on the Hotkey Modifier drop-down field and/or hotkey symbol for the relevant key combination.

- Possible keys: [F1] – [F12], [Plus], [Minus], [Tab]
- Possible modifiers: [Shift], [Ctrl], [Alt], [Alt]+[Ctrl], [Alt]+[Shift], [Ctrl]+[Shift]
- **Toggle SpeedScreen**: Key combination for switching SpeedScreen (client reacts immediately to keyboard inputs or mouse clicks) on and off alternately.

## Mapping

Menu path: **Setup > Sessions > Citrix > Citrix Global > Mapping**

Locally connected devices such as printers or USB storage devices can be made available in ICA sessions.

---

- [Drive Mapping \(Citrix\)](#)(see page 781)
- [COM Ports](#)(see page 783)
- [Printer](#)(see page 784)
- [Device Support](#)(see page 784)

## Drive Mapping (Citrix)

Menu path: **Setup > Sessions > Citrix > Citrix Global> Mapping > Drive Mapping**

Through drive mapping, each directory mounted on the device (including CD-ROMs and disk drives) is made available to you during ICA sessions on Citrix servers.

In this area, you can specify which drives and paths are mapped during the logon. This applies for all ICA sessions.

- **Drive mapping:**
  - Citrix servers can access the device's local drives. (default)

To manage the **Drive Mapping** list, proceed as follows:

- ▶ Click on to create a new entry.
- ▶ Click on to remove the selected entry.
- ▶ Click on to edit the selected entry.
- ▶ Click on to copy the selected entry.



Local (USB) devices which are to be used for drive mapping purposes must first be set up as [storage devices](#)<sup>253</sup>.

Before you unplug a hotplug storage device from the device, you must safely remove it. Otherwise, data on the hotplug storage device can be damaged. Depending on the configuration, there is one or several possibilities to safely remove a hotplug storage device:

- Click on ▲ in the task bar. The taskbar is not available in a fullscreen session.
- Click on in the in-session control bar. Depending on the configuration, the in-session control bar may be available in a fullscreen session. For further information, see [In-session Control Bar](#)<sup>254</sup>.
- Function **Accessories > Safely Remove Hardware** with further starting possibilities; amongst other things, a hotkey can be defined here.  
If the following warning is displayed: **Volume(s) still in use. Dont' remove the device.**, then the hotplug storage device must not be removed. First, exit the program concerned or close all files or directories that reside on the hotplug storage device.

#### Add Drive Mapping

- **Enable:**  The drive will be made available in the session.
- **Drive to map:** DOS-style drive letters on the Citrix Server.

If the drive letter you have selected is no longer available on the Citrix server, the specified directory or local drive will be given the next free letter during the logon.

- **Local drive path:** Unix path name of the local directory to which the mapping is to refer.

If you map a locally connected device, use the pre-defined path names available in the drop-down field.

- **Read access**

Possible options:

- yes
- no
- ask user: The read access right is queried when each ICA session is accessed for the first time.

- **Write access**

Possible options:

- yes
- no

<sup>253</sup> <https://kb.igel.com/display/igelos1005/Storage+Hotplug>

<sup>254</sup> <https://kb.igel.com/display/igelos1005/Session+Control+Bar>



- ask user: The write access right is queried when each ICA session is accessed for the first time.

## COM Ports

Menu path: **Setup > Sessions > Citrix > Citrix Global > Mapping > COM Ports**

- **COM port mapping**

Enables the mapping of serial devices connected to the device to the serial interfaces of the Citrix server. (Default)

If you would like to use signature pads, you must enable them beforehand under **User Interface > Input > Signature Pad**(see page 1167).

To manage the list of **COM port devices**, proceed as follows:

- ▶ Click to create a new entry.
- ▶ Click to remove the selected entry.
- ▶ Click to edit the selected entry.
- ▶ Click to copy the selected entry.

### Add

- **COM port device:** Allows you to select from all serial and USB interfaces on the device.

Possible values:

- "COM 1"
- "COM 2"
- "COM 3"
- "COM 4"
- "USB COM 1": For UD3-LX60 devices (mainboard: M350C<sup>255</sup>), this port must be used instead of "COM 1".
- "USB COM 2"
- "USB COM 3"
- "USB COM 4"

- **Detect Devices....:** Opens a dialog allowing you to select the device file. 3 device files are available for each device; the **Description** column shows the type of device file:

- (GENERIC) [device designation]: Generic type. The name of the device file ends in a consecutive number which depends on the boot procedure or the order of insertion.  
Example: /dev/ttyUSB0
- (BY PORT) [device designation]: According to USB port. The device file is in the /dev/usbserial/ directory. The name of the device file ends in the number of the USB port that the device is plugged into. Example: /dev/usbserial/ttyUSB\_P12
- (BY USBID) [device designation]: According to USB ID. The device file is in the /dev/usbserial/ directory. The name of the device file ends as follows: \_V[Vendor ID]\_P[Product ID]. Example: /dev/usbserial/ttyUSB\_V067b\_P2303

<sup>255</sup> <https://kb.igel.com/display/hardware/Manual+for+UD3+Model+M350C>



- (Virtual) [device designation]: Virtual device; used for signature pads for example. Example: /dev/ttyVST0

If your device has an additional multiport PCI card, more than 2 connections may be available.

## Printer

Menu path: **Setup > Sessions > Citrix > Citrix Global > Mapping > Printer**

You can set up a printer for ICA sessions here.

- **Client printer mapping:** With this function, the locally connected device printer is made available for your ICA sessions, provided that it was not disabled on the server side.
- **Set another default printer:**
  - Allows you to specify a default printer for the client which differs from the one defined in the printer setup.
  - Do not set another default printer. (default)
- **Default printer:** Print queues used on the device to specify the default printer for the session. lp is the locally configured default printer.
- **Default printer driver:** Windows driver name for the printer which is automatically set up. Enter one of the universal drivers or your own driver name here.  
Possible values:
  - Citrix PCL4 universal driver (old)
  - Citrix Universal Printer
  - Citrix XPS Universal Printer
  - User entry

See also, <https://support.citrix.com/article/CTX140208>.

The printers must be set up on the **Devices > Printers > CUPS > Printer** page and must be enabled there for mapping in ICA sessions, see ICA sessions.

Because the device merely places incoming print jobs in a queue, you need to install the printer on the server.

## Device Support

Menu path: **Setup > Sessions > Citrix > Citrix Global > Mapping > Device Support**

In this area, you can enable virtual ICA channels for communicating with various devices connected to the device.



The devices supported are listed in the [IGEL Third Party Hardware Database](#)<sup>256</sup>.

**DriveLock channel:** The virtual DriveLock channel is implemented on the device. The channel must also be installed on the Citrix server.

DriveLock can read hardware data from local USB devices and transfer these data to the Citrix server with the help of the Virtual ICA Channel Extension. From IGEL Linux Version 10.03.500, this is also possible with SATA devices.

When using whitelists, rules based on the hardware properties of the connected drive (e.g. manufacturer details, model and serial number) are taken into account.

Important information regarding DriveLock can be found in the FAQ [Using DriveLock with IGEL Devices](#)(see page 701).

- A virtual channel for DriveLock is enabled.
- No virtual channel for DriveLock is enabled. (Default)

#### **deviceTRUST channel**

- A virtual channel for deviceTRUST is enabled.
- No virtual channel for deviceTRUST is enabled. (Default)

#### **Crossmatch DigitalPersona fingerprint channel**

- A virtual channel for Crossmatch DigitalPersona is enabled.
- No virtual channel for Crossmatch DigitalPersona is enabled. (Default)

#### **Diktamen Channel for Dictation**

- A virtual channel for Diktamen is enabled..
- No virtual channel for Diktamen is enabled. (Default)

#### **Grundig MMC-Kanal for dictation with Grundig devices**

- A virtual channel for communication with Grundig devices is enabled.
- No virtual channel for communication with Grundig devices is enabled. (Default)

**Nuance channel for dictation:** Virtual audio channel for dictation devices. Dictation microphones from Grundig, Philips and Olympus are supported.

This channel is only responsible for audio transmission. The channel for dictation device operating elements is manufacturer-specific and must be enabled separately.

- The Nuance audio channel is enabled.
- The Nuance audio channel is not enabled. (Default)

#### **Olympus Channel for dictation**

- A virtual channel for communication with Olympus devices is enabled.
- No virtual channel for communication with Olympus devices is enabled. (Default)

#### **signotec signature pad channel**

- A virtual channel for communication with signotec signature pads is enabled.
- No virtual channel for communication with signotec signature pads is enabled. (Default)

#### **StepOver signature pad channel**

---

<sup>256</sup> <https://www.igel.com/linux-3rd-party-hardware-database/>



- A virtual channel for communication with StepOver signature pads is enabled.  
 No virtual channel for communication with StepOver signature pads is enabled. (Default)

#### Philips speech channel for dictation

- A virtual channel for communication with Philips dictation devices is enabled.  
 No virtual channel for communication with Philips dictation devices is enabled. (Default)

**DPM server drive:** Via this drive, the Philips PocketMemo dictation device makes the voice recordings available to the server. (Default: P)

The dictation device is automatically assigned to the selected drive letter. Ensure that no other Hotplug storage device is assigned to this drive letter. Further information can be found under [Hotplug storage device](#)(see page 1228) and [Drive mapping](#)(see page 781).

**SpeechAir server drive:** Via this drive, the Philips SpeechAir dictation device makes the voice recordings available to the server. (Default: S)

The dictation device is automatically assigned to the selected drive letter. Ensure that no other Hotplug storage device is assigned to this drive letter. Further information can be found under [Hotplug storage device](#)(see page 1228) and [Drive mapping](#)(see page 781).

#### Kofax SPVC signature pad channel

- The Kofax SPVC signature pad channel is enabled.  
 The Kofax SPVC signature pad channel is not enabled. (Default)

#### Lakeside SysTrack channel

- The Lakeside SysTrack channel is enabled.  
 The Lakeside SysTrack channel is not enabled. (Default)

## Firewall

Menu path: **Setup > Sessions > Citrix > Citrix Global > Firewall**

In this area, you can configure the following firewall settings:

#### Alternative address

- Allows you to use a proxy or Secure Gateway server as an alternative address for connections via a firewall.  
 Do not use an alternative address (default)

## SOCKS / Secure Proxy

#### Proxy type

- [None \(Direct Connection\)](#)
- SOCKS: A proxy that uses the SOCKS protocol
- Secure (HTTPS): An HTTP proxy with TLS/SSL encryption.

**Proxy server:** Name or IP address of the proxy server



**Proxy port:** TCP port of the proxy server (default: 1080)

Secure Gateway (Relay Mode)

**Secure gateway address:** If you would like to use a Citrix Secure Gateway in relay mode, you must give the full DNS name – the IP address is not sufficient in this case.

**Port:** TCP port of the gateway (default: 443)

## Options

Menu path: **Sessions > Citrix > Citrix Global > Options**

In this area, you can set up additional options to optimize the system's general behavior and its performance.

### Use server redraw

- The Citrix server is responsible for refreshing the screen content.
- Do not use server redraw. (Default)

### Disable Windows alert sounds

- Switches off the Windows warning sounds.
- The warning sounds remain enabled. (Default)

### Backing store

- The X Server temporarily stores hidden window content.
- Window content is not stored. (Default)

### Deferred screen update mode

- Enables delayed updates from the local video buffer on the screen. The local video buffer is used if the seamless Windows mode or HDX latency reduction is used.
- No delayed update. (Default)

**Cache size in kB:** (default: 1024)

**Minimum bitmap size in bytes:** The minimum size of the bitmap files that are to be stored in the cache. (Default: 1024)

**Persistent cache path:** The directory where the files are to be stored locally. (Default: \$ICAROOT/cache)

Do not make the cache too big otherwise you run the risk of the device having too little storage space for its own system and other applications. You may have no alternative but to equip your device with additional RAM.

**Scrolling control:** Depending on the speed of your network or the response time of your server, there may be a delay between you letting go of the mouse button on a scroll bar and the scrolling actually stopping (e.g. when using Excel). Changing this value may help. (Default: 100)

### Audio bandwidth limit in StoreFront sessions

- High
- Medium



- Low

Higher quality requires more network and computing resources.

#### **Auto reconnect**

- Automatically attempt to reconnect if connection is terminated. (Default)  
 Do not attempt to reconnect.

**Maximum retries:** (default: 3)

**Delay in seconds before reconnecting:** (default: 30)

#### **Allow Kerberos passthrough authentication in StoreFront sessions**

- Kerberos passthrough authentication is allowed. (Default)  
 Kerberos passthrough authentication is not allowed.

This point concerns Citrix XenApp in Version 6.5 and older.

#### **CGP address**

- Use server address
- Text input
- disabled

#### **Multistream sessions**

- Support multistream ICA.  
 Do not support multistream ICA. (Default)

#### **HDX Adaptive Transport over EDT**

Possible options:

- UDP with fallback to TCP
- TCP Only - UDP disabled
- UDP without fallback to TCP

#### **Native USB Redirection**

Menu path: **Sessions > Citrix > Citrix Global > Native USB Redirection**

USB devices can be permitted or prohibited during a Citrix session on the basis of rules. Sub-rules for specific devices or device classes are also possible. The use of rules is described under [USB Access Control](#)(see page 1231).

#### **Native USB redirection**

- Native USB redirection is enabled globally.

Enable either **native USB redirection** or **Fabulotech USB redirection**, but not both together.



Disable USB redirection if you use DriveLock. Further information can be found under [Using DriveLock with IGEL Devices](#)(see page 701).

**Default rule:** This rule will apply if no special rule was configured for a class or a device.

- [Deny](#)
- [Allow](#)

**Tip**

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

## Class Rules

Class rules apply to USB device classes and sub-classes.

To manage rules, proceed as follows:

- ▶ Click to create a new entry.
- ▶ Click to remove the selected entry.
- ▶ Click to edit the selected entry.
- ▶ Click to copy the selected entry.

Add class rule:

**Rule:**

- [Allow](#)
- [Deny](#)

**Class ID:** Selection list

**Sub-class ID:** Selection list

**Name:** Free text entry

## Device Rules

Device rules apply to specific USB devices.

Add device rule:

**Rule:**

- [Allow](#)
- [Deny](#)

**Vendor ID:** Hexadecimal manufacturer number

**Product ID:** Hexadecimal device number



To find out the **Vendor ID** and **Product ID** of the connected USB device, use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal. You can also use the **System Information** tool, see [Using “System Information” Function](#)(see page 1108).

#### Name: Free text entry

See also an overview and best-practice recommendations for the use of webcams under [Webcam Redirection and Optimization](#)(see page 663).

#### Fabulatech USB Redirection

Menu path: **Sessions > Citrix > Citrix Global > Fabulatech USB Redirection**

Redirection for USB devices can be allowed or denied during a Citrix session on the basis of rules. Sub-rules for specific devices or device classes are also possible. The use of rules is described under [USB Access Control](#)(see page 1231).

For the Fabulatech USB Redirection, a server-side component is required. We recommend the USB for Remote Desktop IGEL Edition; see <http://www.usb-over-network.com/partners/igel/>.

#### Fabulatech USB Redirection

Fabulatech USB Redirection is enabled for all Citrix sessions.

Enable either **Native** or **Fabulatech USB Redirection** – not both together. Disable USB redirection if you use DriveLock.

Ensure that no other Hotplug storage device (USB stick) is connected if a session is started with Fabulatech USB Redirection. Otherwise, the hotplug storage device will not be securely removed when the session starts, and this could lead to data loss. With IGEL Linux Version 10.02.x the Hotplug storage device is already insecurely removed when the Fabulatech USB Redirection is enabled.

**Default rule:** This rule will apply if no special rule was configured for a class or a device.

- Deny
- Allow

#### Tip

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

#### Class Rules

Class rules apply to USB device classes and sub-classes.

Managing rules:

Create a new entry



Remove the selected entry

Edit the selected entry

Copy the selected entry

Class rule properties:

**Rule:**

- Allow: Devices that have the properties defined here are redirected by the Fabulatech USB Redirection.
- Deny: Devices that have the properties defined here are not redirected.

**Class ID:** Device class

**Subclass ID:** Subclass relating to the specified device class

**Name:** Free text entry

**Override serial:** Serial number that will appear in the session

**Override name:** Device name that will appear in the session

**Postpone**

The USB device is only removed from the system (endpoint device) when the session starts.

The USB device is no longer shown immediately after the system is booted.

This setting is only effective if the **Takeaway** parameter is enabled.

**Takeaway**

The USB device may be removed from the system (endpoint device).

The USB device may not be removed.

**No Reset**

The device will not be automatically reset after the connection with the session has been terminated.

The device will be reset after the connection with the session has been terminated.

Device Rules

A device rule applies to a specific device that is identified by its serial number.

Device rule settings:

**Rule:**

- Allow
- Deny

**Vendor ID:** Hexadecimal manufacturer number

**Product ID:** Hexadecimal device number



To find out the **Vendor ID** and **Product ID** of the connected USB device, use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal. You can also use the **System Information** tool, see [Using “System Information” Function\(see page 1108\)](#).

**Name:** Free text entry

**Override serial:** Serial number that will appear in the session.

**Override name:** Device name that will appear in the session.

#### Postpone

- The USB device is only removed from the system (endpoint device) when the session starts.
- The USB device is no longer shown immediately after the system is booted.

This setting is only effective if the **Takeaway** parameter is enabled.

#### Takeaway

- The USB device may be removed from the system (endpoint device).
- The USB device may not be removed.

#### No Reset

- The device will not be automatically reset after the connection with the session has been terminated.
- The device will be reset after the connection with the session has been terminated.

### Fabulatech Scanner Redirection

Menu path: **Sessions > Citrix > Citrix Global > Fabulatech Scanner Redirection**

Redirection for a Fabulatech scanner can be allowed during a Citrix session.

#### Fabulatech Scanner for Remote Desktop

- Fabulatech Scanner for Remote Desktop is enabled.

For more information, see [Citrix Fabulatech Scanner Redirection\(see page 248\)](#).

### HDX Multimedia

Menu path: **Sessions > Citrix > Citrix Global > HDX Multimedia**

HDX multimedia redirection improves the playback of audio and video content during a Citrix session.

Hardware acceleration for multimedia playback is available on specific devices. For further information, see [Hardware Video Acceleration on IGEL OS\(see page 736\)](#).

See also an overview and best-practice recommendations for the use of webcams under [Webcam Redirection and Optimization\(see page 663\)](#).

#### Multimedia redirection



- Multimedia data are sent to the device and decoded there. (Default)  
 Multimedia data are decoded on the server.

#### HDX RealTime Webcam redirection

- Redirection is enabled.  
 Redirection is disabled. (Default)

#### Automatic HDX webcam configuration

- The endpoint device detects the characteristics of the webcam and derives 6 different quality levels from these characteristics. The user can choose a quality level with the **Resolution grade** parameter.  
 The webcam must be configured manually using **HDX Webcam frame rate** and the subsequent parameters. For information on how to determine the capabilities of the webcam, see [Using Webcam Information](#)<sup>257</sup>.

#### Resolution grade

Possible options:

- "Very low"
- "Low"
- "Normal"
- "High"
- "Very high"
- "Best": Highest resolution that is possible while maintaining a fluent video replay

**HDX Webcam frame rate:** The frame rate that is requested from the webcam

**HDX Webcam quality:** The image quality requested from the webcam. Range: 1-63

**HDX Webcam width:** The image width requested from the webcam

**HDX Webcam height:** The image height requested from the webcam

**HDX Webcam delay time:** Time to wait before the webcam is opened, in milliseconds

#### HDX Webcam delay type

Possible options:

- "0": No delay
- "1": If the time interval since the last closing of the webcam is less than the defined delay time (**HDX Webcam delay time**), the delay length is the remaining time.
- "2": The delay time is as defined by **HDX Webcam delay time**.

#### HDX RealTime Media Engine

- The HDX RealTime Media Engine is enabled and significantly improves the performance of Lync / Skype for Business. (Default)  
 The HDX RealTime Media Engine is not used.

#### Browser content redirection

- The browser content is redirected from the server to the device, e.g. to relieve the load on the server.  
 Browser content redirection is disabled. (Default)

---

<sup>257</sup> <https://kb.igel.com/display/ENLITEIGELOSRI4/Using+Webcam+Information>



## Codec

Menu path: **Setup > Sessions > Citrix > Citrix Global > Codec**

- **Graphical codec:** Decoding method for the transferred screen content
  - Automatic: Automatically selects the appropriate codec according to the performance of the hardware.
  - H.264 Deep Compression Codec:
    - High image quality is possible, with lower network load
    - Without available hardware acceleration it is very CPU intensive.

At the Citrix Server following policies must be set:

- **Use video codec for compression** must be enabled.
- **For the entire screen**: Text tracking should be enabled if bandwidth is not a problem to increase readability in Office applications
- **For actively changing regions**: Citrix Receiver 13.6+ required, otherwise JPEG fallback will be loaded
- **Use video codec when preferred**: If **For actively changing regions** is selected by Citrix, a Citrix receiver 13.6+ must be activated, otherwise JPEG fallback is loaded.

- JPEG:
  - High image quality possible, with high network load
  - Moderate CPU load

Additional parameters for H.264 Deep Compression Codec

These parameters are relevant if **Automatic** or **H.264 Deep Compression Codec** is selected.

- **Accelerated H.264 Deep Compression Codec**
    - Enables hardware-accelerated decoding with H.264, which reduces CPU load.
    - Uses the software implementation of H.264 and results in a greater CPU load. (default)
- For more information, read the [Setting up Citrix Sessions with Hardware-Accelerated H.264 Deep Compression Codec<sup>258</sup>](#) How-To.

Following options are available in combination with H.264 Deep Compression Codec:

- **Text tracking:**
  - Loss-free depiction of texts (default)

Text is displayed sharper, especially if "Visual Quality" is set to Low/Medium. Recommended for office applications, but requires a higher available bandwidth. With bad connection and EDT over UDP it can lead to missing text parts.
- **Small frames feature:**

<sup>258</sup> <https://kb.igel.com/display/igelos/Setting+up+Citrix+Sessions+with+Hardware-Accelerated+H.264+Deep+Compression+Codec>



- Pixel-perfect depiction of lines etc. (default)

This feature allows efficient processing when only a small part of the screen changes over time (for example, when a cursor flashes on an otherwise stable background).

#### Additional parameters for JPEG

These parameters are relevant if **JPEG** is selected.

- **JPEG direct-to-screen decoding**
  - Decodes image tiles directly without using a bitmap cache.
  - No JPEG direct-to-screen decoding (default)
- **JPEG batch decoding**
  - Enables batch processing and delayed XSync. (default)

#### Unified Communications

Menu path: **Sessions > Citrix > Citrix Global > Unified Communications**

- [VDI Solutions](#)(see page 795)
- [Skype for Business](#)(see page 796)
- [Cisco](#)(see page 796)

See also an overview and best-practice recommendations for the use of webcams under [Webcam Redirection and Optimization](#)(see page 663).

#### VDI Solutions

Menu path: **Sessions > Citrix > Citrix Global > Unified Communications > VDI Solutions**

##### Microsoft Teams optimization

- The audio and video streams for Microsoft Teams are redirected between the endpoint devices. Audio and video data are not processed by the server.
- The audio and video streams for Microsoft Teams are not redirected.

##### Server and Network Requirements

Microsoft Teams optimization requires additional configuration on the Citrix VDI Desktop image, as well as some additional network configurations.

For more information, please see the following article by Citrix: <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/multimedia/opt-ms-teams.html>

#### Zoom Media Plugin

- The audio and video streams for Zoom are redirected between the endpoint devices. Audio and video data are not processed by the server.
- The audio and video streams for Zoom are not redirected.



## Skype for Business

Menu path: **Sessions > Citrix > Citrix Global > Unified Communications > Skype for Business**

The HDX RealTime Media Engine is required for using Skype for Business in a Citrix session.

### HDX RealTime Media Engine

- The HDX RealTime Media Engine is active. (Default)
- The HDX RealTime Media Engine is not active.

## Cisco

Menu path: **Sessions > Citrix > Citrix Global > Unified Communications > Cisco**

Here, you can activate or deactivate the virtual desktop optimization for Cisco Webex and define settings for the Cisco JVDI client.

**Cisco Webex Meetings VDI:** This virtual desktop optimization contains a media engine and redirects the audio and video streams so that they are exchanged directly between the endpoint devices and Webex Meetings cloud, without going through the hosted virtual desktop in the datacenter.

Make sure both your client-side Cisco Webex Meetings plugin and the server-side application have the same version. Otherwise, the Cisco Webex Meetings VDI solution might not work.

To select the version of the Cisco Webex Meetings plugin:

1. In the UMS configuration dialog or the local Setup, go to **System > Registry > multimedia > ciscomeetings > activeversion**.
2. Select the desired version and click **Apply** or **Ok**.

For further information, see the Cisco documentation:

- General information: <https://help.webex.com/en-us/nfjsqzbb/Cisco-Webex-Meetings-Virtual-Desktop-Software>
- Overview about supported Webex Meetings VDI versions <https://help.webex.com/en-us/nfjsqzbb/Cisco-Webex-Meetings-Virtual-Desktop-Software>
- Administration Guide: [https://www.cisco.com/c/en/us/td/docs/collaboration/webex\\_vdi/admin/webex\\_b\\_admin-cisco-wmmdi-40-8.html](https://www.cisco.com/c/en/us/td/docs/collaboration/webex_vdi/admin/webex_b_admin-cisco-wmmdi-40-8.html)<sup>259</sup>
- Installation: [https://www.cisco.com/c/en/us/td/docs/collaboration/webex\\_vdi/admin/webex\\_b\\_admin-cisco-wmmdi-40-8/webex\\_m\\_wvdi-software-installation.html](https://www.cisco.com/c/en/us/td/docs/collaboration/webex_vdi/admin/webex_b_admin-cisco-wmmdi-40-8/webex_m_wvdi-software-installation.html)

- The Cisco Webex Meetings VDI solution is enabled.

- The Cisco Webex Meetings VDI solution is disabled.

---

❾ [https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.cisco.com%2Fc%2Fen%2Fus%2Ftd%2Fdocs%2Fcollaboration%2Fwebex\\_vdi%2Fadmin%2Fwebex\\_b\\_admin-cisco-wmmdi-40-8.html&data=04%7C01%7Cfeeney%40igel.com%7Cbbb4ae6a9db34ec84a0b08d88cee6ac9%7C3f04441122ea4ba182dfd85e25879b4f9%7C0%7C0%7C637414302911303723%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBtil6Ik1haWwiLCJVCI6Mn0%3D%7C1000&sdata=NrHywiQaoFcql5f%2FCRgK2BJw7%2BFfWirNQNj4MYTz0s%3D&reserved=0](https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.cisco.com%2Fc%2Fen%2Fus%2Ftd%2Fdocs%2Fcollaboration%2Fwebex_vdi%2Fadmin%2Fwebex_b_admin-cisco-wmmdi-40-8.html&data=04%7C01%7Cfeeney%40igel.com%7Cbbb4ae6a9db34ec84a0b08d88cee6ac9%7C3f04441122ea4ba182dfd85e25879b4f9%7C0%7C0%7C637414302911303723%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBtil6Ik1haWwiLCJVCI6Mn0%3D%7C1000&sdata=NrHywiQaoFcql5f%2FCRgK2BJw7%2BFfWirNQNj4MYTz0s%3D&reserved=0)



**Cisco Webex Teams VDI:** This virtual desktop optimization contains a media engine and redirects the audio and video streams so that they are exchanged directly, without going through the hosted virtual desktop in the datacenter. For further information, see the Cisco documentation:

- Overview about supported Webex Teams VDI versions [https://help.webex.com/en-us/ntp1us7/Webex-VDI-Release-Notes#Cisco\\_Reference.dita\\_13d9aace-b6f9-41dc-a6e0-9f7a48834060](https://help.webex.com/en-us/ntp1us7/Webex-VDI-Release-Notes#Cisco_Reference.dita_13d9aace-b6f9-41dc-a6e0-9f7a48834060)

The Cisco Webex Teams VDI solution is enabled.

The Cisco Webex Teams VDI solution is disabled.

Settings for the Cisco JVDI Client

#### Cisco JVDI Client

The Cisco JVDI Client is enabled.

The Cisco JVDI Client is disabled.

For the vendor documentation for the Cisco JVDI client, see [Deployment and Installation Guide for Cisco Jabber Softphone for VDI Release 12.9<sup>260</sup>](#).

If you do not see the option **Cisco JVDI Client**, check if **Cisco JVDI Client** is enabled under **System > Firmware Customization > Features**. Reboot the device if required.

#### Audio

**Default volume:** Headphone volume control. (Default: 80%)

**Default microphone volume:** Microphone volume control. (Default: 80%)

**Default ring volume:** Ringtone volume control. (Default 100%)

**Internal sound card:** Here you have the possibility to define a sound card. If you leave the field empty, the default sound card of the system is used.

For further information, see [Sound Preferences](#)(see page 1066).

#### Video

You can set the Cisco JVDI Client to use the default resolutions of the camera or to use a user-defined set of resolutions. Separate configurations for cameras with and without hardware acceleration are possible.

##### Allow default resolutions (for cameras without hardware resolution)

The default resolutions of the camera are used.

A user-defined set of resolutions is used. You can add a resolution by clicking in the **Camera** area and selecting the desired resolution.

##### Allow default resolutions (for cameras with hardware resolution)

The default resolutions of the camera are used.

A user-defined set of resolutions is used. You can add a resolution by clicking **[+]** in the **Hardware Accelerated Camera** area and selecting the desired resolution.

---

<sup>26</sup> [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/jvdi/12\\_9/dig/jvdi\\_b\\_deploy-install-jvdi-12-9/jvdi\\_b\\_deploy-install-jvdi-12-9\\_chapter\\_01.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jvdi/12_9/dig/jvdi_b_deploy-install-jvdi-12-9/jvdi_b_deploy-install-jvdi-12-9_chapter_01.html)



## Citrix StoreFront

Menu path: **Sessions > Citrix > Citrix StoreFront**

Most of the settings were already configured under Citrix Global.

---

- [Server](#)(see page 798)
- [Login](#)(see page 799)
- [Appearance](#)(see page 800)
- [Reconnect](#)(see page 801)
- [Refresh](#)(see page 803)
- [Logoff](#)(see page 804)
- [Desktop Integration](#)(see page 805)

### Server

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront > Server**

- **Server location:** You can set up up to 5 Citrix master browsers per domain. If the first browser is not available, the second will be queried and so on. Please note that multiple farms can be searched. You can therefore specify addresses for a number of server farms.
- To manage the list, proceed as follows:
  - Click on to create a new entry.
  - Click on to remove the selected entry.
  - Click on to edit the selected entry.
  - Click on to copy the selected entry.

### Add

- **Protocol:**
  - https://
- **Citrix Store site address:** Server name or IP address of the server
- **Port:** Network port on which the service is available (default: 443)
- **Path to Store:** (default: [Citrix/Store](#))
- **Store name:** Name of the Citrix store

### Domains

- To manage the list of **domains**, proceed as follows:
  - Click on to create a new entry.
  - Click on to remove the selected entry.
  - Click on to edit the selected entry.
  - Click on to copy the selected entry.

### Handling of domain in login window:

- [normal](#)



- locked
- hidden

## Login

Menu path: **Sessions > Citrix > Citrix StoreFront > Login**

In this area, you can define session-specific login options.

**Authentication type:** Depending on the Citrix client version, the following types are available:

- Password authentication: Suitable for on-premises connections; connections via Citrix NetScaler or to a cloud environment may cause problems.
- Kerberos passthrough authentication: Uses local login data for listing and launching applications. The option enables single sign-on if login with AD/Kerberos is configured on the device.
- Smartcard authentication (StoreFront only, not Web Interface)
- Citrix authentication mechanism (instead of IGEL), Smartcard disabled
- Citrix authentication mechanism (instead of IGEL), Smartcard enabled

If you have set an authentication type with smartcard, select the type of card on the [Smartcard](#)(see page 1249) page.

Additional options include the following:

### Use passthrough authentication

- Cached login data are used for listing and starting applications.  
 No passthrough authentication (default)

### Auto login

- Uses the login data preset on this page when connecting to the server.  
 Do not log on automatically (default)

**User name:** Can only be filled in with password authentication

**Password:** Can only be filled in with password authentication

Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

**Domain:** Can only be filled in with password authentication

### Remember username and domain:

- Saves the user name and domain from the last login. (default)  
 The user name and domain will not be saved.

### Synchronize Citrix password with screen lock:

- Synchronizes the screen lock password with that of the Citrix application.  
 No synchronization (default)



### **Relaunch Citrix login after logout:**

- Automatically shows the login dialog again after logging off.
- Does not start the login procedure again. (default)

**Start a single published application automatically:** This parameter is relevant if exactly 1 published application is provided for the user whose login is configured here.

- The published application is started when the user has logged in.
- The published application is not started on login. (default)

**Start following applications automatically after server connection is established:** A list of applications to be started in the session.

To edit the list, proceed as follows:

- Click on to create a new entry. In the Add dialog, give the name of the application.

You can also enter part of the name followed by an asterisk (\*).

- Click on to remove the selected entry.
- Click on to move the entry upwards.
- Click on to move the entry downwards.

After a successful login, the associated desktop icon for each available application will be placed on the device desktop. All applications whose name matches one of the names given in the **Start following applications automatically after server connection is established** area will then be launched.

## Apearance

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront > Appearance**

- **Show applications in the start menu**

- Applications will appear in the start menu (default)
- Applications will not appear in the start menu

- **Show in the start menu**

- All: All Citrix applications will be shown in the start menu.
- Follow server settings

- **Resize icons for the start menu**

- The size of icons for the start menu will automatically be adjusted. (default)

Automatic scaling can prolong the logon procedure.

- **Apply display filter to start menu entries**

- Only the applications selected in the display filter will be shown in the start menu.
- Do not use display filter (default)

- **Show applications in the Application Launcher**

- Applications will be shown in the Application Launcher. (default)

- **Apply display filter to Application Launcher entries**

- Only the applications selected in the display filter will be shown in the Application Launcher.



- Do not use display filter (default)
- **Show applications on desktop**
  - The applications will be shown on the desktop. (default)
- **Keep folder structure on desktop**
  - The Citrix sessions are shown in their directory structure on the desktop.
  - The directory structure is not shown. (default)
- **Show desktop shortcuts**
  - All: All Citrix applications will be shown in the Desktop Launcher.
  - Follow server settings
- **Apply display filter to desktop icons**
  - Desktop icons are created only for the applications selected in the display filter (see below). (default)
- **Display filter: Show only the following applications.** In the **Add** dialog, enter the name of the application that is to be shown on the desktop.  
To manage the list, proceed as follows:
  - Click on to create a new entry.
  - Click on to remove the selected entry.
  - Click on to edit the selected entry.
- **Enable following applications in quick start panel:** In the **Add** dialog, enter the name of the application that is to be shown in the quick start panel.

## Reconnect

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront > Reconnect**

- **Automatic reconnection at logon**
  - Connection will take place when logging on.
  - Do not reconnect (default)
- **Connect to**  
Possible values:
  - Active and terminated sessions
  - Terminated sessions only
  - Ask user
- **Automatic reconnection from menu/desktop**
  - Reconnect**
  - Do not reconnect (default)
- **Connect to**  
Possible values
  - Active and terminated sessions
  - Terminated sessions only
  - Ask user
- **Reconnect session name:** Session name (default: Reconnect)

## Starting Methods for Sessions

- **Start menu:** If this option is enabled, the session can be launched from the start menu.



- **Application Launcher:** If this option is enabled, the session can be launched with the Application Launcher.
- **Desktop:** If this option is enabled, the session can be launched with a program launcher on the desktop.
- **Quick start panel:** If this option is enabled, the session can be launched with the quick start panel.
- **Start menu's system icon:** If this option is enabled, the session can be launched with the start menu's system icon.
- **Application Launcher's system icon:** If this option is enabled, the session can be launched with the Application Launcher's system icon.
- **Desktop context menu:** If this option is enabled, the session can be launched with the desktop context menu.
- **Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.
- **Path in the Application Launcher:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.
- **Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.
- **Password protection:** Specifies which password will be requested when launching the session.  
Possible values:
  - **None:** No password is requested when launching the session.
  - **Administrator:** The administrator password is requested when launching the session.
  - **User:** The user password is requested when launching the session.
  - **Setup user:** The setup user's password is requested when launching the session.
- **Hotkey:**  
 The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.
- **Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. **Ctrl**. Here, you will find the available modifiers and the associated key symbols:
  - (No modifier) = None
  -  = Shift
  -  = Ctrl
  -  = Super\_L
  -  = Alt

Key combinations are formed as follows with |:

- **Ctrl + ** = Ctrl | Super\_L

- **Key:** Key for the hotkey



To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field.  
Example: Tab in (`keysym 0xff09, Tab`)

## Refresh

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront > Refresh**

- **Refresh Session Name:** (default: Update)

## Starting Methods for Session

- **Start menu**  
 The session can be started with the start menu. (default)
- **Application Launcher**  
 The session can be started with the Application Launcher. (default)
- **Desktop**:  
 The session can be started with a program starter on the desktop. (default)
- **Quick start panel**  
 The session can be started with the quick start panel. (default)
- **Start menu's system icon**  
 The session can be started with the start menu's system icon.  
 The session cannot be started with the start menu's system icon. (default)
- **Application Launcher's system icon**  
 The session can be started with the Application Launcher's system icon.  
 The session cannot be started with the Application Launcher's system icon. (default)
- **Desktop context menu**  
 The session can be started with the desktop context menu. (default)
- **Menu folder**: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.
- **Desktop folder**: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.
- **Password protection**: Specifies which password will be requested when launching the session. (default: disabled)
  - Possible values:
    - **None**: No password is requested when launching the session.
    - Administrator: The administrator password is requested when launching the session.
    - User: The user password is requested when launching the session.
    - Setup user: The setup user's password is requested when launching the session.
- **Hotkey**: Specifies a hotkey consisting of modifiers and a key which can be used to launch the session. (default: disabled)
  - **Modifiers**: One or two modifiers for the hotkey



- **Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log in as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the character string for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

## Logoff

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront > Logoff**

- **Logoff session name:** Session name (default: Logoff)

### Starting Methods for Session

- **Session name:** Name for the session

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

- **Start menu:**
  - The session can be started with the start menu. (Default)
  - The session cannot be found in the start menu.
- **Application Launcher:**
  - The session can be started with the Application Launcher. (Default)
  - The session cannot be found in the Application Launcher.
- **Desktop:**
  - The session can be started with a program starter on the desktop. (Default)
  - The session does not have a program starter on the desktop.
- **Quick start panel:**
  - The session can be started with the quick start panel.
  - The session cannot be found in the quick start panel. (Default)
- **Start menu's system icon:**
  - The session can be started with the start menu's system icon.
  - The session cannot be found in the start menu's system icon. (Default)
- **Application Launcher's system icon:**
  - The session can be started with the Application Launcher's system icon.
  - The session cannot be found in the Application Launcher's system icon. (Default)
- **Desktop context menu:**
  - The session can be started with the desktop context menu.
  - The session cannot be found in the desktop context menu. (Default)
- **Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.



- **Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.
- **Password protection:** Specifies which password will be requested when launching the session. Possible values:
  - **None:** No password is requested when launching the session.
  - **Administrator:** The administrator password is requested when launching the session.
  - **User:** The user password is requested when launching the session.
  - **Setup user:** The setup user's password is requested when launching the session.
- **Hotkey:** A hotkey with which the session can be started is defined. It consists of modifiers and a key.
- **Modifiers:** One or two modifiers for the hotkey:
  - None
  - = Shift
  - [Ctrl] = Ctrl
  - = Super\_L
  - [Alt] = Alt

Modifiers can be combined by using the pipe character | :

- [Ctrl]+ = Ctrl|Super\_L

- **Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the character string for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

## Desktop Integration

Menu path: **Sessions > Citrix > Citrix StoreFront> Desktop Integration**

**Login session name:** Session name.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.



### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
-  = Ctrl
-  = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.



- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

### Autostart

The session will be launched automatically when the device boots.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

### Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

## Citrix Self-Service

Menu path: **Sessions > Citrix > Citrix Self-Service**

The Citrix Self-Service interface allows access to Citrix Virtual Desktops and Apps via Self-Service UI.

- [Server](#)(see page 807)
- [Options](#)(see page 808)
- [Desktop Integration](#)(see page 809)

### Server

Menu path: **Setup > Sessions > Citrix > Citrix Self-Service > Server**

To manage the list, proceed as follows:

- ▶ Click on to create a new entry.
- ▶ Click on to remove the selected entry.
- ▶ Click on to edit the selected entry.



- ▶ Click on to copy the selected entry.

## Server: Web Interface

Add:

- **Protocol:**
  - [http://](#)
  - [https://](#)
- **Server:** Name or IP address of the server
- **Server port:** Port on which the service is available (default: [80 \(http\)](#), [443 \(https\)](#))
- **Path to config.xml file:** (default: [Citrix/PNAgent/config.xml](#))
- **Store Name:** Name for the store

## Server: StoreFront

Add:

- **Protocol:**
  - [http://](#)
  - [https://](#)
- **Server:** Name or IP address of the server
- **Server port:** Port on which the service is available (default: [80 \(http\)](#), [443 \(https\)](#))
- **Path to the store (default: Citrix/Store)**
- **Store Name:** Name for the store

## Server: StoreFront Legacy Mode

Add:

- **Protocol:**
  - [http://](#)
  - [https://](#)
- **Server:** Name or IP address of the server
- **Server port:** Port on which the service is available (default: [80 \(http\)](#), [443 \(https\)](#))
- **Path to the config.xml file (default: Citrix/Store/PNAgent/config.xml)**
- **Store Name:** Name for the store

## Options

Menu path: **Setup > Sessions > Citrix > Citrix Self-Service > Server > Options**

- **Display mode:** Display type for the Self-Service user interface

Possible values:

- [Window](#)
- Full screen

In full screen mode, the IGEL desktop will not be available.

- **Multi user**

The user data on the client will be deleted after logging off or terminating Self-Service. (default)



- **Reconnect after logon:**
  - The Self-Service user interface reconnects automatically to applications and desktops after being launched.
  - The Self-Service user interface does not reconnect automatically.
- **Reconnect to apps after starting an application:**
  - The Self-Service user interface will attempt to reconnect to ongoing sessions if an application is launched or the store is reloaded.
  - The Self-Service user interface will not attempt to reconnect. (default)

## Desktop Integration

**Self-Service session:** Name for the Self-Service session. (Default: Self-Service)

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

### Autostart

The session will be launched automatically when the device boots.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.



### Autostart requires network

- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.

## 3.8.4 RDP Global

Menu path: **Setup > Sessions > RDP > RDP Global**

This section describes the procedure for configuring the global RDP settings. This configuration applies for all RDP sessions.

The protocol version cannot be configured manually. The version used by the server is automatically recognized and used.

- 
- [Gateway](#)(see page 811)
  - [Local Logon](#)(see page 812)
  - [Window](#)(see page 813)
  - [Keyboard](#)(see page 815)
  - [Mapping](#)(see page 815)
  - [Performance](#)(see page 820)
  - [Options](#)(see page 823)
  - [Native USB Redirection](#)(see page 823)
  - [Fabulotech USB Redirection](#)(see page 825)
  - [Fabulotech Scanner Redirection](#)(see page 827)
  - [Multimedia](#)(see page 827)

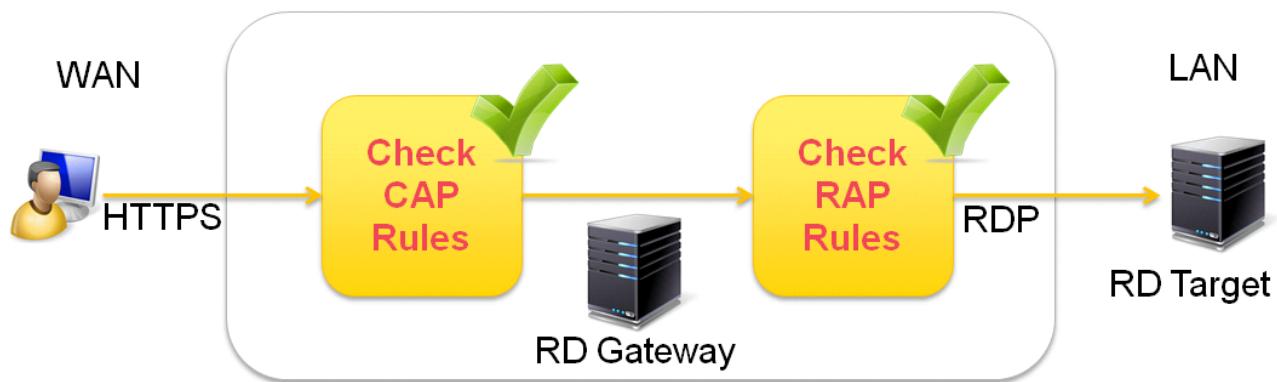
### Gateway

Menu path: **Setup > Sessions > RDP > RDP Global > Gateway**

Via *Microsoft Remote Desktop Gateway*, you can access remote *Windows* systems.

The gateway translates between the internal *Remote Desktop Protocol* (RDP) and the external HTTPS connection.

Access to the Remote Desktop environment is provided via the browser. The browser establishes a secure connection to the gateway. From here, the connection query is forwarded to the target system. In the process, pre-defined *Connection Access Policies* and *Resource Access Policies* (CAP and RAP) for access control are evaluated.



#### Enable gateway support:

- Gateway support is enabled and you can configure the following settings:
- Gateway support is disabled. (default)

- **Gateway address**

**RD gateway** requires *Microsoft Windows Server 2008R2 or Server 2012* with various restrictions for each server version.

The following Windows Server editions can preferably be used as gateway servers:

Server 2008R2 Standard (restricted to 250 RD Gateway connections)  
 Server 2008R2 Enterprise  
 Server 2008R2 Datacenter  
 Server 2012 Standard  
 Server 2012 Datacenter  
 Server 2012 Essential (restricted to the RD Gateway role)  
 Server 2012R2 Standard  
 Server 2012R2 Essential (restricted to the RD Gateway role)

RD Gateway is not supported in the IGEL RDP Legacy Mode.

- **Use other logon data for RD gateway**

- Uses custom data that can be defined below rather than the session access data.
- Uses the session access data. (default)
  - **Gateway user name:** User name when logging on to the gateway
  - **Gateway password:** Password when logging on to the gateway
  - **Gateway domain:** Domain in which the gateway is located

#### Local Logon

Menu path: **Setup > Sessions > RDP > RDP Global > Local Logon**

In this area, you can prepopulate user data. As a result, you can avoid users possibly having to log in a number of times.



You can also use **Local logon** to freely select the server in the logon window of an RDP session.

- **Use local login window**

The RDP login window is used on the terminal side to set the user name and domain when a connection to the terminal server is established for the first time. (default)

You can configure the following presets:

- **Preset login information**

The login window is prepopulated with the user name and domain. (default)

- **Type:** Here, you can prepopulate the user name and domain in the logon window.

Possible values:

- Set user/domain from last login
- Set user/domain from session setup

- **Show domain**

Shows the domain entry in the logon window. (default)

- **Set client name to user name**

The name of the client for the RDP connection will be set to the user name. This setting may help to resolve reconnection problems during load balancing. (default)

- **Relaunch mode**

The RDP login window is displayed in restart mode and cannot be closed.

The RDP window will not be displayed in restart mode. (default)

- **Enable network authentication**

Enables network authentication via NTLM. Smartcards are not supported here. (default)

- **Domains:** Allows you to add domains which are to be available. If you enter a number of domains, these will be shown in the **Domains** drop-down area in the login module.

To manage the list of domains, proceed as follows:

- ▶ Click to create a new entry.
- ▶ Click to remove the selected entry.
- ▶ Click to edit the selected entry.
- ▶ Click to copy the selected entry.

## Window

Menu path: **Sessions > RDP > RDP Global > Window**

In this area, you can configure the window for RDP sessions.

You can change the following settings:

**Number of Colors:** Specifies the color depth.

Possible values:

- 256
- Thousands



- Millions

**Window size:** Specifies the width and height of the window.

- Full-screen: The session is shown on the full screen. The device's taskbar is not visible.
- Work area: The session is shown on the full screen, minus the area needed by the device's taskbar.
- Numeric details: The session is shown in the selected resolution or on the selected percentage of the screen area.

**Desktop scale factor:** Specifies the desktop scaling in percent. Select a value from the selection list or enter a percentage value manually.

Desktop scaling is supported from Windows Server 2012 or higher and from Windows 8.1 or higher.

Possible values:

- Automatic: The resolution set under **User Interface > Display > Options > Monitor-DPI** will be used for the RDP session.
- Numeric details: The display will be magnified by the factor given here. Value range: 100% - 500%

Set the **Desktop scale factor** to a fixed value of 100% to allow server-side desktop scaling take effect. All values other than 100% overwrite the server-side setting.

### Enable Display Control

The window size can be changed during the session. (Default)

If the window size is to be changed during the session, at least Windows 8.1 or Windows Server 2012 R2 must be running on the server.

It is not possible to change the window size during the session if **Window size** is set to **full-screen** or **workarea**.

### Control Bar for RDP-Sessions

A control bar for minimizing and closing a full-screen session will be shown.

No control bar will be shown. (Default)

If the symbol bar is enabled, a session will be shown on one monitor only, even if **Multimonitor fullscreen mode** is set to **Expand full-screen session across all monitors**.

**Multimonitor full-screen mode** - If more than one monitor is connected to the terminal:

- Restrict full-screen session to one monitor
- Display full-screen session on all monitors
- Expand full-screen session across all monitors



## Keyboard

Menu path: **Setup > Sessions > RDP > RDP Global > Keyboard**

Configure how the keyboard reacts within RDP sessions. The following options are available:

- **Enable clipboard**  
 You can use the clipboard. (default)
- **Input language:** Here, you can determine which language is used for auto-correction in the RDP session. This is independent of the keyboard layout. The "Default" setting corresponds to the system setting. (default: Default).
- **Override local window manager keyboard shortcuts**  
 All keyboard entries, including those which would otherwise be processed by the local window manager, will be sent straight to the Windows server.  
 The keyboard shortcuts of the local window manager will not be overridden. (default)

## Mapping

Menu path: **Sessions > RDP > RDP Global > Mapping**

In this area, you can make available locally connected devices such as printers or USB storage devices in RDP sessions.

- [Drive Mapping](#)(see page 815)
- [COM Ports](#)(see page 816)
- [Printers](#)(see page 817)
- [Device Support](#)(see page 818)
- [Audio](#)(see page 819)

### Drive Mapping

Menu path: **Sessions > RDP > RDP Global > Mapping > Drive Mapping**

Through drive mapping, connected mass storage devices can be made available in the session. Specify which folders or drives are mapped during the login.

#### Enable Drive Mapping

- Drive mapping is enabled. (Default)

Local (USB) devices which are to be used for drive mapping purposes must first be set up as devices. See [Storage Hotplug](#)(see page 1228).



Before you unplug a hotplug storage device from the endpoint device, you must safely remove it. Otherwise, data on the hotplug storage device can be damaged. Depending on the configuration, there is one or several possibilities to safely remove a hotplug storage device:

- Click on in the task bar. The taskbar is not available in a fullscreen session.
- Click on in the in-session control bar. Depending on the configuration, the in-session control bar may be available in a fullscreen session. For further information, see [In-Session Control Bar](#)(see page 1154).
- Function **Accessories > Safely Remove Hardware** with further starting possibilities; amongst other things, a hotkey can be defined here.  
If the following warning is displayed: **Volume(s) still in use. Don't remove the device**, then the hotplug storage device must not be removed. First, exit the program concerned or close all files or directories that reside on the hotplug storage device.

#### **Drive Mapping:** List of mapped drives.

To set up drive mapping, proceed as follows:

1. Click **Add** to bring up the mapping window.
2. Click **Enabled** to enable the drive connection.
3. Select a **Drive to map** from the list under which the local device or the folder is to be mapped.

If the drive letter you have selected is no longer available on the server, the specified directory or local drive will be given the next free letter during the login.

4. Give the **Local Drive Path** of the local directory to which the mapping is to refer.

If you map a locally connected device, use the pre-defined path names available in the drop-down field. The directories in question are those on which the devices are mounted by default during the boot procedure (e.g. /autofs/floppy for an integrated floppy drive).

#### COM Ports

Menu path: **Setup > Sessions > RDP > RDP Global > Mapping > Serial Connections**

As with locally connected mass storage devices, you can also map the device's local serial connections (COM ports) during an RDP session:

- **Enable COM port mapping:**  
 COM port mapping is enabled. (default)
- **Server COM Port starts with:** Specifies the lowest device number that is used on the server for mapping. Possible values:
  - COM 1 to COM 6. (default: COM1)
- **COM Port Devices:** List with mapped local serial devices.  
Click to add a serial device.



- **COM Port Device:**

Possible values:

"COM 1"

"COM 2"

"COM 3"

"COM 4"

"USB COM 1": For UD3-LX60 devices (mainboard: M350C), this port must be used instead of "COM 1".

"USB COM 2"

"USB COM 3"

"USB COM 4"

- **Detect Devices....**: Opens a dialog allowing you to select the device file. 3 device files are available for each device; the **Description** column shows the type of device file:

- (GENERIC) [device designation]: Generic type. The name of the device file ends in a consecutive number which depends on the boot procedure or the order of insertion.  
Example: /dev/ttyUSB0
- (BY PORT) [device designation]: According to the USB port. The device file is in the /dev/usbserial/ directory. The name of the device file ends in the number of the USB port that the device is plugged into. Example: /dev/usbserial/ttyUSB\_P12
- (BY USBID) [device designation]: According to USB ID. The device file is in the /dev/usbserial/ directory. The name of the device file ends as follows: \_V[Vendor ID]\_P[Product ID]. Example: /dev/usbserial/ttyUSB\_V067b\_P2303
- (Virtual) [device designation]: Virtual device; used for signature pads for example. Example: /dev/ttyVST0

If your device has an additional multiport PCI card, more than 2 connections may be available.

If you would like to use signature pads, you must enable them beforehand under **User Interface > Input > Signature Pad**(see page 1167).

## Printers

Menu path: **Setup > Sessions > RDP > RDP Global > Mapping > Printers**

In this area, you can configure printer mapping.

### **Enable Client Printer Mapping**

The locally connected device printer is made available for your RDP sessions, provided that it was not disabled on the server-side. (default)



The printers must be set up on the **Devices > Printer > CUPS > Printers**(see page 1217) page and must be enabled there for mapping in RDP sessions.

Because the device merely places incoming print jobs in a queue, you need to install the printer on the server.

## Device Support

Menu path: **Setup > Sessions > RDP > RDP Global > Mapping > Device Support**

In this area, you can enable virtual RDP channels for communicating with various devices connected to the device.

The devices supported are listed in the [IGEL Third Party Hardware Database](#)<sup>261</sup>.

- **Enable plugin support**

- Communication between connected devices and the relevant server applications is enabled.  
The individual channels must also be enabled.  
 Communication between connected devices and server applications is not enabled. (Default)

When using *DriveLock*, ensure that the use of USB devices is not universally restricted; see **Devices > USB Access Control**<sup>262</sup>.

- **DriveLock channel:** The virtual DriveLock channel is implemented on the device. The channel must also be installed on the RDP server.

DriveLock can read hardware data from local USB devices and transfer these data to the server with the help of the virtual RDP channel extension. From IGEL Linux Version 10.03.500 this is also possible with SATA devices. When using whitelists, rules based on the hardware properties of the connected drive (e.g. manufacturer details, model and serial number) are taken into account.

Important information regarding DriveLock can be found in the [Using DriveLock with IGEL Devices](#)<sup>263</sup> FAQ.

- A virtual channel for DriveLock is enabled.  
 No virtual channel for DriveLock is enabled. (Default)

- **Diktamen channel for dictation**

- A virtual channel for Diktamen is enabled.  
 No virtual channel for Diktamen is enabled. (Default)

- **deviceTRUST channel**

- A virtual channel for deviceTRUST is enabled..  
 No virtual channel for deviceTRUST is enabled. (Default)

- **Grundig MMC channel for dictation with Grundig devices**

- A virtual channel for communication with Grundig devices is enabled.  
 No virtual channel for communication with Grundig devices is enabled. (Default)

- **Olympus channel for dictation**

- A virtual channel for communication with Olympus dictation devices is enabled.  
 No virtual channel for communication with Olympus dictation devices is enabled. (Default)

<sup>261</sup> <https://www.igel.com/linux-3rd-party-hardware-database/>

<sup>262</sup> <https://kb.igel.com/display/igelos1005/USB+Access+Control>

<sup>263</sup> <https://kb.igel.com/display/igelos/Using+DriveLock+with+IGEL+Thin+Clients>



- **Philips speech channel for dictation**

- A virtual channel for communication with Philips dictation devices is enabled.  
 No virtual channel for communication with Philips dictation devices is enabled. (Default)  
 • **DPM server drive:** Via this drive, the Philips PocketMemo dictation device makes the voice recordings available to the server. (Default: P)

The dictation device is automatically assigned to the selected drive letter. Ensure that no other Hotplug storage device is assigned to this drive letter. Further information can be found under [Hotplug storage device<sup>264</sup>](#) and [Drive mapping<sup>265</sup>](#).

- **SpeechAir server drive:** Via this drive, the Philips SpeechAir dictation device makes the voice recordings available to the server (default: S)

The dictation device is automatically assigned to the selected drive letter. Ensure that no other Hotplug storage device is assigned to this drive letter. Further information can be found under [Hotplug storage device<sup>266</sup>](#) and [Drive mapping<sup>267</sup>](#).

- **Lakeside SysTrack channel**

- The Lakeside SysTrack channel is enabled.  
 The Lakeside SysTrack channel is not enabled. (Default)

- **Enable smartcard**

- The device's smartcard reader will appear within the RDP session. Applications can access the reader and the smartcards it contains. (Default)  
 The device's smartcard reader will not appear within the RDP session.

## Audio

Menu path: **Setup > Sessions > RDP > RDP Global > Mapping > Audio**

In this area, you can configure the settings for local audio transmission.

- **Enable client audio**

Possible values:

- On: Audio will be transmitted.
- Off: No audio will be transmitted.

- **Audio quality mode**

Possible values:

- Automatic
- High: High audio quality is favored.
- Medium: Medium audio quality is favored.
- Dynamic

- **Audio compression**

Possible values:

<sup>264</sup> <https://kb.igel.com/display/igelos1005/Storage+Hotplug>

<sup>265</sup> <https://kb.igel.com/display/igelos/Drive+Mapping>

<sup>266</sup> <https://kb.igel.com/display/igelos1005/Storage+Hotplug>

<sup>267</sup> <https://kb.igel.com/display/igelos/Drive+Mapping>



- Automatic
  - On: Compressed audio data will be accepted.
  - Off: Compressed audio data will not be accepted.
  - **Audio recording**
- The microphone will be diverted to the session.  
 The microphone will not be diverted to the session. (Default)

## Performance

Menu path: **Setup > Sessions > RDP > RDP Global > Performance**

In this area, you can configure settings in order to improve the performance of the RDP session.

### Enable RemoteFX

Remote FX is enabled. (Default)

### RemoteFX codec mode

Possible options:

- Use server setting
- Optimized for LAN
- Optimized for WAN
- Legacy mode

### Hardware accelerated codecs AVC420/AVC444 (H.264)

Possible options:

- Automatic: H.264 is activated automatically if supported by the device's hardware.
- On: H.264 is activated, regardless of hardware support.

For testing purposes only; this option can lead to display flaws.

- Off: H.264 is deactivated.

► You can disable graphics functions which are not absolutely necessary.

Graphics settings that you can disable in order to improve performance:

### Disable wallpaper

Desktop background is disabled.

Desktop background is enabled. (Default)

### Don't show contents of window while dragging

Window content will be hidden.

Window content will be shown. (Default)

### Disable menu and window animation

Menu and window animation is disabled.

Menu and window animation is enabled. (Default)



#### Disable themes

- Themes are disabled.  
 Themes are enabled. (Default)

#### Disable cursor shadow

- Cursor shadow is disabled.  
 Cursor shadow is enabled. (Default)

#### Disable cursor settings

- Cursor settings are disabled. No "unnecessary" mouse movements will be sent.  
 Cursor settings are enabled. (Default)

#### Enable font smoothing

- Font smoothing is enabled.  
 Font smoothing is disabled. (Default)

#### Compression

In low-bandwidth environments, you should use **compression** in order to reduce network traffic. Note that the use of compression reduces the burden on the network but does use CPU power.

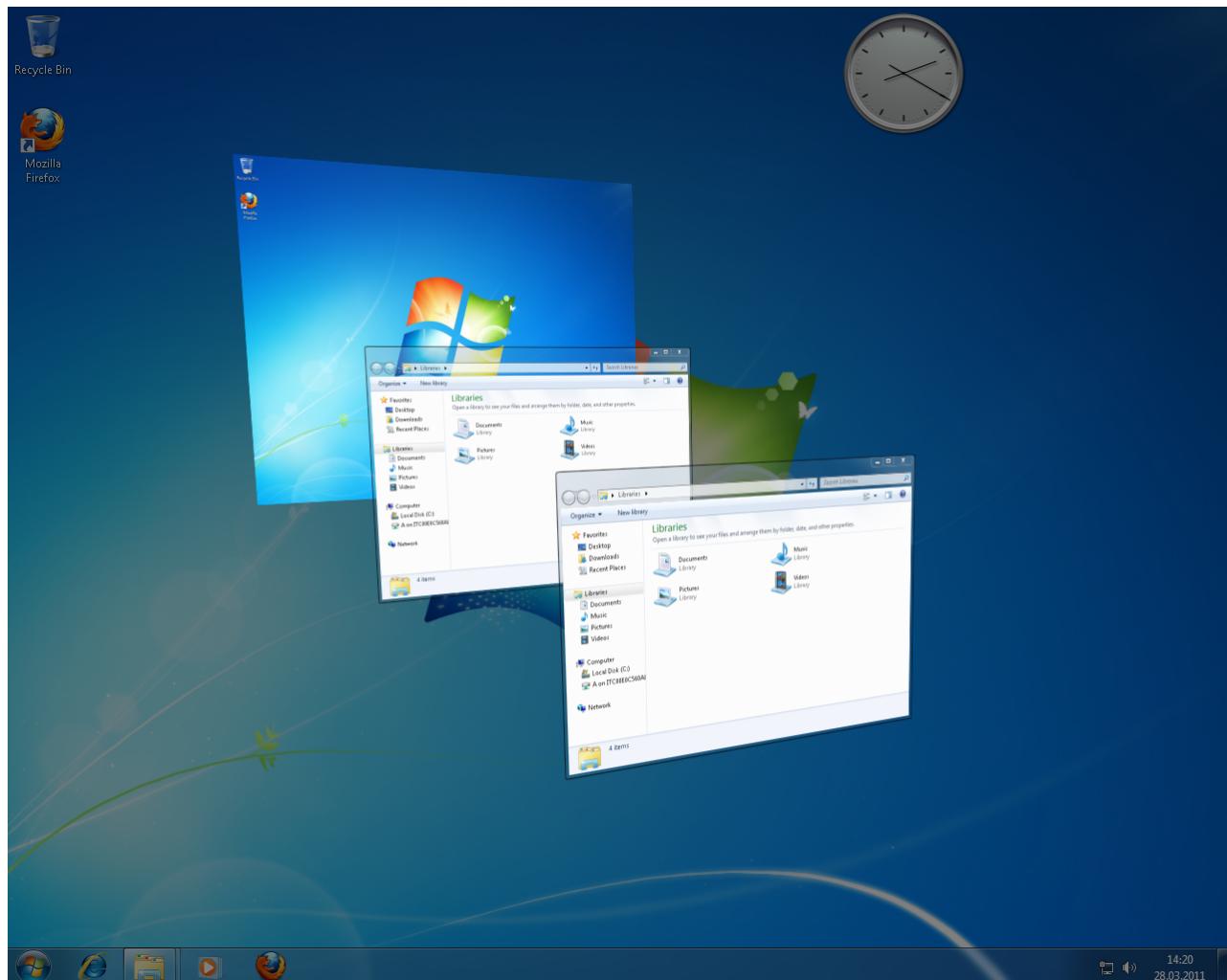
- Data are compressed.  
 Data flow is not compressed. (Default)

#### RemoteFX Support

Menu path: **Setup > Sessions > RDP > RDP Global > Performance > RemoteFX Support**

With the Service Pack 1 for *Windows Server 2008 R2*, local system functions such as *Windows Aero* or 3D display can be made available in RDP sessions too.

In order to do this, the RemoteFX extension for RDP must be enabled. You can configure the relevant settings under **RDP Global > Performance** or in the corresponding session settings.



Globally enabling Remote FX is not recommended as conventional RDP sessions may also be affected by this. With RemoteFX, all graphics effects available under Performance are enabled. This may slow down the session as a result. It is better to enable the function only for individual sessions which establish a connection to appropriately equipped servers.

Further information on Remote FX and the server-related requirements is available from Microsoft at [https://technet.microsoft.com/en-us/library/dd736539\(ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd736539(ws.10).aspx)<sup>268</sup>.

In the IGEL Registry, you can configure the number of frames sent by the server without confirmation under the key `rdp.winconnect.remotefx-ack`. The default value is 1. A value of 2 or 3 can lead to improved performance in networks with high latency.

<sup>268</sup> [http://technet.microsoft.com/en-us/library/dd736539\(ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd736539(ws.10).aspx)



## Options

Menu path: **Setup > Sessions > RDP > RDP Global > Options**

In this area, you can configure the following settings:

- **Inverted cursor color**

Possible values:

- Black
- White
- Dotted

You can also configure your own values custom: ,. The colors must be given in the ARGB8888 format, e.g. 0xFF000000.

- **Reset license**

- The Microsoft license will be removed from the device. The device must then be restarted.
- The license will not be removed. (default)

- **Reset confirmed server certificates**

- All confirmed server certificates will be deleted from the client.
- The certificates will not be deleted. (default)

- **Client name:** Client name for terminal service identification.

Possible values:

- Special client name: Specify a special client name in the next field.
- MAC address: Use the MAC address of the computer as the client name
- Computer name: Use the name of the computer

- **Custom client name:** If you have opted for a special client name, you can enter the name here. If the field remains empty, the MAC address of the client will be used automatically.

- **Verify server certificate**

- The server certificate will be verified if the connection is TLS-encrypted. (default)

## Native USB Redirection

Menu path: **Sessions > RDP > RDP Global > Native USB Redirection**

USB devices can be permitted or prohibited during an RDP session on the basis of default rules. Sub-rules for specific devices or device classes are also possible. The use of rules is described under [USB Access Control](#)(see page 1231).

Enable either **Native** or **Fabulatech USB Redirection** – not both together. For details on **Fabulatech USB Redirection**, see [Fabulatech USB Redirection](#)(see page 825).

Disable USB redirection if you use DriveLock. Further information can be found under [Using DriveLock with IGEL Devices](#)(see page 701).



### Enable native USB redirection

- Native USB redirection is enabled and you can define default rules below.  
 Native USB redirection is not enabled. (Default)

#### Default rule

Possible values:

- Deny
- Allow

#### Tip

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

### Class Rules

Class rules apply to USB device classes and sub-classes.

To manage rules, proceed as follows:

- ▶ Click to create a new entry.
- ▶ Click to remove the selected entry.
- ▶ Click to edit the selected entry.
- ▶ Click to copy the selected entry.

Add a class rule:

#### Rule:

- Deny
- Allow

**Class ID:** Selection list

**Subclass ID:** Selection list

**Name:** Free text entry

### Device Rules

Device rules apply to specific USB devices.

Add a device rule:

#### Rule:

- Allow
- Deny

**Vendor ID:** Hexadecimal manufacturer number

**Product ID:** Hexadecimal device number



To find out the **Vendor ID** and **Product ID** of the connected USB device, use the command `lsusb` (`lsusb | grep -i [search term]`) in the terminal. You can also use the **System Information** tool, see [Using “System Information” Function](#)(see page 1108).

#### Name: Free text entry

See also an overview and best-practice recommendations for the use of webcams under [Webcam Redirection and Optimization](#)(see page 663).

### Fabulatech USB Redirection

Menu path: **Sessions > RDP > RDP Global > Fabulatech USB Redirection**

Redirection for USB devices can be allowed or denied during an RDP session on the basis of rules. Sub-rules for specific devices or device classes are also possible. The use of rules is described under [USB Access Control](#)(see page 1231).

For the Fabulatech USB redirection, a server-side component is required. We recommend the USB for Remote Desktop IGEL Edition; see <http://www.usb-over-network.com/partners/igel/>.

#### Fabulatech USB Redirection

- Fabulatech USB redirection is enabled for all RDP sessions.
- Fabulatech USB redirection is disabled. (Default)

Enable either **Native** or **Fabulatech USB Redirection** – not both together. Disable USB redirection if you use DriveLock.

Ensure that no other Hotplug storage device (USB stick) is connected if a session is started with Fabulatech USB redirection. Otherwise, the Hotplug storage device will not be securely removed when the session starts, and this could lead to data loss. With IGEL Linux Version 10.02.x the Hotplug storage device is already insecurely removed when the Fabulatech USB redirection is enabled.

**Default rule:** This rule will apply if no special rule was configured for a class or a device.

- **Deny**
- **Allow**

#### Tip

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

### Class Rules

Class rules apply to USB device classes and sub-classes.



To manage rules, proceed as follows:

- ▶ Click to create a new entry.
- ▶ Click to remove the selected entry.
- ▶ Click to edit the selected entry.
- ▶ Click to copy the selected entry.

Class rule properties:

**Rule:**

- Allow: Devices that have the properties defined here are redirected by the Fabulatech USB redirection.
- Deny: Devices that have the properties defined here are not redirected.

**Class ID:** Device class

**Subclass ID:** Subclass relating to the specified device class

**Name:** Free text entry

**Override serial:** Serial number that will appear in the session

**Override name:** Device name that will appear in the session

**Postpone**

- The USB device is only removed from the system (endpoint device) when the session starts.
- The USB device is no longer shown immediately after the system is booted. (Default)

This setting is only effective if the **Takeaway** parameter is enabled.

**Takeaway**

- The USB device may be removed from the system (endpoint device).
- The USB device may not be removed. (Default)

**No Reset**

- The device will not be automatically reset after the connection with the session has been terminated.
- The device will be reset after the connection with the session has been terminated. (Default)

**Device Rules**

A device rule applies to a specific device that is identified by its serial number.

Device rule settings:

**Rule:**

- Allow
- Deny

**Vendor ID:** Hexadecimal manufacturer number



**Product ID:** Hexadecimal device number

To find out the **Vendor ID** and **Product ID** of the connected USB device, use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal. You can also use the **System Information** tool, see [Using “System Information” Function](#)(see page 1108).

**Name:** Free text entry

**Override serial:** Serial number that will appear in the session

**Override name:** Device name that will appear in the session

#### Postpone

- The USB device is only removed from the system (endpoint device) when the session starts. (Default)  
 The USB device is no longer shown immediately after the system is booted.

This setting is only effective if the **Takeaway** parameter is enabled.

#### Takeaway

- The USB device may be removed from the system (endpoint device). (Default)  
 The USB device may not be removed.

#### No Reset

- The device will not be automatically reset after the connection with the session has been terminated. (Default)  
 The device will be reset after the connection with the session has been terminated.

## Fabulatech Scanner Redirection

Menu path: **Sessions > RDP > RDP Global > Fabulatech Scanner Redirection**

Redirection for a Fabulatech scanner can be allowed during an RDP session.

#### Fabulatech Scanner for Remote Desktop

- Fabulatech Scanner for Remote Desktop is enabled.

For more information, see [RDP Fabulatech Scanner Redirection](#)(see page 277).

## Multimedia

Menu path: **Setup > Sessions > RDP > RDP Global > Multimedia**

In this area, you can enable video redirection in order to allow optimized video playback in remote sessions.

- **Video redirection**
  - Use video redirection. The device renders the video data.
  - Do not use video redirection. (default)



From *IGEL Linux 5.06.100*, hardware acceleration for multimedia playback is available on certain devices. You will find more detailed information in the FAQ [Hardware Video Acceleration on IGEL OS](#)<sup>269</sup>.

### 3.8.5 RDP Session

Menu path: **Sessions > RDP > RDP Sessions**

You can set up your own RDP sessions here.

The following configuration pages offer you detailed setup options for the RDP session:

- [Server](#)(see page 828)
- [Gateway](#)(see page 829)
- [Logon](#)(see page 830)
- [Window](#)(see page 830)
- [Keyboard](#)(see page 831)
- [Mapping](#)(see page 832)
- [Performance](#)(see page 833)
- [Options](#)(see page 834)
- [USB Redirection](#)(see page 834)
- [Multimedia](#)(see page 834)
- [Desktop Integration](#)(see page 835)

#### Server

Menu path: **Sessions > RDP > RDP Sessions > [Session Name] > Server**

In this area, you can change the information regarding the server connection.

- ▶ Choose between **Server** and **RemoteApps mode**.

#### Server

**Server:** Name or IP address of the server.

**RDP port:** The RDP TCP/IP port which is used for the connection. (Default: 3389)

**Collection:** The name of the Remote Desktop Services (RDS) collection to connect to.

Instead of the collection name, it is also possible to specify under **Collection** the token that directs the RDP client to a specific RDS collection. The token format is `tsv://MS Terminal Services Plugin.1.RDS collection name`. For more information, see [What Is the String for Token-Based Load Balancing?](#)(see page 276).

**Application:** Start application for the terminal server session.

---

<sup>269</sup> <https://kb.igel.com/display/igelos/Hardware+Video+Acceleration+on+IGEL+OS>



**Command line parameter for the executed program:** Command line parameter with which you would like to call up your own application in the RemoteAPP mode.

#### Changeable server URL on local login

The server can be entered freely when the user logs in locally. Local login must be enabled in order to do this.

The terminal server's login window will be shown. When using local login, the device's login window will be shown. (Default)

If the **Passthrough Authentication** option is enabled, the session with the local login data for the terminal user, e.g. from the domain login, is used. However, this setting will be overridden by the **Local Login** global parameter. You should not therefore use both options at the same time.

#### Enable RemoteApp Mode

Like the published applications of a Citrix server, MS Windows Server 2008 offers the option of passing on RemoteApps to the device.

Detailed instructions regarding server configuration can also be found on the Microsoft website: [TS RemoteApp Step-by-Step Guide](#)<sup>270</sup>.

On the client side, only a few parameters need to be configured after enabling the RemoteApp mode.

Please note that the name of the application to be launched must be preceded by two pipe characters (||), e.g. || Excel.

#### Gateway

Menu path: **Setup > Sessions > RDP > RDP Sessions > [Session Name] > Gateway**

Here, you can specify custom gateway details for your RDP session.

- **Enable gateway support**
  - Global setting: The settings from **RDP Global > Gateway** will be carried over.
  - Session setting: Here, you can configure custom settings. The entry options correspond to those under [RDP Global > Gateway](#)(see page 811).
  - Off: No gateway support
- **Gateway address**

RD Gateway requires Microsoft Windows Server 2008R2 or Server 2012 with various restrictions for each server version.

The following Windows Server editions can preferably be used as gateway servers:

Server 2012 Standard

Server 2012 Datacenter

Server 2012 Essential (restricted to the RD Gateway role)

Server 2012R2 Standard

Server 2012R2 Essential (restricted to the RD Gateway role)

<sup>270</sup> [https://technet.microsoft.com/en-us/library/cc730673\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc730673(v=ws.10).aspx)



Server 2016

Server 2019

RD Gateway is not supported in the IGEL RDP Legacy Mode.

- **Use other credentials for RD Gateway authentication:**

- Uses custom data that can be defined below rather than the session access data.
  - **Gateway user name**
  - **Gateway password**
  - **Gateway domain**

## Logon

Menu path: **Sessions > RDP > RDP Sessions > [Session Name] > Logon**

Here, you can specify session-specific settings for login.

### Use passthrough authentication for this session

This option can be used if the local device login takes place via Kerberos or Shared Workspace. The login data saved temporarily when logging in to the device will be used for the user name and password.

The login data are not passed on. (Default)

**User name:** Name of the user

**Password:** Password of the user

Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

**Domain:** Windows domain

## Window

Menu path: **Setup > Sessions > RDP > RDP-Sessions > [Session Name] > Fenster**

Here, you can specify the settings for the RDP session window.

- **Number of colours**

Possible values:

- Global setting
- 256
- Thousands
- Millions

- **Window size**

Possible values:

- Global setting
- Fullscreen: The session is shown on the full screen. The thin client's taskbar is not visible.



- Workarea: The session is shown on the full screen, minus the area needed by the thin client's taskbar.
- Numeric details: The session is shown in the selected resolution or on the selected percentage of the screen area.
- **Desktop scale factor:** Specifies the desktop scaling in percent. This function is available from IGEL Linux Version 10.02.

Desktop scaling is supported from Windows Server 2012 or higher and from Windows 8.1 or higher.

Possible values:

- Global setting (default)
- Automatic: The resolution set under **Setup > User Interface > Display > Options > Monitor-DPI** will be used for the RDP session.
- Numeric details: The display will be magnified by the factor given here. Value range: 100% - 500%

#### • **Display resolution**

Possible values:

- Same as window size
- Value selection: The session runs on the server side with the screen resolution selected here. The session will be shown on the thin client in the screen resolution set with the **Window size** parameter. If the screen resolution on the server side is smaller than the **Window size**, the display will be magnified accordingly and anti-aliasing may be used. Example: Applications that only work or work optimally with a specific screen resolution.

#### • **Start monitor:** Specifies the monitor on which the session is to start.

- No configuration
- Selects a specific monitor

#### • **Multi-monitor fullscreen mode:** This setting is relevant if more than one monitor is connected to the terminal:

- Global setting
- Restrict fullscreen session to one monitor.
- Display fullscreen session on all monitors.
- Expand fullscreen session across all monitors.

## Keyboard

Menu path: **Setup > Sessions > RDP > RDP Sessions > [Session Name] > Keyboard**

Here, you can specify session-specific keyboard settings.

#### • **Keyboard map**

Possible values:

- Automatic
- Country name

#### • **Override local window manager keyboard shortcuts**

Possible values:



- Global setting
- On
- Off

## Mapping

Menu path: **Setup > Sessions > RDP > RDP Sessions > [Session Name] > Mapping**

- **Enable COM port mapping**
  - Global setting:
  - On
  - Off
- **Enable drive mapping**
  - Global setting from **RDP Global > Mapping > Drive Mapping**
  - On
  - Off
- **Enable printer mapping**
  - Global setting from **RDP Global > Mapping > Printers**
  - On
  - Off
- **Enable plugin support**
  - Global setting from **RDP Global > Mapping > Drive Support**
  - Off
- **Enable client audio**
  - Global setting from **RDP Global > Mapping > Audio**
  - On
  - Off
- **Audio quality mode**
  - Global setting from **RDP Global > Mapping > Audio**
  - Automatic
  - High: High audio quality is favored.
  - Medium: Medium audio quality is favored.
  - Dynamic
- **Audio compression**
  - Global setting from **RDP Global > Mapping > Audio**
  - Automatic
  - On
  - Off
- **Audio capture**
  - Global setting from **RDP Global > Mapping > Audio**
  - On
  - Off
- **Enable clipboard**
  - Global setting from **RDP Global > Keyboard**
  - On
  - Off



## Performance

Menu path: **Setup > Sessions > RDP > RDP Sessions > [Session Name] > Performance**

- **Enable RemoteFX**
  - Global setting from **RDP Global > Performance**
    - On
    - Off
- **Hardware accelerated codecs AVC420/AVC444 (H.264)**
  - Global setting from **RDP Global > Performance**
    - On
    - Off
- **Disable wallpaper**
  - Global setting from **RDP Global > Performance**
    - On
    - Off
- **Do not show contents of window while dragging**
  - Global setting from **RDP Global > Performance**
    - On
    - Off
- **Disable menu and window animation**
  - Global setting from **RDP Global > Performance**
    - On
    - Off
- **Disable themes**
  - Global setting from **RDP Global > Performance**
    - On
    - Off
- **Disable cursor shadow**
  - Global setting from **RDP Global > Performance**
    - On
    - Off
- **Disable cursor settings**
  - Global setting from **RDP Global > Performance**
    - On
    - Off
- **Enable font smoothing**
  - Global setting from **RDP Global > Performance**
    - On
    - Off
- **Compression**
  - Global setting from **RDP Global > Performance**
    - On
    - Off



## Options

Menu path: **Setup > Sessions > RDP > RDP Sessions > [Session Name] > Options**

Here, you can specify the name and symbol for the RDP client.

- **Client name:** Specifies the name that is sent to the terminal server for identification purposes.  
Possible values:
  - Global setting: The setting from **RDP Global > Options** will be carried over.
  - Custom client name: The name given under **Custom client name** will be used as the client name.
  - MAC address: The MAC address of the computer will be used as the client name.
  - Host name: The name of the device specified under **Setup > Network > LAN Interfaces > Terminal name** will be used as the client name. See [LAN Interfaces\(see page 1172\)](#).
- **Custom client name:** Custom client name; if the field is empty, the MAC address will be used.
- **Collection:** The name of the Remote Desktop Services (RDS) collection to connect to.

Instead of the collection name, it is also possible to specify under **Collection** the token that directs the RDP client to a specific RDS collection. The token format is tsv://MS Terminal Services Plugin.1.RDS collection name. For more information, see [What Is the String for Token-Based Load Balancing?\(see page 276\)](#).

- **Icon name:** File name of the icon without file extension. (Default: `rdp`)

## USB Redirection

Menu path: **Sessions > RDP > RDP Sessions > [Session Name] > USB Redirection**

### Native USB redirection

- Global setting: The settings from **RDP Global > Native USB Redirection** will be carried over.
- On: Native USB redirection is enabled.
- Off: Native USB redirection is disabled.

Further information regarding the global settings can be found under [Native USB Redirection\(see page 823\)](#).

## Multimedia

Menu path: **Setup > Sessions > RDP > RDP Sessions > [Session Name] > Multimedia**

- **Enable video redirection**
  - Global setting: The setting from **RDP Global > Multimedia** will be used.
  - On: Video redirection is enabled.
  - Off: Video redirection is disabled.

Further information regarding the global settings can be found under [Multimedia<sup>271</sup>](#).

---

<sup>271</sup> <https://kb.igel.com/display/igelos1005/Multimedia>



## Desktop Integration

Menu path: **Sessions > RDP > RDP Sessions > [Session Name] > Desktop Integration**

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

The session can be launched from the start menu.

#### Application Launcher

The session can be launched with the Application Launcher.

#### Desktop

The session can be launched with a program launcher on the desktop.

#### Quick start panel

The session can be launched with the quick start panel.

#### Start menu's system tab

The session can be launched with the start menu's system tab.

#### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.



**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

## Autostart

The session will be launched automatically when the device boots.

## Restart

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

## Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.



- The session is started automatically, even when no network is available.

### 3.8.6 Remote Desktop Web Access

Menu path: **Sessions > RDP > Remote Desktop Web Access**

With Web Access for Remote Desktop (Web Access for RD), users can access RemoteApp and a Remote Desktop connection via the start menu on a computer or via a web browser.

RemoteApps and Remote Desktop connections therefore provide a modified view of RemoteApp programs and virtual desktops for users.

More information on Web access for Remote Desktop can be found under [Microsoft Technet - Web Access for RDP<sup>272</sup>](#).

The settings for launching the session are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Starting Methods for Session

##### Start menu

- The session can be launched from the start menu.

##### Application Launcher

- The session can be launched with the Application Launcher.

##### Desktop

- The session can be launched with a program launcher on the desktop.

##### Quick start panel

- The session can be launched with the quick start panel.

##### Start menu's system tab

- The session can be launched with the start menu's system tab.

##### Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

##### Desktop context menu

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

---

<sup>272</sup> <http://technet.microsoft.com/en-us/library/cc731923.aspx>



**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

The session will be launched automatically when the device boots.



### **Restart**

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

### **Autostart requires network**

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

- [Server](#)(see page 839)
- [Authentication](#)(see page 842)
- [Appearance](#)(see page 843)
- [Logoff](#)(see page 843)
- [Desktop Integration](#)(see page 845)

## Server

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Server**

In this area, you can specify the server configuration.

The Web Access page for *Windows Server 2012* and *Windows Server 2012 R2* can also be used on a Linux endpoint device in the *Firefox* browser. See [Via Browser](#)(see page 841).

### **Server configuration**

Possible values:

- "[Predefined configurationPredefined Configuration](#)(see page 840).
- "Ask user": The connection is preconfigured on the server side. The user only needs to enter their corporate e-mail address. See [Ask User](#)(see page 840).

**Server location:** These settings are needed if **Server configuration** is set to "Predefined configuration".

### **Protocol**

Possible values:

- "[http://](#)"
- "[https://](#)"

**RD Web Access Server:** Name of the Web Access server

**Path to web portal** (Default: [/rdweb/feed/webfeed.aspx](#))



## Enable gateway support

Possible values:

- "Global settings"
- "Session settings"
- "Off"

**Gateway address:** If you would like to carry over the session settings, you must also specify the gateway address.

**Domains:** Domain of the Web Access server

---

- [Predefined Configuration](#)(see page 840)
- [Ask User](#)(see page 840)
- [Via Browser](#)(see page 841)

Predefined Configuration

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Server**

To predefine settings, proceed as follows:

1. Go to **Sessions > RDP > Remote Desktop Web Access > Server**.
2. Under **Server configuration**, select **Predefined configuration**.
3. Create a new session. See the [Server](#)(see page 839) section regarding the session settings.
4. Select a login option under **Remote Desktop Web Access > Authentication**.  
If you have selected **Predefined configuration**, the **Passthrough authentication** mode will be available for logging in in addition to the normal user authentication process.
5. Under [Desktop Integration](#)(see page 845) and [Logoff](#)(see page 843), you can specify how you would like to log in and off.

You must make a setting for the login icon because this is not preconfigured and you will not otherwise have access to the Web Access logon.

The applications can be provided in the Application Launcher, in the start menu, in the quick start panel, or on the desktop. Under [Appearance](#)(see page 843), you can choose from the list of available applications for display on the desktop or in the quick start panel.

Ask User

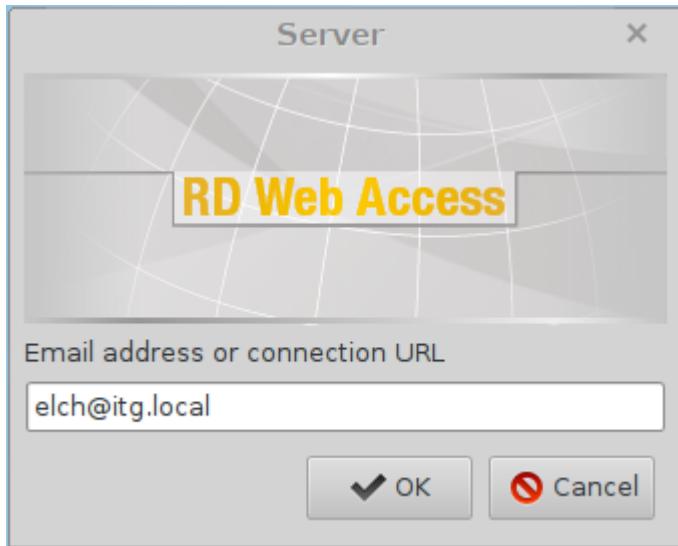
Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Server**

With this logon method, the network connections connected with the user name on the server side must be preconfigured and it must be possible to query them via DNS.

To configure access via **Ask user**, proceed as follows:

- Select **Ask user** under **RD Web Access > Server > Server configuration** menu.

The user is given a login window in which they enter their e-mail address consisting of @:



#### Via Browser

The Web Access page for *Windows Server 2012* and *Windows Server 2012 R2* can also be used on a Linux thin client in the *Firefox* browser.

- The user only needs the corresponding URL which is entered in the address bar.
- They then log in on the browser page using their user name and password.



If the user clicks one of the applications offered by Web Access, the thin client will open a logon mask and then a *Remote Desktop* session for the application chosen.

## Authentication

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Authentication**

You can change login settings on the server and select applications that are launched automatically after logging in.

The login settings on the server are only effective if **Sessions > RDP > Remote Desktop Web Access > Server > Server configuration** is set to **Predefined configuration**. Further information can be found under [Server](#)(see page 839).

**Authentication mode:** Specifies how the user authenticates themselves on the server.

Possible values:

- "Passthrough authentication": This option can be used if the local endpoint device login takes place via Kerberos or Shared Workspace. The login data saved temporarily when logging in to the device will be used for the user name and password.
- "Auto logon": The login data in **Username**, **Password**, and **Domain** will be used to log in.
- "User logon

**Username:** User name when logging in to the server

**Password:** Password when logging in to the server

**Domain:** Domain in which the user name and password are valid

### Save username and domain from the last login

Possible options:

- "Yes": The username and domain from the last login will be saved.
- "No": The username and domain from the last login will not be saved.
- "LegacySessions > RDP > RDP Global > Local Logon > Preset login information is enabled. If it is enabled, the saved data of **Local Logon** will be used also for RD Web Access.

To select an application for automatic launching, proceed as follows:

1. Click **[+]** in the **Start following applications automatically after server connection is established** area.
2. In the **Add** dialog, enter the name of the application. (Example: Word 2013)

You can also enter part of the name followed by an asterisk (\*). If you enter e.g. Word\*, all available versions of *Microsoft Word* as well as *Microsoft WordPad* will be opened.

3. Click on **Ok**.

After a successful login, the associated desktop icon for each available application will be placed on the device desktop. All applications whose name matches one of the names given in the **Start following applications automatically after server connection is established** area will then be launched.



## Appearance

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Appearance**

In this area, you can decide where you would like to display Remote Desktop Web Access applications:

### Show applications in start menu

The applications are shown in the start menu. (Default)

### Apply display filter to start menu entries

Only the applications listed in the display filter will be shown in the start menu.

All applications will be shown in the start menu. (Default)

### Show applications in Application Launcher

The applications are shown in Application Launcher. (Default)

### Apply display filter to Application Launcher entries

Only the applications listed in the display filter will be shown in the Application Launcher.

All applications will be shown in the Application Launcher. (Default)

### Show applications on desktop

The applications will be shown on the desktop. (Default)

### Apply display filter to desktop icons

Only the applications listed in the display filter will be shown on the desktop.

All applications will be shown on the desktop. (Default)

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Display filter: Show only the following applications

- ▶ Via +, you can add applications to the display filter and determine display options for this selected group.

Enable following applications in Quick Start Panel

- ▶ Via +, you can specify applications which will be added to the quick start panel.

## Logoff

Menu path: **Setup > RDP > Remote Desktop Web Access > Logoff**

Here, you can specify how you would like to log off from the application.

**Session name:** Name for the session.



The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. Ctrl.



Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

## Desktop Integration

Menu path: **RDP > Remote Desktop Web Access > Desktop Integration**

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

The session can be launched from the start menu.

#### Application Launcher

The session can be launched with the Application Launcher.

#### Desktop

The session can be launched with a program launcher on the desktop.



### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
-  = Ctrl
-  = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.



- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

The session will be launched automatically when the device boots.

#### Restart

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

#### Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

### 3.8.7 Horizon Client Global

Menu path: **Sessions > Horizon Client > Horizon Client Global**

In this area, you can define the global settings for Horizon Client sessions.

The following setting is carried over from the global settings for RDP sessions if "RDP" is selected as a **preferred desktop protocol**, see [Server Options\(see page 848\)](#) and [Connection Settings\(see page 862\)](#):

- **Number of colors:** see [Window\(see page 813\)](#)

- 
- [Server Options\(see page 848\)](#)
  - [Local Logon\(see page 849\)](#)
  - [Window\(see page 850\)](#)
  - [USB Redirection\(see page 851\)](#)
  - [Fabulotech USB Redirection\(see page 852\)](#)
  - [Fabulotech Scanner Redirection\(see page 855\)](#)
  - [Serial Port Redirection\(see page 855\)](#)



- [Drive Mapping](#)(see page 855)
- [Multimedia](#)(see page 856)
- [Performance](#)(see page 857)
- [Smartcard](#)(see page 857)
- [Unified Communications](#)(see page 858)

## Server Options

Menu path: **Sessions > Horizon Client > Horizon Client Global > Server Options**

In this area, you can specify the settings for the connection between the VMware Horizon Client and the server.

**Preferred desktop protocol:** The selected option is preferred by the client when negotiating the connection protocol.

If the server does not accept the connection protocol preferred by the client, the connection protocol preferred by the server will be used.

Possible values:

- Server setting: The client does not give the server details of a preferred connection protocol. The connection protocol preferred by the server is used.
- RDP: The client tells the server that it prefers RDP as the connection protocol.
- PCoIP: The client tells the server that it prefers PCoIP as the connection protocol.
- VMware Blast: The client tells the server that it prefers VMware Blast as the connection protocol.

Hardware video acceleration can be used for VMware Blast. Information regarding hardware video acceleration on IGEL devices can be found under [Hardware Video Acceleration on IGEL OS](#)(see page 736). For hardware video acceleration, the Multimedia Codec Pack must be installed on IGEL OS versions lower than 11.01.100. If no hardware video acceleration is available, rendering will take place via software, without acceleration.

Fabulatech USB redirection and VMWare Blast are not compatible. If you use Fabulatech USB redirection, ensure that RDP or PCoIP is used as the protocol for VMware Horizon sessions.

### High Color Accuracy Mode

Enables H.264 encoding with High Color Accuracy in VMware Blast Sessions.

Horizon Client uses high color accuracy only if the agent supports it. This feature might reduce battery life and performance.

- High color accuracy is allowed.  
 High color accuracy is not allowed. (Default)

### Kiosk mode

- Horizon client sessions are held in kiosk mode.



Horizon client sessions are held in normal mode. (Default)

**Server certificate verification mode:** Specifies what will happen if server certificate verification fails.

Possible values:

- Reject if verification fails
- Warn if verification fails
- Allow unverifiable connections

**Action to take in case there are running applications from previous sessions:** Specifies the start behavior of an **application**-type session if applications from a previous session are still running.

The session type is defined under **Sessions > Horizon Client > Horizon Client Session > [Session Name] > Connection Settings > Session Type**.

Possible values:

- Ask to reconnect to open applications: When the session starts, the user is asked whether they want to re-establish the connection. If the connection is reestablished, the applications running will be available. The applications will have the same status as when the connection was terminated.
- Reconnect automatically to open applications: The connection will be re-established automatically. The application running will be available. The application will have the same status as when the connection was terminated.
- Do not ask to reconnect and do not reconnect: The connection will not be re-established.

## Local Logon

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Global > Local Logon**

In this area, you can prepopulate user data. As a result, you can avoid users possibly having to log in a number of times.

You can change the following settings:

- **Use local login window:**
  - The local login window of the thin client will be used to log in to the server. If you use the local login window, you can prepopulate login information.
  - The local login window will not be used. (default)
- **Preset logon information:**
  - Login information will appear automatically in the logon window. With **Type**, you can specify the source of the logon information. (default)
- **Type:**
  - Set user/domain from last login: The login information from the last session will appear automatically in the login window.



- Set user/domain from session setup: Session-specific login information will appear automatically in the login window. The session-specific login information is described under [Connection Settings<sup>273</sup>](#).
- Set user/domain from appliance mode: If this option is enabled, the login information specified in the [Appliance Mode<sup>274</sup>](#) for *VMWare Horizon* will appear automatically in the logon window.
- **Show domain:**  
 The domain will be shown in the logon window. (default)
- **Relaunch mode:**  
 The login window is shown in relaunch mode and cannot be closed.  
 The login window is not shown in relaunch mode. (default)
- **Exit on disconnect or when an error occurs:**  
 The session will be ended completely when the connection is terminated.  
 The connection overview will be shown when the connection is terminated. (default)

Working with the domain list:

- Click to add a new entry.
- Click to remove the selected entry.
- Click to edit the selected entry.
- Click to copy the selected entry.

Further settings options can be found under [AD/Kerberos Configuration<sup>275</sup>](#) and [AD/Kerberos<sup>276</sup>](#).

## Window

Menu path: **Sessions > Horizon Client > Horizon Client Global > Window**

**Window size:** Specifies the width and height of the window.

Possible options:

- "Full-screen": The session is shown on the full screen. The device's taskbar is not visible.
- "Work area
- Numeric details: The session is shown in the selected resolution or on the selected percentage of the screen area.

**Multimonitor full-screen mode** - If more than one monitor is connected to the terminal:

- "Restrict full-screen session to one monitor"
- "Display full-screen session on all monitors"
- "Expand full-screen session across all monitors

---

<sup>273</sup> <https://kb.igel.com/display/igelos/Connection+Settings>

<sup>274</sup> <https://kb.igel.com/display/igelos1005/Appliance+Mode>

<sup>275</sup> <https://kb.igel.com/pages/viewpage.action?pageId=23501827>

<sup>276</sup> <https://kb.igel.com/pages/viewpage.action?pageId=23501825>



## USB Redirection

Menu path: **Sessions > Horizon Client > Horizon Client Global > USB Redirection**

In this area, you can enable and configure USB redirection for specific devices. A USB composite device can be split into its components (interfaces). Example: USB dictation device that is split into the components loudspeaker, microphone, storage device/drive, and control buttons.

Ensure that the power supplied by the USB connection is adequate for the device.

If USB redirection is enabled, drive mapping should be disabled; see [Drive Mapping\(see page 855\)](#). Otherwise, USB redirection can cause a storage device to be removed from the drive mapping. This is the case if the **Automatically connect when inserted** option is enabled.

You can change the following settings:

### USB Redirection

- On
- Off

### Automatically connect at startup

USB devices that were inserted before the start of the session are available in the session. (default)

### Automatically connect when inserted

USB devices that are inserted during the session are available in the session. (default)

**Default rule:** This rule will apply if no special rule was configured for a class or a device.

- Allow
- Deny

#### Tip

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

### Automatic splitting of composite USB devices

A USB composite device will automatically be split into its individual components (interfaces). The class rules will be applied to these individual devices.

The device will not be split into its components.

### Creating a Class Rule

1. To create a new rule, click **[+]** in the **Class Rules** area.
2. Choose a **Rule**. The rule specifies whether the use of the device class defined here is allowed or prohibited.



3. Under **Family**, select the class of device for which the rule should apply. Examples: **Audio, Printer, Smartcard, Storage Devices**.
  4. Under **Name**, give a name for the rule.
  5. Click on **Ok**.
  6. Click on **Apply or Ok**.
- The rule is active.

### Creating a Device Rule

When a rule is defined, at least one of the properties **Vendor ID** or **Product ID** must be given.

1. To create a new rule, click **[+]** in the **Device Rules** area.
2. Choose a **Rule**. The following rules are available:
  - Deny: The device will not be redirected via USB redirection.
  - Allow: The device will be redirected via USB redirection.
  - Split: A USB composite device will automatically be split into its individual components (interfaces).
  - No auto-split: A USB composite device will not be split.
3. Give the **Vendor ID** of the device as a hexadecimal value.
4. Give the **Product ID** of the device as a hexadecimal value. The product ID can contain asterisks '\*', each asterisk representing one hexadecimal digit. If the field is left empty, any product ID is matched.

To find out the **Vendor ID** and **Product ID** of the connected USB device, use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal. You can also use the **System Information** tool, see [Using “System Information” Function](#)(see page 1108).

5. Only for USB composite devices: Under **Interface Exclude List**, enter a list of interfaces that are to be excluded from USB redirection. The individual interfaces are separated by spaces. Example: "0 1".
  6. Under **Name**, give a name for the rule.
  7. Click on **Ok**.
  8. Click on **Apply or Ok**.
- The rule is active.

See also an overview and best-practice recommendations for the use of webcams under [Webcam Redirection and Optimization](#)(see page 663).

### Fabulatech USB Redirection

Menu path: **Sessions > Horizon Client > Horizon Client Global > Fabulatech USB Redirection**

For **Fabulatech USB Redirection**, a special Fabulatech server component must be installed on the Citrix server (USB for Remote Desktop Igel Edition).

More detailed information about the function can be found on the Fabulatech partner site: <http://www.usb-over-network.com/partners/igel/>.



Enable either **Native** or **Fabulatech USB Redirection** – not both together. Disable USB redirection if you use DriveLock.

Ensure that no other hotplug storage device (USB stick) is connected if a session is started with Fabulatech USB Redirection. Otherwise, the hotplug storage device will not be securely removed when the session starts, and this could lead to data loss. With IGEL Linux Version 10.02.x the hotplug storage device is already insecurely removed when the Fabulatech USB Redirection is enabled.

### **Fabulatech USB Redirection**

- Fabulatech USB Redirection is used.
- Fabulatech USB Redirection is not used. (Default)

**Default rule:** This rule will apply if no special rule was configured for a class or a device.

Possible options:

- Deny
- Allow

#### **Tip**

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

### Class Rules

Class rules apply to USB device classes and sub-classes.

Managing rules:

- Create a new entry.
- Remove the selected entry.
- Edit the selected entry.
- Copy the selected entry.

Class rule properties:

#### **Rule**

Possible options:

- Deny: Devices that have the properties defined here are not redirected.
- Allow: Devices that have the properties defined here are redirected by the **Fabulatech USB Redirection**.

**Class ID:** Device class

**Subclass ID:** Subclass relating to the specified device class

**Name:** Free text entry

**Override serial:** Serial number that will appear in the session



**Override name:** Device name that will appear in the session

#### Postpone

- The USB device is only removed from the system (endpoint device) when the session starts.
- The USB device is no longer shown immediately after the system is booted. (Default)

This setting is only effective if the **Takeaway** parameter is enabled.

#### Takeaway

- The USB device may be removed from the system (endpoint device).
- The USB device may not be removed. (Default)

#### No Reset

- The device will not be automatically reset after the connection with the session has been terminated.
- The device will be reset after the connection with the session has been terminated. (Default)

### Device Rules

A device rule applies to a specific device that is identified by its serial number.

Device rule settings:

#### Rule

Possible options:

- Deny: The device will not be redirected via Fabulatech USB Redirection.
- Allow: The device will be redirected via Fabulatech USB Redirection.

**Vendor ID:** Hexadecimal manufacturer number

**Product ID:** Hexadecimal device number

To find out the **Vendor ID** and **Product ID** of the connected USB device, use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal. You can also use the **System Information** tool, see [Using “System Information” Function](#)(see page 1108).

**Name:** Free text entry

**Override serial:** Serial number that will appear in the session.

**Override name:** Device name that will appear in the session.

#### Postpone

- The USB device is only removed from the system (endpoint device) when the session starts. (Default)
- The USB device is no longer shown immediately after the system is booted.

This setting is only effective if the **Takeaway** parameter is enabled.

#### Takeaway



- The USB device may be removed from the system (endpoint device). (Default)
- The USB device may not be removed.

#### No Reset

- The device will not be automatically reset after the connection with the session has been terminated. (Default)
- The device will be reset after the connection with the session has been terminated.

## Fabulatech Scanner Redirection

Menu path: **Sessions > Horizon Client > Horizon Client Global > Fabulatech Scanner Redirection**

You can enable or disable Fabulatech scanner redirection.

#### Fabulatech Scanner for Remote Desktop

- Fabulatech scanner redirection is enabled.

## Serial Port Redirection

#### Serial Port Redirection

With the serial port redirection feature, you can redirect locally connected serial (/dev/ttyS) ports, such as built-in RS232 ports or USB-to-Serial adapters, to their RDS-hosted desktops.

- Serial Port Redirection is enabled.
- Serial Port Redirection is disabled. (Default)

## Drive Mapping

Menüpfad: **Horizon Client > Horizon Client Global > Drive Mapping**

Through drive mapping, connected mass storage devices can be made available in the session. Specify which folders or drives are mapped during the login.

#### Enable Drive Mapping

- Drive mapping is enabled. (Default)

Local (USB) devices which are to be used for drive mapping purposes must first be set up as devices. See [Storage Hotplug](#)(see page 1228).



Before you unplug a hotplug storage device from the endpoint device, you must safely remove it. Otherwise, data on the hotplug storage device can be damaged. Depending on the configuration, there is one or several possibilities to safely remove a hotplug storage device:

- Click on in the task bar. The taskbar is not available in a fullscreen session.
- Click on in the in-session control bar. Depending on the configuration, the in-session control bar may be available in a fullscreen session. For further information, see [In-Session Control Bar](#)(see page 1154).
- Function **Accessories > Safely Remove Hardware** with further starting possibilities; amongst other things, a hotkey can be defined here.  
If the following warning is displayed: **Volume(s) still in use. Don't remove the device**, then the hotplug storage device must not be removed. First, exit the program concerned or close all files or directories that reside on the hotplug storage device.

- **Drive Mapping:** List of mapped drives.

To set up drive mapping, proceed as follows:

1. Click **Add** to bring up the mapping window.
2. Click **Enabled** to enable the drive connection.
3. Select a **Drive to map** from the list under which the local device or the folder is to be mapped.

If the drive letter you have selected is no longer available on the server, the specified directory or local drive will be given the next free letter during the login.

4. Give the **Local Drive Path** of the local directory to which the mapping is to refer.

If you map a locally connected device, use the pre-defined path names available in the drop-down field. The directories in question are those on which the devices are mounted by default during the boot procedure (e.g. /autofs/floppy for an integrated floppy drive).

## Multimedia

Menu path: **Sessions > Horizon Client > Horizon Client Global > Multimedia**

You can change the following multimedia settings:

### **VMware Multimedia Redirection**

Possible values:

- Off: The server renders the multimedia data and sends the individual images to the client.
- On: The client renders the multimedia data supplied by the server.

**Real Time Audio Video (RTAV):** Specifies the redirection of video data from the client USB webcam.

Possible values:

- Off: The client does not forward the webcam data as video data.



With USB redirection, data from the webcam can be forwarded to the server even if RTAV is disabled. For an overview and best-practice recommendations for the use of webcams, see [Webcam Redirection and Optimization](#)(see page 663).

- On: The client forwards the webcam data as video data.

## Performance

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Global > Performance**

In this area, you can optimize the performance of *Horizon Client* sessions.

You can change the following settings:

**PCoIP client-side image cache size:** Specifies the size of the cache for images. Caching parts of the display reduces the amount of data to be transferred.

Possible values:

- 50 MB
- 100 MB
- 150 MB
- 200 MB
- 250 MB
- 300 MB

Larger cache sizes of 250 MB or more should only be used if at least 2 GB RAM or more is available.

## Lakeside SysTrack

The Lakeside SysTrack is enabled.

The Lakeside SysTrack is not enabled. (Default)

## Smartcard

Menu path: **Sessions > Horizon Client > Horizon Client Global > Smartcard**

In this area, you can specify which middleware is used for logon with smartcard.

The following middlewares for logging on to VMware Horizon are available to choose from:

### Horizon logon with Gemalto eToken and IDPrime smartcards und token

The middleware for Gemalto/SafeNet eToken, IDPrime smartcards and tokens is used.

The middleware for Gemalto/SafeNet eToken, IDPrime smartcards and tokens is not used. (Default)

### Horizon logon with cryptovision sc/interface smartcards

The middleware for cryptovision sc/interface smartcards is used.

The middleware for cryptovision sc/interface smartcards is not used. (Default)

### Horizon logon with Gemalto IDPrime smartcards



Activate this Gemalto middleware if you want to use Gemalto common criteria devices in unlinked mode.

- The middleware for Gemalto IDPrime smartcards is used.  
 The middleware for Gemalto IDPrime smartcards is not used. (Default)

#### Horizon logon with Athena IDProtect smartcards

- The middleware for Athena IDProtect smartcards is used.  
 The middleware for Athena IDProtect smartcards is not used. (Default)

#### Horizon logon with A.E.T. SafeSign smartcards

- The middleware for A.E.T. SafeSign Smartcards is used.  
 The middleware for A.E.T. SafeSign Smartcards is not used. (Default)

#### Horizon logon with SecMaker Net iD smartcards

- The middleware for SecMaker Net iD smartcards is used.  
 The middleware for SecMaker Net iD smartcards is not used. (Default)

#### Horizon logon with smartcards supported by Coolkey library

- The Coolkey middleware is used.  
 The Coolkey middleware is not used. (Default)

#### Horizon logon with smartcards supported by OpenSC

- The OpenSC middleware is used.  
 The OpenSC middleware is not used. (Default)

#### Horizon logon with smartcards supported by 90meter library

##### Licensed Feature

This feature requires an add-on license; see [Add-On Licenses<sup>277</sup>](#). Please contact your IGEL sales representative.

- The 90meter middleware is used.  
 The 90meter middleware is not used. (Default)

## Unified Communications

Menüpafad: **Sessions > Horizon Client > Horizon Client Global > Unified Communications**

Here, you can change settings relevant to Unified Communications.

- [Skype for Business](#)(see page 859)
- [Cisco](#)(see page 859)
- [VDI Solutions](#)(see page 860)

<sup>277</sup> <https://kb.igel.com/display/licensesmoreigelos11/Add-on+Licenses>



See also an overview and best-practice recommendations for the use of webcams under [Webcam Redirection and Optimization](#)(see page 663).

## Skype for Business

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Global > Unified Communications > Skype for Business**

- **Virtualization Pack Skype for Business:** Defines whether the Virtualization Pack Skype for Business is active.
  - The Virtualization Pack Skype for Business is active. (Default)
  - The Virtualization Pack Skype for Business is not active.

## Cisco

Menu path: **Sessions > Horizon Client > Horizon Client Global > Unified Communications > Cisco**

Here, you can activate or deactivate the virtual desktop optimization for Cisco Webex and define settings for the Cisco JVDI client.

### Cisco Webex Teams VDI

- The Cisco Webex Teams VDI solution is enabled.
- The Cisco Webex Teams VDI solution is disabled.

### Settings for the Cisco JVDI Client

#### Cisco JVDI Client

- The Cisco JVDI Client is enabled.
- The Cisco JVDI Client is disabled.

For the vendor documentation, see [Deployment and Installation Guide for Cisco Jabber Softphone for VDI Release 12.9](#)<sup>278</sup>.

## Audio

**Default volume:** Headphone volume control. (Default: 80%)

**Default microphone volume:** Microphone volume control. (Default: 80%)

**Default ring volume:** Ringtone volume control. (Default 100%)

**Internal sound card:** Here you have the possibility to define a sound card. If you leave the field empty, the default sound card of the system is used.

For further information, see [Sound Preferences](#)(see page 1066).

## Video

You can set the Cisco JVDI Client to use the default resolutions of the camera or to use a user-defined set of resolutions. Separate configurations for cameras with and without hardware acceleration are possible.

**Allow default resolutions** (for cameras without hardware resolution)

---

<sup>278</sup> [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/jvdi/12\\_9/dig/jvdi\\_b\\_deploy-install-jvdi-12-9/jvdi\\_b\\_deploy-install-jvdi-12-9\\_chapter\\_01.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jvdi/12_9/dig/jvdi_b_deploy-install-jvdi-12-9/jvdi_b_deploy-install-jvdi-12-9_chapter_01.html)



The default resolutions of the camera are used.

A user-defined set of resolutions is used. You can add a resolution by clicking in the **Camera** area and selecting the desired resolution.

#### Allow default resolutions (for cameras with hardware resolution)

The default resolutions of the camera are used.

A user-defined set of resolutions is used. You can add a resolution by clicking in the **Hardware Accelerated Camera** area and selecting the desired resolution.

### VDI Solutions

Menu path: **Sessions > Horizon Client > Horizon Client Global > Unified Communications > VDI Solutions**

Here, you can activate or deactivate various virtual desktop optimizations.

#### HTML5 multimedia redirection

HTML5 multimedia redirection is enabled.

#### Microsoft Teams optimization

The Microsoft Teams optimization is enabled.

#### Zoom VDI Media Plugin

The Zoom VDI Media Plugin is enabled.

### 3.8.8 Horizon Client Session

Menu path: **Sessions > Horizon Client > Horizon Client Sessions > [Session Name]**

You can configure one or more Horizon Client sessions.

The settings for launching the session are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

The session can be launched from the start menu.

#### Application Launcher

The session can be launched with the Application Launcher.

#### Desktop

The session can be launched with a program launcher on the desktop.

#### Quick start panel



- The session can be launched with the quick start panel.

#### Start menu's system tab

- The session can be launched with the start menu's system tab.

#### Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

#### Desktop context menu

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. **Ctrl**.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
-  = Ctrl
-  = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

-  = Alt



Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

### Autostart

The session will be launched automatically when the device boots.

### Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

### Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

- [Connection Settings](#)(see page 862)
- [Window](#)(see page 863)
- [Mouse and Keyboard](#)(see page 864)
- [Mapping](#)(see page 864)
- [Performance](#)(see page 865)
- [Options](#)(see page 866)
- [Multimedia](#)(see page 866)
- [Proxy](#)(see page 867)
- [Desktop Integration](#)(see page 867)

## Connection Settings

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Connection Settings**

In this area, you can specify the settings for the connection between the *Horizon Client* and the server.

- **Server URL:** URL of the *VMware Horizon* server



- **Use passthrough authentication for this session**
    - The user name and password are temporarily saved and used for authentication purposes in this session.
    - Passthrough authentication is not used. (default)
  - **User name:** User name when logging on to the *VMware Horizon* server
  - **User password:** Password when logging on to the *VMware Horizon* server
  - **Domain:** Domain when logging on to the *VMware Horizon* server
  - **Session type:** Specifies whether the session contains a desktop or an individual application.  
Possible values:
    - Desktop: The session contains a desktop.
    - Application: The session contains an individual application.
  - **Desktop name:** Specifies a name for the desktop. This option is available if **Session Type** is set to “Desktop”.
  - **Application:** Application that is launched during the session. This option is available if **Session Type** is set to “Application”.
  - **Autoconnect**
    - When the session starts, the connection to the desktop or application will automatically be established. For this to be possible, the name of the desktop or application must be defined.
    - When the session starts, the overview will be shown. (default)
  - **Preferred desktop protocol:** The selected option is preferred by the client when negotiating the connection protocol.  
Possible values:
    - Global setting
    - Server setting
    - RDP
    - PCoIP
    - VMWare Blast
  - **Enable kiosk mode**
    - Global setting
    - On
    - Off
- Further settings options can be found under [AD/Kerberos Configuration\(see page 1247\)](#) and [AD/Kerberos\(see page 1242\)](#).

## Window

Menu path: **Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Window**

In this area, you can change the way in which the session is displayed.

**Window size:** Specifies the width and height of the window.

Possible values:

- Global setting: The window size is carried over from the global settings for Horizon Client sessions, see [Window\(see page 850\)](#).
- Fullscreen: The session is shown on the full screen.
- User selection



- Numeric details: The session is shown in the selected resolution or on the selected percentage of the screen area.

**Number of colors:** Specifies the color depth.

- Global setting: The color depth is carried over from the global settings for RDP sessions, see [Window](#)(see page 813).
- 256
- Thousands
- Millions

**Start monitor:** Specifies the monitor on which the session is shown.

## Mouse and Keyboard

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Mouse and Keyboard**

In this area, you can define the settings for the mouse and keyboard.

- **Disable Mouse Motion Events**

The mouse pointer will only be shown locally on the thin client. If the user moves the mouse over a session item, no reaction of the item will be shown.

Further settings options can be found in the user interface setup area under [Language](#)<sup>279</sup> as well as [Keyboard](#)<sup>280</sup> and [Additional keyboard layouts](#)<sup>281</sup>.

## Mapping

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Mapping**

In this area, you can specify the data transmission between the thin client and *Horizon Client* session.

These settings only apply to RDP-based sessions.

► Check whether **Sessions > Horizon Client Sessions > Horizon Client Session > Connection Settings > Preferred Connection Protocol** selection is set to "RDP".

- **Enable Client Audio**

- Global setting
- On - enhanced
- On - secure
- Off

- **Enable Clipboard**

- Global setting
- On
- Off

<sup>279</sup> <https://kb.igel.com/pages/viewpage.action?pageId=23501722>

<sup>280</sup> <https://kb.igel.com/pages/viewpage.action?pageId=23501728>

<sup>281</sup> <https://kb.igel.com/display/igelos/Additional+Keyboard+Layouts>



- **Enable Printer Mapping**
  - Global setting
  - On
  - Off
- **Enabling COM Port Mapping**
  - Global setting
  - On
  - Off
- **Enable Drive Mapping**
  - Global setting
  - On
  - Off
- **Enable USB Redirection**
  - Global setting
  - Off

Further settings options can be found in the RDP Global setup area under [Drive Mapping<sup>282</sup>](#), [COM Ports<sup>283</sup>](#), [Printers](#)(see page 817), [Audio<sup>284</sup>](#), [Keyboard<sup>285</sup>](#) and in the Devices area under [Printer](#)(see page 1216).

## Performance

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Performance**

In this area, you can save system resources by disabling certain visual functions of the user interface.

- **Disable wallpaper:**
  - On: No desktop background image is shown.
- **Do not show contents of window while dragging:**
  - On: The content of a window will not be shown while the window is being moved.
- **Disable menu and window animation:**
  - On: Transitions for menus and windows will not be animated.
- **Disable themes:**
  - On: No optional desktop theme can be used.
  - Off: An optional desktop theme can be used.
- **Disable cursor shadow:**
  - On: The mouse pointer will be shown without a shadow.
  - Off: The mouse pointer will be shown with a shadow.
- **Disable cursor settings**
  - On: The mouse pointer settings cannot be changed.
  - Off: The mouse pointer settings can be changed.
- **Enable font smoothing:**
  - Global setting: The setting under Sessions > Horizon Client > Horizon Client Global will be used.

<sup>282</sup> <https://kb.igel.com/display/igelos1005/Drive+Mapping>

<sup>283</sup> <https://kb.igel.com/pages/viewpage.action?pageId=23501358>

<sup>284</sup> <https://kb.igel.com/display/igelos/Audio>

<sup>285</sup> <https://kb.igel.com/pages/viewpage.action?pageId=23501355>



- On: Edges will be smoothed when text is displayed.
- Off: Edges will not be smoothed when text is displayed.

Further settings options can be found in the Horizon Global setup area under [Performance\(see page 857\)](#) and in the RDP Global area under [Performance\(see page 820\)](#).

## Options

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Options**

In this area, you can change the following settings:

- **Working directory:** Directory that is used after logging on
- **Compression:**
  - Global setting: The setting from **Setup > Sessions > Horizon Client > Horizon Client Global** will be carried over.
  - On: The data flow between the client and server will be compressed.
  - Off: The data flow will not be compressed.
- **Enforce TLS-encrypted connections:**
  - Global setting: The setting from **Setup > Sessions > Horizon Client > Horizon Client Global** will be carried over.
  - On: Encryption of the connection with TLS will be forced.
  - Off: Encryption will not be forced.
- **Network level authentication:**
  - On: The user will authenticate themselves on the network level (network layer authentication) in order to establish an RDP connection.

If network level authentication is enabled, the local logon window is used. This also applies if the **Use local logon window** option under **Setup > Sessions > Horizon Client > Horizon Client Global > Local Logon** is disabled.

- Off: Conventional authentication

Further settings options can be found in the RDP Global setup area under [Options\(see page 823\)](#), [Performance\(see page 820\)](#) and in the Horizon Global area under [Local Logon\(see page 849\)](#).

## Multimedia

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Multimedia**

You can change the following multimedia setting:

- **Enable VMware multimedia redirection**

Possible values:

- Global setting: The setting under **Sessions > Horizon Client > Horizon Client Global** will be used.
- off: The server renders the multimedia data and sends the individual images to the client.



## Proxy

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Proxy**

In this area, you can configure the use of a proxy for the connection between the client and server.

You can change the following settings:

- **Direct connection to the Internet:**

No proxy will be used.

- **Manual proxy configuration:**

A proxy will be used. The configuration must be specified in the following fields.

- **HTTP proxy:** URL of the proxy for HTTP

- **Port:** Port of the proxy for HTTP

- **SSL proxy:** URL of the proxy for SSL

- **Port:** Port of the proxy for SSL

- **SOCKS host:** URL of the proxy for SOCKS

- **Port:** Port of the proxy for SOCKS

- **SOCKS protocol version:** Version of the SOCKS protocol used. Possible values:

- SOCKS v4

- SOCKS v5

- **No proxy for:** List of URLs for which no proxy is to be used (separated by commas).

- **System-wide proxy configuration:**

The proxy configured under **Setup > Network > Proxy** will be used.

You will find further settings options in the setup under [Network > Proxy](#)(see page 867).

## Desktop Integration

Menu path: **Sessions > Horizon Client > Horizon Client Sessions > [Session name] > Desktop Integration**

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

The session can be launched from the start menu.

#### Application Launcher

The session can be launched with the Application Launcher.

#### Desktop

The session can be launched with a program launcher on the desktop.

#### Quick start panel

The session can be launched with the quick start panel.



### **Start menu's system tab**

The session can be launched with the start menu's system tab.

### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

### **Desktop context menu**

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### **Hotkey**

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. **Ctrl**.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:



- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

#### Autostart

The session will be launched automatically when the device boots.

#### Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

#### Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

### 3.8.9 Appliance Mode

Menu path: **Sessions > Appliance Mode**

In the appliance mode, only one specific session is accessible. You can activate the appliance mode for one of the following session types (if available on your system):

- VMware Horizon(see page 870)
- Browser(see page 871)
- Citrix Self-Service(see page 871)
- RHEV/Spice(see page 872)
- Imprivata(see page 872)
- RDP MultiPoint Server(see page 874)
- XDMCP for This Display(see page 875)

The system hotkey [Ctrl]+[Alt]+[S] for launching the setup application does not work in the appliance mode. Use [Ctrl]+[Alt]+[F2] instead.



You can set up a hotkey to start quick setup in appliance mode.

By default, access to other applications is not possible in appliance mode. However, these applications can be made available by activating **Appliance Mode Access** at the corresponding **Desktop Integration** page:

- [ICA Connection Center](#)(see page 1038)
- [Task Manager](#)(see page 1078)
- [Application Launcher](#)(see page 1063)
- [Firmware Update](#)(see page 1116)
- [Quick Settings](#)(see page 1053)
- [Sound Preferences](#)(see page 1066)
- [Disk Utility](#)(see page 1109)
- [Commands](#)(see page 1093)
- [Webcam Information](#)(see page 1125)
- [Touchscreen Calibration](#)(see page 1076)
- [Screen Lock/Saver](#)(see page 1155)
- [Monitor Calibration](#)(see page 1091)
- [Network Tools](#)(see page 1095)
- [Screenshot Tool](#)(see page 1084)
- [System Information](#)(see page 1105)
- [Bluetooth Tool](#)(see page 1100)
- [Display Switch](#)<sup>286</sup>
- [Identify Monitors](#)(see page 1122)
- [System Log Viewer](#)(see page 1070)
- [Local Terminal](#)(see page 1042)
- [SSH Session](#)(see page 946)
- [Custom Application](#)(see page 1267)
- [Mobile Device Access](#)(see page 1114)
- [Open VPN](#)(see page 1195)
- [OpenConnect VPN](#)(see page 1200)
- [genucard](#)(see page 1202)

Additionally, the in-session control bar can be used in an appliance mode session. With the in-session control bar, the user can eject a USB drive, start the wireless manager, start the Mobile Device Access USB tool and end the session. For further information, see [In-Session Control Bar](#)(see page 1154).

## VMware Horizon

Menu path: **Sessions > Appliance Mode > VMware Horizon**

**Server URL:** URL of the VMware Horizon server.

**User name:** User name when logging on to the VMware Horizon server.

**User password:** Password when logging on to the VMware Horizon server.

---

<sup>286</sup> <https://kb.igel.com/display/igelos1101/Display+Switch>



Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

**Domain:** Domain when logging on to the VMware Horizon server.

**Desktop name:** Desktop that is to be launched automatically.

#### Autoconnect

The desktop given in **Desktop name** is launched automatically.

#### Network level authentication

- **on:** The user will authenticate themselves on the network level (network layer authentication) in order to establish an RDP connection.
- **off:** Conventional authentication.

If network level authentication is enabled, the local login window is used. This also applies if the **Use local login window** option under **Sessions > Horizon Client > Horizon Client Global > Local Logon** is disabled.

## Browser

Menu path: **Sessions > Appliance Mode > Browser**

When this appliance mode is active, the Firefox browser is started to establish a connection with a session, e.g. a Citrix XenDesktop session. With a Citrix session, the browser is restarted after the session has been closed.

If your session requires an on-screen keyboard, you can jump to the relevant configuration page via the link **On-screen keyboard** on the right-hand side. See also [On-Screen Keyboard](#)(see page 1088).

**Web URL:** URL for the session

## Citrix Self-Service

Menu path: **Sessions > Appliance Mode > Citrix Self-Service**

At least Citrix Receiver Version 13 is required.

**Self-Service delivery server URL:** Server address including the `https://` prefix.

In the appliance mode, only one server can be used for Self-Service.

#### Multi User (**StoreFront servers only**)

The user data on the client will be deleted after logging off or terminating Self-Service.

#### Reconnect after logon



- The Self-Service GUI reconnects automatically after being launched.

#### **Reconnect to apps after starting an application**

- The Self-Service GUI will attempt to reconnect to ongoing sessions if an application is launched or the store is reloaded.

## RHEV/Spice

Menu path: **Sessions > Appliance Mode > RHEV/Spice**

**Connection Broker:** URL of the Connection Broker.

## Imprivata

Menu path: **Sessions > Appliance Mode > Imprivata**

Imprivata offers digital security solutions for healthcare organizations. For more information, see [imprivata.com](https://www.imprivata.com)<sup>287</sup>.

Enable the following in the Setup if you use Imprivata versions above 6.3: **System > Registry > imprivata.gain\_permission**.

**Set the URL to the server:** URL address of the single sign-on server.

**Path to the appliance:** Path to the application on the single sign-on server. (Default: sso/servlet/getembeddedloader?arch=amd64)

#### **Enable component's logging**

- Log files will be generated. You will need them if support is required in the future.

#### **Redirection of smartcards**

- A smartcard will be redirected into a session.

#### **PIE application launcher for Citrix**

- Enables the grid theme for organizing Citrix apps.

The following setting is active if **Enable component's logging** is enabled.

**Component's logging verbosity:** Specifies the level of detail for the log files.

Possible options:

- "debug": Detailed information on the flow through the system.
- "info": Runtime events (startup/shutdown).
- "warning": Events that may lead to unexpected behavior.
- "error": Other errors or unexpected conditions.
- "critical": Events that may break the workflow.

**Path to certificate:** Absolute path to the certificate your Imprivata Appliance or Certification Authority issued. (Default: /wfs/ca-certs/ssoCA.cer)

---

<sup>287</sup> <https://www.imprivata.com/>



### IMPORTANT NOTE

If you rename the certificate or decide to store it in a different place, you have to adjust the path accordingly under **Sessions > Appliance Mode > Imprivata > Path to Certificate**.  
Best practice is to change it directly through the profile which also issued the firmware update.

## Fast User Switching

**FUS user:** The username for the preconfigured session.

Possible options:

- Hostname: The hostname of the endpoint device will be used as a username.
- MAC address: The MAC address of the device will be used as a username.
- Serial of the board: The serial number of the device will be used as a username.
- Free text entry

**FUS user's domain:** The domain the user belongs to.

**FUS user's password:** The password of the user running the preconfigured session.

**Citrix Store URL:** URL of the StoreFront website or of XenApp Services.

**FUS resource:** The resource, like the Desktop or Application, that is assigned to the username.

**Single Application Kiosk:** The Imprivata PIE agent will be signaled that the FUS resource is an application.

More on FUS at: <https://www.imprivata.com/resources/datasheets/fast-user-switching-imprivata-onesign>

## Enable on-screen keyboard

If a touchscreen is used, the on-screen keyboard is enabled.

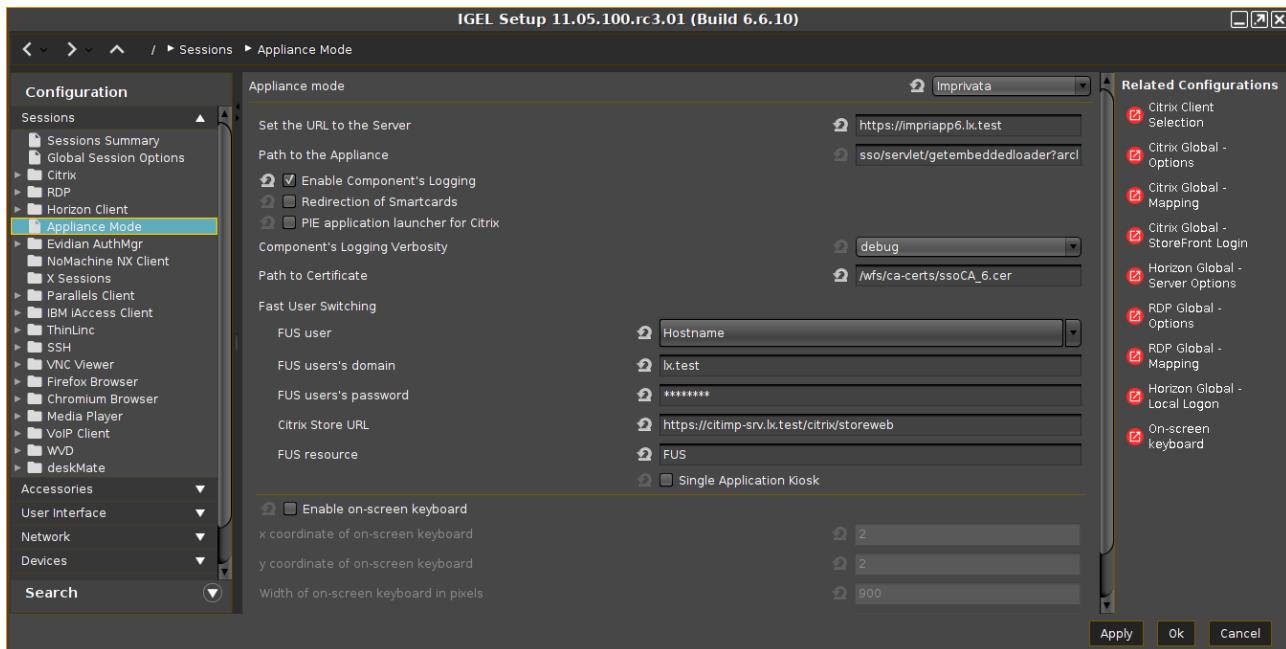
The following settings are active if **Enable on-screen keyboard** is activated.

**x coordinate of on-screen keyboard:** Specifies the X position of the on-screen keyboard in pixels. (Default: 2)

**y coordinate of on-screen keyboard:** Specifies the Y position of the on-screen keyboard in pixels. (Default: 2)

**Width of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height. (Default: 900)

**Height of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height. (Default: 0)



If you need to modify and adjust the sessions, see [Imprivata: Session Customization](#)(see page 323).

Imprivata automatically creates a data partition, i.e. storage location for internal data. If you are asked by your support to delete the data partition or you want to delete it for other reasons, see [Imprivata: Clear the Imprivata Data Partition](#)(see page 323).

### Useful Registry Keys

- If you need to set a default AD domain for PIE agent, go to **System > Registry > imprivata.default\_domain** and specify the NetBIOS name of your AD domain.
- If you need to ignore the VMware protocol selected by the Imprivata appliance, activate **System > Registry > imprivata.ignore\_horizon\_protocol**. In this case, the local selection under **Horizon Client > Horizon Client Global > Server Options > Preferred desktop protocol** will be used.
- To avoid focus theft from other windows, activate **System > Registry > imprivata.avoid\_focus\_ownership**.

## RDP MultiPoint Server

Menu path: **Sessions > Appliance Mode > RDP MultiPoint Server**

**Connect to server as soon as it is found:** If you always have to connect to the same server, you can preset the connection here by giving the DNS name of your RDP MultiPoint Server. Otherwise, the device will find one or more RDP MultiPoint Servers automatically as soon as you launch the session.



For this to be possible, the servers must be in the same network as the device and obtain their IP address from the same DHCP server as the device.

### XDMCP for This Display

Menu path: **Sessions > Appliance Mode > XDMCP for this display**

If this session type is selected, the device acts as an XDMCP client.

**Connection type:** The type of the connection.

Possible values:

- "Indirect via localhost
- "Indirect": At startup, a list of XDMCP hosts is displayed. This list is generated by the server specified under **Name or IP of the server**. The user can select a host.
- "Direct": The login mask of the host specified under **Name or IP of the server** is displayed.
- "Broadcast": The device starts a broadcast request. The login mask of that XDMCP host is displayed which is the first to respond to the broadcast request.

**Name or IP of server:** The name or IP of the XDMCP server.

**Enable hotkeys for XDMCP Display:** Defines whether hotkeys are managed by the device or the host.

Hotkeys are managed by the device. When the user enters a shortcut key that is defined as a hotkey on the device, it starts the appropriate action. The input is not forwarded to the server. (Default)

Hotkeys are not managed by the device. Almost all keyboard shortcuts are forwarded to the server. The hotkey [Ctrl + Alt + S] for opening the IGEL Setup can still be used, provided that this hotkey is activated under **Accessories > Setup**.

### 3.8.10 AppliDis

Menu path: **Setup > Sessions > AppliDis**

AppliDis Fusion is a virtualization solution which combines the virtualization of desktops and applications in a single console.

If you create an AppliDis session, you can configure the following settings:

**Connection**([see page 875](#)): Details of the **Server URL** and **Connect Type** for logging in. If you use AppliDis SLB Linux in the connector mode, the name of the application that uses the connector can be specified here.

**Options**([see page 876](#)): Allows you to define the language, credentials, access path, and further settings for the AppliDis client.

**Desktop Integration**([see page 878](#)): Start option settings for this session.

#### Connection

Menu path: **Setup > Sessions > AppliDis > Connection**

**Server URL:** Address of the AppliDis server or the administration server



**HTTP/HTTPS service port:** Protocol for communication with the AppliDis server  
 Possible options:

- [http](#)
- [https](#)

#### Connect type

Possible options:

- [Last option used](#)
- TS desktop
- Virtual desktop
- Session maker
- VDI desktop

**Forces the VDI desktop:** Name of the desktop to be started, e.g. Win10Test, TD-RD Desktop. This feature is active if "VDI desktop" is selected under **Connect type**.

**AppliDis SLB connector mode:** Name of the application which the connector uses if AppliDis SLB Linux is to be used in the connector mode.

## Options

Menu path: **Setup > Sessions > AppliDis > Options**

#### Language

Possible options:

- [English](#)
- French

**How the password is sent to the RDP Client:** The method for sending the password configured below to the RDP Client

Possible options:

- [cmdline](#)
- prompt

**Working directory:** Complete path of the work directory for the application on the server

**User name:** User name when logging in to the server

**Password:** Password when logging in to the server

Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

**Domain:** Domain when logging in to the server

**Full path to cert:** Path to the certificate with file name

**Timeout:** Maximum time that the system waits for a response from the server. (Default: 30)

**AppliDisXML access path:** Path for XML communication with the AppliDis administration server. (Example: /AppliDisXML/AppliDisServer.asp)

**Lock connection type**

- The connection type is locked. (Default)  
 The connection type is not locked.

**Hide “Close” tab**

- The “Close” tab is hidden. (Default)  
 The “Close” tab is not hidden.

**Close AppliDis client at end of session**

- The client is closed when the session ends. (Default)  
 The client is not closed.

**Force insecure mode**

- Insecure mode is forced.  
 Insecure mode is not forced. (Default)

**Enable debug mode**

- Debug mode is enabled.  
 Debug mode is disabled. (Default)
- Activate SSL mode**
- SSL mode is enabled.  
 SSL mode is disabled. (Default)

**Remember user**

- AppliDis remembers the user name. (Default)  
 AppliDis does not remember the user name.

**Discard credentials**

- The credentials are not saved. (Default)  
 The credentials are saved.

**Hide “Filter” tab**

- The “Filter” tab is not shown.  
 The “Filter” tab is shown. (Default)

**Hide “Service” tab**

- The “Service” tab is not shown.  
 The “Service” tab is shown. (Default)

**Hide “Server” tab**

- The “Server” tab is not shown.  
 The “Server” tab is shown. (Default)



## Desktop Integration

Menu path: **Setup > Sessions > AppliDis > Desktop Integration**

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### **Start menu**

The session can be launched from the start menu.

#### **Application Launcher**

The session can be launched with the Application Launcher.

#### **Desktop**

The session can be launched with a program launcher on the desktop.

#### **Quick start panel**

The session can be launched with the quick start panel.

#### **Start menu's system tab**

The session can be launched with the start menu's system tab.

#### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### **Hotkey**

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.



**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

## Autostart

The session will be launched automatically when the device boots.

## Restart

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

## Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.



- The session is started automatically, even when no network is available.

### 3.8.11 Evidian AuthMgr

Menu path: **Sessions > Evidian AuthMgr**

The procedure for configuring your Evidian AuthMgr session is described below.

- [Evidian AuthMgr Global](#)(see page 880)
- [Evidian AuthMgr Session](#)(see page 882)

#### Evidian AuthMgr Global

Menu path: **Setup > Sessions > Evidian AuthMgr > Evidian AuthMgr Global**

Here, you can configure the global settings for Evidian AuthMgr sessions.

- [Restart](#)(see page 880)
- [Options](#)(see page 882)

#### Restart

Menu path: **Setup > Sessions > Evidian AuthMgr > Evidian AuthMgr Global > Restart**

Here, you can define the desktop integration for restarting Evidian AuthMgr.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Starting Methods for Session

##### **Start menu**

- The session can be launched from the start menu.

##### **Application Launcher**

- The session can be launched with the Application Launcher.

##### **Desktop**

- The session can be launched with a program launcher on the desktop.

##### **Quick start panel**

- The session can be launched with the quick start panel.

##### **Start menu's system tab**

- The session can be launched with the start menu's system tab.



### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey



To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

## Options

Menu path: **Setup > Sessions > Evidian AuthMgr > Evidian AuthMgr Global > Options**

### Options

**Language selection:** Language selection of catalog messages.

Possible values:

- [Global setting](#)
- English (UK)
- English (US)
- German
- French
- Danish
- Custom

**Custom catalog of messages:** Choose here the file for the custom catalog of messages. (Default: `/services/evidian/share/locale/en/rsUserAuth.cat`)

## Data Partition

### Evidian AuthMgr Data Partition

- The data partition is activated so that additional data can be stored persistently.  
 The data partition is deactivated. (Default)

**Size:** Size of the Evidian AuthMgr data partition in MB. (Default: 10)

## Evidian AuthMgr Session

Menu path: **Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions**

Here, you can set up your own Evidian AuthMgr session.

- [Connection](#)(see page 882)
- [Options](#)(see page 883)
- [Desktop Integration](#)(see page 885)

## Connection

Menu path: **Setup > Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions > [Session name] > Connection**

In this area, you can specify the settings for the connection between Evidian AuthMgr and the server.

**Protocol:** Protocol that is used for user access.

Possible values:



- "HTTP"
- "HTTPS"

**Server:** IP address or DNS name that is used for user access.

**Port:** Port that is used for user access.

Possible values:

- "9764 (HTTP)"
- "9765 (HTTPS)"
- "Custom"

**Custom port:** If you selected "Custom" above, you can enter a port of your own here.

**Path to service:** Service path that is used for user access. (Default: /soap)

**CA certificate:** Path to the CA certificate with file name. The certificate is needed for HTTPS connections. (Example: /wfs/ca-certs/ca.crt)

- Download the Certificate for Evidain from the EAM in **base64 encoded x509 CER** format,
- Convert it to crt by the following command: **openssl x509 -inform PEM -in YOUR\_CERT.cer -out YOUR\_CRT.crt**
- Eventually **move YOUR\_CRT.crt** to the endpoint

**Roaming session secret:** Password for the roaming session.

#### Fallback User Access Services

Click on the logo to specify up to four alternative connections. These will be used if the primary authentication server is not available. The alternative servers will be queried in sequence.

#### Options

Menu path: **Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions > [Session name] > Options**

Specify further options for your Evidian AuthMgr session.

#### Session type

Possible values:

- Citrix ICA
- RDP
- VMware Horizon
- RDWEB
- Custom

If you have selected the user-defined session type, you can enter your own start and stop commands here:

**Custom start command:** Command that is executed when the card is inserted. (Example: /wfs/start.bash)

**Custom stop command:** Command that is executed when the card is removed. (Example: /wfs/stopp.bash)



**Language selection:** Language selection of catalog messages.

Possible values:

- Automatic
- English (UK)
- English (US)
- German
- French
- Custom

**Custom catalog of messages:** Choose here the file for the custom catalog of messages. (Default: /services/evidian/share/locale/en/rsUserAuth.cat)

#### Availability message

- A message is shown when the authentication tool is available.  
 A message is not shown when the authentication tool is available.

#### Tapping mode

- The operating mode can be changed by briefly tapping the card on the reader. Each tap triggers an action.  
 The operating mode cannot be changed by tapping the card on the reader.

**Delay for dynamic tapping:** Tapping delay in seconds.

#### Allow password authentication

- Password is required for the authentication.  
 Password is not required for the authentication.

#### Allow password forgotten

- Resetting the password is allowed.  
 Resetting the password is not allowed.

**Default domain name for password authentication:** Domain name used by default for password authentication.

#### Debug mode

- Debug mode is activated, and all outputs are switched to the default error output.  
 Debug mode is deactivated.

**Level for trace:** Specifies the trace level. The level of detail of the log messages decreases as you move down through the selection list.

Possible values:

- none
- low
- medium
- high
- details

#### Use configuration file

- Instead of the preconfigured session, a custom configuration file is used. All other session settings are ignored.  
 A custom configuration file is not used.



**Path:** Path to the configuration file with file name. (Example: /etc/rsUserAuth/rsUserAuth.ini)

#### UPN format

- The UPN (User Principal Name) format for credentials is allowed.
- The UPN format cannot be used.

#### No trivial PIN code

- A trivial PIN, i.e. consisting of three or more consecutive numbers or identical digits, is not allowed.
- A PIN can consist of three or more consecutive numbers or identical digits. (Example: 2345, 1111)

#### 4-eye authentication

- 4-eye authentication is enabled. For details, see <https://www.vidian.com/products/enterprise-sso/4eyes-authentication/>.
- 4-eye authentication is disabled.

**Ignore smartcard removal on this reader:** You can ignore the removal of the smartcard/RFID badge on the reader which you specify here via the reader's name or its product ID. The use of wildcards is possible. Example: \*3x21\*

### Desktop Integration

Menu path: **Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions > [Session name] > Desktop Integration**

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

- The session can be launched from the start menu.

#### Application Launcher

- The session can be launched with the Application Launcher.

#### Desktop

- The session can be launched with a program launcher on the desktop.

#### Quick start panel

- The session can be launched with the quick start panel.

#### Start menu's system tab

- The session can be launched with the start menu's system tab.

#### Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

#### Desktop context menu

- The session can be launched with the desktop context menu.



**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.  
Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. **Ctrl**.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- = Alt

Key combinations are formed as follows with |:

- + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)



### Autostart

The session will be launched automatically when the device boots.

### Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

### Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

## 3.8.12 NoMachine NX Client

Menu path: **Sessions > NoMachine NX Client > [Session Name]**

You can configure one or more NoMachine NX sessions.

Further information regarding configuration can be found in the original documentation provided by NoMachine: <http://www.nomachine.com/documents>.

The settings for launching the session are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

The session can be launched from the start menu.

#### Application Launcher

The session can be launched with the Application Launcher.

#### Desktop

The session can be launched with a program launcher on the desktop.

#### Quick start panel

The session can be launched with the quick start panel.



### **Start menu's system tab**

The session can be launched with the start menu's system tab.

### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

### **Desktop context menu**

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### **Hotkey**

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
- [Ctrl] = Ctrl
-  = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:



- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

#### Autostart

The session will be launched automatically when the device boots.

#### Restart

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

#### Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

- [Server](#)(see page 889)
- [Unix Desktop](#)(see page 890)
- [Unix Display](#)(see page 891)
- [Windows Desktop](#)(see page 892)
- [Windows Display](#)(see page 893)
- [VNC Desktop](#)(see page 894)
- [VNC Display](#)(see page 894)
- [Shadow Display](#)(see page 895)
- [Logon](#)(see page 896)
- [Advanced](#)(see page 897)
- [Services](#)(see page 898)
- [Desktop Integration](#)(see page 898)

#### Server

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Server**

Here, you can specify the connection data for the *NoMachine NX* session.

- **Host:** Host name or IP address of the *NoMachine NX* server.



- **Port:** Port for connecting with the *NoMachine NX* server (default: 22).
- **Connection service:** Protocol for connecting to the *NoMachine NX* server.  
Possible values:
  - SSH
  - NX
- **Session:** Session type  
Possible values:
  - Unix: The session will run under Unix/Linux on the server side. X11 serves as the transmission protocol.
  - Windows: The session will run under Windows on the server side. RDP serves as the transmission protocol.
  - VNC: The session will be transmitted with VNC (Virtual Network Computing) via RFP (Remote Framebuffer Protocol). On the server side, the session can run on any operating system. A VNC server is required on the server.
  - Shadow: Protocol version for older VNC servers
- **Use following DSA key:** DSA key which is to be used instead of the default key when logging on to the server. If no key is entered here, i.e. the field is empty, the thin client's default key will be used. The default key is saved under /wfs/nxkeys/server.id\_dsa.key.

## Unix Desktop

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Unix Desktop**

Here, you can specify which window manager or display manager is to be launched on the server when the user logs on with the *NoMachine NX* client. The window manager must be available on the server.

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Session** is set to "Unix".

- **Desktop**

Possible values:

- KDE: KDE will be launched.
- Gnome: Gnome will be launched.
- CDE: CDE will be launched.
- XDM: The display manager XDM will be launched.
- Custom: A custom window manager will be used.

Settings options if "Desktop" is set to "XDM":

- **Login:** These options are available if **Desktop** is set to "XDM".
  - **Let the NX server decide:** The configuration of the *NoMachine NX* server will be used for logon purposes.
  - **Query an X desktop manager:** The *NoMachine NX* client will connect to the X desktop manager of the computer defined under **Host**. The set **Port** will be used for this connection (default: 177).
  - **Broadcast XDM request:** The *NoMachine NX* client will send a request for available XDM servers in the subnet via the set **Port** (default: 177). The *NoMachine NX* client will use the first XDM server that responds to the request.



- **Get a list of available X desktop managers:** The *NoMachine NX* client will send a request to the computer defined under **Host** via the set **Port** (default: 177). This computer will reply with a list of available XDM servers. This option is relevant to older versions of the *NoMachine NX* server.

Settings options if "Desktop" is set to "Custom":

#### Application

- **Run console:** The terminal set by default will be launched. Example: Xfce terminal
- **Run default X client script on server:** The script for the default desktop environment set by default will be launched. Example: /home/user/startxfce.sh
- **Run the following command:** Start command for the desired application or the desired window manager. Example: startxfce

#### Options

- **Floating window:** The session will be shown in a separate window. This option makes particularly efficient use of bandwidth.
- **Use X agent encoding**
  - The data traffic will be decoded by the NX agent rather than in the X protocol. (default)
  - The data traffic will remain in the X protocol and will be tunneled and compressed by the NX proxy.
- **Use taint of X replies**
  - Trivial sources of X roundtrips will be suppressed by generating the response on the side of the X client. This option is relevant to older versions of the *NoMachine NX* server. (default)
- **New virtual desktop:** The session will take place on a new virtual desktop on the server side.

## Unix Display

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Unix Display**

Here, you can define the properties for image transmission from the *NoMachine NX* server to the *NoMachine NX* client.

The image transmission properties can also be defined on the server side. If a server-side setting competes with a client-side setting, the server-side setting will be effective.

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Server > Session** is set to "Unix".

**Display:** Size of the display area that is used for the session.

Possible values:

- "640x480"
- "800x600"
- "1024x768"
- "Available area": The entire display area is used for the session. The taskbar is not visible.



- "Fullscreen
- "Custom": The **Width** and **Height** can be freely defined.
- "Multimonitor fullscreen": The session will be shown in full-screen mode on all available monitors, i.e. stretched across the entire screen of each monitor.

**Width:** Width of the display area for the session. (Default: 800)

**Height:** Height of the display area for the session. (Default: 600)

#### Use custom settings

- The image transmission properties can be changed on the client side.
- The image transmission properties are specified on the server side only. (Default)

**Use both JPEG and RGB compression:** JPEG compression (results in losses) as well as RGB compression (loss-free) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.

**Use JPEG and RGB compression, and use custom JPEG quality:** JPEG compression (results in losses) as well as RGB compression (loss-free) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.

**Only use JPEG compression:** Only JPEG compression (results in losses) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.

**Use JPEG compression and custom JPEG quality:** Only JPEG compression (results in losses) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.

**Only use RGB compression:** Only RGB compression (loss-free) will be used.

**Use plain X bitmaps:** The images will be transmitted as bitmaps without compression.

**JPEG quality:** If **Use both JPEG and RGB compression, and use custom JPEG quality** or **Use JPEG compression and custom JPEG quality** is enabled, the quality of images in JPEG format can be defined. (Default: 6)

## Windows Desktop

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Windows Desktop**

Here, you can specify which *Windows* terminal server (or remote desktop service) is used, how the user logs on and whether the entire desktop or an individual application is launched.

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Session** is set to "Windows".

- **Windows terminal server:** Host name or IP address of the *Windows* server on which the desktop or the application runs
- **Windows terminal server domain:** Domain in which the *Windows* terminal server is located
- **Use the NX user's credentials:** When the session starts, the logon information under **Setup > NoMachine NX Client Sessions > [Session Name] > Logon** will be used. (default)
- **Use following credentials:** When the session starts, the logon information under **Username** and **Password** will be used.
  - **Username:** User name for starting the session
  - **Password:** Password for starting the session
- **Start Windows login screen:** When starting the session, the user must enter their logon information.



- **Run desktop:** When starting the session, the *Windows* desktop is shown (default)
- **Run application:** When starting the session, the *Windows* application given in the text field is launched.

## Windows Display

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Windows Display**

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Session** is set to "Windows".

- **Display:** Size of the display area that is used for the session

Possible values:

- 640x480
- 800x600
- 1024x768
- Available area:
- Full screen: The session will be shown in full-screen mode, i. e. stretched across the entire screen.
- Custom: The **width** and **height** can be freely defined.
- Multi-monitor full screen:

- **Width:** Width of the display area for the session (default: 800)

- **Height:** Height of the display area for the session (default: 600)

- **Colors**

Possible values:

- 256
- 32K
- 64K
- 16M

- **Use custom settings**

The image transmission properties can be changed on the client side.

The image transmission properties are specified on the server side only. (default)

- **Use JPEG and RGB compression:** JPEG compression (results in losses) as well as RGB compression (loss-free) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.
- **Use JPEG and RGB compression, and define JPEG quality:** JPEG compression (results in losses) as well as RGB compression (loss-free) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.
- **Only use JPEG compression:** Only JPEG compression (results in losses) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.
- **Use JPEG compression and custom JPEG quality:** Only JPEG compression (results in losses) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.
- **Only use RGB compression:** Only RGB compression (loss-free) will be used.
- **Use plain X bitmaps:** The images will be transmitted as bitmaps without compression.



- **JPEG quality:** If **Use JPEG and RGB compression and define JPEG quality** or **Use JPEG compression and define JPEG quality** is enabled, the quality of images in JPEG format can be defined (default: 6).
- **Enable RDP image cache**  
 The cache is enabled. This increases the amount of memory needed. However, the speed of the session may be increased. (default)

## VNC Desktop

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > VNC Desktop**

Here, you can specify the VNC server as well as the password for the VNC session.

These settings are only relevant up to NoMachine NX Server Version 3.5.

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Session** is set to "VNC".

- **VNC server:** Name or IP address of the server
- **: Number of the display.**
- **Password:** Password for the VNC session

## VNC Display

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > VNC Display**

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Session** is set to "VNC".

These settings are only relevant up to NoMachine NX Server Version 3.5.

- **Display:** Size of the display area that is used for the session  
 Possible values:
  - 640x480
  - 800x600
  - 1024x768
  - Available area
  - **Fullscreen:** The session will be shown in full-screen mode, i. e. stretched across the entire screen.
  - Custom: The **width** and **height** can be freely defined.
  - Multimonitor Fullscreen
- **Width:** Width of the display area for the session (default: 800)
- **Height:** Height of the display area for the session (default: 600)
- **Use custom settings**  
 The image transmission properties can be changed on the client side.  
 The image transmission properties are specified on the server side only. (default)



- **Use both JPEG and RGB compression:** JPEG compression (results in losses) as well as RGB compression (loss-free) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.
- **Use JPEG and RGB compression, and use custom JPEG quality:** JPEG compression (results in losses) as well as RGB compression (loss-free) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.
- **Only use JPEG compression:** Only JPEG compression (results in losses) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.
- **Use JPEG compression and custom JPEG quality:** Only JPEG compression (results in losses) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.
- **Only use RGB compression:** Only RGB compression (loss-free) will be used.
- **Use plain X bitmaps:** The images will be transmitted as bitmaps without compression.
- **JPEG quality:** If **Use JPEG and RGB compression and define JPEG quality** or **Use JPEG compression and define JPEG quality** is enabled, the quality of images in JPEG format can be defined (default: 6).

## Shadow Display

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Shadow Display**

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Session** is set to "Shadow".

These settings are only relevant up to NoMachine NX Version 3.5.

- **Display:** Size of the display area that is used for the session  
Possible values:
  - 640x480
  - 800x600
  - 1024x768
  - Available area:
    - **Fullscreen:** The session will be shown in fullscreen mode, i. e. stretched across the entire screen.
    - Custom: The **width** and **height** can be freely defined.
    - Multi-monitor full screen:
- **Width:** Width of the display area for the session (default: 800)
- **Height:** Height of the display area for the session (default: 600)
- **Enable custom settings**
  - The image transmission properties can be changed on the client side.
  - The image transmission properties are specified on the server side only. (default)
    - **Use both JPEG and RGB compression:** JPEG compression (lossy) as well as RGB compression (lossless) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.



- **Use JPEG and RGB compression, and use custom JPEG quality:** JPEG compression (lossy) as well as RGB compression (lossless) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.
- **Only use JPEG compression:** Only JPEG compression (lossy) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.
- **Use JPEG compression and custom JPEG quality:** Only JPEG compression (lossy) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.
- **Only use RGB compression:** Only RGB compression (lossless) will be used.
- **Use plain X images:** The images will be transmitted as bitmaps without compression.
- **JPEG quality:** If **Use JPEG and RGB compression and use custom JPEG quality** or **Use JPEG compression and custom JPEG quality** is enabled, the quality of images in JPEG format can be defined (default: 6).
- **Enable render extension**  
 The "Render" or "XRender" protocol extension is enabled. This allows a transparency effect where windows overlap on the screen. (default)
- **Disable the backing store**  
 The cache is disabled. This reduces the amount of memory needed. However, the speed of the session may be reduced.  
 The cache is enabled. (default)
- **Disable the composite extension**  
 The "Composite" protocol extension is disabled. Transparency effects where windows overlap on the screen are not possible.  
 The "Composite" protocol extension is enabled. (default)
- **Disable the shared memory extension**  
 The shared memory extension is disabled.  
 The shared memory extension is enabled. (default)
- **Disable emulation of shared pixmaps**  
 The emulation of shared images (shared pixmaps) is disabled.  
 The emulation of shared images (shared pixmaps) is enabled. (default)

## Logon

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Logon**

Here, you can specify the logon information for starting the session.

- **Login method**

Possible values:

- **Password:** The user logs on with a logon and password.
- **Private key:** The logon takes place with a private key.

- **Login:** User name when logging on to the server

- **Password:** Password when logging on to the server

Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.



## Advanced

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Advanced**

Here, you can change advanced settings.

- **Link speed**

Possible values:

- Modem
- ISDN
- ADSL
- WAN
- LAN

- **Disable ZLIB stream compression**

Possible values:

- The data traffic between the client and server will not be compressed.

Switching off compression can be helpful if the data traffic is compressed on another level, e.g. by VPN software.

- The data traffic between the client and server will be compressed. (default)

- **Enable SSL encryption on all traffic**

- Connections with NX, SSH and UDP will be encrypted. (default)

- Connections with NX and SSH will be encrypted, connections with UDP will remain unencrypted.

- **Connect through a HTTP proxy**

- The connection between the client and server will be routed via an HTTP proxy.

- The connection between the client and server will be direct. (default)

- **Host:** Host name or IP address of the HTTP proxy

- **Port:** Port of the HTTP proxy (default: 8080)

- **Username:** User name when logging on to the HTTP proxy

This setting is only relevant up to NoMachine NX Server Version 3.5.

- **Password:** Password when logging on to the HTTP proxy

This setting is only relevant up to NoMachine NX Server Version 3.5.

- **Remember my password**

This setting is only relevant up to NoMachine NX Server Version 3.5.

- The password will be saved.

- The password will not be saved and must therefore be entered again for each session. (default)

- **Disable deferred screen updates:** Delayed screen refreshing ("lazy encoding") compensates for bottlenecks in data transmission. If a bottleneck occurs, refresh procedures requiring large amounts of bandwidth are delayed in favor of interactivity. There are two levels of delayed screen



refreshing. With Level 1, refresh actions which are not displayed directly ("offscreen") are dismissed. With Level 2, refresh actions which are displayed directly ("onscreen") are dismissed.

This setting is only relevant up to NoMachine NX Server Version 3.5.

- Bottlenecks in data transmission are not compensated for through delayed screen refreshing.
- If the connection speed is set to "WAN", Level 1 delayed screen refreshing will be used. If the connection speed is set to "MODEM", "ISDN" or "ADSL", Level 2 delayed screen refreshing will be used. (default)

- **Disk cache:** Size of the persistent memory for caching images (default: 64 MB)

This setting is only relevant up to NoMachine NX Server Version 3.5.

- **Memory cache:** Size of the volatile memory for caching images (default: 16 MB)

This setting is only relevant up to NoMachine NX Server Version 3.5.

## Services

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Services**

Here, you can enable or disable services for printers and audio playback on your thin client.

- **Enable multimedia support**

You will find further information regarding audio playback on the *NoMachine NX* client in the [NoMachine Knowledge Base](#)<sup>288</sup>.

- Audio output is forwarded to the media player via esound.
- A dedicated channel is used for audio output. (default)

- **Enable CUPS printing**

- Printing via the thin client is enabled. (default)
- Printing via the thin client is disabled.

- **Port:** Port via which CUPS can be configured with a browser (default: 631)

- **Public printer**

- The printer connected to the thin client is shared via the network. A server-side configuration is required for this purpose.

- The printer is not shared. (default)

## Desktop Integration

Menu path: **Sessions > NoMachine NX Client > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the NoMachine NX session.

**Session name:** Name for the session.

<sup>288</sup> <https://www.nomachine.com/?q=AR03D00355>



The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. Ctrl.



Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

## Autostart

The session will be launched automatically when the device boots.

## Restart

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

## Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.



### 3.8.13 X Sessions

Menu path: **Sessions > X Sessions > [Session Name]**

You can configure one or more X sessions.

The settings for launching the session are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Starting Methods for Session

##### **Start menu**

The session can be launched from the start menu.

##### **Application Launcher**

The session can be launched with the Application Launcher.

##### **Desktop**

The session can be launched with a program launcher on the desktop.

##### **Quick start panel**

The session can be launched with the quick start panel.

##### **Start menu's system tab**

The session can be launched with the start menu's system tab.

##### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

##### **Desktop context menu**

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.



- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

### Autostart

The session will be launched automatically when the device boots.

### Restart

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.



No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

#### Autostart requires network

- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.

- [Server](#)(see page 903)
- [Desktop Integration](#)(see page 904)

## Server

Menu path: **Setup > Sessions > X Sessions > [session name] > Server**

**Connection type:** Connection type for the XDMCP session

Possible options:

- Indirect via localhost: At startup, the thin client generates a list of found XDMCP hosts. The user can select a host.
- Indirect: At startup, a list of XDMCP hosts is displayed. This list is generated by the server specified under **Name or IP of server**. The user can select a host.
- Direct: The login mask of the host specified under **Name or IP of server** is displayed
- Broadcast: The thin client starts a broadcast request. The login mask of that XDMCP host is displayed which responds first.
- Local display: The command specified under **Command to be displayed** is run.

**Name or IP of server:** Hostname or IP address of the XDMCP server

**Command to be displayed:** Command to be executed. The display is set in the DISPLAY environment variable.

#### Access control

Access to this display from other computers will be controlled.

#### Terminate after one session

The session is terminated when the user has logged out from the remote server.

#### Use quit hotkey

The session can be terminated with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. **Ctrl**. Here, you will find the available modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
-  = Ctrl
-  = Super\_L
-  = Alt

Key combinations are formed as follows with |:



Ctrl + = Ctrl | Super\_L

**Quit hotkey:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

### Use fullscreen

The XDCMP session is displayed in fullscreen mode.

### Use fullscreen restricted to workarea

The thin client's local taskbar is visible.

**Window size:** Window size for the XDMCP session. Default: 640x480

**Color depth:** Color depth for the XDMCP session.

Possible options:

- Same as display: The system settings for the thin client is used.
- 256 colors
- 65535 colors
- True Color (24)
- True Color (32)

### Color allocation policy

Possible options:

- Default
- Mono
- Gray
- Color

**Start monitor:** Selects the monitor on which the XDMCP session ist displayed.

Possible options:

- No configuration: The monitor is selected according to already existing windows and to the current position the mouse pointer.
- 1st monitor
- 2nd monitor
- Fullscreen on all monitors

## Desktop Integration

Menu path: **Sessions > X Sessions > [Session Name] > Desktop Integration**

You can configure one or more X sessions.

The settings for launching the session are described below.

**Session name:** Name for the session.



The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. Ctrl.



Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

### Autostart

The session will be launched automatically when the device boots.

### Restart

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

### Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.



### 3.8.14 Parallels Client Global

Menu path: **Sessions > Parallels Client > Parallels Client Global**

In this area, you can configure global settings for all Parallels Client sessions.

- [Keyboard](#)(see page 907)
- [USB Redirection](#)(see page 907)

#### Keyboard

Menu path: **Setup > Sessions > Parallels Client > Parallels Client Global > Keyboard**

In this area, you can select the keyboard layout for Parallels Client sessions.

##### **Keyboard layout**

Possible values:

- System presets as well as all available input schemes.

#### USB Redirection

Menu path: **Setup > Sessions > Parallels Client > Parallels Client Global > USB Redirection**

In this area, you can configure USB Redirection for Parallels Client sessions.

##### **USB Redirection**

USB redirection is enabled.

USB redirection is disabled. (Default)

**Automatically redirect all USB devices:** Defines whether the **Device Rules** will be ignored and all USB devices redirected.

All USB devices will be redirected.

USB devices will be redirected according to the **Device Rules**. (Default)

#### Device Rules

In this area, you can define device rules for USB redirection.

Defining new rules:

Click to get to the **Add** dialog.

In the **Add** dialog, you can define the following settings:

##### **Rule**

Possible values:

- "Deny"
- "Allow"

**Vendor ID:** Hexadecimal manufacturer number.



**Product ID:** Hexadecimal device number.

To find out the **Vendor ID** and **Product ID** of the connected USB device, use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal. You can also use the **System Information** tool, see [Using “System Information” Function](#)(see page 1108).

**Name:** Free text entry.

#### PTP/MTP redirection

PTP/MTP redirection is enabled.

PTP/MTP redirection is disabled. (Default)

**Automatically redirect all PTP/MTP devices:** Defines whether the **Device Rules** will be ignored and all PTP/MTP devices redirected.

All PTP/MTP devices will be redirected.

PTP/MTP devices will be redirected according to the **Device Rules**. (Default)

#### Device Rules

In this area, you can define device rules for PTP/MTP redirection.

Defining new rules:

Click to get to the **Add** dialog.

In the **Add** dialog, you can define the following settings:

##### Rule

Possible values:

- "Deny"
- "Allow"

**Vendor ID:** Hexadecimal manufacturer number.

**Product ID:** Hexadecimal device number.

To find out the **Vendor ID** and **Product ID** of the connected USB device, use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal. You can also use the **System Information** tool, see [Using “System Information” Function](#)(see page 1108).

**Name:** Free text entry.

### 3.8.15 Parallels Client Session

Menu path: **Sessions > Parallels Client > Parallels Client Sessions > [Session Name]**

You can configure one or more Parallels Client sessions.

**Session name:** Name for the session.



The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### **Start menu**

The session can be launched from the start menu.

### **Application Launcher**

The session can be launched with the Application Launcher.

### **Desktop**

The session can be launched with a program launcher on the desktop.

### **Quick start panel**

The session can be launched with the quick start panel.

### **Start menu's system tab**

The session can be launched with the start menu's system tab.

### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

### **Desktop context menu**

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### **Hotkey**

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".



These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with | :

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

### Autostart

The session will be launched automatically when the device boots.

### Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

### Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

- [Connection](#)(see page 911)
- [Display](#)(see page 912)
- [Local Resources](#)(see page 913)
- [Experience](#)(see page 914)
- [Network](#)(see page 915)



- [Advanced \(see page 915\)](#)
- [Desktop Integration \(see page 916\)](#)

## Connection

Menu path: **Setup > Sessions > Parallels Client > Parallels Client Sessions > [Session Name] > Connection**

In this area, you can specify the settings for the connection between the Parallels Client and the server.

### Application Server

**Primary Server:** Name or IP address of the primary application server.

**Secondary Server:** Name or IP address of the secondary application server. The secondary application server is used if the primary application server cannot be contacted.

### Connection Mode

Possible values:

- "Gateway Mode": This mode is suitable if the Parallels Client does not have access to a physical server and no special demands as regards security apply. The Parallels Client establishes a connection to the Parallels SecureClientGateway via port 80. The RDP sessions runs in a tunnel within this connection.
- "Direct Mode": This mode is suitable if the Parallels Client has direct access to a physical server. The Parallels Client establishes a connection to the Parallels SecureClientGateway via port 80 in order to negotiate connection data for the RDP session with the application server. The Parallels Client then terminates the connection to the gateway and establishes the session with the application server. This mode is the most efficient because the connection to the gateway is temporary and the data traffic is correspondingly low.
- "Gateway SSL Mode": This mode is suitable if the Parallels Client does not have access to a physical server and there are high demands as regards security. The Parallels Client establishes a connection to the Parallels SecureClientGateway via port 443. The RDP sessions runs in a tunnel within this connection.
- "Direct SSL Mode": This mode is suitable if the Parallels Client has direct access to a physical server and there are high demands as regards security. The Parallels Client establishes a connection to the Parallels SecureClientGateway via port 443 in order to negotiate connection data for the RDP session with the application server. The Parallels Client then terminates the connection to the gateway and establishes the session with the application server.

**Port:** Port for communication with the application server. (Default: 80)

### Logon

#### Use system credentials

The system-wide logon data will be used for logging on to the application server (single sign-on). This option can be used if the local device logon takes place via Kerberos. The logon data saved temporarily when logging on to the device will be used for the user name and password.

The logon data given under **User name**, **Password**, and **Domain** will be used when logging on to the application server. (Default)



**User:** User name when logging on to the application server.

**Password:** Password when logging on to the application server.

Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

**Domain:** Domain when logging on to the application server.

#### **Enable support for FIPS 140-2 compliance**

- The support for FIPS 140-2 standard is enabled.  
 The support for FIPS 140-2 standard is disabled. (Default)

### Display

**Display color depth:** Number of colors displayed

Possible values:

- 8 bit
- 15 bit
- 16 bit
- 24 bit
- 32 bit

**Graphics acceleration:** Type of graphics acceleration. Higher graphics acceleration means better graphics quality, but requires more CPU power.

Possible options:

- "None": No acceleration
- "Basic": Basic acceleration
- "RemoteFX": Microsoft RemoteFX will be used.
- "RemoteFX Adaptive- "AVC Adaptive": H.264/AVC will be used.

If "RemoteFX" or "RemoteFX Adaptive" is enabled, the color depth will automatically be set internally to 32 bit, regardless of the value set under **Display color depth**.

#### **Use all monitors for desktop session (if applicable)**

- All monitors will be used for the desktop session.  
 The primary monitor will be used for the desktop session. (Default)

#### **Use only primary monitor for published applications**

Published applications run on the server, the input and output data is exchanged between the client and the application server.

- Published applications will only be shown on the primary monitor.  
 Published applications will only be shown on all available monitors. (Default)



### Span desktop across all monitors

- The desktop will be shown across all available monitors.
- The desktop will only be shown on the primary monitor. (Default)

## Local Resources

Menu path: **Setup > Parallels Client > Parallels Client Sessions > [Session Name] > Local Resources**

### Remote audio playback

Possible values:

- "Bring to this computer
- "Do not play": The device does not play back the audio data supplied by the application server.
- "Leave at remote computer": The audio data will be played back on the application server.

### Remote audio recording

Possible values:

- "Record from this computer": The audio input (microphone) is redirected to the application server.
- "Do not record": The audio input (microphone) is not redirected to the application server.

### Apply Windows key combinations for desktops only

Possible values:

- "On the local computer": Windows-specific hotkeys are used for the local desktop only.
- "On the remote computer": Windows-specific hotkeys are used for the application server only.
- "In full-screen mode only": Windows-specific hotkeys are used for remote applications in full-screen mode only.

## Local devices

### Connect local serial ports

- The device's serial interfaces can be used in the Parallels Client session.
- The serial interfaces cannot be used in the Parallels Client session. (Default)

### Connect local smartcards

- The device's card reader can be used in the Parallels Client session.
- The card reader cannot be used in the Parallels Client session. (Default)

### Connect local drives

- The drives connected to the device can be used in the Parallels Client session.
- The drives cannot be used in the Parallels Client session. (Default)

### Connect local printers

- The printer connected to the device can be used in the Parallels Client session.
- The printer cannot be used in the Parallels Client session. (Default)

### Connect clipboard



- The clipboard of the Parallels Client session can be used. (Default)
- The clipboard of the Parallels Client session cannot be used.

## Experience

Menu path: **Setup > Parallels Client > Parallels Client Sessions > Parallels Client Session > Experience**

You can enable or disable the features for the graphical display according to the bandwidth of the network connection. The features can also be activated or deactivated individually.

**Connection speed:** Activates the features for the graphical display depending on the bandwidth of the network connection to provide the optimal performance.

Possible options:

- "Modem 56 Kbps": The features **Themes** and **Bitmap caching** will be enabled.
- "Low speed broadband (256 Kbps-2 Mbps)": The features **Themes** and **Bitmap caching** will be enabled.
- "Satellite (2 Mbps-16 Mbps with high latency)": The features **Menu and window animation**, **Desktop composition**, **Themes**, and **Bitmap caching** will be enabled.
- "High speed broadband (2 Mbps-16 Mbps)": The features **Menu and window animation**, **Desktop composition**, **Themes**, and **Bitmap caching** will be enabled.
- "WAN (10 Mbps or higher with high latency)": All features below will be enabled.
- "LAN (10 Mbps or higher)
- "Detect connection quality automatically": The automatically detected quality of the network connection determines which of the features below should be used for the optimal user experience. The individual feature selection is not possible.

### Desktop background

- The desktop background image for the session will be shown.

### Font smoothing

- Edges will be smoothed when text is displayed.

### Menu and window animation

- Transitions for menus and windows will be animated.

### Desktop composition

- Visual effects can be used for the desktop. For details on desktop composition, see e.g. <https://docs.microsoft.com/en-us/windows/win32/dwm/dwm-overview>.

### Show contents of window while dragging

- The window content will be shown when a window is moved.

### Themes

- The design of the desktop can be modified.

### Bitmap caching

- Bitmap resources, e.g. icons or images, are cached locally. This allows reducing the amount of data sent, and, thus improves the performance.



## Network

Menu path: **Setup > Parallels Client > Parallels Client Sessions > [Session Name] > Network**

Here, you can configure a proxy for communication between the Parallels Client and application server.

### Use proxy server

- A proxy is used for communication between the Parallels Client and the application server.
- A direct network connection is used for communication between the Parallels Client and the application server. (default)

**Proxy type:** Type or protocol of the proxy used

Possible values:

- SOCKS 4
- SOCKS 4A
- SOCKS 5
- HTTP 1.1

**Proxy host:** URL of the proxy

**Proxy port:** Port of the proxy (default: 8080)

**Use proxy credentials:** If a proxy demands a logon, this option must be enabled and the logon data must be entered under **Proxy user** and **Proxy password**.

- The logon data in **Proxy user** and **Proxy password** will be sent to the proxy.

**Proxy user:** User name when logging on to the proxy

**Proxy password:** Password when logging on to the proxy. The password is relevant if either the “SOCKS 5” or “HTTP 1.1” protocol is selected as the proxy type.

## Advanced

Menu path: **Setup > Sessions > Parallels Client > Parallels Client Sessions > [Session Name] > Advanced**

### Redirect URLs to client

- URLs will be opened on the client.
- URLs will be opened on the application server. (Default)

### Redirect MAIL to client

- E-mails will be opened on the client.
- E-mails will be opened on the application server. (Default)

### Compression

- The data flow between the Parallels Client and the application server will be compressed. (Default)

Compression reduces network traffic but requires more CPU power.

- The data flow between the Parallels Client and the application server will not be compressed.



### Use pre-windows 2000 login format

- Legacy login format (pre-Windows 2000) can be used. (Default)
- Legacy login format (pre-Windows 2000) cannot be used.

### Network level authentication

- Network level authentication (NLA) is activated for the Parallels Client session. The client has to authenticate before connecting to the server. (Default)

For more information about NLA, see <https://technet.microsoft.com/en-us/magazine/hh750380.aspx>.

- Network level authentication is disabled.

**Override computer name:** The name entered here will override the name of the application server shown at the top of the session window.

## Desktop Integration

Menu path: **Sessions > Parallels Client > Parallels Client Sessions > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the Parallels Client session.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

- The session can be launched from the start menu.

#### Application Launcher

- The session can be launched with the Application Launcher.

#### Desktop

- The session can be launched with a program launcher on the desktop.

#### Quick start panel

- The session can be launched with the quick start panel.

#### Start menu's system tab

- The session can be launched with the start menu's system tab.

#### Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

#### Desktop context menu

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.



**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

The session will be launched automatically when the device boots.

#### Restart

The session will be relaunched automatically after the termination.



**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

#### Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

### 3.8.16 PowerTerm Selection

Menu path: **Sessions > PowerTerm Terminal Emulation > PowerTerm Selection**

Here, you can choose between various versions of the PowerTerm terminal emulator in order to ensure the best possible compatibility with your terminal applications.

#### PowerTerm version

- 12.0.1.0.20170219.2-\_dev\_-34574
- 14.0.0.45623 (Default)

#### Licensed Feature

This feature requires an add-on license; see [Add-On Licenses<sup>289</sup>](#). Please contact your IGEL sales representative.

<sup>289</sup> <https://kb.igel.com/display/licensesmoreigelos11/Add-on+Licenses>



### 3.8.17 PowerTerm Session

Menu path: **Sessions > PowerTerm Terminal Emulation > PowerTerm Session**

You can configure one or more sessions for PowerTerm terminal emulation.

To edit the list, proceed as follows:

- Click on to create a new entry.
- Click on to remove the selected entry.
- Click on to edit the selected entry.
- Click on to copy the selected entry.

The configuration dialogs were designed to look as similar as possible to the setup pages described in the original documentation from ERICOM Software Ltd.

You will find detailed information on configuring the PowerTerm software in the [PowerTerm Interconnect Manual on the Ericom website<sup>290</sup>](#).

#### Desktop Integration

Menu path: **Sessions > PowerTerm Terminal Emulation > PowerTerm Sessions > [Session Name] > Desktop Integration**

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Starting Methods for Session

##### Start menu

The session can be launched from the start menu.

##### Application Launcher

The session can be launched with the Application Launcher.

##### Desktop

The session can be launched with a program launcher on the desktop.

##### Quick start panel

The session can be launched with the quick start panel.

##### Start menu's system tab

The session can be launched with the start menu's system tab.

---

<sup>290</sup> <http://www.ericom.com/help.asp?cat=support>



### Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

### Desktop context menu

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. **Ctrl**.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
-  = Ctrl
-  = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

-  = Alt

Key combinations are formed as follows with |:

-  +  = Ctrl | Super\_L

**Key:** Key for the hotkey



To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

### **Autostart**

The session will be launched automatically when the device boots.

### **Restart**

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

### **Autostart requires network**

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

## 3.8.18 IBM iAccess Client

Menu path: **Sessions > IBM iAccess Client**

IBM iAccess Client is an emulation of the IBM-5250 terminal in Java and supports numerous encodings.

- ▶ Add a session in order to be able to use the IBM iAccess Client.
- ▶ Under the **Connection** point under **Destination address**, give at least the DNS name or the IP address of a server. The client can also retrieve further logon information interactively.
- ▶ Under **Help > Information Center** in the IBM iAccess Client menu, you can read the help provided by the manufacturer in your browser.

*IBM iAccess certificates for server authentication and encryption can be distributed as files using the Universal Management Suite (UMS).*

- [iAccess Global](#)(see page 921)
- [IBM iAccess Session](#)(see page 923)

### iAccess Global

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Global**



Here you can define global settings for the emulation.

- [Tab Setup](#)(see page 922)
- [Font](#)(see page 922)

## Tab Setup

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Global > Tab Setup**

### **Open new sessions in a new tab**

- The new session will be opened in a new tab. (Default)  
 A new session will be opened in a new window.

### **Always display the tab bar**

- The tab bar will always be displayed.  
 The tab bar will not be displayed. (Default)

### **Switch to new tab when created**

- Switches to new tab. (Default)  
 Remains in current tab.

### **Send a warning when closing multiple tabs**

- Sends warning. (Default)  
 Multiple tabs are closed without warning.

### **Do not start tabbed sessions until the tab is selected**

- Applies.  
 Does not apply. (Default)

### **New Tab Action**

- Disable and hide
- Run the same
- Run other...

### **Tab Placement**

- Top
- Bottom
- Left
- Right

## Font

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Global > Font**

**Font File or Directory:** Enter the path to your font file or font directory.



## IBM iAccess Session

Menu path: **Sessions > IBM iAccess Client > iAccess Sessions > [Session Name]**

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### **Start menu**

The session can be launched from the start menu.

#### **Application Launcher**

The session can be launched with the Application Launcher.

#### **Desktop**

The session can be launched with a program launcher on the desktop.

#### **Quick start panel**

The session can be launched with the quick start panel.

#### **Start menu's system tab**

The session can be launched with the start menu's system tab.

#### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

#### **Desktop context menu**

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

#### **Hotkey**

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. Ctrl L.



Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

## Autostart

The session will be launched automatically when the device boots.

## Restart

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

## Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.



- **Connection**(see page 925)
- **Screen**(see page 927)
- **Preferences**(see page 930)

## Connection

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Connection**

**Destination Address:** Name or IP of the server

**Destination Port:** Server port (Default value: "default")

If you leave **Destination Address** set to the string value "default" (default value) while **Use TLS/SSL** is enabled, port 229 is used. Without **Use TLS/SSL** enabled, port 23 is used. However, you are free to enter a custom port number.

### Use TLS/SSL

- TLS/SSL is used.  
 TLS/SSL is not used. (Standard)

**Server Authentication:** Defines if the client validates the authenticity of the server when connecting.

To perform server authentication, the thin client must have the CA certificate that is associated with the server certificate. For instructions on how to deploy the certificate on the thin client, see [Registering a File on the UMS Server<sup>291</sup>](#) (use **IBM iAccess certificate**) and [Transferring a File to a Device<sup>292</sup>](#).

- The client requires the server to authenticate itself. (Default)  
 The client connects to the server without server authentication.

**Workstation ID:** Name of the client that is presented to the server. This name must be unique. For more information, go to **Help > Information Center** in your iAccess client.

### Screen Size

Possible values:

- 24x80
- 27x132

### Host Code Page

Possible values:

- 1140 United States Euro
- 1141 Germany Euro
- 1141 Austria Euro
- 1142 Denmark Euro
- ...

<sup>291</sup> <https://kb.igel.com/display/endpointmgmt605/Registering+a+file+on+the+UMS+server>

<sup>292</sup> <https://kb.igel.com/display/endpointmgmt605/Transferring+a+file+to+a+device>



### **Enable Unicode Data Stream**

- Unicode Data Stream is enabled.
- Unicode Data Stream is disabled. (Default)

### **Enable DBCS in Unicode Fields**

- DBCS is enabled in unicode fields.
- DBCS is disabled in unicode fields. (Default)

### **Auto-Connect**

- Automatically connect to the server on client startup. (Default)

### **Auto-Reconnect**

- Automatically make a reconnect attempt if the server connection is lost. (Default)

- [Advanced](#)(see page 926)

## Advanced

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Connection > Advanced**

**Connection Timeout (seconds)** (Default: 0)

**Inactivity Timeout (minutes)** (Default: 0)

### **Keep-Alive**

- Keep-Alive is enabled.
- Keep-Alive is disabled. (Default)

### **Enable ENPTUI**

- ENPTUI is enabled. (Default)

### **Password Prompting**

Possible values:

- Use default user name to prompt once for each system: The credentials preconfigured in the fields **User ID** and **Password (optional)** are used.
- Prompt for user name and password every time
- Use Kerberos authentication: The credentials from the Active Directory login are used; only available if the user has logged in to the thin client via Active Directory. For more information, see [Active Directory/Kerberos](#)(see page 1242).

**User ID:** The user ID to be used when **Password Prompting** is set to "Use default user name to prompt once for each system".

**Password (optional):** The password to be used when **Password Prompting** is set to "Use default user name to prompt once for each system".



Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

#### Bypass sign-on:

- The logon to the system is bypassed. (Default)

#### Screen

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Screen**

#### Cursor Shape

Possible Values:

- Underline
  - Block
- 

- [Font](#)(see page 927)
- [Cursor](#)(see page 928)
- [Rule Line](#)(see page 929)
- [Color](#)(see page 929)

#### Font

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Screen > Font**

#### Fixed Font

- Use a fixed font.
- Use no fixed font. (Default)

#### Fixed Font Size

Possible values:

- 8
- 10
- 12
- 14
- ...
- 58

#### Font Scaling

- Font is scaled. (Default)

#### Antialiasing

- Antialiasing is activated.
- Antialiasing is disabled. (Default)



## Font Name

Possible values:

- IBM3270
- Monospaced
- Courier 10 Pitch
- DejaVu Sans Mono
- Liberation Mono
- Lucida Sans Typewriter
- Numbus Mono L
- PComm Session
- Ubuntu Mono

## Font Style

Possible values:

- Plain
- Bold
- Italic

## Cursor

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Screen > Cursor**

### Cursor Shape

Possible values:

- Underline
- Block

### Cursor Pointer

Possible values

- Default
- Crosshair

### Allow blinking cursor

Blinking cursor is allowed.

Blinking cursor is disabled. (Default)

### Show blinking text with

Possible values:

- Blinking Text
- Host Color
- Mapped color

**Blink Color:** Select a color in which the cursor should blink.

**Blink Color Background:** Select a background color.



## Rule Line

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Screen > Rule Line**

### Rule Line

- Rule line is activated.
- Rule line is disabled. (Default)

### Follow Cursor

- The follow cursor effect is enabled.
- The follow cursor effect is disabled. (Default)

### Style

Possible values:

- Crosshair
- Vertical
- Horizontal

## Color

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Screen > Color**

**Field Color:** Choose respective colors.

**OIA Color:** Select a suitable color for the respective indicators.

- Status Indicators
- Information Indicators
- Attention Indicators
- Error Indicators
- OIA Background

### Other

- **Screen Background:** Choose a color.

This color overrides all Field Color Background colors which are set to black.

- **Highlight active field**

- Active field is highlighted.
- Active field is not highlighted. (Default)
- **Active field:** Choose a color
- **Active Field Background:** Choose a color
- **Crosshair Ruler Color:** Choose a color
- **Column Separator:** Choose a color



## Preferences

Menüpfad: **Sessions > IBM iAccess Client > iAccess Sessions > [session name] > Preferences**

### Start window maximized

- The windows starts in maximal size.
- The windows does not start in maximal size. (Default)

### Automatic Resize

- Automatic window resizing is enabled. (Default)
- Automatic window resizing is disabled.

### Show Border

- The session screen is framed by a border.
- No additional border is added. (Default)

### Graphical OIA

- The Graphical OIA (Graphical Operator Information Area) is displayed. (Default)
- The Graphical OIA (Graphical Operator Information Area) is hidden.

### Textual OIA

- The Textual OIA (Textual Operator Information Area) is displayed.
- The Textual OIA (Textual Operator Information Area) is hidden. (Default)

### Keypad

- The Keypad is displayed.
- The Keypad is hidden. (Default)

### Toolbar

- The toolbar is displayed. (Default)
- The toolbar is hidden.

### Toolbar Text

- Textual items are added to the toolbar icons.
- No textual items are added to the toolbar icons. (Default)

### Status Bar

- The status bar is displayed. (Default)
- The status bar is hidden.

### Macro Manager

- The Macro Manager toolbar is displayed.
- The Macro Manager toolbar is hidden. (Default)

### Right Mouse Button Popup Keypad



- Right-clicking will bring up the the Popup Keypad.
- Right-clicking will bring up the default menu. (Default)

### Scratch Pad

- The Scratch Pad (integrated basic text editor) is displayed.
- The Scratch Pad (integrated basic text editor) is hidden. (Default)

### 'Save' in Scratch Pad

- The **Save** button in the Scratch Pad is active.
- The **Save** button in the Scratch Pad is inactive. (Default)

### Quick Connect

- The Quick Connect toolbar is displayed.
- The Quick Connect toolbar is hidden. (Default)

### Search Text

- The Search Text area is displayed.
- The Search Text area is hidden. (Default)

### Screen History

- The Screen History area is displayed.
- The Screen History area is hidden. (Default)

### History Screen Type Simple (Text)

- The History Screen will be displayed black and white.
- The History Screen will have the default terminal (green screen) look and feel. (Default)

### Menu Bar

- The main menu bar is displayed. (Default)
  - The main menu bar is hidden.
- 

- [Window](#)(see page 931)
- [Start Options](#)(see page 932)
- [Language](#)(see page 932)
- [Keyboard](#)(see page 932)
- [Popup Keypad](#)(see page 932)
- [Toolbar](#)(see page 932)

### Window

Menu path: **Sessions > IBM iAccess Client > [session name] > Preferences > Window**

Here you can define how the iAccess client application window is positioned and sized by default on start. If you leave the fields empty, the window will be positioned and sized automatically.

**Width:** Width of the window



**Height:** Height of the window

**Horizontal offset:** Horizontal offset of the window

**Vertical offset:** Vertical offset of the window

## Start Options

Menu path: **Sessions > IBM iAccess Client > iAccess Sessions > [session name] > Preferences > Start Options**

### Session ID

Possible values:

- Automatic
- [Various alphabetic values]

## Language

Menu path: **Sessions > IBM iAccess Client > iAccess Sessions > [session name] > Preferences > Language**

### Emulation Language

Possible values:

- **Default:** The language of the IGEL User Interface (**User Interface > Language**) will be used.
- [Various languages]

## Keyboard

Menu path: **Sessions > IBM iAccess Client > iAccess Sessions > [session name] > Preferences > Keyboard**

**Keyboard Remapping File:** Enter the file name (Default: IBMi.kmp)

The directory /userhome/IBM/iAccessClient/Emulator is used by default.

## Popup Keypad

Menu path: **Sessions > IBM iAccess Client > iAccess Sessions > [session name] > Preferences > Popup Keyboard**

**Popup Keypad File:** Enter the file name.

The directory /userhome/IBM/iAccessClient/Emulator is used by default.

## Toolbar

Menu path: **Sessions > IBM iAccess Client > iAccess Sessions > [session name] > Preferences > Toolbar**

**Toolbar File:** Enter the file name.

The directory /userhome/IBM/iAccessClient/Emulator is used by default.



### 3.8.19 ThinLinc Global

Menu path: **Sessions > ThinLinc > ThinLinc Global**

In this area, you can change the global settings for ThinLinc sessions.

- [Server](#)(see page 933)
- [Window](#)(see page 933)
- [Options](#)(see page 934)
- [Optimization](#)(see page 935)
- [VNC Optimization](#)(see page 935)

#### Server

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > Server**

You can specify the port for communication between the client and server and allow remote monitoring of the client through shadowing.

- **SSH port**  
Possible values:
  - Default SSH (22): Port 22 is used.
  - HTTP (80): Port 80 is used.
  - Custom: Under **Custom port number**, you can enter an alternative port number.
- **Custom port number**: Alternative port number
- **Allow shadowing**
  - The session can be remote monitored by shadowing via VNC.
  - The session cannot be remote monitored by shadowing. (default)

#### Window

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > Window**

In this area, you can define the window settings for ThinLinc sessions.

##### Screen size

Possible values:

- "800x600"
- "1024x768"
- "1280x1024"
- "1600x1200"
- "Current monitor
- "All monitors": The display area of all monitors is used for the ThinLinc session.
- "Work area (maximized)": The display area of the current monitor minus the height of the taskbar is used for the ThinLinc session.
- "Custom size": The display area specified with **Custom screen width** and **Custom screen height** is used for the ThinLinc session.

**Custom screen width:** Width of the display area for the session in pixels.



**Custom screen height:** Height of the display area for the session in pixels.

#### Full-screen mode

The entire display area is used for the ThinLinc session. (Default)

#### Full-screen all monitor

The entire display area of all monitors is used for the ThinLinc session. (Default)

#### Control bar for ThinLinc sessions

If the ThinLinc session takes place in full-screen mode, an in-session control bar will be shown. You can minimize or close the session with the control bar. Further information can be found under [In-Session Control Bar](#)(see page 1154).

The in-session control bar will not be shown. (Default)

## Options

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > Options**

You can change various settings and enable local directories.

#### Enable sound

Audio output will be forwarded from the server to the device. The audio data can then be played back via the built-in loudspeaker or the headset.

Audio output will not be forwarded to the device. (Default)

#### Redirect serial port

The serial port data will be forwarded from the device to the server. The serial port can be used in the ThinLinc session.

The serial port data will not be forwarded to the server. (Default)

#### Enable printer

The local printer can be used in the ThinLinc session. (Default)

The local printer cannot be used in the ThinLinc session.

#### Enable smartcard readers

The server has access to the device's local smartcard reader.

The server does not have access to the local smartcard reader. (Default)

#### Enable drive access

The server has access to local directories. These directories can be selected in the **Exported Paths and Permissions** area.

The server does not have access to local directories. (Default)

## Exported Paths and Permissions

To edit the list, proceed as follows:

- Click on to create a new entry.



- Click on to remove the selected entry.
- Click on to edit the selected entry.
- Click on to copy the selected entry.

To select a local directory for server-side access, proceed as follows:

1. Click on .
2. In the **Path** field, enter the local directory path. Example: /user/home
3. Select the **Permission** that the server is to have for the directory.
  - Read only: The server has read rights for the directory but no write rights.
  - Read/write: The server has read and write rights for the directory.
  - Disabled: The server has no read rights and no write rights for the directory.

If you set a directory to “Disabled”, ensure that it is not a sub-directory of a directory for which the server has read or write rights.

4. Click on **Ok**.

## Optimization

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization**

You can select a suitable compression procedure in order to optimize the transmission speed between the client and server.

- **Enable custom compression level**
  - You can specify how much the data transmitted between the client and server are compressed.
  - The default value will be used for the compression level. (default)
- **Compression level:** Allows you to select the compression level; 9 is the highest compression (default: 8)
- **Enable JPEG compression:** If this option is enabled, graphical data will be compressed using the JPEG procedure.

A higher JPEG compression level saves bandwidth but reduces the image quality.

- Graphical data will be compressed in accordance with the JPEG procedure. (default)
- **JPEG quality:** Allows you to select the image quality. 1 means the highest compression and the lowest image quality, 9 means the lowest compression and the highest image quality. (default: 7)
- **SSH compression**
  - The data will be compressed using SSH compression.
  - The data will not be compressed using SSH compression. (default)

## VNC Optimization

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > VNC Optimization**

You can change VNC protocol settings in order to optimize transmission.



### VNC autoselect

The preferred coding and color depth will be specified automatically. (Default)

The **Preferred coding** and **Color depth** can be specified by the user.

**Preferred encoding:** Specifies how the data to be transmitted are to be coded. The coding is negotiated between the client and server.

Possible values:

- "Tight
- "ZRLE": Compatible with RealVNC.
- "Hextile": Recommended for fast networks.
- "Raw": No compression.

**Color depth:** Allows you to select the color resolution.

Possible values:

- "Full (all colors)
- "Medium (256 colors)"
- "Low (64 colors)"
- "Very low (8 colors)"

## 3.8.20 ThinLinc Session

Menu path: **Sessions > ThinLinc > ThinLinc Sessions > [Session Name]**

► Click on **Add** to create a ThinLinc session.

In this area, you can configure desktop integration for the ThinLinc session.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

The session can be launched from the start menu.

#### Application Launcher

The session can be launched with the Application Launcher.

#### Desktop

The session can be launched with a program launcher on the desktop.

#### Quick start panel

The session can be launched with the quick start panel.

#### Start menu's system tab



- The session can be launched with the start menu's system tab.

#### **Application Launcher's system tab**

- The session can be launched with the Application Launcher's system tab.

#### **Desktop context menu**

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### **Hotkey**

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L



**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

### Autostart

The session will be launched automatically when the device boots.

### Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

### Autostart requires network

- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.

- [Server](#)(see page 938)
- [Login](#)(see page 939)
- [Window](#)(see page 940)
- [Options](#)(see page 941)
- [Optimization](#)(see page 942)
- [VNC Optimization](#)(see page 942)
- [User Interface](#)(see page 943)
- [Desktop Integration](#)(see page 944)

## Server

Menu path: **Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Server**

**Server:** Name or IP address of the ThinLinc server

**User:** User name for the connection to the ThinLinc server

**Password:** Password for the connection to the ThinLinc server

Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.



### Use global SSH port settings

The port set under **Sessions > ThinLinc > ThinLinc Global > Server** will be used. (Default)

The port set in **SSH port** or **Custom port number** will be used.

#### SSH port

Possible values:

- **Default SSH (22)**: Port 22 is used.
- **HTTP (80)**: Port 80 is used.
- **Custom**: Under **Custom port number**, you can enter an alternative port number.

**Custom port number**: Alternative port number

## Login

Menu path: **Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Login**

**Method of authentication**: A method used for the authentication.

Possible values:

- **"Password"**
- **"Public key"**
- **"Smartcard"**
- **"Kerberos"**

**User**: The user credentials are taken from **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Server > User**.

**Password**: A password specified under **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Server > Password** is used for the authentication. (Available if **Password** is selected as **Method of authentication**).

If modified here (under **Login**), **User** and **Password** will automatically be changed under **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Server**.

The following settings can be configured if **Smartcard** is used as a **Method of authentication**.

Smartcard only

#### Use certificate subject as name for login

The certificate subject will be used as login name. (Default)

The user credentials from **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Server > User** will be used as login name.

#### Connect the client automatically if a smartcard is found

The client will be connected automatically if a smartcard is detected (available if **Use subject of smartcard as name for login** is enabled). (Default)

The client will not be connected automatically by the smartcard detection.

#### Disconnect the client automatically when the smartcard is removed



- The client will be disconnected automatically if the smartcard is removed. (Default)  
 The client will not be disconnected at the smartcard removal.

#### Allow transmission of the smartcard's passphrase for logging in

- The transmission of the smartcard's passphrase for logging in is allowed.  
 The transmission of the smartcard's passphrase for logging in is not allowed. (Default)

The transmission of the smartcard's passphrase is not recommended by Cendio.

**Smartcard filter:** The smartcard filter must be specified in the format described under "SMARTCARD\_FILTER\_n" in <https://www.cendio.com/resources/docs/tag/clientconf.html>.

## Window

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Window**

In this area, you can define the window settings for the specific ThinLinc session.

You can enable the in-session control bar for ThinLinc sessions only in the global settings, see [Window\(see page 933\)](#).

#### Use global screen settings

- The settings under **Setup > Sessions > ThinLinc > ThinLinc Global > Window** will be used. (Default)  
 The settings for this session are defined here.

#### Screen size

Possible values:

- "800x600"
- "1024x768"
- "1280x1024"
- "1600x1200"
- "Current monitor
- "All monitors": The display area of all monitors is used for the ThinLinc session.
- "Work area (maximized)": The display area of the current monitor minus the height of the taskbar is used for the ThinLinc session.
- "Custom size": The display area specified with **Custom screen width** and **Custom screen height** is used for the ThinLinc session.

**Custom screen width:** Width of the display area for the session in pixels.

**Custom screen height:** Height of the display area for the session in pixels.

#### Full-screen mode

- The entire display area is used for the ThinLinc session. (Default)

#### Full-screen all monitor



- The entire display area of all monitors is used for the ThinLinc session. (Default)

## Options

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Options**

You can change various settings and enable local directories.

### Use global shadowing settings

- The option **Setup > Sessions > ThinLinc > ThinLinc Global > Server > Enable Shadowing** will be used.
- The global setting **Enable shadowing** will not be used for this session.

### Enable shadowing

- The session can be monitored remotely by shadowing via VNC.
- The session cannot be remotely monitored by shadowing. (Default)

### Use global resource settings

- The settings under **Setup > Sessions > ThinLinc > ThinLinc Global > Options** will be used. (Default)
- The settings for this session are defined here.

### Enable sound

- Audio output will be forwarded from the server to the device. The audio data can then be played back via the built-in loudspeaker or the headset.
- Audio output will not be forwarded to the device. (Default)

### Enable serial port

- The serial port data will be forwarded from the device to the server. The serial port can be used in the ThinLinc session.
- The serial port data will not be forwarded to the server. (Default)

### Enable printer

- The local printer can be used in the ThinLinc session. (Default)
- The local printer cannot be used in the ThinLinc session.

### Enable smartcard readers

- The server has access to the device's local smartcard reader.
- The server does not have access to the local smartcard reader. (Default)

### Enable drive access

- The server has access to local directories. These directories can be selected in the **Exported Paths and Permissions** area.
- The server does not have access to local directories. (Default)

**Options popup key:** Key to be used for opening the options menu during the session. (Default: F8)



## Optimization

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Optimization**

You can select a suitable compression procedure in order to optimize the transmission speed between the client and server.

- **Use global compression level**

The global settings under **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization > Use custom compression level** option and **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization > Compression level** selection will be used. (default)

The specific settings for this session will be used.

- **Enable custom compression level**

You can specify how much the data transmitted between the client and server are compressed.

The default value will be used for the compression level. (default)

- **Compression level:** Allows you to select the compression level; 9 is the highest compression (default: 8)

- **Use global JPEG quality settings**

The global settings under **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization > Use JPEG compression** option and **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization > JPEG Quality** selection will be used. (default)

The specific settings for this session are defined here.

- **Enable JPEG compression**

A higher JPEG compression level saves bandwidth but reduces the image quality.

Graphical data will be compressed in accordance with the JPEG procedure. (default)

- **JPEG quality:** Allows you to select the image quality. 1 means the highest compression and the lowest image quality, 9 means the lowest compression and the highest image quality. (default: 7)

- **Use global SSH connection settings**

The global settings under **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization > SSH Compression** option will be used. (default)

The specific setting for this session will be used.

- **SSH compression**

The data will be compressed using SSH compression.

The data will not be compressed using SSH compression. (default)

## VNC Optimization

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > VNC Optimization**

You can change VNC protocol settings in order to optimize transmission.

### Use global VNC settings

The global settings under **Setup > Sessions > ThinLinc > ThinLinc Global > VNC optimization** will be used. (Default)

The specific settings for this session are defined here.



### VNC auto select

The **Preferred encoding** and **Color level** will be specified automatically. (Default)

The **Preferred encoding** and **Color level** can be specified by the user.

**Preferred encoding:** Specifies how the data to be transmitted are to be coded. The coding is negotiated between the client and server.

Possible values:

- "Tight
- "ZRLE": Compatible with RealVNC.
- "Hextile": Recommended for fast networks.
- "Raw": No compression.

**Color level:** Allows you to select the color resolution.

Possible values:

- "Full (all colors)
- "Medium (256 colors)"
- "Low (64 colors)"
- "Very low (8 colors)"

## User Interface

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > User Interface**

You can change the fields and settings options of the logon window as well as the **ThinLinc Client Options** dialog.

### • Lock server name

The server name given under **Setup > Sessions > ThinLinc Sessions > Server** will be used and it will not be possible to change it in the logon window. (default)

### • Hide options button

The **Options** button will not appear in the logon window. The **ThinLinc Client Options** dialog therefore cannot be opened. (default)

### • Advanced mode

The fields that can be opened under **Advanced** will appear when starting the session.  
 The fields that can be opened under **Advanced** will not appear when starting the session. (default)

### • Lock ThinLinc options tab

The settings in the **Options** tab of the **ThinLinc Client Options** dialog cannot be changed. (default)

### • Lock Local Devices options tab

The settings in the **Local Devices** tab of the **ThinLinc Client Options** dialog cannot be changed. (default)

### • Lock ThinLinc Screen tab

The settings in the **Screen** tab of the **ThinLinc Client Options** dialog cannot be changed. (default)

### • Lock ThinLinc Optimization tab

The settings in the **Optimization** tab of the **ThinLinc Client Options** dialog cannot be changed. (default)



- **Lock Security tab**  
 The settings in the **Security** tab of the **ThinLinc Client Options** dialog cannot be changed.  
 (default)
- **Debug level:** Specifies how detailed the debugging information is to be. 1 is the lowest level  
 (default), 5 is the highest.

## Desktop Integration

Menu path: **Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the ThinLinc session.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

The session can be launched from the start menu.

#### Application Launcher

The session can be launched with the Application Launcher.

#### Desktop

The session can be launched with a program launcher on the desktop.

#### Quick start panel

The session can be launched with the quick start panel.

#### Start menu's system tab

The session can be launched with the start menu's system tab.

#### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

#### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.



**Password protection:** Specifies which password will be requested when launching the session.  
Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- = Alt

Key combinations are formed as follows with |:

- + = Ctrl | Super\_L

#### Key: Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

#### Autostart

The session will be launched automatically when the device boots.

#### Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.



**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

- For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.
- No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

#### Autostart requires network

- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.

### 3.8.21 SSH Session

Menu path: **Sessions > SSH > [Session Name]**

You can launch applications on a remote computer via SSH (Secure Shell). The display is usually on the terminal; X11 connections too can be routed via SSH.

- Click on **Add** to create an SSH session.

In the following area, you can configure desktop integration for the SSH session.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Starting Methods for Session

##### Start menu

- The session can be launched from the start menu.

##### Application Launcher

- The session can be launched with the Application Launcher.

##### Desktop

- The session can be launched with a program launcher on the desktop.

##### Quick start panel

- The session can be launched with the quick start panel.

##### Start menu's system tab

- The session can be launched with the start menu's system tab.

##### Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

##### Desktop context menu



- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey



To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

## Autostart

- The session will be launched automatically when the device boots.

## Restart

- The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

## Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode\(see page 869\)](#).

- The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

- 
- [Command\(see page 948\)](#)
  - [Options\(see page 949\)](#)
  - [Desktop Integration\(see page 949\)](#)

## Command

Menu path: **Sessions > SSH > [Session Name] > Command**

**Remote user name:** User name under which the application runs on the remote computer If you do not give a name, you will be asked when the session starts.



**Remote host:** Host name or IP address of the remote computer.

**Command line:** Command which is to be executed on the remote computer immediately after logging in.

## Options

Menu path: **Sessions > SSH > [Session Name] > Options**

As of IGEL OS 11.04.100, SSHv1 is no longer supported. Migrate to SSHv2 if you have not yet done so.

Here, you can change the following settings:

### Enable X11 connection forwarding

X11 applications on the remote computer that are launched via the SSH session will be shown on your device. (Default)

No X11 programs can be launched on the remote computer via the SSH session.

### Enable compression

The data will be compressed for transmission.

**Port:** SSH port. (Default: 22)

## Desktop Integration

Menu path: **Sessions > SSH > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the SSH session.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.



### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey



To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

### **Autostart**

- The session will be launched automatically when the device boots.

### **Restart**

- The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

### **Autostart requires network**

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode\(see page 869\)](#).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

## 3.8.22 VNC Viewer Sessions

Menu path: **Sessions > VNC Viewer > VNC Viewer Sessions > [Session Name]**

With the VNC viewer, you can access the graphical user interface of a remote computer.

- Click on to create a VNC viewer session.

The settings for starting the session are described below.

**Session name:** Name for the session.



The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. Ctrl.



Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

### Autostart

The session will be launched automatically when the device boots.

### Restart

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

### Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.



- [Connection](#)(see page 954)
- [Compression](#)(see page 954)
- [Input](#)(see page 954)
- [Misc](#)(see page 955)
- [Desktop Integration](#)(see page 955)

## Connection

Menu path: **Setup > Sessions > VNC Viewer > VNC Viewer Sessions > [Session Name] > Connection**

- **Name or IP address of VNC server:** Host name or IP address of the VNC server
- **Password:** User password for logging on to the VNC server, if necessary

Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

## Compression

Menu path: **Setup > Sessions > VNC Viewer > VNC Viewer Sessions > [Session Name] > Compression**

- **Compression level (default = 2):** Allows you to select the compression level; 9 is the highest compression (default: 2)
- **JPEG quality level:** Allows you to select the image quality. 1 means the highest compression and the lowest image quality, 9 means the lowest compression and the highest image quality. (default: 8)

## Input

Menu path: **Setup > Sessions > VNC Viewer > VNC Viewer Sessions > [Session Name] > Input**

Here, you can change the settings for keyboard input for the VNC session.

- **View only**
  - Mouse and keyboard inputs are not forwarded to the remote computer. You can only observe the remote computer.
  - Mouse and keyboard inputs are forwarded to the remote computer. You can remote control the remote computer. (default)
- **Pass system keys directly to the server (full-screen)**
  - You can use system key combinations in the VNC session, e.g. [Alt] + [Tab]. (default)
  - System key combinations cannot be used in the VNC session.
- **Menu key:** Key which brings up the menu.  
Possible options (default: F8):
  - [F2] ... [F12]
  - [Pause]
  - [Print]
  - [Scroll lock]
  - [Esc]



- [Ins]
- [Del]
- [Home]
- [Page up] ▲
- [Page down] ▼

## Misc

Menu path: **Setup > Sessions > VNC Viewer > VNC Viewer Sessions > [Session Name] > Misc**

- **Shared mode**

- When starting a session, other users' sessions with the same server are not terminated. The sessions run alongside each other with equal status.
- If another user has a VNC session with the same server, the other user's session will be terminated when the session is started. (default)

- **Fullscreen mode**

- The session will be shown in full-screen mode. The taskbar is not visible.
- The taskbar is visible. (default)

- **Color level:** Number of possible colors

Possible values:

- Default: The highest available color depth will be used.
- Very low (8 colors)
- Low (64 colors)
- Medium (256 colors)

## Desktop Integration

Menu path: **Sessions > VNC Viewer > VNC Viewer Sessions > [Session Name] > Desktop Integration**

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

- The session can be launched from the start menu.

#### Application Launcher

- The session can be launched with the Application Launcher.

#### Desktop

- The session can be launched with a program launcher on the desktop.

#### Quick start panel

- The session can be launched with the quick start panel.



### **Start menu's system tab**

The session can be launched with the start menu's system tab.

### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

### **Desktop context menu**

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### **Hotkey**

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
- [Ctrl] = Ctrl
-  = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:



- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

The session will be launched automatically when the device boots.

#### Restart

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

#### Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

### 3.8.23 Firefox Browser Global

Menu path: **Sessions > Firefox Browser > Firefox Browser Global**

In this area, you can define the start page, display resolution, and font size for the browser.

You can change the following settings:

**When browser starts:** Specifies what pages are shown when the browser is launched.

- Start with a blank page
- Show my start page (default)
- Resume previous session: All tabs from the last session are reopened.

**Start page:** Specifies the URL of the start page. You can specify the number of start pages by separating the URLs of the start pages with a vertical dash "|".

**Default web browser:** Defines which browser will be chosen by the system, e.g. for opening Citrix Storefront.

Possible options:

- "Firefox Browser"
- "Chromium Browser"



**Display resolution:** Specifies the display resolution for the browser in DPI. Typical values are **72** for medium screens and **96** for large screens.

Possible values:

- [System setting](#)
- [\(Various discreet values\)](#)

**Minimum font size:** Specifies the minimum size of the fonts displayed on websites. The formats of the websites are overwritten in the process.

Possible values:

- None: The fonts can be as small as you like. (default)
- [\(Various discreet values\)](#)

### Show browser splash screen

While the browser is starting, a Firefox logo will be shown in the middle of the screen. (default)

No Firefox logo will be shown.

For information on the kiosk mode, see [Use the Firefox Browser in Kiosk Mode](#)(see page 358).

- [Tabs](#)(see page 958)
- [Content](#)(see page 959)
- [Print](#)(see page 960)
- [Proxy](#)(see page 961)
- [Privacy](#)(see page 963)
- [Security](#)(see page 965)
- [Advanced](#)(see page 965)
- [Encryption](#)(see page 968)
- [Certificates](#)(see page 968)
- [Smartcard Middleware](#)(see page 969)
- [Restart](#)(see page 970)
- [Window](#)(see page 970)
- [Menus & Toolbars](#)(see page 971)
- [Hotkeys](#)(see page 974)
- [Context](#)(see page 975)
- [Commands](#)(see page 976)

## Tabs

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Tabs**

In this area, you can define settings for the browser tabs.

**New pages should be opened in:** Specifies how links to new pages are to be opened.

Possible values:

- Current window: The page will open in the current window, even if the link defines a new window as the target.



- New window: If the link does not define a target, the page will open in the current window. If the link defines a new window as the target, the page will open in a new window. (default)
- New tab: If the link does not define a target, the page will open in the current window. If the link defines a new window as the target, the page will open in a new tab.

#### **Warn me when closing multiple tabs**

- A warning will be shown as soon as you attempt to close a browser window with a number of tabs.
- No warning will be shown if you close a number of browser windows. (default)

#### **Warn me when opening multiple tabs might slow down the browser**

- A warning will be shown if a very large number of tabs are loaded simultaneously. (default)
- No warning will be shown if a very large number of tabs are loaded simultaneously.

#### **When a link is opened in a new tab, switch to it immediately**

- When a new tab is opened via a link, the focus will switch to the new tab.
- When a new tab is opened via a link, the focus will not change. (default)

## Content

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Content**

In this area, you can change settings regarding popups, JavaScript, downloads and the browser display.

#### **Block pop-up windows**

- The automatic opening of popup windows by websites will be blocked. With **Exceptions...**, you can allow popups to be opened automatically for specific websites.
- The automatic opening of popup windows will not be blocked. (default)

To add an exception for the automatic opening of popups, proceed as follows:

1. Click on **Exceptions....**
2. Click on **[+]**.
3. In the **Website** field, give the URL of the website for which the exception is to apply.
4. Click on **Ok**.

#### **Load images automatically**

- Websites will be loaded fully including all images. (default)
- Images in websites will not be loaded; placeholders will be shown instead of the images. As a result of this, websites can be loaded more quickly, but the layout is impaired. With **Exceptions...** you can allow or prevent automatic loading for specific websites.

To add an exception for the automatic loading of images, proceed as follows:

1. Click on **Exceptions....**
2. Click on **[+]**.
3. In the **Website** field, give the URL of the website for which the exception is to apply.
4. Using the **Status** drop-down menu, specify whether the automatic loading of images is to be allowed or prevented for the given website.



## 5. Click on **Ok**.

**Type of download directory:** Specifies the directory in which a downloaded file is saved.

- User directory: The file is saved locally on the thin client desktop.
- Custom path: You can specify whether the downloaded file is to be opened with an application or saved locally. (default)

**Download path:** Local directory in which the downloaded file is saved if **Type of download directory** is set to **Custom path**. (default: /tmp)

### Enable JavaScript

- JavaScript code will be executed on websites. (default)  
 JavaScript code will not be executed.

### Raise or lower windows

- A website can place windows in the background or foreground via JavaScript. (default)  
 Websites cannot place windows in the background or foreground via JavaScript.

### Move or resize existing windows

- A website can move windows or change the window size via JavaScript.  
 Websites cannot move windows or change the window size via JavaScript. (default)

### Disable or replace context menus

- A website can define a custom context menu via JavaScript; the browser's own context menu will be suppressed in the process.  
 Websites cannot define a custom context menu.

**Languages for web pages:** One or more preferred languages for multilingual websites, given in the form of language abbreviations separated by commas. The languages should be given in the order of preference. Example: With de, en, fr, it, the website will be shown in German, if available, otherwise in English, etc.

## Print

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Print**

In this area, you can set the default paper size for the printer.

### Use system settings for default paper size

- The globally set paper size will be used when printing websites. (Default)  
 You can set the paper size via **Default paper size**.

**Default paper size:** Preset paper size when printing websites.

Possible values:

- Letter
- Legal
- Executive
- A5
- A4



- A3

## Proxy

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Proxy**

In this area, you can change the proxy configuration.

To change the proxy configuration, proceed as follows:

1. In the **Proxy Configuration** pull-down menu, select the type of proxy configuration.  
The following proxy configurations are available:
  - Direct connection to the Internet
  - Manual proxy configuration
  - Automatic proxy configuration
  - System-wide proxy configuration
  - Auto-detect proxy settings for this network
2. Enter the necessary configuration data for the selected proxy configuration.

### Direct Connection to the Internet

With this proxy configuration, no proxy is used.

### Manual Proxy Configuration

The configuration data must be specified in the following fields.

**FTP proxy:** URL of the proxy for FTP

**Port:** Port of the proxy for FTP

**HTTP proxy:** URL of the proxy for HTTP

**Port:** Port of the proxy for HTTP

**SSL proxy:** URL of the proxy for SSL

**Port:** Port of the proxy for SSL

**SOCKS host:** URL of the proxy for SOCKS

**Port:** Port of the proxy for SOCKS

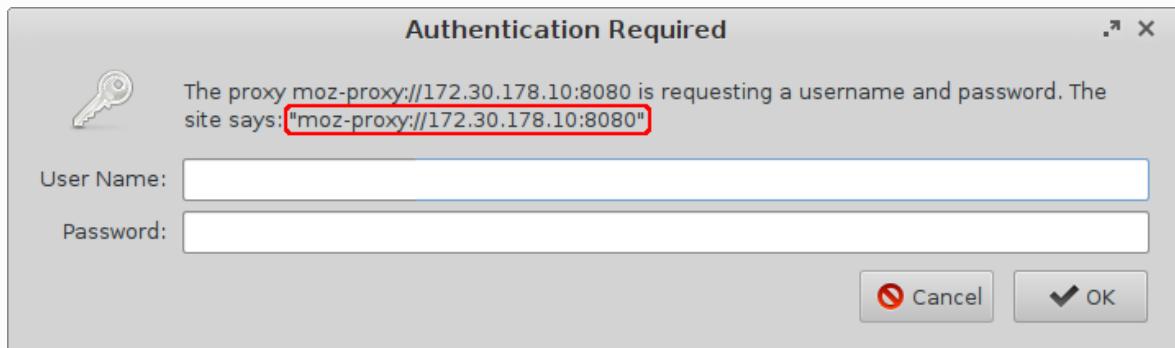
**SOCKS protocol version:** Version of the SOCKS protocol used (default: SOCKS v5)

**No proxy for:** List of URLs for which no proxy is to be used (default: localhost, 127.0.0.1)

**Proxy realm:** Area in which the browser authenticates itself for the proxy. Together with the user name and password, this information is necessary for authentication.



The **Proxy realm** field is internally pre-populated with the value `moz-proxy:// [HTTP Proxy] : [Port]`. If the field is empty, this value will be used when authenticating the browser. If the proxy expects another unknown value for the proxy realm, you can determine this as follows: Leave the **User name** and **Password** fields empty and launch the browser. The dialog window which appears will contain the correct value for the **Proxy realm** field:



In the example above, the value for the **Proxy realm** field is as follows: `moz-proxy:// 172.30.178.10:8080`

#### **Use passthrough authentication:** This option can be used if the local thin client logon takes place via Kerberos.

The logon information saved temporarily when logging on to the thin client will be carried over when logging on to the proxy.

**User name:** User name with which the browser authenticates itself for the proxy.

**Password:** Password with which the browser authenticates itself for the proxy.

#### **Do not prompt for proxy authentication if credentials are saved**

If logon data are already saved in the browser, the user will not be asked for a user name and password. (default)

This option should not be enabled in multiuser environments. If this option is enabled in a multiuser environment, a user can use the logon data of a previous user.

#### Automatic Proxy Configuration

With this proxy configuration, the PAC file (Proxy Auto Config) available under **URL** will be used.

**URL:** URL of the proxy configuration file

#### **Do not prompt for proxy authentication if credentials are saved**

If logon data are already saved in the browser, the user will not be asked for a user name and password. (default)

This option should not be enabled in multiuser environments. If this option is enabled in a multiuser environment, a user can use the logon data of a previous user.



## System-Wide Proxy Configuration

With this proxy configuration, the proxy configured under **Setup > Network > Proxy** will be used.

### **Do not prompt for proxy authentication if credentials are saved**

- If logon data are already saved in the browser, the user will not be asked for a user name and password. (default)

This option should not be enabled in multiuser environments. If this option is enabled in a multiuser environment, a user can use the logon data of a previous user.

## Auto-Detect Proxy Settings for This Network

With this proxy configuration, WPAD (Web Proxy Autodiscovery Protocol) will be used. The browser will determine the URL of the WPAD file wpad.dat automatically with the help of DNS.

### **Do not prompt for proxy authentication if credentials are saved**

- If logon data are already saved in the browser, the user will not be asked for a user name and password. (default)

This option should not be enabled in multiuser environments. If this option is enabled in a multiuser environment, a user can use the logon data of a previous user.

## Privacy

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Privacy**

In this area, you can configure settings relevant to data protection.

**Save browsing history (in days):** Specifies how long your browsing history will be stored. If you select **Do not store history**, all browsing history data will be lost when the browser restarts. (default: 9)

All browsing history data stored before the period specified here will be lost.

### **Save information entered in forms and the search bar**

- Entries in forms and search bars will be retained after the browser restarts.  
 Entries in forms and search bars will be retained only for the duration of the session. (default)

### **Remember passwords**

- Passwords entered will be retained after the browser restarts.  
 Passwords entered will be retained only for the duration of the session. (default)

### **Clear private data when closing browser**

- Data entered will be deleted when the browser is closed. What data are deleted is specified in the following options.  
 Data entered will not be deleted when the browser is closed. (default)



## Select the Items to Be Cleared

The options in this area are effective if **Clear private data when closing browser** is enabled.

### Browsing & download history

Addresses (URLs) of visited websites and the list of downloads will be deleted when the browser is closed. (default)

### Form & search history

Entries in the search window and in website forms will be deleted when the browser is closed. (default)

### Saved passwords

Passwords entered will be deleted when the browser is closed.

Passwords entered will be retained after the browser restarts. (default)

### Cookies

Cookies will be deleted when the browser is closed. (default)

### Cache

The cache for temporarily saving websites will be emptied when the browser is closed. (default)

### Active logins

Ongoing sessions on websites will be terminated when the browser is closed and will need to be restarted after the browser restarts. (default)

Ongoing sessions on websites will be retained after the browser restarts.

### Allow private browsing feature

You can open one or more private windows in the browser. All data from private windows will be deleted after the browser is closed.

Private windows cannot be opened. (default)

### Always start in private browsing mode

The browser will start in private mode. All data will be deleted after the browser is closed.

The browser will start in default mode. (default)

### Enable "Do Not Track" feature

The browser will inform the website you are visiting that you do not wish to be tracked, i.e. you do not want your surfing history to be recorded. (default)

The browser will use the DNT ("Do Not Track") field in the HTTP header for this purpose. Observing this setting is voluntary; from a technical point of view, websites can still record the surfing history even when DNT is set to 1.

### Enable built-in tracking protection

The browser will block specific domains and websites that use tracking. The browser has an internal list for selecting the domains and websites to be blocked. (default)



If tracking protection is enabled, a shield symbol will be shown at the left-hand edge of the address bar.

#### Suggest visited sites in URL bar

Suggestions will be shown while an address is being typed in the address bar. The suggestions will be based on previously visited websites which are stored in the history. (default)

#### Suggest only typed visited sites

The suggestions will be based only on the websites that were typed directly into the address bar. Websites that were visited via bookmarks or links in other websites will not be used for the suggestions.

Websites that were visited via bookmarks or links in other websites will also be used for the suggestions. (default)

#### Suggest bookmarked sites in URL bar

Suggestions will be shown while an address is being typed in the address bar. The suggestions will be based on bookmarks. (default)

#### Suggest open tabs in URL bar

Suggestions will be shown while an address is being typed in the address bar. The suggestions will be based on previously opened tabs. (default)

## Security

### Menu path: Sessions > Firefox Browser > Firefox Browser Global > Security

In this area, you can define settings for preventing phishing and malware.

#### Safe browsing

The browser will check each address entered as to whether it can be found in the black list of fraudulent websites which use phishing. If this is the case, you will be given a warning.

The browser will not check whether an address is on the black list of fraudulent websites.

#### Malware protection

The browser will check before a file is downloaded whether the relevant website can be found in the black list of fraudulent websites which provide malware for downloading. If this is the case, you will be given a warning.

The browser will not check whether an address is on the black list of fraudulent websites which provide malware for downloading.

#### Hide local filesystem

The local file system will not be shown in the dialogs for saving data. The user cannot change the location for saving files.

The local file system will be shown in the dialogs for saving data.

## Advanced

### Menu path: Sessions > Firefox Browser > Firefox Browser Global > Advanced

In this area, you can change various settings as well as add or change custom configuration parameters.

You can change the following settings:



### Use old search bar

- The logo of the search engine currently set will be shown in the search window.
- The search engine currently set will not be shown in the search window, and search suggestions will be shown in the drop-down menu. (default)

### Caret browsing on browser start

- Caret browsing is enabled when the browser starts. If caret browsing is enabled, you can navigate with the keyboard in websites without using the mouse. With the insertion mark, you can copy text to the clipboard.

You can enable or disable caret browsing at any time by pressing [F7]. To prevent caret browsing being disabled, you will also need to enable the **Sessions > Firefox Browser > Firefox Browser Global > Hotkeys > Disable hotkeys for caret browsing** option.

- Caret browsing is not enabled when the browser starts. (default)

### Find as you type

- Search suggestions that match the characters typed will be shown while you type.
- No search suggestions will be shown while you type. (default)

### Warn me when websites try to redirect or reload the page

- A message window will be shown as soon as a website tries to get the browser to load another website or reload the current page.
- No message window will be shown if a website tries to load another website or reload the current page. (default)

### Check my spelling as I type

Possible options:

- "Off": Your spelling will not be checked while you type.
- "On for text fields": Your spelling will be checked if you are typing in text fields with multiple lines. (default)
- "On for text fields and lines": Your spelling will be checked if you are typing in text fields with one line or multiple lines.

### Use autoscrolling

- You can launch automatic page scrolling by clicking on the middle mouse button to place a scroll symbol in the text and then positioning the mouse pointer above or below the anchor.
- Autoscrolling is disabled. (default)

### Use smooth scrolling

- You can browse through a page using the [Page Up/Down] keys smoothly as with scrolling.
- When you press the [Page Up/Down] keys, the display will jump immediately. (default)

### Disable GStreamer in Browser

- GStreamer will not be used to play back videos. This may be a good idea if you experience problems when playing back videos.



We recommend that you disable this option if there is no multimedia codec pack installed on your thin client and you wish to view videos on HTML5 websites.

GStreamer will be used to play back videos.

#### Disable OpenGL acceleration

Hardware acceleration with OpenGL will not be used. This may be a good idea if you experience problems with OpenGL applications.

To add a custom preference, proceed as follows:

Changes to the advanced Firefox browser settings can impair its stability, security and speed. IGEL Support is not responsible for problems caused by changing the browser configuration, even if the browser configuration was changed in the IGEL setup.

Custom preferences can also be changed in the browser via about:config. To do this, the **Firefox Browser > Firefox Browser Global > Window > Hide configuration page of the browser** option must be disabled.

#### Custom Preferences

In this area, you can add custom preferences.

► Click  to get to the **Add** dialogue.

In the **Add** dialogue, you can define the following settings:

**Active:** Defines whether the preference is active.

The preference is active. (Default)

The preference is not active.

**Mode:** The mode of the preference.

Possible values:

- "pref
- "defaultPref": You can change the value in the browser via about:config. When the browser restarts, this change will remain.
- "lockPref": You cannot change the value in the browser via about:config.
- "clearPref": You cannot change the value in the browser via about:config and the value will not be shown via about:config.

**Custom preference:** The name of the custom preference. Example: ui.textSelectBackground

**Type:** The type of the custom preference.

Possible values:

- "String": The value is a string of characters.
- "Integer": The value is a whole number.
- "Boolean



**Value:** The value of the custom preference. The possible entries depend on the **Type** selected.

- ▶ Click **Ok** to add the custom preference.

The custom preference will take effect the next time that the browser is launched.

You will find information regarding custom preferences in Firefox in the MozillaZine Knowledge Base under [Firefox About:config entries](#)<sup>293</sup>.

## Encryption

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Encryption**

In this area, you can define the settings for encryption methods.

**Minimum required encryption protocol:** This protocol will be used to establish a secure connection if no higher protocol is available. Higher protocols are preferred.

Possible options:

- SSL3
- TLS 1.0
- TLS 1.1
- TLS 1.2

**Maximum supported encryption protocol:** This protocol is requested when negotiating the connection. If this protocol is not available, the next lowest protocol will be requested.

Possible options:

- SSL3
- TLS 1.0
- TLS 1.1
- TLS 1.2

## Certificates

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Certificates**

In this area, you can define the settings for certificate validation.

**When a website requests a certificate:** Specifies how the browser behaves if a website requests a security certificate.

Possible values:

- Select one automatically: The browser selects a certificate automatically. (default)
- Ask me every time: A dialog window requesting the certificate will be displayed.

**View certificates:** If you click on this button, the certificates saved in the browser's **Certificate Manager** will be displayed.

**Certificate validation:** Specifies the validation of certificates using OCSP (Online Certificate Status Protocol).

- Do not use OCSP for certificate validation: The certificate will not be validated using OCSP.

---

<sup>293</sup> [http://kb.mozilla.org/About:config\\_entries](http://kb.mozilla.org/About:config_entries)



- **Validate a certificate if it specifies an OCSP server:** The certificate will be validated with the OCSP server specified in the certificate. If no OCSP server is specified, no certificate validation will take place. (default)
- Validate all certificates with the following OCSP server: All certificates will be validated with the OCSP server specified under the **Service URL**, irrespective of which OCSP server is specified in the certificate.

**Response signer:** Signer of the response from the OCSP server

**Service URL:** URL of the OCSP server

**When an OCSP server connection fails, treat the certificate as invalid:**

- If, owing to a failed connection to the OCSP server, no validation can take place, the certificate will be treated as invalid. In this case, the browser will show the “This connection is not trusted” error message.
- The certificate will not be deemed invalid if no check can take place because there is no connection to the OSCP server. (default)

## Smartcard Middleware

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Smartcard Middleware**

In this area, you can activate or deactivate smartcard middleware that is to be used for encryption.

### Gemalto SafeNet security device

- Gemalto/SafeNet eToken will be used for encryption.
- Gemalto/SafeNet eToken will not be used for encryption. (Default)

### cryptovision sc/interface security device

- cryptovision sc/interface will be used for encryption.
- cryptovision sc/interface will not be used for encryption. (Default)

### Gemalto IDPrime security device

- Gemalto IDPrime will be used for encryption. Enable this Gemalto middleware when you want to operate Gemalto Common Criteria devices in unlinked mode.
- Gemalto IDPrime will not be used for encryption. (Default)

### Athena IDProtect security device

- Athena IDProtect will be used for encryption.
- Athena IDProtect will not be used for encryption. (Default)

### A.E.T. SafeSign security device

- A.E.T. SafeSign will be used for encryption.
- A.E.T. SafeSign will not be used for encryption. (Default)

### SecMaker Net iD security device

- SecMaker Net iD will be used for encryption.
- SecMaker Net iD will not be used for encryption. (Default)

### Coolkey security device



- Coolkey will be used for encryption.  
 Coolkey will not be used for encryption. (Default)

#### OpenSC security device

- OpenSC will be used for encryption.  
 OpenSC will not be used for encryption. (Default)

#### 90meter security device

##### Licensed Feature

This feature requires an add-on license; see [Add-On Licenses](#)<sup>294</sup>. Please contact your IGEL sales representative.

- 90meter will be used for encryption.  
 90meter will not be used for encryption. (Default)

## Restart

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Restart**

In this area, you can specify whether the browser automatically starts and whether it is automatically restarted after being closed and after what delay time.

#### Restart

- The browser automatically restarts if it was closed.  
 The browser does not automatically restart if it was closed. (default)

#### Restart after idle time

- If no action on the part of the user has occurred after the idle time has elapsed, the browser will automatically be restarted.  
 There will be no automatic restart after a specific idle time has elapsed. (default)

**Idle time after which a restart occurs:** Time interval after which the browser is automatically restarted if in the meantime no action on the part of the user has occurred. (default: 5)

The time unit can be selected under **Unit**.

**Unit:** Time interval for the idling time

Possible options:

- Minutes
- Seconds

## Window

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Window**

In this area, you can define the window settings for a browser session.

---

<sup>294</sup> <https://kb.igel.com/display/licensesmoreigelos11/Add-on+Licenses>



### Start in full-screen mode

- The browser will start in fullscreen mode.  
 The browser will start in a standard window. (default)

### Firefox translation: Language of the user interface

Possible values:

- System setting: The language set under **User Interface > Language > Language** will be used for the browser. (default)
- English
- German
- French
- Dutch
- Spanish
- Italian

### Hide configuration page of the browser

- The browser configuration page (about:config) is locked. As a result, the user cannot change the configuration. (default)  
 The browser configuration page (about:config) can be used.

## Menus & Toolbars

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Menus & Toolbars**

In this area, you can change the browser's menus and toolbars.

### Hide app menu/menu bar

- The button for opening the browser menu will not be shown.  
 The button for opening the browser menu will be shown. (default)

### Use old menu bar

- The browser menu will be shown in the menu bar as in earlier browser versions.  
 The browser menu can be opened via a button. (default)

### Hide the Following Items in App Menu/Menu Bar

#### Hide bookmarks menu

- The bookmarks menu will not be shown in the menu bar.  
 The bookmarks menu will be shown in the menu bar. (default)

#### Hide tools menu

- The “Tools” menu will not be shown.  
 The “Tools” menu will be shown. (default)

#### Hide history entry

- The button for showing the browser history will not be shown.



The button for showing the browser history will be shown. (default)

#### **Hide tabs toolbar**

The tabs will not be shown in the menu bar. The user cannot switch between a number of tabs.

The tabs will be shown in the menu bar. (default)

#### **Hide bookmarks toolbar**

The bookmarks toolbar will not be shown. (default)

The bookmarks toolbar will be shown.

#### **Hide sidebar**

The sidebar will not be shown.

The sidebar will be shown. The bookmarks can be shown in the sidebar. (default)

#### **Hide navigation toolbar**

The navigation bar will not be shown.

The navigation bar will be shown. (default)

#### **Hide the toolbar for searching the page**

The search bar will not be shown.

The search bar will be shown. (default)

### Toolbar Items

#### **Hide URL input**

Only search terms can be entered in the entry field; URLs cannot be entered manually.

Both search terms and URLs can be entered in the entry field. (default)

#### **Hide "Print" button**

The button for printing websites will not be shown.

The button for printing websites will be shown. (default)

#### **Hide "Home" button**

The Home button will not be shown.

The Home button will be shown. (default)

#### **Hide "Search" input**

The search field will not be shown.

The search field will be shown. (default)

#### **Hide "Bookmarks" and "RSS Feed" button**

The button for displaying bookmarks and RSS feeds will not be shown.

The button for displaying bookmarks and RSS feeds will be shown. (default)



## Toolbarconfig

### User customization of toolbars

The user can customize the toolbars. (default)

The user cannot customize the toolbars.

**Navigation toolbar:** Specifies which symbols are shown in the navigation toolbar. The symbols are given as follows; multiple symbols should be separated by commas ",":

|                               |  |
|-------------------------------|--|
| <b>loop-button</b>            |  |
| <b>zoom-controls</b>          |  |
| <b>edit-controls</b>          |  |
| <b>history-panelmenu</b>      |  |
| <b>privatebrowsing-button</b> |  |
| <b>save-page-button</b>       |  |
| <b>find-button</b>            |  |
| <b>open-file-button</b>       |  |
| <b>developer-button</b>       |  |
| <b>sidebar-button</b>         |  |
| <b>feed-button</b>            |  |
| <b>print-button</b>           |  |



|                                 |  |
|---------------------------------|--|
| <b>characterencoding-button</b> |  |
| <b>social-share-button</b>      |  |
| <b>panic-button</b>             |  |
| <b>web-apps-button</b>          |  |
| <b>new-window-button</b>        |  |
| <b>fullscreen-button</b>        |  |
| <b>tabview-button</b>           |  |
| <b>downloads-button</b>         |  |

**Application menu:** Specifies which symbols are shown in the application menu. Multiple symbols should be separated by commas “,”.

## Hotkeys

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Hotkeys**

In this area, you can disable Firefox hotkeys.

### Disable hotkey Quit/Close

- The hotkey for terminating/closing the browser is disabled.
- The hotkey for terminating/closing the browser is enabled. (default)

### Disable hotkey for print dialog

- The hotkey for opening the print dialog is disabled.
- The hotkey for opening the print dialog is enabled. (default)

### Disable hotkey for save page

- The hotkey for saving a website is disabled.
- The hotkey for saving a website is enabled. (default)

### Disable hotkeys for opening new window/tab



- The hotkey for opening a new window or tab is disabled.
- The hotkey for opening a new window or tab is enabled. (default)

#### **Disable hotkeys for opening a new webpage/location and download window**

- The hotkey for opening a new website/location and the download window is disabled.
- The hotkey for opening a new website/location and the download window is enabled. (default)

#### **Disable hotkeys to show history and page info**

- The hotkey for showing the history and page information is disabled.
- The hotkey for showing the history and page information is enabled. (default)

#### **Disable hotkeys for creating bookmarks**

- The hotkey for creating a bookmark is disabled.
- The hotkey for creating a bookmark is enabled. (default)

#### **Disable hotkeys for opening help pages**

- The hotkey for displaying help is disabled.
- The hotkey for displaying help is enabled. (default)

#### **Disable hotkeys for caret browsing**

- The hotkey for starting caret browsing is disabled.
- The hotkey for starting caret browsing is enabled. (default)

## Context

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Context**

In this area, you can disable various items in the browser context menu.

#### **Disable navigation elements in context menu**

- The navigation elements will not be shown in the context menu.
- The navigation elements will be shown in the context menu. (default)

#### **Disable button for save page**

- The button for saving a page will not be shown in the context menu.
- The button for saving a page will be shown in the context menu. (default)

#### **Disable button for open new window/tab**

- The button for opening a new window/tab will not be shown in the context menu.
- The button for opening a new window/tab will be shown in the context menu. (default)

#### **Disable button for show info/source**

- The button for showing page information/page source text will not be shown in the context menu.
- The button for showing page information/page source text will be shown in the context menu. (default)

#### **Disable button for creating and editing bookmarks**



- The button for creating and editing bookmarks will not be shown in the context menu.
- The button for creating and editing bookmarks will be shown in the context menu. (default)

#### **Disable button for searching the web**

- The button for searching the web will not be shown in the context menu.
- The button for searching the web will be shown in the context menu. (default)

#### **Hide the browser's context menu**

- The context menu will not be shown.
- The context menu will be shown. (default)

## Commands

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Commands**

In this area, you can define start options for browser commands.

The following commands are available:

#### **Restart Browser**

To open the dialogue for defining start options, proceed as follows:

1. Select the command. Example: **Restart Browser**
2. Click **Modify...**

The following start options are available:

#### **Start menu**

- The session can be launched from the start menu.

#### **Application Launcher**

- The session can be launched with the Application Launcher.

#### **Desktop**

- The session can be launched with a program launcher on the desktop.

#### **Quick start panel**

- The session can be launched with the quick start panel.

#### **Start menu's system tab**

- The session can be launched with the start menu's system tab.

#### **Application Launcher's system tab**

- The session can be launched with the Application Launcher's system tab.

#### **Desktop context menu**

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.



**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)



### 3.8.24 Firefox Browser Session

Menu path: **Sessions > Firefox Browser > Firefox Browser Sessions > [Session Name]**

In this area, you can configure desktop integration for the browser session.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Starting Methods for Session

##### **Start menu**

The session can be launched from the start menu.

##### **Application Launcher**

The session can be launched with the Application Launcher.

##### **Desktop**

The session can be launched with a program launcher on the desktop.

##### **Quick start panel**

The session can be launched with the quick start panel.

##### **Start menu's system tab**

The session can be launched with the start menu's system tab.

##### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

##### **Desktop context menu**

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.



## Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

## Autostart

The session will be launched automatically when the device boots.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

## Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.



- The session is started automatically, even when no network is available.

- [Settings](#)(see page 980)
- [Desktop Integration](#)(see page 980)
- [Plugins](#)(see page 982)

## Settings

Menu path: **Sessions > Firefox Browser > Firefox Browser Sessions > [Session Name] > Settings**

In this area, you can change the following settings:

**When browser starts:** Specifies what pages are shown when the browser is launched.

Possible options:

- "[Global setting](#)"
- "Start with a blank page"
- "Show my home page"
- "Resume previous session": All tabs from the last session are reopened.

**Start page:** Specifies the URL of the start page. You can specify a number of start pages by separating the URLs of the start pages with a vertical dash "|". This setting is active only when "Show my home page" is chosen under **When browser starts**.

**Start monitor:** Specifies the monitor on which the browser is launched. (Default: [1st monitor](#))

### Autostart

- The browser is automatically launched when the system starts.

## Desktop Integration

Menu path: **Sessions > Firefox Browser > Firefox Browser Sessions > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the Firefox browser session.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

- The session can be launched from the start menu.

### Application Launcher

- The session can be launched with the Application Launcher.

### Desktop

- The session can be launched with a program launcher on the desktop.



### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:



- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

### Autostart

The session will be launched automatically when the device boots.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

### Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

## Plugins

Menu path: **Sessions > Firefox Browser > Plugins**

To obtain an overview of the plugins available in the browser, proceed as follows:

- ▶ Click on the **About:Plugins** button.

The browser will start with the `about:plugins` page. The plugins available in the browser will be shown.

## 3.8.25 Chromium Browser Global

Menu path: **Sessions > Chromium Browser > Chromium Browser Global**

Here, you can change settings that will be valid for all Chromium sessions.

### Use IGEL Setup for configuration

The settings made in the IGEL Setup or the UMS configuration dialog will be effective.

The settings made in the IGEL Setup or the UMS configuration dialog will not have any effect on the behavior of Chromium.

**Default web browser:** Defines which browser will be chosen by the system, e.g. for opening Citrix Storefront. Possible options:

- "Firefox Browser"
- "Chromium Browser"



### **Automatic browser restart on exit**

- Chromium is restarted when the user closes it.
- Chromium is not restarted on exit.

### **Show browser splash screen**

- The Chromium splash screen is shown on start.
- Chromium starts without a splash screen.

- [General](#)(see page 983)
- [Content](#)(see page 984)
- [Proxy](#)(see page 984)
- [Privacy](#)(see page 985)
- [Security](#)(see page 987)
- [Encryption](#)(see page 987)
- [Menus & Toolbars](#)(see page 987)
- [Window](#)(see page 988)
- [Custom Setup](#)(see page 988)
- [Smartcard Middleware](#)(see page 989)

## General

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > General**

In this area, you can change the following settings:

**On startup:** Specifies what pages are shown when Chromium is launched.

Possible options:

- "Open the new tab page"
- "Open a specific page or set of pages": The page or set of pages specified under **Startup page** are opened.
- "Continue where you left off": All tabs from the last session are reopened.

**Startup page:** Specifies the URL of the start page. You can specify a set of start pages by separating the URLs of the start pages with a vertical dash "|". This setting is active only when "Open a specific page or set of pages" is chosen under **On startup**.

**New tab page setting:** Specifies the page that is shown when a new tab is opened.

Possible options:

- "Open a blank page"
- "Open a specific page": The page defined under **New tab page location** is shown.

**New tab page location:** Specifies the page that is shown when the user opens a new tab. This is effective only if **New tab page setting** is set to "Open a specific page".

**Font size:** Specifies the font size for web content.

Possible options:

- "Very small"



- "Small"
- "Medium (recommended)"
- "Large"
- "Very large"

## Content

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Content**

### **Block pop-ups and redirects**

Pop-up windows and redirects are blocked.

**Exceptions....**: Add websites on which pop-up windows and redirects are not blocked.

### **Load images automatically**

Images from websites are loaded automatically.

**Exceptions....**: Add websites on which images are not loaded automatically.

### **Type of download directory**

Possible options:

- "Custom location": The user will be prompted for a location to download a file.
- "userhome": Files will be downloaded to /userhome/Downloads.

**Location**: Defines the path files are downloaded to. Only effective when **Type of download directory** is set to "Custom location".

### **JavaScript**

JavaScript is enabled.

**Languages**: One or more preferred languages for multilingual websites, given in the form of language abbreviations separated by commas. The languages should be given in the order of preference. Example: With "de, en, fr, it", the website will be shown in German, if available, otherwise in English and so on.

### **Integrated translation service of Chromium**

When a web page has a language that differs from your system language, Chromium will offer to translate the page.

### **Autoplay**

Embedded audio and video content on a web page is played automatically when the page is loaded.

Audio and video content is not played automatically.

## Proxy

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Proxy**

In this area, you can change the proxy configuration.

To change the proxy configuration, proceed as follows:

1. In the **Proxy Configuration** menu, select the type of proxy configuration.  
The following proxy configurations are available:



- "Never use a proxy"
  - "Use fixed proxy servers"
  - "Use a .pac proxy script"
  - "Use system proxy settings"
  - "Auto detect proxy settings"
2. Enter the necessary configuration data for the selected proxy configuration.

"Never use a proxy"

With this proxy configuration, no proxy is used.

"Use fixed proxy servers"

The configuration data must be specified in the following fields.

- **FTP proxy:** URL of the proxy for FTP
- **Port:** Port of the proxy for FTP
- **HTTP proxy:** URL of the proxy for HTTP
- **Port:** Port of the proxy for HTTP
- **SSL proxy:** URL of the proxy for SSL
- **Port:** Port of the proxy for SSL
- **SOCKS host:** URL of the proxy for SOCKS
- **Port:** Port of the proxy for SOCKS
- **SOCKS protocol version:** Version of the SOCKS protocol used (default: SOCKS v5)
- **No proxy for:** List of URLs for which no proxy is to be used (default: localhost, 127.0.0.1)

"Use a .pac proxy script"

With this proxy configuration, the PAC file (Proxy Auto Config) available under **URL** will be used.

- **URL:** URL of the proxy configuration file

"Use system proxy settings"

With this proxy configuration, the proxy configured under **Network > Proxy** will be used.

"Auto detect proxy settings"

With this proxy configuration, WPAD (Web Proxy Autodiscovery Protocol) will be used. The browser will determine the URL of the WPAD file wpad.dat automatically with the help of DNS.

## Privacy

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Privacy**

### Autofill addresses and more

Entries in forms and search bars will be retained after Chromium restarts.

Entries in forms and search bars will be retained only for the duration of the session.



### Autofill payments

- Entries in payment forms will be retained after Chromium restarts.
- Entries in payment forms will be retained only for the duration of the session.

### Autofill passwords

- Passwords entered will be retained after Chromium restarts.
- Passwords entered will be retained only for the duration of the session.

### Clear browsing data

- Data entered will be deleted when Chromium is closed. What data are deleted is specified in the following options.
- Data entered will not be deleted when the browser is closed.

### Browsing & download history

- Addresses (URLs) of visited websites and the list of downloads will be deleted when Chromium is closed.

### Saved passwords

- Passwords entered will be deleted when Chromium is closed.

### Cookies

- Cookies will be deleted when Chromium is closed.

### Cache

- The cache for temporarily saving web pages will be emptied when Chromium is closed.

**Allow incognito mode:** When the incognito mode is active, all data from private windows will be deleted after Chromium is closed.

Possible options:

- "Enabled": The user can open browser windows in incognito mode.
- "Disabled": The user cannot open browser windows in incognito mode.
- "Forced": All browser windows started by the user are in incognito mode.

### Enable "Do Not Track" feature

- Chromium will inform the website you are visiting that you do not wish to be tracked, i.e. you do not want your surfing history to be recorded.

The browser will use the DNT ("Do Not Track") field in the HTTP header for this purpose. Observing this setting is voluntary; from a technical point of view, websites can still record the surfing history even when DNT is set to 1.

### Enable search suggestions

- Suggestions will be shown while an address is being typed in the address bar. The suggestions will be based on previously visited websites which are stored in the history.



## Security

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Security**

On this page, you can define settings for safe browsing and for the handling of files.

### Safe browsing

Chromium will check all web content, including e.g. images and scripts, against a continuously updated list of known phishing and malware websites. If Chromium finds suspicious content, you will be given a warning.

Chromium will not check web content.

### File access

Chromium can access local files on the endpoint device. Downloads and uploads are allowed. Before a file is downloaded, a confirmation dialog is shown.

Local files cannot be accessed by Chromium. Neither downloads nor uploads are allowed. When the user tries to download a file, a message informs the user that downloads are blocked.

**Download allowlist:** The MIME types listed here are not blocked even when **File access** is deactivated. The storage location is defined under **Sessions > Chromium Browser > Chromium Browser Global > Content**, parameter **Location**. If the file suffix matches with one of the entries in **Open file types automatically after downloading**, the file is opened immediately after download. The list entries are separated by semicolons ";".

**Open file types automatically after downloading:** Any file whose suffix is listed here will be opened immediately after download. The list entries are separated by semicolons ";".

## Encryption

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Encryption**

In this area, you can define the settings for encryption methods.

**Minimum SSL/TLS version:** This protocol will be used to establish a secure connection if no higher protocol is available. Higher protocols are preferred.

Possible options:

- TLS 1.0
- TLS 1.1
- TLS 1.2
- TLS 1.3

**Maximum SSL/TLS version:** This protocol is requested when negotiating the connection. If this protocol is not available, the next lowest protocol will be requested.

Possible options:

- TLS 1.2
- TLS 1.3

## Menus & Toolbars

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Menus & Toolbars**

In this area, you can change the browser's menus and toolbars.



### **Hide home button**

The home button will not be shown.

The home button will be shown.

### **Hide bookmarks toolbar**

The bookmarks menu will not be shown in the menu bar.

The bookmarks menu will be shown in the menu bar.

## Window

Menu path: **Sessions > Chromium Browser > Chromium Global > Window**

In this area, you can define the window settings for a Chromium session.

### **Enable kiosk mode**

Chromium starts in kiosk mode.

Chromium starts in normal mode.

### **Start maximized**

Chromium starts in a maximized window.

Chromium starts in a window with default size.

**Chromium translation:** Changes the default language when Chromium offers to translate a web page.

### **Block Chromium settings**

The settings menu of Chromium can not be accessed by the user.

The user can access the settings menu.

## Custom Setup

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Custom Setup**

- [Policies\(see page 988\)](#)
- [Custom Command-Line Options\(see page 989\)](#)

### Policies

Menu path: **Sessions > Chromium Browser > Chromium Browser Global >Custom Setup > Policies**

Here, you can define policies for Chromium. For further information, see [https://chromium.googlesource.com/chromium/src/+/master/docs/enterprise/add\\_new\\_policy.md](https://chromium.googlesource.com/chromium/src/+/master/docs/enterprise/add_new_policy.md).

► Click on **Add** to create a policy.

**Policy name:** Name of the policy

**Policy value:** Value of the policy



## Custom Command-Line Options

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Custom Setup > Custom Command-Line Options**

Here, you can define command-line parameters that are passed to Chromium on startup. The syntax is exactly the same as if Chromium would be started from a terminal.

**Custom command-line parameters:** One or more command-line parameters. Multiple parameters are separated by whitespace.

Example:

```
--proxy-server="socks://localhost:8080" --incognito
```

## Smartcard Middleware

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Smartcard Middleware**

In this area, you can activate or deactivate smartcard middleware that is to be used for encryption.

### Gemalto SafeNet security device

- Gemalto/SafeNet eToken will be used for encryption.
- Gemalto/SafeNet eToken will not be used for encryption.

### cryptovision sc/interface security device

- cryptovision sc/interface will be used for encryption.
- cryptovision sc/interface will not be used for encryption.

### Gemalto IDPrime security device

- Gemalto IDPrime will be used for encryption. Enable this Gemalto middleware when you want to operate Gemalto Common Criteria devices in unlinked mode.
- Gemalto IDPrime will not be used for encryption.

### Athena IDProtect security device

- Athena IDProtect will be used for encryption.
- Athena IDProtect will not be used for encryption.

### A.E.T. SafeSign security device

- A.E.T. SafeSign will be used for encryption.
- A.E.T. SafeSign will not be used for encryption.

### SecMaker Net iD security device

- SecMaker Net iD will be used for encryption.
- SecMaker Net iD will not be used for encryption.

### Coolkey security device

- Coolkey will be used for encryption.
- Coolkey will not be used for encryption.



### OpenSC security device

- OpenSC will be used for encryption.
- OpenSC will not be used for encryption.

### 90meter security device

#### Licensed Feature

This feature requires an add-on license; see [Add-On Licenses<sup>295</sup>](#). Please contact your IGEL sales representative.

- 90meter will be used for encryption.

- 90meter will not be used for encryption.

### Use a custom security device

- The PKCS#11 module stored under the **Path to the library** is used.
- The custom security device will not be used for encryption.

**Name of the security device:** Name of the custom security device that uses the library specified under **Path to the library**

**Path to the library:** Path to the custom PKCS#11 module

## 3.8.26 Chromium Sessions

Menu path: **Sessions > Chromium Browser > Chromium Sessions > [Session Name]**

In this area, you can configure desktop integration for the Chromium session.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

- The session can be launched from the start menu.

#### Application Launcher

- The session can be launched with the Application Launcher.

#### Desktop

- The session can be launched with a program launcher on the desktop.

#### Quick start panel

---

<sup>295</sup> <https://kb.igel.com/display/licensesmoreigelos11/Add-on+Licenses>



- The session can be launched with the quick start panel.

#### Start menu's system tab

- The session can be launched with the start menu's system tab.

#### Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

#### Desktop context menu

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

#### Hotkey

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey



To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

## Autostart

- The session will be launched automatically when the device boots.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

- For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.
- No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

- [Settings](#)(see page 992)
- [Desktop Integration](#)(see page 992)

## Settings

Menu path: **Sessions > Chromium Browser > Chromium Sessions > [Session Name] > Settings**

In this area, you can change the following settings:

**On startup:** Specifies what pages are shown when Chromium is launched.

Possible options:

- "Global setting"
- "Open the new tab page"
- "Open a specific page or set of pages": The page or set of pages specified under **Startup page** are opened.
- "Continue where you left off": All tabs from the last session are reopened.

**Startup page:** Specifies the URL of the start page. You can specify a set of start pages by separating the URLs of the start pages with a vertical dash "|". This setting is active only when "Show my home page" is chosen under **On startup**.

## Desktop Integration

Menu path: **Sessions > Chromium Browser > Chromium Sessions > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the Chromium session.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )



## Starting Methods for Session

### **Start menu**

The session can be launched from the start menu.

### **Application Launcher**

The session can be launched with the Application Launcher.

### **Desktop**

The session can be launched with a program launcher on the desktop.

### **Quick start panel**

The session can be launched with the quick start panel.

### **Start menu's system tab**

The session can be launched with the start menu's system tab.

### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

### **Desktop context menu**

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

### **Hotkey**

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
- [Ctrl] = Ctrl
-  = Mod4



When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

The session will be launched automatically when the device boots.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

#### Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

### 3.8.27 Media Player Global

Menu path: **Sessions > Media Player > Media Player Global**

Here, you can change the global settings for the device's media player:

- [Window](#)(see page 994)
- [Playback](#)(see page 995)
- [Video](#)(see page 996)
- [Options](#)(see page 996)

#### Window

Menu path: **Setup > Sessions > Media Player > Media Player Global > Window**



**Aspect ratio:** Aspect ratio for video playback

Possible values:

- Auto: The aspect ratio of the playback window will adapt to the video being played.
- Square
- 4:3 (TV)
- 16:9 (widescreen)
- 2.11:1 (DVB)

#### **Fullscreen**

- The media player will be shown in full-screen mode.
- The media player will be shown in a standard window. (Default)

#### **Automatically resize the player window when a new video is loaded**

- The window size will adapt to the video being played.
- The window size will not change. (Default)

#### **Main window should stay on top**

- The media player window will always remain in the foreground. Other windows cannot be placed on top of the media player window.
- The media player window will behave like a standard window. Other windows can be placed on top of the media player window. (Default)

#### **Show controls**

- The media player operating components will be shown. (Default)
- The media player operating components will not be shown; only the playback window is visible.

## Playback

Menu path: **Sessions > Media Player > Media Player Global > Playback**

#### **Repeat mode**

- The playlist will be repeated until the user stops playback.
- The playlist will be played back once only. (default)

#### **Shuffle mode**

- The playlist will be played back in a random order.
- The playlist will be played back in the set order. (default)

#### **Show visual effects when an audio file is played**

- Visual effects will be shown when playing back audio data.
- No visual effects will be shown. (default)

**Type of visualization:** The type of visual effects when playing back audio data

Possible values:

- Monoscope



- Goom!

**Visualization size:** The size of the visual effects shown

This parameter is effective only if gstreamer 0.10 is selected as the multimedia framework, which results in Totem being selected as the media player. With the default setting for IGEL OS 10.05 and higher (gstreamer 1.x in combination with Parole) the parameter is not effective.

The multimedia framework and media player can be changed in the Registry under **System > Registry > multimedia > gstreamer > version** (registry key: multimedia.gstreamer.version).

Possible values:

- Small
- Normal
- Large
- Extra large

## Video

Menu path: **Setup > Sessions > Media Player > Media Player Global > Video**

- **Video output:** Specifies the video output method.

Possible options:

- Auto: The video output method will be set depending on availability. The following options will be queried in this order. Examples: If available, hardware acceleration will be used. If hardware acceleration is not available but the X video extension is, the X video extension will be used.
- Hardware accelerated: Hardware acceleration will be used.
- X video extension: The images will be written to the graphics card memory using *shared memory*. Hardware acceleration will be used.
- X Window System: Video will be output via the X11 protocol. Hardware acceleration will not be used.

## Options

Menu path: **Setup > Sessions > Media Player > Media Player Global > Options**

- **Disable screensaver when playing audio**

The screensaver will not be started during audio playback. (default)

The screensaver will start after the set idling time, even if audio is being played back.

- **Network connection speed**

Possible values:

- 56 kbps modem/ISDN
- 112 kbps dual ISDN/DSL
- 256 kbps DSL/cache
- 384 kbps DSL/cache
- 512 kbps DSL/cache



- 1.5 MBps T1/Intranet/LAN
  - Intranet/LAN
- **Buffer size:** The buffer compensates for fluctuations in the network speed. (default: 3)
- **Autoload subtitle**
  - Subtitles contained in the video will be shown automatically. (default)
  - Subtitles contained in the video will only be shown if the user has enabled them via **View > Subtitles**.
- **Subtitle encoding:** Character coding for the subtitles. The value is set to UTF-8.
- **Font name:** Font that is used for the subtitles  
Possible values:
  - Sans
  - Sans Bold
  - Serif
  - Serif Bold
- **Font size:** Size of the font that is used for the subtitles (default: 20)

### 3.8.28 Media Player Session

Menu path: **Sessions > Media Player > Media Player Sessions > [Session Name]**

In this area, you can configure desktop integration for the media player.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Starting Methods for Session

##### **Start menu**

The session can be launched from the start menu.

##### **Application Launcher**

The session can be launched with the Application Launcher.

##### **Desktop**

The session can be launched with a program launcher on the desktop.

##### **Quick start panel**

The session can be launched with the quick start panel.

##### **Start menu's system tab**

The session can be launched with the start menu's system tab.

##### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

##### **Desktop context menu**



- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey



To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

## Autostart

- The session will be launched automatically when the device boots.

## Restart

- The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

- For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.
- No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

## Autostart requires network

- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.

- [Playback](#)(see page 999)
- [Options](#)(see page 1000)
- [Desktop Integration](#)(see page 1000)

## Playback

Menu path: **Setup > Sessions > Media Player > Media Player Sessions > [Session Name] > Playback**

In this area, you can specify which audio data or video data are played back with which window settings when the media player session starts.

- **Medium / filename:** Path to the audio data or video data that are to be played back when the media player session starts. This can be a local path or a URL.
- **Use default fullscreen mode configuration**
  - The setting under **Setup > Sessions > Media Player > Media Player Global > Window** will be used. (default)
  - The setting will be set on a session-specific basis with **Play video in fullscreen**.
- **Play video in fullscreen**
  - The media player will be shown in fullscreen mode.
  - The media player will be shown in a standard window. (default)
- **Use image aspect ratio setting**
  - The setting under **Setup > Sessions > Media Player > Media Player Global > Window** will be used. (default)



- The setting will be set on a session-specific basis with **Aspect ratio**.
- **Aspect ratio:** Aspect ratio for video playback
  - Possible values:
    - **Auto:** The aspect ratio of the playback window will adapt to the video being played.
    - Square
    - 4:3 (TV)
    - 16:9 (widescreen)
    - 2.11:1 (DVB)

## Options

Menu path: **Setup > Sessions > Media Player > Media Player Sessions > [Session Name] > Options**

- **Use default controls configuration**
  - The setting under **Setup > Sessions > Media Player > Media Player Global > Window** will be used. (default)
  - The setting will be set on a session-specific basis with **Show controls**.
- **Show controls**
  - The media player operating components will be shown. (default)
  - The media player operating components will not be shown; only the playback window is visible.

## Desktop Integration

Menu path: **Sessions > Media Player > Media Player Sessions > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the media player.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.



### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey



To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

### **Autostart**

- The session will be launched automatically when the device boots.

### **Restart**

- The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

### **Autostart requires network**

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

## 3.8.29 VoIP Client

Menu path: **Sessions > VoIP Client**

Ekiga Voice over IP client allows you to use the SIP (Session Initiation Protocol) and H.323; see <http://ekiga.org><sup>296</sup>.

You will find a detailed description of all Ekiga options under <http://wiki.ekiga.org/index.php/Manual>.

In this area, you can configure desktop integration for the VoIP session.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### **Start menu**

- The session can be launched from the start menu.

#### **Application Launcher**

- The session can be launched with the Application Launcher.

---

<sup>296</sup> <http://ekiga.org/>



## Desktop

The session can be launched with a program launcher on the desktop.

## Quick start panel

The session can be launched with the quick start panel.

## Start menu's system tab

The session can be launched with the start menu's system tab.

## Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

## Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

## Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
-  = Ctrl
-  = Mod4



When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

### Autostart

The session will be launched automatically when the device boots.

### Restart

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

### Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

- [Account](#)(see page 1004)
- [Audio](#)(see page 1006)
- [SIP](#)(see page 1007)
- [H.323](#)(see page 1007)
- [Call Options](#)(see page 1008)
- [Phone Book](#)(see page 1008)
- [Preferences](#)(see page 1009)
- [Desktop Integration](#)(see page 1009)

## Account

Menu path: **Setup > Sessions > VoIP Client > User Account**



You can set up or change one or more user accounts as well as specify the name displayed.

- **Full Name:** Name of the user; this name will be shown to the other person. Example: John Doe

To set up an SIP user account, proceed as follows:

Ensure that the VoIP client was terminated before you start setting up or changing a user account. Changes will only be saved if the client is not running.

1. Click **[+]**.
2. If the user account is to be active once set up, enable the **Enable Account** option.
3. Enter the following data:
  - **Protocol:** Select **SIP**.
  - **Name:** Name for this user account.

Choose a name which allows a distinction to be made easily between a number of user accounts.

- **Registrar:** URI with which the VoIP client registers. This can be a DNS name or an IP address.
- **User name:** Numerical or alphanumerical value. The user name is part of the SIP address. Example: john.doe in john.doe@example.com
- **Login Name:** Numerical or alphanumerical value. Name with which the VoIP client registers on the registrar. This name can differ from the name given under **user name**.
- **Password:** Password with which the VoIP client registers on the registrar
- **Registration Update Timeout:** Timeout after which the registration should be updated (default: 3600)

4. Click **Ok**.  
The user account has been set up.

To set up an H.323 user account, proceed as follows:

Ensure that the VoIP client was terminated before you start setting up or changing a user account. Changes will only be saved if the client is not running.

1. Click **[+]**.
2. If the user account is to be active once set up, enable the **Enable Account** option.
3. Enter the following data:
  - **Protokoll:** Wählen Sie **H323**.
  - **Name:** Name für dieses Benutzerkonto.

Choose a name which allows a distinction to be made easily between a number of user accounts.

- **Gatekeeper:** URI with which the VoIP client registers. This can be a DNS name or an IP address.
- **User name:** Numerical or alphanumerical value. Example: john.doe in john.doe@example.com



- **Passwort:** Password with which the VoIP client logs on to the registrar
  - **Registration Update Timeout:** Timeout after which the registration should be updated (default: 3600)
4. Click **Ok**.  
The user account has been set up.

## Audio

Menu path: **Setup > Sessions > VoIP Client > Audio**

You can change the audio settings of the VoIP client.

Recommendation: Configure the settings **Device for ringtone**, **Device for audio playback** and **Device for audio recording** in the VoIP client. All available audio devices of the thin client are shown in the VoIP client.

To configure the audio devices in the VoIP client, proceed as follows:

1. In the */GEL* setup, ensure that the option **Save configuration changes made in the application** is enabled under **Sessions > VoIP Client > Preferences**.
2. Start the VoIP client.
3. Configure your desired settings in the VoIP client under **Edit > Preferences > Audio > Devices**.
4. To save your settings, close the VoIP client window, right-click on  in the system tray and select **Close**.

The changes will be saved in the */GEL* setup once the VoIP client is terminated.

Settings in the setup:

- **Sound event output device:** Specifies which audio device is used for the ringtone.

It is recommended that you select the audio device that is connected to the thin client's built-in loudspeaker.

- **Audio output device:** Specifies which audio device is used for playback. Example: the audio device that is connected to the loudspeakers of the headset.
- **Audio input device:** Specifies which audio device is used for recording. Example: the audio device that is connected to the microphone of the headset.
- **Enable silence detection:** If this option is enabled, audio transmission will be suppressed in the absence of voice activity. This helps to save bandwidth.

Voice activity detection can reduce the voice quality.

- **Enable echo cancelation:** If this option is enabled, the VoIP client will suppress echoes of your own voice.
- **Maximum jitter buffer (in milliseconds):** The jitter buffer improves voice quality by compensating for delay variations when transmitting voice packets. The VoIP client continuously



measures delay variations and automatically adjusts the buffer size. The bigger the delay variations are, the bigger the jitter buffer will be set. (Default: 500)

A bigger jitter buffer results in greater latency.

## SIP

Menu path: **Setup > Sessions > VoIP Client > SIP**

You can change SIP-specific settings for the proxy, forwarding and the multi-frequency dialing process (DTMF).

- **Outbound Proxy:** URI of the SIP proxy that handles outbound calls.
- **Forward URI:** SIP URI to which inbound calls are forwarded if forwarding is enabled. You will find further information on forwarding under [Call Options\(see page 1008\)](#).
- **Send DTMF as:** Specifies how key sequences are transmitted while a connection is in place.  
Possible values:
  - INFO: The key sequence is transmitted as SIP INFO.
  - RFC 2833: The key sequence is transmitted using RTP (Real-time Transport Protocol).

## H.323

Menu path: **Setup > Sessions > VoIP Client > H.323**

You can change H.323-specific settings for forwarding, H.245, quick start and for the multi-frequency dialing process (DTMF).

- **Forward URI:** H.323 URI to which inbound calls are forwarded if forwarding is enabled. You will find further information on forwarding under [Call Options\(see page 1008\)](#).
- **Enable H.245 tunneling**  
 H.245 messages will be packaged in H.225 messages. In this way, no additional TCP connection must be established. (Default)

For H.245 tunneling, port 1720 is required.

A separate TCP connection is established for H.245.

- **Enable early H.245**  
 H.245 will be launched at an earlier point in the connection process. The voice connection can be established more quickly as a result. (Standard)
- **Enable Fast Start procedure**  
 The voice connection will be established in quick start mode (fast connect, part of H.323 v2). (Standard)
- **DTMF senden als:** Specifies how key sequences are transmitted while a connection is in place.  
Mögliche Werte:
  - String: The key sequence is transmitted using H.245 User Input Indication.
  - Tone: The key sequence is transmitted as a tone sequence in the audio data flow.
  - RFC 2833: The key sequence is transmitted using RTP (Real-time Transport Protocol).
  - Q.931: The key sequence is transmitted via the signaling channel.



## Call Options

Menu path: **Setup > Sessions > VoIP Client > Call Options**

You can change settings for inbound calls.

- **Always forward calls to the given address:** If this option is enabled, inbound calls will immediately be forwarded to the address defined in **Setup > Sessions > VoIP Client > SIP > Forward URI** (see [SIP\(see page 1007\)](#)) or **Setup > Sessions > VoIP Client > H.323> Forward URI** (see [H.323\(see page 1007\)](#)).
- **Forward calls to the given address if no answer:** If this option is enabled, inbound calls will be forwarded to the address defined in **Setup > Sessions > VoIP Client > SIP > URI for Forwarding** (see [SIP\(see page 1007\)](#)) or **Setup > Sessions > VoIP Client > H.323> URI for Forwarding** (see [H.323\(see page 1007\)](#)) after the time specified under **Time limit for calls not taken**. If this option is disabled, inbound calls will be rejected after the time specified under **Time limit for calls not taken**.
- **Forward calls to the given address if busy:** If this option is enabled, inbound calls during a call will be forwarded to the address defined in **Setup > Sessions > VoIP Client > SIP > URI for Forwarding** (see [SIP\(see page 1007\)](#)) or **Setup > Sessions > VoIP Client > H.323> URI for Forwarding** (see [H.323\(see page 1007\)](#)).
- **No Answer Timeout:** Time in seconds after which calls not taken are rejected or forwarded.

## Phone Book

Menu path: **Setup > Sessions > VoIP Client > Telephone Book**

You can add one or more LDAP address books or local contacts.

To add an LDAP address book, proceed as follows:

1. In the **List of LDAP address books** area, click on .
2. Enter the following data:
  - **Name:** Name with which the LDAP address book will be displayed in the VoIP client
  - **Server Name:** Host name of the LDAP server
  - **Port:** Port for the connection to the LDAP server (Default: 389)
  - **Base DN:** Basis for the search in the LDAP tree
  - **Scope:** Area for the LDAP search
 

Possible options:

    - Single level
    - Subtree
  - **Display name attribute:** LDAP attribute that is displayed as the name of the contact in the VoIP client. (Default: cn)
  - **Call Attribute:** LDAP attribute that contains the telephone number (Standard: telephoneNumber)
  - **Filter Template:** Filter for the LDAP search (Default: (cn=\$))
  - **Bind ID:** Identifier for the LDAP search. This identifier is sent to the LDAP server in a BIND request.
  - **Password:** Password for the user account for the LDAP search



3. Click **Ok**.

To add a contact to the local contact list, proceed as follows:

1. In the **List of Contacts** area, click on **[+]**.
2. Enter the following data:
  - **Name:** Name of the SIP or H.323 address displayed
  - **Address:** SIP or H.323 address. Example: `sip:500@example.com`
  - **Group:** Optional group name in order to group contacts
3. Click **Ok**.

## Preferences

Menu path: **Setup > Sessions > VoIP Client > Settings**

You can change VoIP client settings.

- **Save configuration changes made in the application**  
 changes made in the VoIP client will be saved in the *IGEL* setup when the VoIP client is terminated. This applies to all settings available in the *IGEL* setup, with the exception of settings for the LDAP address book. (Default)

## Desktop Integration

Menu path: **Sessions > VoIP Client > Desktop Integration**

In this area, you can configure desktop integration for the VoIP client session.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

The session can be launched from the start menu.

#### Application Launcher

The session can be launched with the Application Launcher.

#### Desktop

The session can be launched with a program launcher on the desktop.

#### Quick start panel

The session can be launched with the quick start panel.

#### Start menu's system tab

The session can be launched with the start menu's system tab.



### Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

### Desktop context menu

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey



To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

### **Autostart**

The session will be launched automatically when the device boots.

### **Restart**

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

### **Autostart requires network**

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

## 3.8.30 Teradici PCoIP Session

Menu path: **Sessions > Teradici PCoIP Client > PCoIP Sessions**

### **Licensed Feature**

This feature requires an add-on license; see [Add-On Licenses<sup>297</sup>](#). Please contact your IGEL sales representative.

If you are using Amazon WorkSpace, note that Linux connectivity is usually disabled by default, see [Amazon WorkSpaces Linux Client Application<sup>298</sup>](#)

You will have to enable this before connecting.

- [Connection Settings](#)(see page 1012)
- [Login](#)(see page 1012)
- [Window](#)(see page 1012)

<sup>297</sup> <https://kb.igel.com/display/licensesmoreigelos11/Add-on+Licenses>

<sup>298</sup> <https://docs.aws.amazon.com/workspaces/latest/userguide/amazon-workspaces-linux-client.html>



- [Desktop Integration](#)(see page 1013)

## Connection Settings

Menu path: **Sessions > Teradici PCoIP Client > PCoIP Sessions > PCoIP Session > Connection Settings**

### **Use IGEL Setup for configuration**

- The connection settings are configured via IGEL Setup.  
 IGEL Setup does not control the connection settings. (Default)

### **Broker type**

Possible options:

- '[PCoIP broker](#)'
- 'Direct hardhost'

**Server:** Host name or IP address of the PCoIP server.

**Desktop:** Name of the virtual desktop. This parameter is only relevant if the user is assigned to more than one virtual desktop on the server, e. g. Amazon Web Services (AWS). If the user has several desktops and the field **Desktop** is empty, a selection of all available desktops is displayed after login. If the field **Desktop** contains the name of an available desktop, the session is started with this desktop.

### **Server certificate verification mode**

Possible options:

- 'Not required'
- '[Warn but allow](#)'
- 'Full verification': For secure operation, this verification mode is recommended.

## Login

Menu path: **Sessions > Teradici PCoIP Client > PCoIP Sessions > PCoIP Session > Login**

### **Authentication type**

Possible options:

- '[Password authentication](#)'
- 'Smartcard authentication'

**Smartcard PIN:** PIN required for smartcard authentication; only valid if **Authentication type** is set to **Smartcard authentication**.

## Window

Menu path: **Sessions > Teradici PCoIP Client > PCoIP Sessions > PCoIP Session > Window**

### **Window mode**

Possible options:

- '[User defined
- 'Fullscreen one monitor'
- 'Fullscreen all monitors'](#)



- 'Window'

### User interface translation

Possible options:

- 'System setting'
- 'English'
- 'German'
- 'French'
- 'Spanish'
- 'Portuguese (EU)'
- 'Portuguese (Brazil)'
- 'Italian'
- 'Japanese'
- 'Chinese (Simplified)'
- 'Chinese (Traditional)'

## Desktop Integration

Menu path: **Sessions > Teradici PCoIP Client > PCoIP Sessions > PCoIP Session > Desktop Integration**

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

The session can be launched from the start menu.

#### Application Launcher

The session can be launched with the Application Launcher.

#### Desktop

The session can be launched with a program launcher on the desktop.

#### Quick start panel

The session can be launched with the quick start panel.

#### Start menu's system tab

The session can be launched with the start menu's system tab.

#### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

#### Desktop context menu

The session can be launched with the desktop context menu.



**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.  
Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. **Ctrl**.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- = Alt

Key combinations are formed as follows with |:

- + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)



### Autostart

The session will be launched automatically when the device boots.

### Restart

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

### Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

## 3.8.31 AVD Global

Menu path: **Sessions > AVD > AVD Global**

- [Plugins\(see page 1015\)](#)

### Plugins

Menu path: **Sessions > AVD > AVD Global > Plugins**

- [Fabulatech\(see page 1015\)](#)

### Fabulatech

Menu path: **Sessions > AVD > AVD Global > Plugins > Fabulatech**

The Fabulatech redirection of webcams and scanners as well as the common Fabulatech USB redirection can be enabled or disabled. The Fabulatech USB redirection can be controlled based on class rules and device rules.

For the Fabulatech USB redirection, a server-side component is required. We recommend the USB for Remote Desktop IGEL Edition; see <http://www.usb-over-network.com/partners/igel/>.

Enable either native USB redirection or Fabulatech USB redirection – not both together. Disable USB redirection if you use DriveLock.



Ensure that no other hotplug storage device (USB stick) is connected if a session is started with Fabulatech USB redirection. Otherwise, the hotplug storage device will not be securely removed when the session starts, and this could lead to data loss.

You can enable or disable all Fabulatech redirections for each individual session; go to **Sessions > AVD > AVD Sessions > [Session name] > Plugins** and set **Fabulatech Webcam/Scanner/USB Redirection** accordingly (see [Plugins](#)(see page 1024)).

#### **Fabulatech Webcam Redirection**

Fabulatech webcam redirection is enabled.

#### **Fabulatech Scanner Redirection**

Fabulatech scanner redirection is enabled.

#### **Fabulatech USB Redirection**

Fabulatech USB redirection is enabled.

**Default rule:** This rule will apply if no special rule was configured for a class or a device.

- Deny
- Allow

#### **Tip**

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

#### Class Rules

Class rules apply to USB device classes and sub-classes.

Managing rules:

Create a new entry

Remove the selected entry

Edit the selected entry

Copy the selected entry

Class rule properties:

#### **Rule:**

- Allow: Devices that have the properties defined here are redirected by the Fabulatech USB Redirection.
- Deny: Devices that have the properties defined here are not redirected.

**Class ID:** Device class



**Subclass ID:** Subclass relating to the specified device class

**Name:** Free text entry

**Override serial:** Serial number that will appear in the session

**Override name:** Device name that will appear in the session

#### Postpone

The USB device is only removed from the system (endpoint device) when the session starts.

The USB device is no longer shown immediately after the system is booted.

This setting is only effective if the **Takeaway** parameter is enabled.

#### Takeaway

The USB device may be removed from the system (endpoint device).

The USB device may not be removed. (Default)

#### No Reset

The device will not be automatically reset after the connection with the session has been terminated.

The device will be reset after the connection with the session has been terminated.

### Device Rules

A device rule applies to a specific device that is identified by its serial number.

Device rule settings:

#### Rule:

- Allow
- Deny

**Vendor ID:** Hexadecimal manufacturer number

**Product ID:** Hexadecimal device number

To find out the **Vendor ID** and **Product ID** of the connected USB device, use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal. You can also use the **System Information** tool, see [Using “System Information” Function](#)(see page 1108).

**Name:** Free text entry

**Override serial:** Serial number that will appear in the session.

**Override name:** Device name that will appear in the session.

#### Postpone

The USB device is only removed from the system (endpoint device) when the session starts.

The USB device is no longer shown immediately after the system is booted.



This setting is only effective if the **Takeaway** parameter is enabled.

#### **Takeaway**

- The USB device may be removed from the system (endpoint device).
- The USB device may not be removed.

#### **No Reset**

- The device will not be automatically reset after the connection with the session has been terminated.
- The device will be reset after the connection with the session has been terminated.

### 3.8.32 AVD Session

Menu path: **Sessions > AVD > AVD Sessions > [Session Name]**

In this area, you can configure desktop integration for the AVD session.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Starting Methods for Session

##### **Start menu**

- The session can be launched from the start menu.

##### **Application Launcher**

- The session can be launched with the Application Launcher.

##### **Desktop**

- The session can be launched with a program launcher on the desktop.

##### **Quick start panel**

- The session can be launched with the quick start panel.

##### **Start menu's system tab**

- The session can be launched with the start menu's system tab.

##### **Application Launcher's system tab**

- The session can be launched with the Application Launcher's system tab.

##### **Desktop context menu**

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.



**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

The session will be launched automatically when the device boots.



### Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

### Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

- 
- [Logon](#)(see page 1020)
  - [Options](#)(see page 1021)
  - [Proxy](#)(see page 1022)
  - [Display](#)(see page 1022)
  - [Printing](#)(see page 1023)
  - [Plugins](#)(see page 1024)
  - [Desktop Integration](#)(see page 1024)

## Logon

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Logon**

**Username@domain or @domain:** A user name or a preset domain name used for the [automatic connection](#)(see page 1021) to the AVD session. The string after "@" is taken as a preset domain name.

Example:

`avd@your.domain.com`: To log in, the user does not need to enter the username and the domain name.

`@your.domain.com`: To log in, the user only needs to enter the username, e.g. `avd`. The preset domain – `your.domain.com` – will automatically be appended.



### Overwriting the Preset Domain Name

Use the following registry key to specify whether the user should be able to overwrite the preset domain, e.g. with `username@other-domain.com`:

| Path     | <b>System &gt; Registry</b>                                                                                                                |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Registry | <code>sessions.wvd%.options.allow-preset-domain-overwrite</code>                                                                           |
| Value    | <code>enabled</code> / <code>disabled</code>                                                                                               |
| Note     | If enabled: the domain entered by the user is accepted.<br>If disabled: the domain entered by the user is replaced with the preset domain. |

**Password:** Password used for the [automatic connection](#)(see page 1021) to the AVD session.

### If the Login Credentials Should Not Be Applied Automatically

You can use the following registry key to always prompt for a user name and password or only for a password when connecting to an AVD session:

| Path      | <b>System &gt; Registry</b>                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------|
| Parameter | <b>Always prompt for username and password upon session host connection</b>                                                      |
| Registry  | <code>sessions.wvd%.options.always-prompt-for-session-username-and-password</code>                                               |
| Value     | <code>enabled</code> / <code>disabled</code>                                                                                     |
| Path      | <b>System &gt; Registry</b>                                                                                                      |
| Parameter | <b>Always prompt for password upon session host connection</b>                                                                   |
| Registry  | <code>sessions.wvd%.options.always-prompt-for-session-password</code>                                                            |
| Value     | <code>enabled</code> / <code>disabled</code>                                                                                     |
| Note      | On the server side, you can enable the RDP group policy "Always prompt for password upon connection" to achieve the same result. |

**Workspace resource to automatically start when connected:** Name of the resource that is to be started automatically.

For an example, see [How to Connect IGEL OS to Azure Virtual Desktop](#)(see page 327).

## Options

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Options**

See also the list of implemented features: [Feature Matrix: AVD \(RDP3\) for IGEL OS 11](#)(see page 324).



### Clipboard redirection

Text and images from the clipboard are shared between the AVD session and the local client.

### Drive redirection

Redirection is bound to the /media folder, so that locally mounted storage devices, including USB sticks, are forwarded to the AVD session. (Default)

### Smartcard redirection

Smartcards are forwarded to the AVD session.

### Exit on last session closed

When the last session window is closed, the entire IGEL AVD Client automatically closes. (Default)

### In-session toolbar

The in-session toolbar is enabled. (Default)

### Audio output redirection

The audio output is redirected between the AVD session and the local client. (Default)

### AAC Codec

The AAC (Advanced Audio Coding) codec used for support of audio output redirection is enabled. (Default)

### Audio input redirection

The audio input (microphone) is redirected between the local client and the AVD session. (Default)

## Proxy

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Proxy**

**Proxy mode:** Specifies if a proxy should be used.

Possible options:

- "Off": A proxy is disabled. The direct connection to the Internet is used.
- "Global HTTP proxy setting": The HTTP proxy configured under **Network > Proxy** is used, see [Proxy](#)(see page 1214).
- "Session specific proxy": The proxy configuration specified under **Proxy host** and **Proxy port** is used.

The following fields are active if **Proxy mode** is set to "Session specific proxy":

**Proxy host:** Hostname or IP address of the proxy server

**Proxy port:** Port on which the proxy service is available

## Display

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Display**

**Window size:** Specifies the width and height of the window.

Possible options:

- "Full-screen": The session is shown on the full screen. The device's taskbar is not visible.



- "Work area": The session is shown on the full screen, minus the area needed by the device's taskbar.
- Numeric details: The session is shown in the selected resolution or on the selected percentage of the screen area.

**Start monitor:** Specifies the monitor on which the session is displayed.

Possible options:

- "No configuration
- "1st monitor"
- "2nd monitor"

**Multimonitor full-screen mode:** This setting is relevant if more than one monitor is connected to the terminal.

Possible options:

- "Global setting": Currently the same as "Multiple monitors".
- "Single monitor": Restricts the full-screen session to one monitor.
- "Multiple monitors
- "Expand to all monitors": Expands the full-screen session across all monitors.

**Scale factor:** Specifies the desktop scaling in percent.

Possible values:

- "Automatic scaleUser Interface > Display > Options > Monitor-DPI is used for the session.
- Numeric details: The display is magnified by the factor given here.

## Printing

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Printing**

- [CUPS Printer Redirection](#)(see page 1023)
- [ezeep by ThinPrint](#)(see page 1024)

### CUPS Printer Redirection

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Printing > CUPS Printer Redirection**

#### CUPS Printer Redirection

CUPS printers configured under **Devices > Printer > CUPS > Printers** are redirected to the AVD session from the local endpoint. To disable/enable a CUPS printer for the AVD session, go to **Devices > Printer > CUPS > Printers > [printer name] > Mapping in sessions > Map printer in AVD sessions**, see [Printers](#)(see page 1217).

- Set the printer driver name under **System > Registry > print.cups.printer%.wvd\_printer\_driver**:
- The default Windows driver name is "Microsoft PS Class Driver"; it is usually installed by default and works generically.
  - In the case of a custom printer driver, make sure the driver is installed on the AVD side and enter the exact name of the driver.



## ezeep by ThinPrint

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Printing > ezeep by ThinPrint**

### Printing with ezeep

- ezeep cloud printing is enabled for the AVD session. To add and enable/disable ezeep printers, go to **Devices > Printer > ThinPrint > Printer**, see [Printer](#)(see page 1225).

ezeep is directly related to the ThinPrint configuration. When the ThinPrint configuration under **Devices > Printer > ThinPrint** is changed, close running AVD sessions and reconnect to make ezeep work again in these sessions.

## Plugins

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Plugins**

### Fabulatech Webcam/Scanner/USB Redirection

- The Fabulatech plugin is active for this session. Please note that the individual redirections enabled by the plugin, i.e. webcam redirection, scanner redirection, and USB redirection are configured system-wide under **Sessions > AVD > AVD Global > Plugins > Fabulatech**; see [Fabulatech](#)(see page 1015).

- The Fabulatech plugin is not active for this session.

### Zoom VDI Media Plugin

- The audio and video streams for Zoom are redirected between the endpoint devices resp. between the endpoint devices and the Zoom server. Audio and video data is not processed by the AVD server.

- The audio and video streams for Zoom are not redirected.

## Desktop Integration

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the AVD session.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

- The session can be launched from the start menu.

### Application Launcher

- The session can be launched with the Application Launcher.

### Desktop



- The session can be launched with a program launcher on the desktop.

#### Quick start panel

- The session can be launched with the quick start panel.

#### Start menu's system tab

- The session can be launched with the start menu's system tab.

#### Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

#### Desktop context menu

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
- [Ctrl] = Ctrl
-  = Mod4



When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

The session will be launched automatically when the device boots.

#### Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

#### Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

### 3.8.33 Amazon WorkSpaces

Menu path: **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces > [Session Name]**

Amazon WorkSpaces is a cloud-native desktop virtualization, which is built on the AWS Cloud and used to provide Windows or Linux desktops. For more information, see <https://aws.amazon.com/workspaces/>.

With the integrated Amazon WorkSpaces Client, you can easily configure Amazon WorkSpaces sessions on IGEL OS.

In this area, you can configure desktop integration for the Amazon WorkSpaces session.

**Session name:** Name for the session.



The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. Ctrl.



Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

### Autostart

The session will be launched automatically when the device boots.

### Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

### Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.



- [Connection Settings](#)(see page 1029)
- [Local Settings](#)(see page 1029)
- [Network Settings](#)(see page 1029)
- [Window](#)(see page 1029)
- [Desktop Integration](#)(see page 1030)

## Connection Settings

Menu path: **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces > [Session Name] > Connection Settings**

**Registration code:** The WorkSpaces registration code which you got from Amazon

**WorkSpace name:** Name of the WorkSpace, e.g. AWS\_TechDOC\_RD

**Keep me logged in**

Login credentials will be saved.

## Local Settings

Menu path: **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces > [Session Name] > Local Settings**

**Log level**

Possible options:

- "Normal logging": Standard logging, which includes info-level details such as runtime events, authorization requests, etc. and is used for informative purposes.
- "Advanced logging": Detailed logging, which includes debug-level details and is used for diagnostic or troubleshooting purposes.
- "Verbose logging": The most detailed logging, which includes trace-level details and is used for very extended diagnostics.

Logs can be found under /var/tmp/awsc#/Amazon Web Services/Amazon WorkSpaces/logs.

## Network Settings

Menu path: **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces > [Session Name] > Network Settings**

**Use proxy**

A proxy will be used.

**Proxy address:** Hostname or IP address of the proxy server

**Proxy port:** Port on which the proxy service is available

## Window

Menu path: **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces > [Session Name] > Window**

**Window size**

Possible options:

- "Window mode": The session is shown in a standard window.



- "Full-screen mode": The entire display area is used for the session.

### **High DPI streaming mode**

The support for high pixel density (high DPI) displays is activated, and the screen resolution of the WorkSpace matches the high DPI resolution of the monitor. Note that this setting may affect the performance. For more information on high DPI mode, see [WorkSpaces high DPI display support](#)<sup>299</sup>.

## Desktop Integration

Menu path: **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces > [Session Name] > Desktop Integration**

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### **Start menu**

The session can be launched from the start menu.

#### **Application Launcher**

The session can be launched with the Application Launcher.

#### **Desktop**

The session can be launched with a program launcher on the desktop.

#### **Quick start panel**

The session can be launched with the quick start panel.

#### **Start menu's system tab**

The session can be launched with the start menu's system tab.

#### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

#### **Desktop context menu**

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

---

<sup>299</sup> [https://docs.aws.amazon.com/workspaces/latest/userguide/high\\_dpi\\_support.html](https://docs.aws.amazon.com/workspaces/latest/userguide/high_dpi_support.html)



**Password protection:** Specifies which password will be requested when launching the session.  
Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. **Ctrl**.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

#### Key: Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

The session will be launched automatically when the device boots.

#### Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.



**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

- For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.
- No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

#### Autostart requires network

- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.

### 3.8.34 deskMate Session

Menu path: **Sessions > deskMate > deskMate Sessions > [Session Name]**

In this area, you can configure desktop integration for the deskMate session.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Starting Methods for Session

##### Start menu

- The session can be launched from the start menu.

##### Application Launcher

- The session can be launched with the Application Launcher.

##### Desktop

- The session can be launched with a program launcher on the desktop.

##### Quick start panel

- The session can be launched with the quick start panel.

##### Start menu's system tab

- The session can be launched with the start menu's system tab.

##### Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

##### Desktop context menu

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.



**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

The session will be launched automatically when the device boots.



## Restart

- The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

- For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

- No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

## Autostart requires network

- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.

- [Provider](#)(see page 1034)
- [Options](#)(see page 1034)
- [Network](#)(see page 1035)
- [Desktop Integration](#)(see page 1035)

## Provider

Menu path: **Sessions > deskMate > deskMate Sessions > [Session Name] > Provider**

**Provider URL:** URL to the deskMate portal, issued by your deskMate provider. Example: <https://example.tocario.com>

**Login email address:** Email address used for logging in to the deskMate session.

## Options

Menu path: **Sessions > deskMate > deskMate Sessions > [Session Name] > Options**

### Full-screen

- The entire display area will be used for the deskMate session.

### Clipboard redirection

- Clipboard data can be shared between a session and the local computer. (Default)

### Display scaling

- Local display of the deskMate session can be resized.

### Adaptive resolution

- The remote desktop resolution will automatically be adjusted in accordance with the local resolution. (Default)

### Enable logging



- Debug logs will be created.

**LogFile destination:** Path to the debug logs generated if **Enable logging** is activated. (Default: /userhome/deskmate.log)

## Network

Menu path: **Sessions > deskMate > deskMate Sessions > [Session Name] > Network**

### Use a proxy server

- An HTTP proxy will be used.

**Proxy host address:** Hostname or IP address of the proxy server

**Proxy host port:** Port on which the proxy service is available

## Desktop Integration

Menu path: **Sessions > deskMate > deskMate Sessions > [Session Name] > Desktop Integration**

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

- The session can be launched from the start menu.

### Application Launcher

- The session can be launched with the Application Launcher.

### Desktop

- The session can be launched with a program launcher on the desktop.

### Quick start panel

- The session can be launched with the quick start panel.

### Start menu's system tab

- The session can be launched with the start menu's system tab.

### Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

### Desktop context menu

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.



**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

The session will be launched automatically when the device boots.



### **Restart**

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

### **Autostart requires network**

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

## 3.8.35 Unified Communications

Menu path: **Sessions > Unified Communications**

- [Zoom Client Selection](#)(see page 1037)
- [Cisco WebEx Meetings VDI Selection](#)(see page 1037)

### Zoom Client Selection

Menu path: **Sessions > Unified Communications > Zoom Client Selection**

**Zoom client version:** Selects the Zoom client version to be used for the Zoom VDI Media Plugin. The Zoom client for the relevant sessions can be activated as follows:

- **Sessions > Citrix > Citrix Global > Unified Communications > VDI Solutions**(see page 795), parameter **Zoom VDI Media Plugin**
- **Sessions > Horizon Client > Horizon Client Global > Unified Communications > VDI Solutions**(see page 860), parameter **Zoom VDI Media Plugin**
- **Sessions > AVD > AVD Sessions > [session name] > Plugins**(see page 1024), parameter **Zoom VDI Media Plugin**

### Cisco WebEx Meetings VDI Selection

Menu path: **Sessions > Unified Communications > Cisco WebEx Meetings VDI Selection**

**Cisco WebEx Meetings client version:** Selects the desired client version to be used for Cisco WebEx Meetings VDI. The Cisco WebEx Meetings client for the relevant sessions can be activated as follows:

- **Sessions > Citrix > Citrix Global > Unified Communications > Cisco**(see page 796), parameter **Cisco WebEx Meetings VDI**
- **Sessions > Horizon Client > Horizon Client Global > Unified Communications > Cisco**(see page 859), parameter **Cisco WebEx Meetings VDI**



## 3.9 Accessories

- [ICA Connection Center](#)(see page 1038)
- [Terminals](#)(see page 1042)
- [Change Smartcard Password](#)(see page 1044)
- [Change Password](#)(see page 1047)
- [Setup](#)(see page 1049)
- [Quick Settings](#)(see page 1053)
- [Display Switch](#)(see page 1055)
- [Application Launcher](#)(see page 1063)
- [Sound Preferences](#)(see page 1066)
- [System Log Viewer](#)(see page 1070)
- [UMS Registration](#)(see page 1073)
- [Touchscreen Calibration](#)(see page 1076)
- [Task Manager](#)(see page 1078)
- [Screenshot Tool](#)(see page 1084)
- [On-Screen Keyboard](#)(see page 1088)
- [Monitor Calibration](#)(see page 1091)
- [Commands](#)(see page 1093)
- [Network Tools](#)(see page 1095)
- [Bluetooth Tool](#)(see page 1100)
- [System Information](#)(see page 1105)
- [Disk Utility](#)(see page 1109)
- [Disk Removal](#)(see page 1112)
- [Mobile Device Access](#)(see page 1114)
- [Firmware Update](#)(see page 1116)
- [Smartcard Personalization](#)(see page 1119)
- [Identify Monitors](#)(see page 1122)
- [Webcam Information](#)(see page 1125)
- [ICG Agent Setup](#)(see page 1127)
- [Licensing](#)(see page 1130)
- [Login Enterprise](#)(see page 1133)
- [Connector ID Key Software](#)(see page 1133)
- [OS 11 Upgrade](#)(see page 1134)
- [Conky System Monitor](#)(see page 1136)

### 3.9.1 ICA Connection Center

Menu path: **Accessories > ICA Connection Center**

With the *Citrix ICA Connection Center*, you are given an overview of the existing connections to *Citrix* servers as well as information regarding connection properties. You can also terminate server connections and log off from *Citrix* servers. For details of how to use the **ICA Connection Center**, see [Using ICA Connection Center](#)(see page 1041).

The settings for starting the function are described below.

**Session name:** Name for the session.



The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. Ctrl.



Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev –event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

## Autostart

The session will be launched automatically when the device boots.

## Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)



- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

- 
- [Using ICA Connection Center](#)(see page 1041)

## Using ICA Connection Center

To obtain an overview of the existing connections to Citrix servers, proceed as follows:

- Start the ICA Connection Center. The start options are described under [ICA Connection Center](#)(see page 1038). All applications are shown in a tree structure with the associated *Citrix* servers.

With the help of the tree structure, you can see which applications run on which servers. If a number of applications run on the same server, this will make the exchanging of data between these applications easier.

To view the properties of a connection to a *Citrix* server, proceed as follows:

1. Start the ICA Connection Center. The start options are described under [ICA Connection Center](#)(see page 1038).
2. Click on the server whose connection properties you want to view.
3. Click on the **Properties** button.  
The connection properties as well as constantly updated information regarding the number of incoming and outgoing bytes and frames will be shown.
4. If you would like to reset the counter for incoming and outgoing bytes to 0, click on **Reset**.

To terminate a server connection, proceed as follows:

1. Start the ICA Connection Center. The start options are described under [ICA Connection Center](#)(see page 1038).
2. Click on the server whose connection you want to terminate.
3. Click on **Terminate**.  
The connection to the server is terminated. The *Citrix* session will be interrupted. The applications will not be terminated on the server. As a result, the application status will be retained until the session is resumed.

To log off from the *Citrix* server, proceed as follows:

1. Start the ICA Connection Center. The start options are described under [ICA Connection Center](#)(see page 1038).
2. Click on the server from which you want to log off.



### 3. Click on **Log off**.

The connection to the server is terminated. The *Citrix* session will end. The applications on the server will be terminated.

## 3.9.2 Terminals

Menu path: **Accessories > Terminals > Local Terminal**

With the local terminal, you can execute local commands on your device. For details of how to use the local terminal, see [Using Local Terminal](#)(see page 1044).

It is also possible to access a local shell without a terminal session: Alternatively, you can switch to the virtual terminals `tty11` and `tty12` by pressing `[Ctrl]+[Alt]+[F11]` or `[Ctrl]+[Alt]+[F12]`. Pressing `[Ctrl]+[Alt]+[F1]` takes you back to the user interface.

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

The session can be launched from the start menu.

#### Application Launcher

The session can be launched with the Application Launcher.

#### Desktop

The session can be launched with a program launcher on the desktop.

#### Quick start panel

The session can be launched with the quick start panel.

#### Start menu's system tab

The session can be launched with the start menu's system tab.

#### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

#### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.



**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

#### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

The session will be launched automatically when the device boots.

#### Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.



**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

- 
- [Using Local Terminal](#)(see page 1044)

## Using Local Terminal

To use the local terminal, proceed as follows:

1. Start the local terminal. The start options are described under [Terminals](#)(see page 1042).
2. Log in as user or root.

If under **Setup > Security > Password**, in the **Administrator** area, the option **Use password** is enabled, you will need to enter the administrator password to access a local terminal as root.

If an administrator password is set, accessing a local terminal as user is only possible if the following two conditions are met:

- Access to local terminals has been activated for user. This is possible with the registry key `system.security.usershell`. The default setting of the registry key forbids terminal access for user.
- Under **Setup > Security > Password**, in the **User** area, the option **Use password** is enabled.

For accessing a local terminal as user, the user password will have to be entered.

You can enter the shell commands supported by IGEL OS.

### 3.9.3 Change Smartcard Password

Menu path: **Accessories > Change Smartcard Password**



With this function, you can change the password for your IGEL smartcard. For details of how to use the function, see [Using "Change smartcard password" Function\(see page 1046\)](#).

Further information regarding the IGEL smartcard can be found under [Authentication with IGEL Smartcard\(see page 485\)](#).

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.



- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

- [Using Change Smartcard Password Function](#)(see page 1046)

### Using Change Smartcard Password Function

With this function, you can change the password for your IGEL smartcard. In order to do this, the **Logon with IGEL smartcard** option must be enabled under **Security > Logon > IGEL Smartcard**.

To change the password for your IGEL smartcard, proceed as follows:

1. Start the **Change Smartcard Password** function. The start options are described under [Change Smartcard Password](#)(see page 1044).
2. Enter the following data in the dialog:
  - **Old smartcard password:** Previous password



- **New smartcard password:** Chosen password
- **Reenter new smartcard password:** Chosen password (entered again)

The password for your IGEL smartcard will be changed.

### 3.9.4 Change Password

Menu path: **Accessories > Change Password**

With this function, the user can change the password or PIN for the login method he used for his current session, provided one of the following login methods was used:

- Active Directory with username and password
- Active Directory with third-party smartcard
- IGEL smartcard
- Local user password

The **Change Password** function starts when the user clicks the password change button in the dialog informing him that a change of password is required. This dialog is presented after login.

For details of how to use the **Change Password** function, see [Using "Change password" function](#)(see page 1049).

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

The session can be launched from the start menu.

#### Application Launcher

The session can be launched with the Application Launcher.

#### Desktop

The session can be launched with a program launcher on the desktop.

#### Quick start panel

The session can be launched with the quick start panel.

#### Start menu's system tab

The session can be launched with the start menu's system tab.

#### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.



### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
- [Ctrl] = Ctrl
-  = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super\_L

**Key:** Key for the hotkey



To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

- [Using Change Password Function](#)(see page 1049)

## Using Change Password Function

To change your password for your current login method (Active Directory with user and password, Active Directory with third-party smartcard, IGEL smartcard, or local user with screenlock password), proceed as follows

1. Start the **Change password** function. The start options are described under [Change password](#)(see page 1047).
  2. Enter the changed password or PIN in the dialog. The dialog differs according to the login method that is currently used.
  3. Click **OK**.
- The password is changed.

## 3.9.5 Setup

Menu path: **Accessories > Setup**

With the IGEL Setup, you can configure your endpoint device. For details of how to allow the user access to the individual areas of the Setup, see [Setup User Permissions](#)(see page 1051). For details of how to change the setup options, see [Options](#)(see page 1053).

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

The session can be launched from the start menu.

#### Application Launcher

The session can be launched with the Application Launcher.

#### Desktop

The session can be launched with a program launcher on the desktop.

#### Quick start panel

The session can be launched with the quick start panel.



### **Start menu's system tab**

The session can be launched with the start menu's system tab.

### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

### **Desktop context menu**

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

### **Hotkey**

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
-  = Ctrl
-  = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super\_L

**Key:** Key for the hotkey



To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

- [Setup User Permissions](#)(see page 1051)
- [Setup Administrator Permissions](#)(see page 1052)
- [Options](#)(see page 1053)

## Setup User Permissions

Define which areas should be visible and/or configurable for the setup user.

If a password was set up for the administrator, the IGEL Setup can only be opened with administrator rights, i.e., after entering the password (see [Password](#)(see page 1236)). However, individual areas of the setup can be enabled for the user, e.g. to allow them to change the system language or configure a left-handed mouse.

To enable setup pages for the user, proceed as follows:

1. Here, enable those areas to which the user is to have access.

Possible settings:

| <b>Node</b> | <b>Setup Page</b> |
|-------------|-------------------|
| not visible | not visible       |
| visible     | not visible       |
| visible     | configurable      |

This is an example of possible settings:

The screenshot shows a tree view of setup categories. The 'User Interface' category is expanded, revealing its sub-categories: 'Display', 'Desktop', 'Language', 'Screen Lock/Saver', 'Input', 'Keyboard', 'Additional keyboard layouts', 'Mouse', and 'Touchpad'. The 'Keyboard', 'Mouse', and 'Touchpad' items under 'Input' have their checkboxes checked, while others are unchecked.



If you enable a setup page on the lower levels, the node points required for access will automatically be marked as visible (but blocked for editing purposes).

2. Under **Security > Password**, enable the password for the **administrator** and the **setup user**.

If users are to be allowed to edit parts of the setup even without a password, create a [quick setup](#)(see page 773) session, the password for the **setup user** will not be enabled in this case.

## Setup Administrator Permissions

Configure which area should be visible for the setup administrator.

If a password was set up for the administrator, the IGEL Setup can only be opened with administrator rights, i.e., after entering the password (see [Password](#)(see page 1236)). However, individual areas of the setup can be enabled for the setup administrator.

To enable setup pages for the setup administrator, proceed as follows:

1. Here, enable those areas to which the setup administrator is to have access.

Possible settings:

|  | <b>Node</b> | <b>Setup Page</b> |
|--|-------------|-------------------|
|  | not visible | not visible       |
|  | visible     | not visible       |
|  | visible     | configurable      |

If you enable a setup page on the lower levels, the node points required for access will automatically be marked as visible (but blocked for editing purposes).

2. Under **Security > Password**, enable the password for the **administrator** and the **setup administrator**.

If administrators are to be allowed to edit parts of the setup even without a password, create a [quick setup](#)(see page 773) session, the password for the **setup administrator** will not be enabled in this case.



## Options

Menu path: **Accessories > Setup > Options**

You can configure the display of tooltips in the setup.

### Enable Tooltips

- When the mouse pointer is placed over a parameter, the associated tooltip will be shown after the set **delay**.
- No tooltip will be shown.

**Tooltip Delay:** Time interval in tenths of a second during which the mouse pointer must be placed over a parameter for the tooltip to be shown.

## 3.9.6 Quick Settings

Menu path: **Accessories > Quick Settings**

With the IGEL Setup, you can allow the user access to individual areas of the Setup. Instructions can be found under [Setup User Permissions](#)(see page 1051).

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

- The session can be launched from the start menu.

#### Application Launcher

- The session can be launched with the Application Launcher.

#### Desktop

- The session can be launched with a program launcher on the desktop.

#### Quick start panel

- The session can be launched with the quick start panel.

#### Start menu's system tab

- The session can be launched with the start menu's system tab.

#### Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

#### Desktop context menu

- The session can be launched with the desktop context menu.



**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. **Ctrl**.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

### Key: Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)



- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

- [Setup User Permissions](#)(see page 1055)

## Setup User Permissions

Menu path: **Accessories > Quick Settings > Setup User Permissions**

Define which setup pages are visible to users.

You will find instructions for this function under [Setup User Permissions](#)(see page 1051).

## 3.9.7 Display Switch

Menu path: **Accessories > Display Switch**

With this function, you can configure the display on several screens. For details of how to set the function, see [Options](#)(see page 1057). For details of how to use the function, see [Using "Display Switch" Function](#)(see page 1061).

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab



- The session can be launched with the Application Launcher's system tab.

#### Desktop context menu

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey



To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

### **Autostart**

- The session will be launched automatically when the device boots.

### **Restart**

- The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode\(see page 869\)](#).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

- 
- [Options\(see page 1057\)](#)
  - [Minimal Dialog\(see page 1059\)](#)
  - [Advanced Dialog\(see page 1060\)](#)
  - [Using Display Switch\(see page 1061\)](#)

## Options

Menu path: **Accessories > Display Switch > Options**

You can change the way the **Display Switch** function behaves.

### **Dialog type**

Possible values:

- Minimal dialog: The **Display Switch** function starts with the simple dialog.
- Advanced dialog: The **Display Switch** function starts with the advanced dialog.



### Smart display configuration

- Every configuration of your monitors will be saved.
- Monitor configurations will not be saved.

### Preserve settings over reboot

- The settings for the **Display Switch** function will be preserved over a reboot.
- The settings for the **Display Switch** function will be reset to the default settings in the event of a reboot. (Default)

### Configure new displays when connected

- The **Display Switch** function starts as soon as new screens are connected. You can then configure the new screens.
- The **Display Switch** function does not start automatically when new screens are connected. (Default)

### Options in Minimal Dialog

#### Mirror displays

- The **Mirror screens** option is shown in the minimal dialog. (Default)
- The option is not shown in the minimal dialog.

#### Extend to the left

- The **Extend to the left** option is shown in the minimal dialog. (Default)
- The option is not shown in the minimal dialog.

#### Extend to the right

- The **Extend to the right** option is shown in the minimal dialog. (Default)
- The option is not shown in the minimal dialog.

#### Rotate displays (Page orientation)

- The **Rotate displays (Page orientation)** option is shown in the minimal dialog.
- The option is not shown in the minimal dialog. (Default)

#### Mouse options

- The **Left-handed mouse**, **Pointer speed** and **Double click interval** settings are shown.
- The mouse settings are not shown. (Default)

#### Advanced

- The **Advanced** button is shown. With **Advanced**, you can switch to the advanced dialog. (Default)
- The **Advanced** button is not shown.

#### Reset

- The **Reset** button is shown. With **Reset**, you can restore the default settings. (Default)
- The **Reset** button is not shown.

**Timeout for confirmation dialog:** Specifies how long a dialog for confirming the configuration should be shown. (Default: 10 seconds)

For more information, see the manual chapters

- [Minimal Dialog](#)(see page 1059)
- [Advanced Dialog](#)(see page 1060)
- [Using Display Switch](#)(see page 1061)

or the how-to [Display Switch](#)(see page 513).

## Minimal Dialog

| Selection                                                                           | Function                                                             |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------|
|    | Uses only display 1.                                                 |
|   | Shows the same content on all screens, i.e. clone mode or mirroring. |
|  | Extends the display area to the screen on the right.                 |
|  | Extends the display area to the screen on the left                   |
|  | Uses only display 2.                                                 |
|  | Rotates the selected display to the left or to the right.            |

**Identify Displays:** Starts the monitor detection.

**Advanced:** Switches to **Advanced** mode of display configuration.

**Reset:** Restores the default settings.



**Close:** Closes the **IGEL Display Switch** window.

#### Mouse options

- **Lefthand Mode**

Lefthand mode is active.

Righthand mode is active. (Default)

- **Pointer speed:** Value for the mouse speed in percentage between 1 (slow) and 100 (fast). (Default: 50)

- **Double click:** Maximum interval in milliseconds between two mouse clicks to still be recognized as a double-click. (Default: 300)

For more information, see [Using Display Switch](#)(see page 1061) and [Display Switch](#)(see page 513).

#### Advanced Dialog

You can access the advanced settings by clicking **Advanced** in the minimal dialog.

Advanced settings (pan/scale/resolution) can be configured in a collapsible area on the right. To enlarge the **Advanced** modes window, click the arrow on the right side of the window.

The following parameters must be activated for the **Display Switch** function to be able to save the settings:

- **Display Switch > Options > Preserve settings over reboot**
- **Display Switch > Options > Smart display configuration**

In the collapsible area:

- **Use this display**

Enables the selected display.  
 Disables the selected display.

- **Index:** Give the selected display an order number.

- **Rotation:** Rotation of selected display

Possible values:

- None
- Left
- Inverted
- Right

- **Resolution:** Select the resolution of the selected display. (Default: Automatic)

- **Refresh rate:** Depends on the resolution (Default: Automatic)

- **Panning:** Set up a virtual screen that is larger than your physical screen. It will look like an enlarged screen. By moving the mouse to the edge of the screen, hidden parts become visible. (Default: None)

- **Reflection:** Transforms the display as if being reflected by a mirror.

Possible values:

- None
- Horizontal
- Vertical
- Horizontal and Vertical



- **Scale from:** A software variant of the resolution. This can be useful if you need a resolution that is not available on the hardware. (Default: None)

For more information, see the articles [Using Display Switch\(see page 1061\)](#) and [Display Switch\(see page 513\)](#).

## Using Display Switch

The function **Display Switch** has been extended with IGEL OS 11.01.100. It is now possible to use several different profiles, which are automatically selected at runtime depending on the currently connected monitors. A profile is created when the current monitor layout, or the current resolution, is configured via **Display Switch**. The profile is automatically assigned to the currently connected monitors and recognizes the manufacturer, model by plug and, if available, the status of the laptop cover. When the screen configuration changes (by hot (un)plugging), the system will automatically switch to the profile. The **Display Switch** function has been redesigned in IGEL OS 11.01.100 with a new graphical user interface. All basic functions can be configured by drag-and-drop.

- ▶ Start the **Display Switch** function. The start options are described under [Display Switch\(see page 1055\)](#).

### Identify Displays

- ▶ To start screen detection, click on **Identify Displays**

The names and properties of the screens will be detected. The connection, the assigned number (**1** = main screen) and the name will be shown on each screen. Example: **1: DVI-D(II): Samsung 24"**

### Defining Main Screen

1. If necessary, switch to the advanced dialog with **Advanced**.
  2. Select the screen that you wish to define as the main screen.
  3. Set the **Index** to **1**.
- The display is now marked as the main screen.

### Split Display over Several Screens

You have various options for using several screens. In the dialog, the connection, the assigned number (**1** = main screen) and the name is shown for each screen. Example: **1: DVI-D(II): Samsung 24"**

The procedure with the minimal dialog is described below. To switch from the advanced to the minimal dialog, click on **Simple**.

- ▶ To show the same content on all screens (Shadow screens), click on  .
- ▶ If you would like to expand the display to all screens and the other screens are to the left of the main screen, click on  .
- ▶ If you would like to expand the display to all screens and the other screens are to the right of the main screen, click on  .

From IGEL OS 11.01.100, a drag-and-drop interface is available for individual customization. Click **Advanced** to show the drag-and-drop interface:



- ▶ Use drag-and-drop to move the displays to the desired configuration. They will snap together when they touch each other at the edge.
- ▶ If you no longer need a monitor, in **Advanced** mode you can simply drag it to the upper right corner to the **Disabled** area to disable it.
- ▶ To display the same content on multiple displays, drag them one on top the other. **Mirror \<other>** will be displayed. The mirroring monitor is displayed in the lower right corner.
- ▶ Click **Apply** to set the current status. Click **Yes** in the **Keep Configuration** window to save the configuration permanently and associate it with the profile.

#### Rotate Displays (Page Orientation)

The procedure with the minimal dialog is described below; **Setup > Accessories > Display Switch > Options > Rotate displays (Page orientation)** must be enabled. To switch from the advanced to the minimal dialog, click on **Basic**.

- ▶ To rotate the display counterclockwise, click on .
- ▶ To rotate the display clockwise, click on .

#### Change Mouse Settings

The procedure with the minimal dialog is described below; **Setup > Accessories > Display Switch > Options > Mouse Options** must be enabled. To switch from the advanced to the minimal dialog, click on **Simple**.

- ▶ To adjust the mouse for left-handed users, enable the **Lefthanded Mode**.
- ▶ To adjust the speed of the mouse pointer, change the value under **Pointer speed**. The higher the value, the further the mouse pointer will move when the mouse is moved.
- ▶ To change the time interval within which two consecutive mouse clicks are recognized as a double-click, change the number of milliseconds under **Double click interval**.

#### Zoom Display (Screen Magnifying Glass)

You can magnify the screen content. The effect is the same as with the screen magnifying glass in Microsoft Windows: All text and graphics are magnified by the same factor; this results in a virtual display area which is bigger than the monitor's available display area. The user therefore sees a magnified section of the entire screen; the section can be moved by moving the mouse to the edge of the screen.

1. If necessary, switch to the advanced dialog with **Advanced**.
  2. Under **Panning**, set the desired value. Example: 3860x2160
  3. Under **Resolution**, set a low value. This value simulates the actual resolution of the screen.  
Example: 1280x800
  4. Click on **Apply**.
- The screen content will be magnified. The magnification factor results from the ratio of the virtual resolution and the simulated actual resolution.



If the same content is displayed on a number of screens (Shadow screens), all screens will show the same section. However, you can set a different magnification level for each of the screens.

## Change Refresh Rate

This is only possible if a resolution has been selected. The respective resolutions can be different. A refresh rate of 60 Hz is usually suitable for standard screens.

1. If necessary, switch to the advanced dialog with **Advanced**.
2. Under **Refresh rate**, set the desired value.

## Restore Default Settings

- Click on **Reset** to restore the default settings.

For more information, see the article [Display Switch](#)(see page 513).

### 3.9.8 Application Launcher

Menu path: **Accessories > Application Launcher**

With the Application Launcher, you can launch predefined sessions and device functions/tools. You are also given information regarding the device and the licenses used.

Further information can be found under [Application Launcher](#)(see page 768).

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel



- The session can be launched with the quick start panel.

#### Start menu's system tab

- The session can be launched with the start menu's system tab.

#### Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

#### Desktop context menu

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. **Ctrl**.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
-  = Ctrl
-  = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

-  = Alt



Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

- The session will be launched automatically when the device boots.

#### Restart

- The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

- For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

- No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

- The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

- The session cannot be started in appliance mode.

- [Application Launcher Configuration](#)(see page 1065)

## Application Launcher Configuration

Menu path: **Setup > Accessories > Application Launcher > Application Launcher Configuration**

You can hide individual areas and elements of the Application Launcher.

- **Hide system page**



- The button for displaying the system tools (accessories) will not be shown.



- The  button for displaying the system tools (accessories) will be shown. (default)
- **Hide reboot button**
  - The  button for restarting the thin client will not be shown.
  - The  button for restarting the thin client will be shown. (default)
- **Hide shut down button**
  - The  button for shutting down the thin client will not be shown.
  - The  button for shutting down the thin client will be shown. (default)
- **Show current user name in about, application launcher and startmenu**
  - The current user will be shown at the top edge of the relevant window.
  - The current user will not be shown.

In order for user names to be recognized and passed on, you must configure two settings beforehand:

- Enable Active Directory/Kerberos: **Security > Active Directory/Kerberos**
- Enable local logon: **Security > Logon > Active Directory/Kerberos**

- **Single click mode:**

- Sessions are started with a single-click. This option was set up specially for users of touchscreen monitors.
- Sessions are started with a double-click. (default)

### 3.9.9 Sound Preferences

Menu path: **Accessories > Sound Preferences**

With this function, you can configure your device's audio system. For details of how to change the presets for the audio system, see [Options\(see page 1069\)](#). For details of how to use the function, see [Using "Sound Preferences" Function\(see page 1070\)](#).

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Starting Methods for Session

##### Start menu

- The session can be launched from the start menu.

##### Application Launcher



- The session can be launched with the Application Launcher.

#### Desktop

- The session can be launched with a program launcher on the desktop.

#### Quick start panel

- The session can be launched with the quick start panel.

#### Start menu's system tab

- The session can be launched with the start menu's system tab.

#### Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

#### Desktop context menu

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol / combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. **Ctrl**.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
- [Ctrl] = Ctrl
-  = Mod4



When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

The session will be launched automatically when the device boots.

#### Restart

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

- 
- [Options](#)(see page 1069)
  - [Using Sound Preferences Function](#)(see page 1070)



## Options

Menu path: **Accessories > Sound Preferences > Options**

With this function, you can change presets for the audio system. The settings can be changed at any time via the "Sound Preferences" function; see [Using "Sound Preferences" function\(see page 1070\)](#).

### Show volume control in taskbar

- The  button is shown in the taskbar. When the user clicks on this button, the volume control will be shown. (Default)
- The  button will not be shown. The user must start the Audio Settings function to change the volume. Further information can be found under [Using "Sound preferences" function\(see page 1066\)](#).

### Remote volume settings

- The settings for the parameters **Mute**, **PCM volume**, **Input mute**, and **Input volume** are restored after each system restart.
- The last settings set by the user will remain after the next system start. (Default)

#### Mute

- Audio playback is off.
- Audio playback is on. (Default)

**PCM volume:** Preset volume in percent (default: 50)

#### Input mute

- The audio input is muted. Sounds from a microphone that are recorded are not transferred via the thin client.
- The audio input is switched on. Sounds from a microphone that are recorded can be transferred via the thin client. (Default)

**Input volume:** Volume in percent at which sounds at the audio input are recorded, for example from a microphone. (Default: 100)

## Default Sound Output

### Port name

Possible options:

- Automatic: The audio output is automatically assigned to a device. The following order applies here:
  1. USB devices
  2. PCI devices; this also includes the HDMI interface.
  3. Internal speaker
 Not connected ports will be ignored.
- HDMI / DisplayPort
- Speaker
- Headset

**Device name:** Select the device for audio output from a list of available devices. If the device is not present at the moment, you can type its name in. Examples: "Built-in Audio Analog Stereo", "Microsoft LifeChat LX-3000".



## Default Sound Input

### Port name

Possible options:

- Automatic: The audio input is automatically assigned to a device. The following order applies here:
  1. USB devices
  2. PCI devices
 Not connected ports will be ignored.
- Microphone
- Headset microphone

**Device name:** Select the device for audio input from a list of available devices. If the device is not present at the moment, you can type its name in. Example: "Microsoft LifeChat LX-3000".

## Using Sound Preferences Function

- Start the **Sound Preferences** function. The start options are described under [Sound Preferences\(see page 1066\)](#).

To change the playback volume, proceed as follows:

- Move the playback volume slider to the right to increase the volume or to the left to reduce the volume.

To select and configure the device for playback, proceed as follows:

1. Click on the **Output** tab.
2. Under **Play sound through**, select the device which is to be used for playback.
3. If necessary, adjust the **Balance**, **Fade** and **Subwoofer** settings.

To select and configure the device for recording, proceed as follows:

1. Click on the **Input** tab.
2. Under **Record sound from**, select the device which is to be used for recording.
3. Adjust the **Input volume** if necessary.

To change the playback volume for specific applications, proceed as follows:

1. Click on the **Applications** tab.
2. Adjust the volume control for the relevant application.

## 3.9.10 System Log Viewer

Menu path: **Accessories > System Log Viewer**

With this function, you can view your device's system logs. For details of how to add additional logs to the logs shown by default, see [Options\(see page 1073\)](#). For details of how to use the function, see [Using "System Log Viewer" function\(see page 1073\)](#).

The settings for starting the function are described below.



**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".



These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

The session will be launched automatically when the device boots.

#### Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.



- [Options\(see page 1073\)](#)
- [Using System Log Viewer Function\(see page 1073\)](#)

## Options

Menu path: **Setup > Accessories > System Log Viewer > Options**

Here, you can add additional files to the files shown by default. The **System Log Viewer** function shows the following files by default:

- /config/Xserver/card0
- /config/Xserver/xorg.conf-0
- /config/sound/card0
- /config/sound/card1
- /config/sound/default\_card\_name
- /var/log/Xorg.0.log

To add a further file to the display, proceed as follows:

1. Click on **[+]**.
2. In the **Add** dialog, enter the path and the file name of the desired file. Example: /var/log/igfmount.log

If you want to add several files, you can also use the asterisk \*. Example: /var/log/\*.log or /var/log/\*.txt

3. Click **OK**.

When the **System Log Viewer** function is started, the file that you have added will be shown.

## Using System Log Viewer Function

1. Start the **System Log Viewer** function. The start options are described under [System Log Viewer\(see page 1070\)](#).
2. In the left-hand column, select the file that you want to view.  
The selected file will be shown in the right-hand column.

### 3.9.11 UMS Registration

Menu path: **Accessories > UMS Registration**

With this function, you can register your endpoint device in the *UMS (IGEL Universal Management Suite)* locally. For details of how to use the function, see [Using "UMS Registration" Function\(see page 1075\)](#).

The settings for starting the function are described below.

**Session name:** Name for the session.



The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. Ctrl.



Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

- Using UMS Registration Function(see page 1075)

## Using UMS Registration Function

Menu path: **Accessories > UMS Registration**

1. Start the **UMS Registration** function. The start options are described under [UMS Registration\(see page 1073\)](#).
2. Enter the following data:
  - **Server address:** IP address or host name and port number of the UMS Server if it is not the default port. Example: IP address : 30002
  - **Login:** User name for logging in to the UMS Console.
  - **Password:** Password for logging in to the UMS Console.



Any UMS user with sufficient rights can be specified under **Login** and **Password**.

Example:

If a device has to be registered in the root folder "Devices", "scan for devices" permission will suffice.

If a device has to be registered in a particular folder, the user must also have the "move" permission for this folder.

- **Structure Tag:** Character string for assigning the device to a specific UMS directory.
  - **New host name:** Name under which the device is registered in the UMS. This name will also be displayed under **Network > LAN Interfaces > Terminal name**.
3. If you want to assign a specific UMS directory to the device, click on **Select** under **Directory** and select the desired directory from the list.
  4. Click on **Register**.

### 3.9.12 Touchscreen Calibration

Menu path: **Accessories > Touchscreen Calibration**

With this function, you can calibrate the touchscreen connected to your endpoint device. For details of how to use the function, see [Using “Touchscreen Calibration” function](#)(see page 1078).

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

The session can be launched from the start menu.

#### Application Launcher

The session can be launched with the Application Launcher.

#### Desktop

The session can be launched with a program launcher on the desktop.

#### Quick start panel

The session can be launched with the quick start panel.

#### Start menu's system tab

The session can be launched with the start menu's system tab.

#### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.



### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
- [Ctrl] = Ctrl
-  = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super\_L

**Key:** Key for the hotkey



To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

### **Autostart**

- The session will be launched automatically when the device boots.

### **Restart**

- The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

- 
- [Using Touchscreen Calibration](#)(see page 1078)

### Using Touchscreen Calibration

- Ensure that **Enable touchscreen** is enabled under **User Interface > Input > Touchscreen**.

You will find a description of the touchscreen calibration procedure in the [Touchscreen Calibration](#)(see page 625) how-to.

### 3.9.13 Task Manager

Menu path: **Accessories > Task Manager**



This function provides an overview of the applications and other processes running on the device. You can also pause or end processes and change the priority of processes. For details of how to use the Task Manager, see [Using Task Manager](#)(see page 1081).

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.



## Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

## Autostart

The session will be launched automatically when the device boots.

## Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.



**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

- 
- [Using Task Manager](#)(see page 1081)

## Using Task Manager

With the Task Manager, you can observe and influence applications and processes in the following ways:

- Determining thin client processor usage
- Determining thin client memory usage
- Determining processor usage by a specific application
- Determining memory usage by a specific application
- Pausing and continuing an application
- Closing an application
- Force closing an application
- Changing the priority of an application

► Launch the **Task Manager** function. The launch options are described under [Task Manager](#)(see page 1078).

To determine the thin client's total processor usage, proceed as follows:

► Read the percentage value under **CPU**:



To determine the thin client's total memory usage, proceed as follows:

► Read the percentage value under **RAM**:



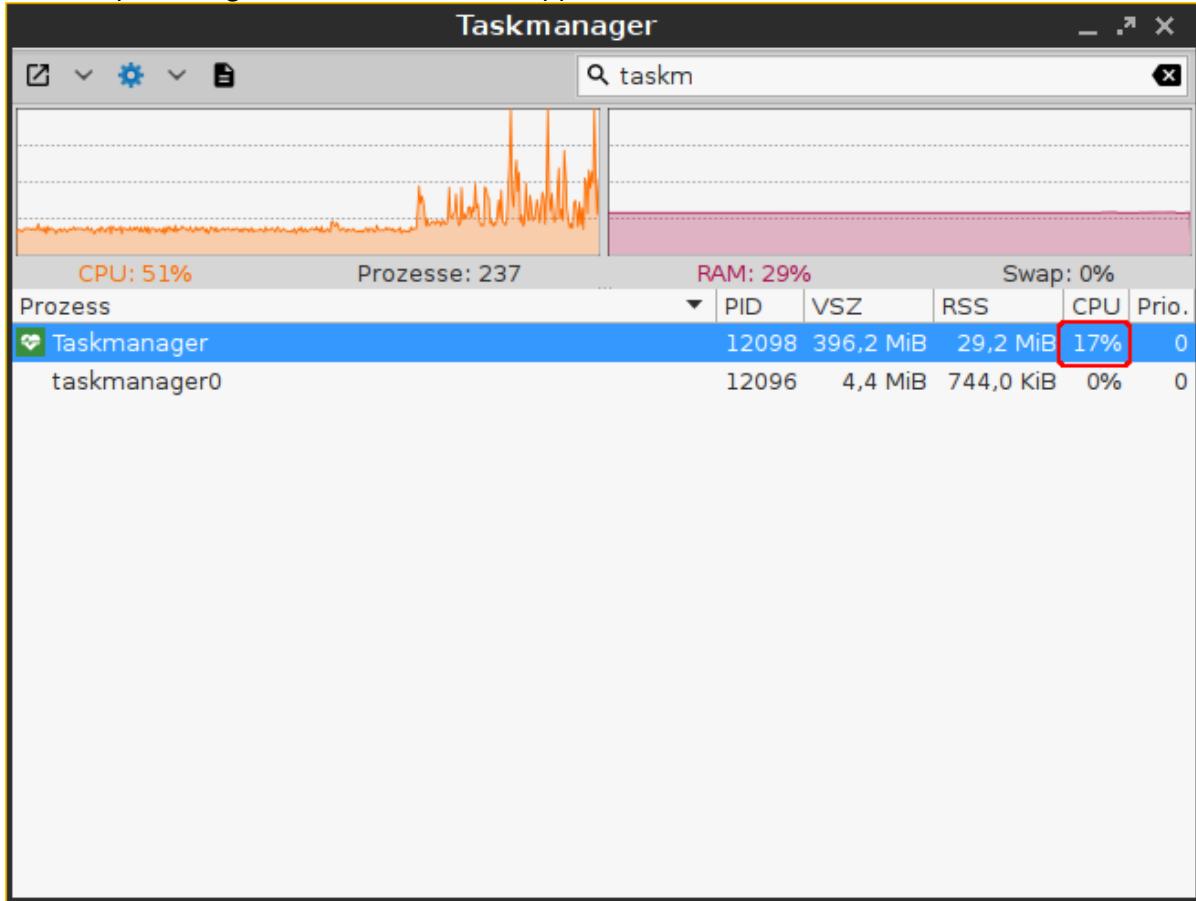
► To calculate the value in bytes, click on and enable the option **Show memory usage in bytes**.

To determine the extent to which a specific application contributes to processor usage, proceed as follows:

1. In the search window, enter the name of the application or part of the name.  
The Task Manager will now show only the relevant applications and processes.

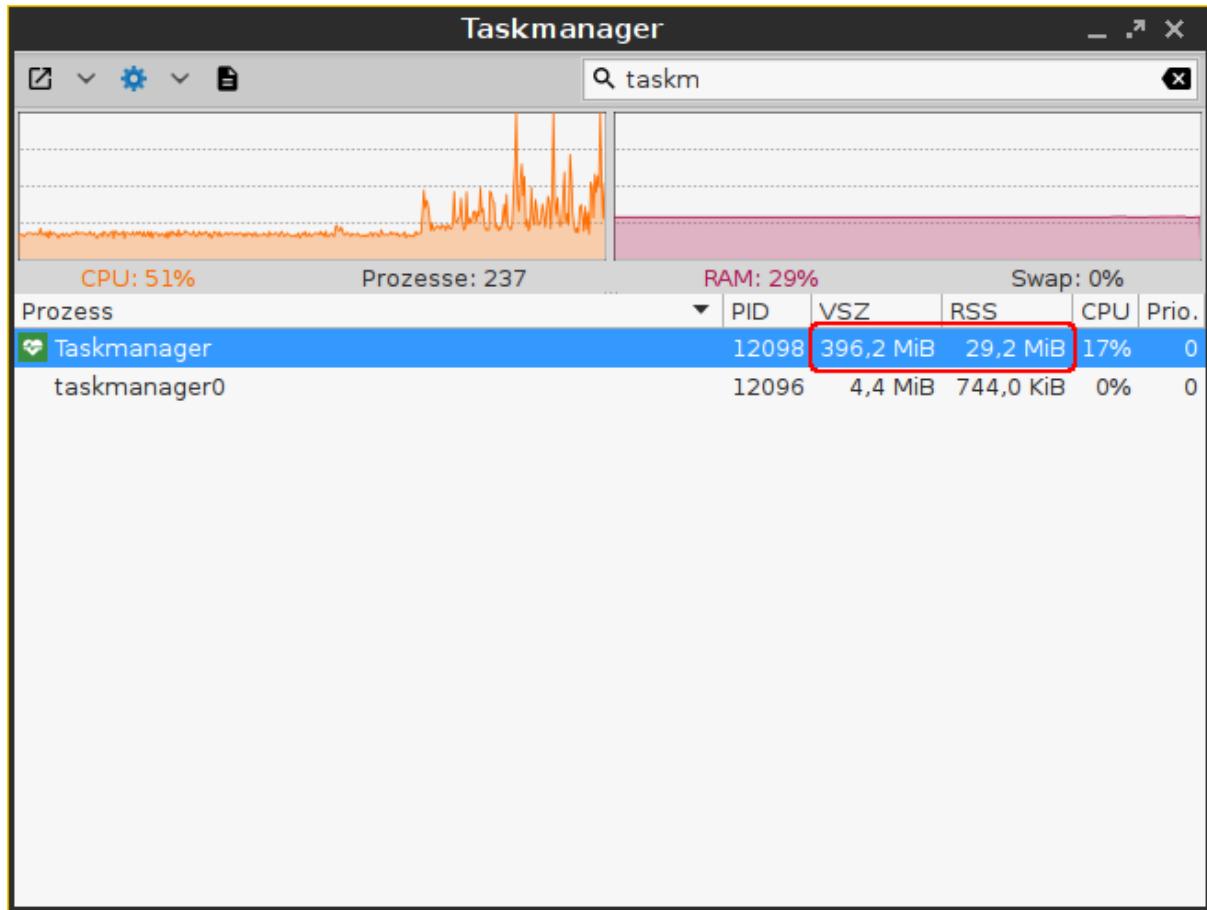


2. Read the percentage value for the relevant application in the **CPU** column.



To determine the extent to which a specific application contributes to memory usage, proceed as follows:

1. Click next to on and ensure that **Virtual Bytes** and **Private Bytes** are enabled.
2. In the search window, enter the name of the application or part of the name.  
The Task Manager will now show only the relevant applications and processes.
3. Read the values in the **VSZ** and **RSS** columns.  
The **VSZ** column shows how much memory is available for the application. The **RSS** column shows how much memory the application is currently using.



To pause an application, proceed as follows:

1. Highlight the application.
2. Open the application's context menu by right-clicking on it and select **Pause**.  
The application will be paused (Signal SIGSTOP). You can then continue the application.

To continue an application, proceed as follows:

1. Highlight the application.
2. Open the application's context menu by right-clicking on it and select **Continue**.  
The application will continue (Signal SIGCONT).

To close an application, proceed as follows:

1. Highlight the application.
2. Open the application's context menu by right-clicking on it and select **Close**.  
The application will close (Signal SIGTERM).



In this case, the application is instructed to close by the operating system. If the application does not react to this instruction, you can force it to close with the **Kill** command.

To force an application to close, proceed as follows:

1. Highlight the application.
2. Open the application's context menu by right-clicking on it and select **Kill**.  
The application will be forced to close (Signal SIGKILL).

To change the priority of an application, proceed as follows:

1. Highlight the application.
2. Open the application's context menu by right-clicking on it and select **Priority**.
3. Select one of the following values for the priority:

As a normal user, you can only change the priority from a higher value to a lower value. Example: If you have changed the priority from "Normal" to "Low", you can only then change it to "Very low" – you can no longer change it back to "Normal". The administrator can increase the priority.

The priority corresponds to the nice value. High values result in a low priority, while low values result in a high priority.

- **Very low** (nice value: 15)
- **Low** (nice value: 5)
- **Normal** (nice value: 0)
- **High** (nice value: -5). This value can only be set by the administrator.
- **Very high** (nice value: -15) This value can only be set by the administrator.

### 3.9.14 Screenshot Tool

Menu path: **Accessories > Screenshot Tool**

With this function, you can take a screenshot. For details of how to use the function, see [Using “Screenshot Tool” \(see page 1087\)](#).

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )



## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".



These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with | :

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

The session will be launched automatically when the device boots.

#### Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)



- The session cannot be started in appliance mode.

## Special Hotkeys

With the hotkeys defined under **User Interface > Hotkeys > Commands**, you can use the function as follows:

- **Screenshot of the active window:** This hotkey takes a screenshot of the window currently active.
- **Screenshot of the entire screen:** This hotkey takes a screenshot of the entire screen.

- 
- [Using Screenshot Tool](#)(see page 1087)

## Using Screenshot Tool

1. Launch the **Screenshot Tool** function. The launch options are described under [Screenshot Tool](#)(see page 1084).
2. Select the **area** you would like to photograph. You have the following options:

If you start the function via **User Interface > Hotkeys > Commands > Screenshot of active window** or **User Interface > Hotkeys > Commands > Screenshot of entire screen**, no options will be shown.

- **Entire screen**  
     The entire screen content will be photographed.
- **Active window**  
     The window that is currently active will be photographed.
- **Select a region**  
     You can select a section of the screen using the mouse.
- **Capture mouse pointer**  
     The mouse pointer is visible on the screenshot.

3. Specify the **Delay before capturing** in seconds. The minimum value is 1.
4. Click on **OK**.

If you have enabled **Entire screen** or **Active window**, the screenshot will be taken after the **Delay before capturing** has elapsed.

If you have enabled **Select a region**, you can select the desired part of the screen using the mouse. To do this, press and hold the left mouse button while dragging the mouse across the screen.

5. Specify how the screenshot is to be used. You have the following options:
  - **Save:** If this option is enabled, the screenshot will be saved in PNG format via your thin client. You can save the screenshot locally, on a network drive or on a USB mass storage device.
  - **Copy to the clipboard:** If this option is enabled, the screenshot will be available in the thin client's local cache. You can access the local cache from an RDP session and open the image in an RDP session application.
  - **Open with:** If this option is enabled, the screenshot will be opened in your thin client's image viewer as soon as it is taken.



### 3.9.15 On-Screen Keyboard

Menu path: **Accessories > On-Screen Keyboard**

This function shows an on-screen keyboard on the desktop.

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Starting Methods for Session

##### **Start menu**

The session can be launched from the start menu.

##### **Application Launcher**

The session can be launched with the Application Launcher.

##### **Desktop**

The session can be launched with a program launcher on the desktop.

##### **Quick start panel**

The session can be launched with the quick start panel.

##### **Start menu's system tab**

The session can be launched with the start menu's system tab.

##### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

##### **Desktop context menu**

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.



- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### **Autostart**

The session will be launched automatically when the device boots.

#### **Restart**

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode\(see page 869\)](#).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

- [Appearance\(see page 1089\)](#)
- [Application Integration\(see page 1090\)](#)

## Appearance

Menu path: **Accessories > On-Screen Keyboard > Appearance**

- **Show Function Keys**  
 The on-screen keyboard features the function keys [F1] ... [F12]. (default)
- **Show Navigation Keys**  
 The on-screen keyboard features the arrow keys for navigating on the screen. (default)
- **Show Numpad**  
 The on-screen keyboard features the number block.  
 The on-screen keyboard does not feature the number block. (default)
- **Enable switching to alternative layout**



This option is available from IGEL Linux version 10.04.100 onwards.

- The on-screen keyboard has an additional key by which the user can toggle between the normal layout and a reduced layout. The reduced layout resembles the numpad, with the following differences:
- Additional backspace key [←]
  - Additional tab key [→]
  - Additional space key [ ]
  - Additional escape key [Esc]
  - Return key [↵] instead of [Enter] key
- Switching to the reduced layout is not possible. (default)

## Application Integration

### Taskbar settings for the login dialog

These settings are relevant if a login is necessary in order to use the device. This applies to all logon methods that are possible with the device.

#### Show on-screen keyboard button

- A button for launching the on-screen keyboard will be shown during the login dialog.
- The on-screen keyboard cannot be launched during the login dialog. (Default)

#### Start on-screen keyboard automatically

- The on-screen keyboard is shown during the login dialog. The on-screen keyboard can be used for input in the logon dialog.
- The on-screen keyboard is not shown during the login dialog. However, it can be launched via a button if **Show on-screen keyboard button** is enabled. (Default)

### Taskbar settings when the screenlock is active

#### Show on-screen keyboard button

- If the screen is locked, a button for launching the on-screen keyboard will be shown.
- If the screen is locked, the on-screen keyboard cannot be launched. (Default)

#### Start on-screen keyboard automatically

- If the screen is locked, the on-screen keyboard will be shown.
- If the screen is locked, the on-screen keyboard will not be shown. However, it can be launched via a button if **Show on-screen keyboard button** is enabled. (Default)

### On-Screen Keyboard Toggle Button

#### Show button

- A button for switching the on-screen keyboard on and off will be shown on the desktop.



- The button will not be shown. (Default)

**Touch and hold delay:** Time in milliseconds, after which the button reacts to movement. (Default: 1000 ms)

**Button size:** A size between 40 and 80 pixels can be chosen. (Default: 60px)

#### **Automatically show on-screen keyboard when text field is selected**

- The on-screen keyboard is shown automatically when an input field gets the focus.
- The on-screen keyboard is not shown automatically.

For further information, see [Configuring the Automatic Appearance of on-screen software keyboard](#)(see page 526).

### 3.9.16 Monitor Calibration

Menu path: **Accessories > Monitor Calibration**

With this function, you can calibrate the monitor connected to your endpoint device.

A test image which you can modify using the arrow keys will appear. Using this test image, you can automatically or manually recalibrate your screen. This applies to old, analog monitors in particular. New monitors calibrate themselves.

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Starting Methods for Session

##### **Start menu**

- The session can be launched from the start menu.

##### **Application Launcher**

- The session can be launched with the Application Launcher.

##### **Desktop**

- The session can be launched with a program launcher on the desktop.

##### **Quick start panel**

- The session can be launched with the quick start panel.

##### **Start menu's system tab**

- The session can be launched with the start menu's system tab.

##### **Application Launcher's system tab**

- The session can be launched with the Application Launcher's system tab.



### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
- [Ctrl] = Ctrl
-  = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super\_L

**Key:** Key for the hotkey



To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

### **Autostart**

The session will be launched automatically when the device boots.

### **Restart**

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode\(see page 869\)](#).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

### 3.9.17 Commands

Menu path: **Accessories > Commands**

The following system commands can be made accessible to the user:

- **Logoff:** Logs the user off from the device.
- **Reboot Terminal:** Restarts the device.
- **Restart windowmanager:** Restarts the device's user interface.
- **Shutdown terminal:** Shuts down the device.
- **Sort icons:** Sorts the symbols on the desktop so that they form a block.

► To edit a user command, double click the relevant entry in the list.

If you have made changes to the hotkey, you can check these by clicking the relevant entry in the **Key** column.

You can change the following starting methods:



### **Start menu**

The session can be launched from the start menu.

### **Application Launcher**

The session can be launched with the Application Launcher.

### **Desktop**

The session can be launched with a program launcher on the desktop.

### **Quick start panel**

The session can be launched with the quick start panel.

### **Start menu's system tab**

The session can be launched with the start menu's system tab.

### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

### **Desktop context menu**

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### **Hotkey**

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. **Ctrl**.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
- [Ctrl] = Ctrl



- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode\(see page 869\)](#).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

### 3.9.18 Network Tools

Menu path: **Accessories > Network Tools**

This function provides the following tools for network analysis:

- **Devices**
- **Ping**
- **Netstat**
- **Traceroute**
- **Lookup**

For how to use the network tools, see [Using “Network Tools” function - Devices\(see page 1099\)](#).

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )



## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".



These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with | :

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

The session will be launched automatically when the device boots.

#### Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)



The session cannot be started in appliance mode.

- 
- [Using Network Tools Function](#)(see page 1099)



## Using Network Tools Function

- ▶ Start the **Network Tools** function. The start options are described under [Network Tools](#)(see page 1095).

To obtain information regarding a network device available on your thin client, proceed as follows:

1. Click on the **Devices** tab.
2. Under **Network device**, select the network device for which you would like to obtain information.  
The information regarding the selected network device will be shown.

To send a ping query to a device in your network, proceed as follows:

1. Click on the **Ping** tab.
2. Under **Network address**, enter the IP address or the host name of the device to which you would like to send a ping query.
3. If necessary, add the number of ping queries under **Send**.
4. Click on the **Ping** button.  
The set number of ping queries will be sent. The results will then be shown.

To obtain information regarding the network status of your thin client, proceed as follows:

1. Click on the **Netstat** tab.
2. Select the desired information under Display:
  - **Routing Table Information**
  - **Active Network Services**
  - **Multicast Information**
3. Click on the **Netstat** button.  
The desired information will be shown.

To identify the router via which an IP data packet from your thin client reaches a specific target computer, proceed as follows:

1. Click on the **Traceroute** tab.
2. Under **Network address**, give the IP address of the target computer.
3. Click on the **Trace** button.  
The thin client will send IP packets to the target computer at short intervals, each with a TTL (Time To Live, i.e. maximum number of hops) increased by 1.  
When the packet reaches the target computer, "reached" will be shown in the last line and no further packet will be sent.  
If no computer replies, "no reply" will be shown.

With the **Lookup** function, you can request DNS information regarding any address on the Internet from your thin client.

Further information regarding the DNS (Domain Name System) can be found on Wikipedia under [Domain Name System](#)<sup>300</sup>.

Detailed descriptions of the Domain Name concept can be found in [RFC 1034](#)<sup>301</sup> and in related RFCs.

To obtain DNS information regarding an address on the Internet, proceed as follows:

---

<sup>300</sup> [https://en.wikipedia.org/wiki/Domain\\_Name\\_System](https://en.wikipedia.org/wiki/Domain_Name_System)

<sup>301</sup> <https://tools.ietf.org/html/rfc1034>



1. Click on the **Lookup** tab.
2. Under **Network address**, give the IP address or the host name.
3. Under **Information type**, select which information is to be shown. The following information types are available:
  - Default information
  - Internet address
  - Canonical name
  - Processor type/operating system
  - Mailbox exchange
  - Mailbox information
  - Name server
  - Computer name for address
  - Text information
  - Generally known services
  - Any / all information
4. Click on **Lookup**.

The desired information will be shown.

### 3.9.19 Bluetooth Tool

Menu path: **Accessories > Bluetooth Tool**

With the **Bluetooth Tool**, you can connect Bluetooth devices, e.g. a keyboard, a mouse, or a headset, to your thin client. For details of how to use the function, see [Using Bluetooth Tool](#)(see page 1102).

In order to be able to use Bluetooth, it must be enabled under **Devices > Bluetooth**.

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Starting Methods for Session

##### Start menu

The session can be launched from the start menu.

##### Application Launcher

The session can be launched with the Application Launcher.

##### Desktop

The session can be launched with a program launcher on the desktop.

##### Quick start panel

The session can be launched with the quick start panel.



### **Start menu's system tab**

The session can be launched with the start menu's system tab.

### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

### **Desktop context menu**

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### **Hotkey**

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. **Ctrl**.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
-  = Ctrl
-  = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:



- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

#### Autostart

The session will be launched automatically when the device boots.

#### Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode\(see page 869\)](#).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

- 
- [Using Bluetooth Tool\(see page 1102\)](#)

#### Using Bluetooth Tool

Menu path: **Accessories > Bluetooth Tool**

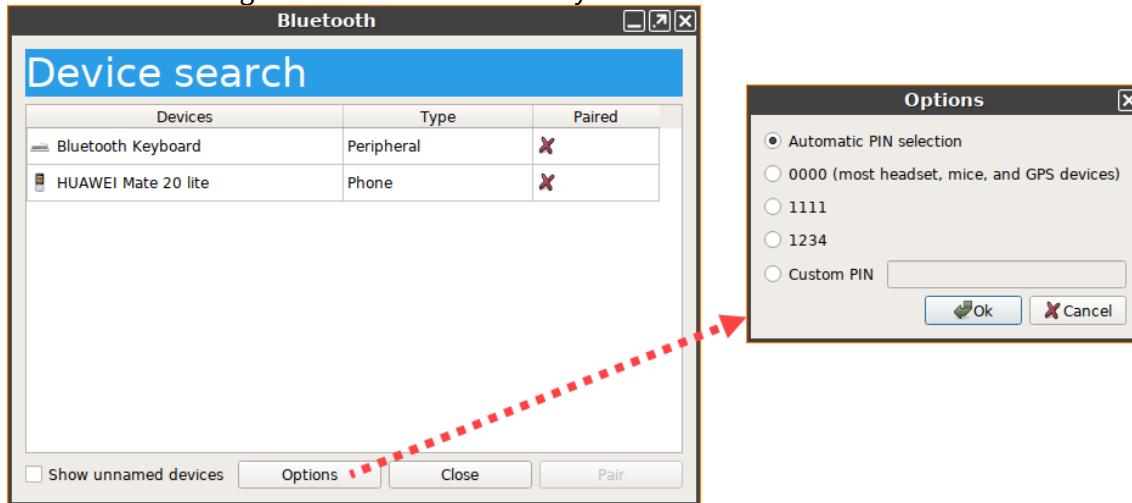
##### Overview

With the **Bluetooth Tool**, you can connect Bluetooth devices, e.g. a keyboard, a mouse, or a headset, to your endpoint device.

If your endpoint device (e.g. UD2 D220) does not support Bluetooth, it is necessary to connect a Bluetooth USB adapter to it.

The **Bluetooth Tool** supports the following coupling methods, i.e. the mutual authentication of the Bluetooth device and endpoint device:

- **Automatic PIN selection:** Pairing with automatic PIN allocation
- **0000, 1111, 1234:** Pairing with a fixed PIN (for most headsets, mice, or GPS devices)
- **Custom PIN:** Pairing with a fixed PIN entered by the user.



In addition, also Bluetooth devices that do not require pairing are supported.

#### Connecting a Bluetooth Device with Automatic PIN Selection

1. Ensure that the coupling mode is enabled on the Bluetooth device.
2. Start the **Bluetooth Tool**. The start options are described under [Bluetooth Tool](#)(see page 1100). The **Device search** dialog will be shown.
3. Enable **Show unnamed devices** if you want to include unnamed Bluetooth devices in the search list.  
After a few seconds, the Bluetooth devices found by the endpoint device will be displayed.
4. Highlight the desired Bluetooth device.
5. Under **Options**, enable **Automatic PIN selection**.
6. Click on **Pair**.
7. A PIN will be shown in the dialog on your endpoint device.
  - If the PIN is identical to the PIN shown on your Bluetooth device, confirm the coupling.
  - If a Bluetooth device requires the manual entering of a PIN (e.g. keyboard), type in the PIN shown in the dialog.
 In a few seconds, the status of the connection will be shown.
8. On successful connection, close the dialog.

For an example on how to connect a Bluetooth device, see [Bluetooth Tool](#)(see page 674).



## Connecting a Bluetooth Device with a Fixed PIN

1. Ensure that the coupling mode is enabled on the Bluetooth device.
2. Start the **Bluetooth Tool**. The start options are described under [Bluetooth Tool\(see page 1100\)](#).  
The **Device search** dialog will be shown.
3. Enable **Show unnamed devices** if you want to include unnamed Bluetooth devices in the search list.  
After a few seconds, the Bluetooth devices found by the endpoint device will be displayed.
4. Highlight the desired Bluetooth device.
5. Under **Options**, select one of the specified PINs or enable **Custom PIN** and enter the PIN for the Bluetooth device. You will find this PIN in the documentation for your Bluetooth device.
6. Click on **Pair**.  
In a few seconds, the status of the connection will be shown.
7. On successful connection, close the dialog.

## Cancelling Coupling to a Bluetooth Device

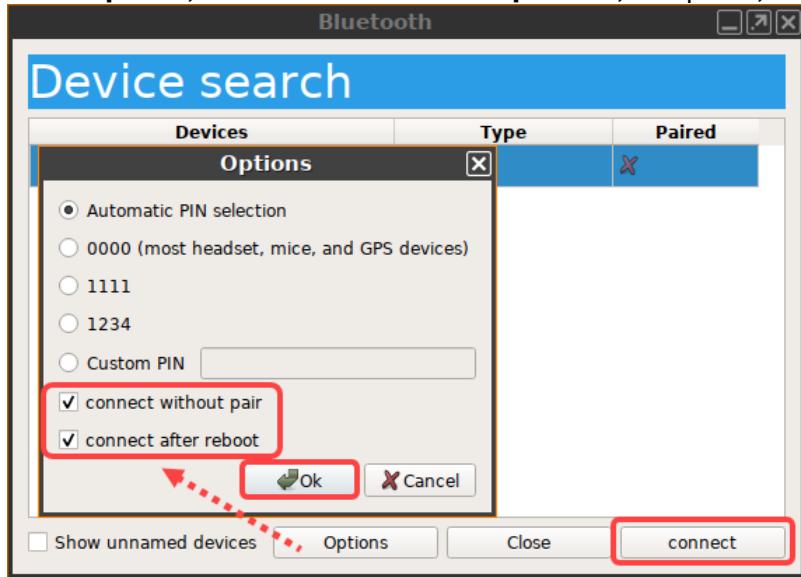
1. Start the **Bluetooth Tool**. The start options are described under [Bluetooth Tool\(see page 1100\)](#).  
The connected Bluetooth device will be shown in the **Device search** dialog.
2. Highlight the connected Bluetooth device and click on **Unpair**.  
The status of the connection will be shown.
3. Close the dialog.

## Enabling Support for Devices That Do Not Require Coupling

1. Open the Setup (or the configuration dialog of the UMS), go to **System > Registry > devices > bluetooth > connect\_only** and activate **Connect devices without pairing** (registry key: `devices.bluetooth.connect_only`).
2. Click **Apply** or **Ok** to confirm the changes.
3. Start the **Bluetooth Tool**. The start options are described under [Bluetooth Tool\(see page 1100\)](#).  
The **Device search** dialog will be shown.
4. Highlight the desired Bluetooth device.



5. Under **Options**, enable **Connect without pair** and, if required, **Connect after reboot**.



6. Click on **Connect**.

Some devices do not connect automatically after the reboot. To fix that, you can use the following command in a script:

```
bluetoothctl connect <device-ID>
```

The return value tells you if the device is connected (0) or not (1).

### 3.9.20 System Information

Menu path: **Accessories > System Information**

With this function, you can obtain information regarding the operating system of your device and the installed system components, internal and connected hardware and the network. You can also measure the performance of your device using various benchmarks.

The information shown can be copied to the clipboard in order to send it to the IGEL Support department for example.

For details of how to use the function, see [Using “System Information” Function\(see page 1108\)](#).

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )



## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".



These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with | :

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

### Autostart

The session will be launched automatically when the device boots.

### Restart

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)



- The session cannot be started in appliance mode.

- [Using System Information Function\(see page 1108\)](#)

## Using System Information Function

Menu path: **Accessories > System Information**

To obtain system information regarding a specific component of your device, proceed as follows:

1. Start the **System Information** function. The start options are described under [System Information\(see page 1105\)](#).
2. Click on the desired area, e.g. **Computer > Operating System**.  
The information regarding the desired area will be shown.
3. To send the information shown, e.g. to the IGEL Support department, click on the **Copy to Clipboard** button.  
The information is on your clipboard. With **Paste** or [Ctrl] + [V], you can paste the information into an e-mail or a web form.

You can use the **System Information** function to find out the **Vendor ID** and **Product ID** of your connected hardware. They are required, for example, if you want to configure **Device Rules**, see e.g. [USB Access Control\(see page 1231\)](#) or [Native USB Redirection\(see page 823\)](#).

The screenshot shows the 'Devices - USB Devices - System Information' window. The left sidebar has a tree view with nodes like Computer, Summary, Operating System, Security, Kernel Modules, Boots, Languages, Memory Usage, Filesystems, Display, Environment Variables, Devices, System DMI, Processor, Graphics Processors, Monitors, Memory Devices, PCI Devices, and USB Devices. The 'USB Devices' node is selected and highlighted in blue. The main pane lists USB devices with their IDs and names. A specific device, '003:002 logitech Webcam C270', is selected and highlighted in blue. Below it, a 'Device Information' panel is displayed, containing the following details:

|              |                                                        |
|--------------|--------------------------------------------------------|
| Product      | [0x0825] Webcam C270                                   |
| Vendor       | [0x046d] Logitech, Inc.                                |
| logitech     |                                                        |
| URL:         | <a href="http://www.logitech.com">www.logitech.com</a> |
| Device       | (Unknown)                                              |
| Manufacturer | (Unknown)                                              |
| Max Current  | 500 mA                                                 |
| USB Version  | 2.00                                                   |
| Speed        | 480 Mb/s                                               |

See also [Issues with USB IDs in USB Devices Rules\(see page 708\)](#).



### 3.9.21 Disk Utility

Menu path: **Accessories > Disk Utility**

With this function, you can obtain information regarding the hotplug storage devices connected to your thin client. You can also remove hotplug storage devices safely, i.e. without the risk of losing data.

The **Disk Utility** function can only be started if the automatic mounting of hotplug storage devices is enabled. The automatic mounting of hotplug storage devices is enabled if the option "**Dynamic**" is selected under **Setup > Devices > Storage Devices > Storage Hotplug > Client drive mapping** or the number in **Setup > Devices > Storage Devices > Storage Hotplug > Number of drives** is greater than "0".

For details of how to use the function, see [Using “Disk Utility”](#)(see page 1111).

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Starting Methods for Session

##### **Start menu**

The session can be launched from the start menu.

##### **Application Launcher**

The session can be launched with the Application Launcher.

##### **Desktop**

The session can be launched with a program launcher on the desktop.

##### **Quick start panel**

The session can be launched with the quick start panel.

##### **Start menu's system tab**

The session can be launched with the start menu's system tab.

##### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

##### **Desktop context menu**

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.



**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

The session will be launched automatically when the device boots.



## Restart

- The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

- For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

- No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode\(see page 869\)](#).

- The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode [XDMCP for this Display](#))
- **Desktop Context Menu** (not in appliance mode [XDMCP for this Display](#))
- **Application Launcher** (includes [Application Launcher's system tab](#); not in appliance mode [XDMCP for this Display](#))
- **Hotkey**
- **Autostart** (not in appliance mode [XDMCP for this Display](#))

- The session cannot be started in appliance mode.

- 
- [Using Disk Utility\(see page 1111\)](#)

## Using Disk Utility

To obtain information regarding a hotplug storage device connected to your thin client, proceed as follows:

1. Start the **Disk Utility** function. The start options are described under [Disk Utility\(see page 1109\)](#).
2. Click on the desired hotplug storage device in the left-hand column.  
The information regarding the hotplug storage device is shown in the right-hand column.

To remove a hotplug storage device safely, proceed as follows:



1. Start the **Disk Utility** function. The start options are described under [Disk Utility\(see page 1109\)](#).
2. Click on the **Safely Remove Hardware** button in the right-hand column.  
The hotplug storage device is disconnected from the thin client. Once it has been disconnected, the storage device can be removed from the thin client.

If **Setup > Devices > Storage Devices > Storage Hotplug > Hotplug beep** is enabled, a signal tone will signal that the device has been disconnected successfully. If **Setup > Devices > Storage Devices > Storage Hotplug > Hotplug message** is enabled, a message window will signal that the device has been disconnected successfully. Further information can be found under [Storage Hotplug\(see page 1228\)](#).

### 3.9.22 Disk Removal

Menu path: **Accessories > Disk Removal**

With this function, you can remove a hotplug storage device connected to your endpoint device safely without the risk of losing data.

The settings for starting the function are described below:

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Starting Methods for Session

##### **Start menu**

The session can be launched from the start menu.

##### **Application Launcher**

The session can be launched with the Application Launcher.

##### **Desktop**

The session can be launched with a program launcher on the desktop.

##### **Quick start panel**

The session can be launched with the quick start panel.

##### **Start menu's system tab**

The session can be launched with the start menu's system tab.

##### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

##### **Desktop context menu**

The session can be launched with the desktop context menu.



**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. **Ctrl**.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

### Key: Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)



- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

#### Disk utility in eject menu:

Allows to start the disk utility from the eject menu.

See also [Using “Disk Utility”](#)(see page 1111).

### 3.9.23 Mobile Device Access

Menu path: **Accessories > Mobile Device Access**

#### Feature Not Available on IZ Devices

This feature is not available on IGEL IZ devices (IGEL Zero HDX, IGEL Zero RFX, or IGEL Zero Horizon).

With this function, you can access the directories and files of a mobile device. Mobile device access is available from IGEL OS 10.04.100 onwards.

**Feature with limited support!** The mobile device access feature comes with limited support and without any warranty. Any support for this feature is provided on a non-binding, “best effort” basis.

The following device types can be used:

- Smartphones with Android (via MTP / PTP) or iOS
- Tablets with Android via MTP / PTP) or iOS
- Digital cameras

The functionality may differ according to the specific device and operating system version.

To use the mobile device access feature, you must first activate the function. For information about the activation and use, see [Using Mobile Device Access](#)(see page 692).

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

The session can be launched from the start menu.



### **Application Launcher**

The session can be launched with the Application Launcher.

### **Desktop**

The session can be launched with a program launcher on the desktop.

### **Quick start panel**

The session can be launched with the quick start panel.

### **Start menu's system tab**

The session can be launched with the start menu's system tab.

### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

### **Desktop context menu**

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### **Hotkey**

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift



- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

The session will be launched automatically when the device boots.

#### Restart

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

### 3.9.24 Firmware Update

Menu path: **Accessories > Firmware Update**



With this function, you can update your endpoint device's firmware. For details of how to use the function, see [Using “Firmware Update”](#)(see page 1119).

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey



- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

### Autostart

- The session will be launched automatically when the device boots.

### Restart

- The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.



**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

- [Using Firmware Update Function](#)(see page 1119)

## Using Firmware Update Function

To launch the firmware update for your endpoint device, proceed as follows:

1. Ensure that the settings under **System > Update > Firmware Update** are correct. Further information can be found under [Firmware Update](#)(see page 1252).
2. Start the **Firmware Update** function. The start options are described under [Firmware Update](#)(see page 1116).
3. Confirm this by clicking **Yes**.  
The latest firmware will be loaded onto your endpoint device. The device will restart in the process.

### 3.9.25 Smartcard Personalization

Menu path: **Accessories > Smartcard Personalization**

With this function, you can change the password for your IGEL smartcard. For details of how to use the function, see [Using “Smartcard Personalization” function](#)(see page 1121).

Further information regarding the IGEL smartcard can be found in the [Authentication with IGEL Smartcard](#)(see page 485) how-to.

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu



- The session can be launched from the start menu.

#### **Application Launcher**

- The session can be launched with the Application Launcher.

#### **Desktop**

- The session can be launched with a program launcher on the desktop.

#### **Quick start panel**

- The session can be launched with the quick start panel.

#### **Start menu's system tab**

- The session can be launched with the start menu's system tab.

#### **Application Launcher's system tab**

- The session can be launched with the Application Launcher's system tab.

#### **Desktop context menu**

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### **Hotkey**

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None



- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

## Autostart

- The session will be launched automatically when the device boots.

## Restart

- The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

- [Using Smartcard Personalization Function](#)(see page 1121)

## Using Smartcard Personalization Function

With this function, you can change your user name, the associated password and sessions on your IGEL smartcard.

To personalize an IGEL smartcard, proceed as follows:

1. Start the **Smartcard Personalization** function. The start options are described under [Smartcard Personalization](#)(see page 1119).
2. Specify the access data on your IGEL smartcard:
  - **First name:** First name of the user
  - **Last name:** Surname of the user



- **Require password**

- A password must be entered when logging on with this IGEL smartcard.
- No password must be entered when logging on.

- **Password:** Password for logging on with this IGEL smartcard.

3. Select the sessions and functions that are to be available on this IGEL smartcard.

4. Specify the start behavior for the sessions and functions on this IGEL smartcard:

- **Autostart**

- The session/function will automatically start after you log on. The application launchers configured in the desktop integration are available.
- The session will not automatically start. The application launchers configured in the desktop integration are available.

- **Restart**

- The session/function will automatically restart after being closed.
- The session/function will not automatically restart.

5. Click on **Write smartcard**.

Do not remove the IGEL smartcard before the writing operation is complete.

A confirmation dialog will appear when the writing operation is complete.

You can now remove the IGEL smartcard.

### 3.9.26 Identify Monitors

Menu path: **Accessories > Identify Monitors**

With this function, you can identify the monitors connected to your thin client. For details of how to use the function, see [Using “Identify Monitors” function](#)(see page 1124).

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Starting Methods for Session

##### Start menu

- The session can be launched from the start menu.

##### Application Launcher

- The session can be launched with the Application Launcher.

##### Desktop

- The session can be launched with a program launcher on the desktop.

##### Quick start panel



- The session can be launched with the quick start panel.

#### Start menu's system tab

- The session can be launched with the start menu's system tab.

#### Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

#### Desktop context menu

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.  
Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. **Ctrl**.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
-  = Ctrl
-  = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

-  = Alt



Key combinations are formed as follows with | :

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

The session will be launched automatically when the device boots.

#### Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

- 
- [Using Identify Monitors Function](#)(see page 1124)

#### Using Identify Monitors Function

To identify the monitors connected to your thin client, proceed as follows:

► Start the **Identify Monitors** function. The start options are described under [Identify Monitors](#)(see page 1122). The following data are shown for each monitor:

- Socket to which the monitor is connected
- Type of monitor
- Resolution currently used
- Maximum resolution of the monitor if the resolution currently used is a different one



### 3.9.27 Webcam Information

Menu path: **Accessories > Webcam Information**

With this function, you can change and check the settings for a connected webcam. For details of how to use the **Webcam Information** function, see [Using Webcam Information](#)(see page 1127).

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Starting Methods for Session

##### **Start menu**

The session can be launched from the start menu.

##### **Application Launcher**

The session can be launched with the Application Launcher.

##### **Desktop**

The session can be launched with a program launcher on the desktop.

##### **Quick start panel**

The session can be launched with the quick start panel.

##### **Start menu's system tab**

The session can be launched with the start menu's system tab.

##### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

##### **Desktop context menu**

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.



- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### **Hotkey**

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

#### **Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### **Autostart**

The session will be launched automatically when the device boots.

#### **Restart**

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

- [Using Webcam Information](#)(see page 1127)

## Using Webcam Information

You can determine and change the width, height and frame rate for the webcam connected.

Alternatively, you can determine the values supported by the webcam in the local terminal with the command `webcam-info -l`.

To determine and change the values for width, height and frame rate, proceed as follows:

1. Start the **Webcam Information** function.

The following values will be shown:

- **Width:** Width of the image in pixels
- **Height:** Height of the image in pixels
- **Rate:** Frame rate in fps (frames per second: individual images per second). Example: **1/30** means 30 individual images per second.

2. Click on one of the fields to change the value. The supported values will be shown in the process.

3. Click on **Test**.

The video image generated by the webcam with the current settings will be shown.

In order to check whether the webcam is functioning in a session (e.g. redirected via Citrix HDX Webcam Redirection), open <https://www.onlinemictest.com/webcam-test/> in your browser within the session.

### 3.9.28 ICG Agent Setup

Menu path: **Accessories > ICG Agent Setup**



This tool helps you configure the connection to IGEL Cloud Gateway (ICG). To learn how to use it, please refer to [Using ICG Agent Setup](#)(see page 1130).

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.



**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

## Autostart

The session will be launched automatically when the device boots.

## Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

- 
- [Using ICG Agent Setup](#)(see page 1130)



## Using ICG Agent Setup

This assistant helps you configure the connection to IGEL Cloud Gateway (ICG):

- ▶ Start **ICG Agent Setup**. Start options are described in [ICG Agent Setup \(see page 1127\)](#).
  - **Address:** IP address or DNS name of the server running ICG. You can specify a TCP port by appending a colon and the port number.
- ▶ After entering the server address, click **Connect**.
  - If you are using an ICG certificate signed by an unknown CA:  
**Root certificate fingerprint:** Fingerprint identifying the root certificate - three of four fields are prefilled.  
 Supply the missing fingerprint field from the credentials you received from your system administrator.
  - **ICG One-Time Password:** The one-time-password you received from your system administrator.
    - Click this icon in order to make the one-time password readable.
    - de\_DE Click this icon in order to change the keyboard layout for entering the password.
  - **Login:** Click this button to connect the thin client to ICG.
  - **Finish:** Click this button for instant connection to ICG. Otherwise, it will be started automatically on the next boot.



This cloud icon in the system tray indicates that the thin client is connected to ICG.

If you are switching between home office and company office often, it may be feasible to configure your IGEL OS so that it prefers the local UMS over the ICG. This prevents your device from connecting to the ICG instead of the local UMS although the device is located in the company network.

To make the device prefer the local UMS, make the following settings:

- a. Go to **IGEL Setup > System > Registry > system > remotemanager > icg\_try\_ums\_connect** (Search parameter: **system.remotemanager.icg\_try\_ums\_connect**).
- b. Enable **Prefer UMS over ICG**.
- c. Confirm your setting with **Ok**.

### 3.9.29 Licensing

Menu path: **Accessories > Licensing**



With this function, you can acquire a license from IGEL. An internet connection is required. The following license types are supported:

- Enterprise Management Pack (EMP)
- Software Maintenance

For information on how to use the license browser, see [Activate Your IGEL OS - Manual License Deployment\(see page 760\)](#).

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### **Start menu**

The session can be launched from the start menu.

#### **Application Launcher**

The session can be launched with the Application Launcher.

#### **Desktop**

The session can be launched with a program launcher on the desktop.

#### **Quick start panel**

The session can be launched with the quick start panel.

#### **Start menu's system tab**

The session can be launched with the start menu's system tab.

#### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

#### **Desktop context menu**

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.



## Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

## Autostart

The session will be launched automatically when the device boots.

## Restart

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.



**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

### 3.9.30 Login Enterprise

Menu path: **Setup > Accessories > Login Enterprise**

#### Login Enterprise Launcher

This accessory can be enabled to act as a remote endpoint that can launch test sessions for the purpose of evaluating the performance and availability of the resources it connects to. To use this feature, there must already be a Login Enterprise Virtual Appliance to which this Launcher can connect.

To learn more about using Login Enterprise with IGEL, see <https://www.loginvsi.com/igel/>. See also the how-to [Login Enterprise Configuration](#)(see page 340).

**Server URL:** URL of the Login Enterprise server

**Secret:** See [Getting the Secret for Login Enterprise Launcher](#)(see page 344).

### 3.9.31 Connector ID Key Software

Menu path: **Accessories > Connector ID Key Software**

Stratusphere UX is used to assess or inventory the current environment as the basis for designing the target environment.

The Stratusphere IGEL agent will detect RDP/RFX, ICA/HDX, PCoIP and Blast protocols to precisely measure the user experience and validate that the new desktops meet performance and security demands.

#### Enable Stratusphere UX CID Key

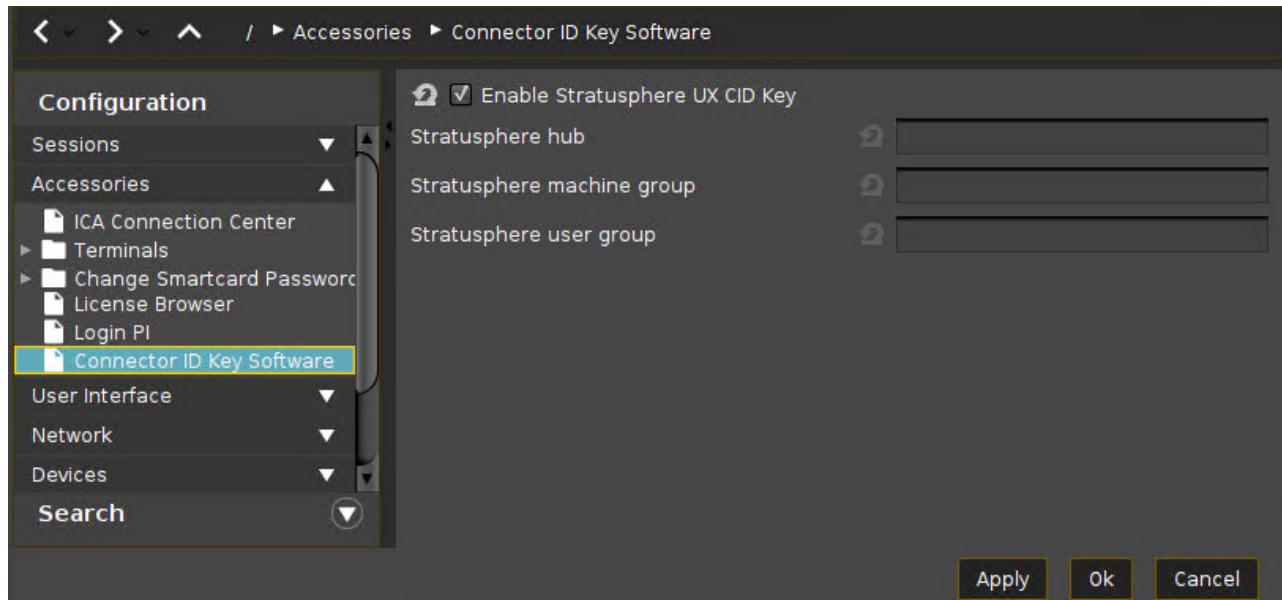
Stratusphere UX CID Key is enabled.

**Stratusphere hub:** The hub (IP-address or DNS) of the Stratusphere.

**Stratusphere machine group:** Machine group of the Stratusphere.



**Stratusphere user group:** User group of the Stratusphere.



### 3.9.32 OS 11 Upgrade

Menu path: **Accessories > OS 11 Upgrade**

With this tool, you can upgrade a device from IGEL OS 10 to IGEL OS 11. For more information about this tool, see [Testing the Upgrade](#)(see page 179); for instructions on how to upgrade, see [Upgrading IGEL Devices from IGEL OS 10 to IGEL OS 11](#)(see page 174).

The settings for starting the function are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Start menu

The session can be launched from the start menu.

#### Application Launcher

The session can be launched with the Application Launcher.

#### Desktop

The session can be launched with a program launcher on the desktop.

#### Quick start panel

The session can be launched with the quick start panel.

#### Start menu's system tab



- The session can be launched with the start menu's system tab.

#### **Application Launcher's system tab**

- The session can be launched with the Application Launcher's system tab.

#### **Desktop context menu**

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### **Hotkey**

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L



**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

#### Autostart

The session will be launched automatically when the device boots.

#### Restart

The session will be restarted automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode\(see page 869\)](#).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

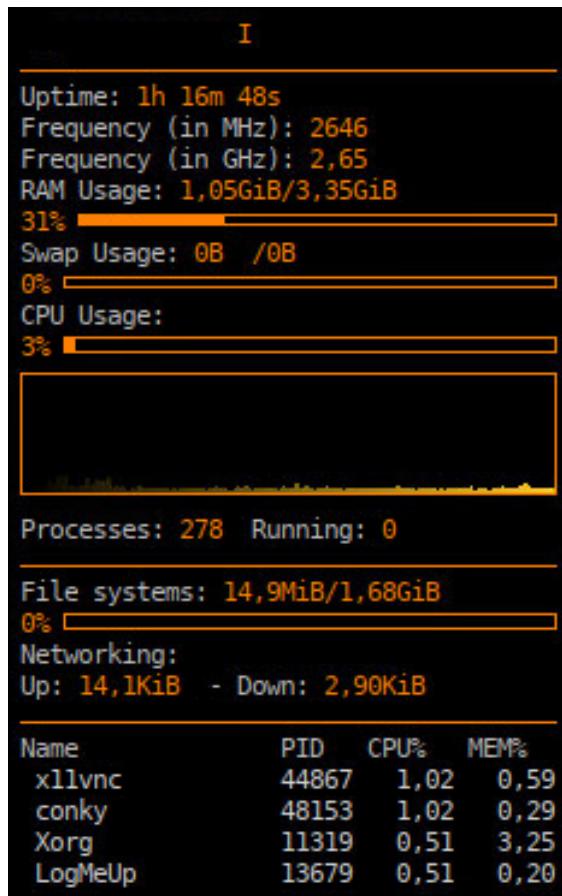
- **Desktop** (desktop icon; not in appliance mode [XDMCP for this Display](#))
- **Desktop Context Menu** (not in appliance mode [XDMCP for this Display](#))
- **Application Launcher** (includes [Application Launcher's system tab](#); not in appliance mode [XDMCP for this Display](#))
- **Hotkey**
- **Autostart** (not in appliance mode [XDMCP for this Display](#))

The session cannot be started in appliance mode.

### 3.9.33 Conky System Monitor

Menu path: **Accessories > Conky System Monitor**

The Conky system monitor displays current system data such as uptime, CPU frequency, RAM usage, and process-specific data. For details of how to configure the Conky system monitor, see [Options\(see page 1139\)](#) and [Custom Setup\(see page 1140\)](#).



The settings for starting Conky are described below. The start icons also function as stop icons.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.



### **Start menu's system tab**

The session can be launched with the start menu's system tab.

### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

### **Desktop context menu**

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### **Hotkey**

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:



- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

## Autostart

The session will be launched automatically when the device boots.

## Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode\(see page 869\)](#).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

- 
- [Options\(see page 1139\)](#)
  - [Custom Setup\(see page 1140\)](#)

## Options

Menu path: **Accessories > Conky System Monitor > Options**

### Use IGEL Setup for configuration

The settings on this Setup page are effective.



The configuration under **Accessories > Conky System Monitor > Custom Setup** (see [Custom Setup\(see page 1140\)](#)) is always effective, regardless of whether **Use IGEL Setup for configuration** is activated or not.

**Monitor:** Monitor on which the Conky system monitor is to be displayed.

#### Window type

Possible options:

- "Normal": The window layout and behavior can be further specified by the following parameters:
  - **Layer**
  - **Decorations**
  - **Show in the taskbar**
  - **Opacity**
  - **Borders**
- "Desktop": No window decorations; always visible on the desktop; no appearance in the pager or taskbar; sticky across all workspaces. The parameters **Decorations** and **Show in taskbar** are not effective.
  - **Layer**
  - **Opacity**
  - **Borders**
- "Dock": Behavior as documented under <https://linux.die.net/man/1/conky>
- "Panel": The window reserves space along a desktop edge, just like panels and taskbars, preventing maximized windows from overlapping them.
- "Override": The window is not under the control of the window manager.

**Alignment:** Defines where the window is placed on the screen.

**Layer:** Defines whether the Conky window is displayed above or below other application windows.

Possible options:

- "Below": The Conky window is always below other application windows.
- "Above": The Conky window is always above other application windows.
- "None": The Conky window is above or below other application windows, depending on the focus.

**Font type:** Defines the font type for Conky.

**Font size:** Defines the font size for Conky.

**Opacity:** Defines the opacity for Conky. If the value is set to 0, the window is completely transparent; if the value is set to 255, there is no transparency.

**Offset horizontal:** Defines the horizontal offset from the position that is defined by **Alignment**.

**Offset vertical:** Defines the vertical offset from the position that is defined by **Alignment**.

## Custom Setup

Menu path: **Accessories > Conky System Monitor > Custom Setup**

On this Setup page, you can customize Conky in full. For details, see <https://linux.die.net/man/1/conky>.

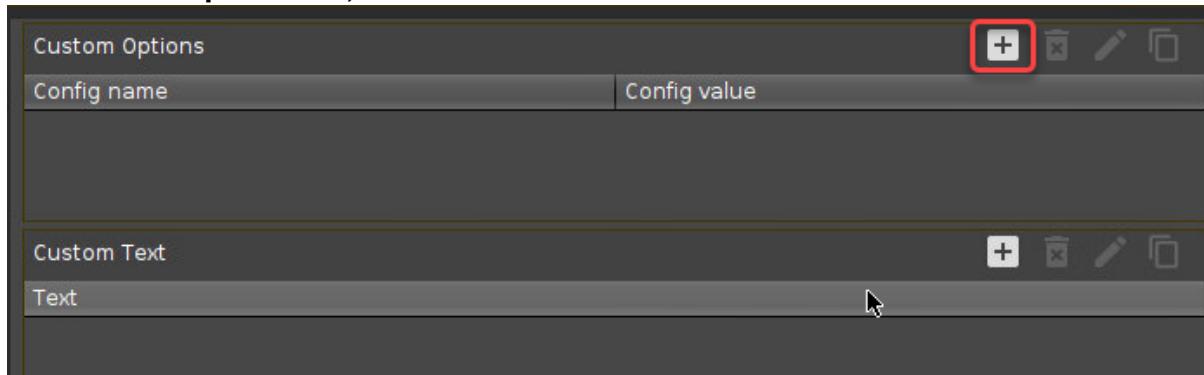


## Custom Options

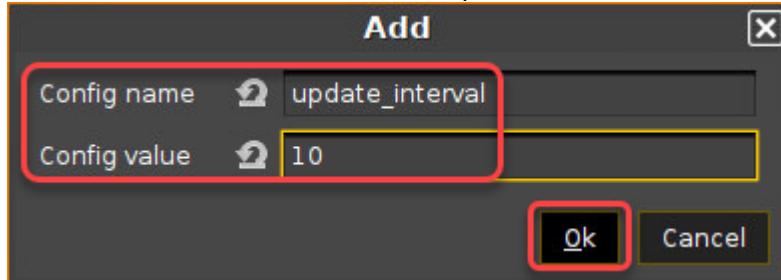
You can find the configuration options of Conky under <https://linux.die.net/man/1/conky>, section "Configuration Settings".

To add a custom option:

1. In the **Custom Options** area, click .



2. Enter the name and the value of the option and click **Ok**.



3. In the main window, click **Apply** or **Ok**.

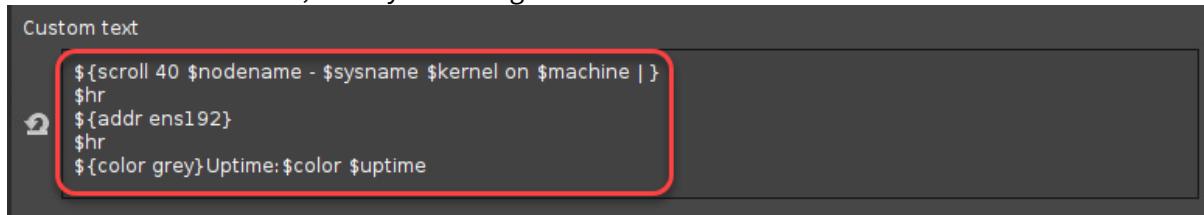
If Conky is already running, you can see the effect immediately.

## Custom Text

In this area, you can define the complete text body of Conky. You can find the relevant details under <https://linux.die.net/man/1/conky>, section "OBJECTS/VARIABLES". The configuration is stored at /etc/conky/conky.conf

To add or edit the custom text:

1. In the **Custom Text** area, enter your configuration text.



2. In the main window, click **Apply** or **Ok**.

If Conky is already running, you can see the effect immediately.



## 3.10 User Interface

- [Display\(see page 1142\)](#)
- [Desktop\(see page 1146\)](#)
- [Language\(see page 1155\)](#)
- [Screenlock / Screensaver\(see page 1155\)](#)
- [Input\(see page 1161\)](#)
- [Hotkeys\(see page 1167\)](#)
- [Font Services\(see page 1170\)](#)

### 3.10.1 Display

Menu path: **User Interface > Display**

Every screen connected to the IGEL UD device can be configured independently. The position of the individual screens can be determined in relation to Screen 1.

- ▶ Click on to show the screen identifier on each device.

For details of the display resolution supported by your IGEL thin client, please see the relevant data sheet.

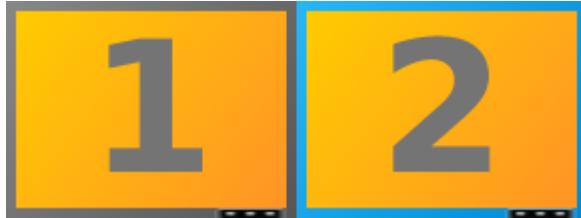
If you work in an environment with a number of monitors, see the How-To [Multimonitor\(see page 517\)](#).

If you use the Shared Workplace (SWP) feature with user-specific display resolutions, see the How-To [Display Configuration for Shared Workplace \(SWP\)\(see page 512\)](#).

#### Screen Configuration

**Number of screens:** Select how many monitors you would like to use.

|  |                                                                                                       |
|--|-------------------------------------------------------------------------------------------------------|
|  | Identifies each screen connected and specifies the connection and display resolution for each screen. |
|  | Arranges the screens in a single row.                                                                 |
|  | Arranges the screens in two rows.                                                                     |
|  | Rotates the selected screen anti-clockwise.                                                           |
|  | Rotates the selected screen clockwise.                                                                |
|  | Removes the screen which was last added.                                                              |
|  | Adds a screen.                                                                                        |



The selected screen is highlighted with a blue frame. The black bar at the bottom edge of the screen represents the physical orientation of the monitor.

**Selected screen:** Selects a screen using this selection box to configure the following settings.

**Screen resolution:** Move the slider to the resolution which the selected screen is to have. The resolution is shown in the right-hand box.

From IGEL Linux Version 10.03.100, you have the option of defining your own resolutions via the registry (`x.xserver0.custom_resolution`). In order for the values set there to take effect, the resolution must be set to "Automatic" (slider at the far left). The following parameters apply to the entry in the registry:

- `WxH` : W = width, H = height (example: 1920x1080)
- `WxH@R` : W = width, H = height, R = refresh rate (example: 1920x1080@60 or 1920x1200@59.8)

## Advanced

### Detect refresh rate automatically

- A refresh rate for the monitor is identified automatically. (Default)  
 A refresh rate for the monitor is to be set manually.

**Refresh rate:** Number of individual images per second.

Possible values:

- 30 ... 100. (Default: 60)

**Graphic card:** Graphics card assigned to the selected screen. A graphics card can have more outputs than are actually used. In order to ensure transparency, you may need to assign the graphics cards manually.

If **Automatic** is set for the **Monitor** and no configurable monitor is found for the selected graphics card, the next available monitor will be used by another graphics card.

**Monitor:** Assigns the screen selected under **Selected screen** to a monitor connection. Example: **HDMI(II)**. (Default: Automatic)

- [Power Options](#)(see page 1144)
- [Access Control](#)(see page 1144)
- [Gamma Correction](#)(see page 1145)
- [Options](#)(see page 1145)



## Power Options

Menu path: **Setup > User Interface > Screen > Power Options**

In this area, you can handle display power management.

Please note: Your screen must support *Display power management signaling (DPMS)*.

- **Handle Display Power Management**

The DPMS energy saving functions are enabled.

- Specify separately for battery and mains operation the number of minutes before the screen switches to a specific energy-saving mode:

Three different modes are offered:

- **Standby Time** (standby mode)
- **Suspend Time** (sleep mode)
- **Off Time** (Off)

If a device is switched on but not used for some time, energy can also be saved by **Brightness Reduction**.

- Specify by how many percent the brightness of the screen is to be reduced and how long the period of inactivity before brightness reduction should be. Values between 10 seconds and two minutes are available to choose from.

Naturally, all stages are gone through only if the X-Server does not receive any new entries during this period.

## Access Control

Menu path: **Setup > User Interface > Screen > Access Control**

In this area, you can control access to the screen. Thin client access control is enabled by default.

### Disable console switching

Access to your terminal screen is possible from any UNIX host. You can no longer access the console using [Ctrl] + [Alt] + [F11] or [Ctrl] + [Alt] + [F12].

You can access the console using [Ctrl] + [Alt] + [F11] or [Ctrl] + [Alt] + [F12]. (default)

### Access Control

Access to this display from other computers will be controlled. This access control is enabled by default. (default)

### Disable TCP connections

All TCP connections to the display are prohibited. Only local applications are displayed. The xhost mechanism no longer functions.

This parameter is ignored if XDMCP is configured.

### Fixed X-Key

You can grant specific users permanent remote access to the thin client:



1. Click on **Calculate**.  
A 32-digit key will appear in the **X-Key** field.
2. Enter this key in the Xauthority file on the user's computer.

### List of trusted X hosts

Here, you can approve specific computers for console access:

1. Click on the **Add** button to open the entry mask.
2. Give the name of the remote host (not the IP address) you would like to add.
3. Confirm this by clicking **OK**.  
The computer will be entered in the list.

### Gamma Correction

Menu path: **Setup > User Interface > Screen > Gamma Correction**

In this area, you can increase or decrease the various brightness ranges in order to adjust the display on your screen to your preferences.

- **Selected screen:** Select the screen whose brightness you would like to adjust (default: First Screen).

You can then change the gamma values for red, green and blue. The scale ranges from 0.10 (dark) to 10 (light) and is set to 1.00 by default.

- **Gamma value Red:** Changes the brightness curve for the red color portion.
- **Gamma value Green:** Changes the brightness curve for the green color portion.
- **Gamma value Blue:** Changes the brightness curve for the blue color portion.
- **Link Sliders**
  - All sliders are moved equally in order to change the brightness harmoniously. (default)
  - Each slider can be moved individually. This way, you can also change the color ratio.

### Options

Menu path: **Setup > User Interface > Screen > Options**

Configure the options for the display here:

- **Monitor probing (DDC)**
  - You can share information between the system and the screen via the Display Data Channel. DDC is enabled by default and the native resolution supported by the screen is determined automatically. (default)
  - Screen properties are not automatically detected.
- **Monitor DPI detection:** Defines how the DPI value should be determined.  
Possible options:
  - Off: The DPI value is defined by **Monitor DPI**. There is no automatic detection.
  - Smart: The DPI value is defined automatically. With this setting, the user interface is readable also on monitors with very high resolutions, e.g. 4k monitors. The DPI value is set to either 96, 125, 150, 175, 200, 225, 250, 275 or 300, depending on which value is closest to the value calculated based on the monitor resolution.



- **Pixel-Precise:** The DPI value is defined automatically. With this setting, the user interface is readable also on monitors with very high resolutions, e.g. 4k monitors. Unlike the "Smart" option, the value calculated based on the monitor resolution is used directly.
- **Monitor DPI:** Enter the DPI resolution (dots per inch) for your monitor (default: 96). This parameter is only available if **Monitor DPI detection** is set to "Off".
- **Color Depth:** Selects the desktop color depth.  
The following options are available:
  - True Color (24)
  - True Color (32)

Make sure that all screens connected to the thin client support the color setting.

### 3.10.2 Desktop

Menu path: **Setup > User Interface > Desktop**

On this page, you can configure general settings for the appearance of the desktop:

**Local window manager for this display:** Here, you can disable the window manager if you only work in full-screen sessions and do not require this service.

**User interface theme:** The colors of windows such as the Application Launcher, the start menu, the local terminal, the taskbar and messages can be varied. You can either select one of our predefined color schemes or define a color scheme of your own.

- IGEL Dark: The frame color is dark gray, IGEL logos are yellow.
- IGEL Light: The frame color is light gray, IGEL logos are dark gray.
- Custom Colors: Define your own color combinations below.

**Desktop icon size:** Specify the size in which you would like the icons to be displayed on the desktop.

**Desktop icon font color:** Specify the font color for the labels associated with the desktop icons. Click **Choose color** to open the color picker.

**Monitor for desktop icons:** If you use several monitors, select the one which is to display desktop icons.

- All monitors
- As taskbar
- 1st monitor
- 2nd monitor
- (other monitors if connected)

**Single click mode:**

Open programs with a single click. This option was set up especially for users of touchscreen monitors.

#### Desktop fonts

**Default font:** Choose between serif and sans-serif text and between standard and bold. The following are available to choose from:

- Sans



- Sans bold
- Serif
- Serif Bold

**Default font size:** Specify your desired font size in pt (points) here.

**Desktop icon font size:** Specify your desired font size for desktop icons in pt (points) here.

**Titlebarfont:** Choose between serif and sans-serif text and between standard and bold. The following are available to choose from:

- Sans
- Sans bold
- Serif
- Serif Bold

**Titlebar font size:** Specify your desired font size in pt (points) here.

---

- [Background](#)(see page 1147)
- [Taskbar](#)(see page 1149)
- [Taskbar Background](#)(see page 1151)
- [Taskbar Items](#)(see page 1151)
- [Pager](#)(see page 1152)
- [Start Menu](#)(see page 1153)
- [In-Session Control Bar](#)(see page 1154)

## Background

Menu path: **Setup > User Interface > Desktop > Background**

In this area, you can configure the desktop background with predefined *IGEL* backgrounds, a fill color or a color gradient.

You can also use a background image of your own.

You can set up a separate background image for each monitor that is connected to the thin client.

**Wallpaper** selection options beginning with "Desktop Color" are transparent so that the background colors will shine through.

- **Wallpaper:** Provides a selection of predefined *IGEL* backgrounds:
  - Neutral
  - Off
  - Black
  - Blue
  - Gray
  - Orange
  - Green



- Yellow
  - Desktop Color Light
  - Desktop Color Dark
  - Desktop Color Light Neutral
  - Desktop Color Dark Neutral
  - **Wallpaper Style:** Provides various design versions:
    - Auto
    - Centered
    - Tiled
    - Stretched
    - Scaled
    - Zoomed
  - **Color Style:** Sets a fill color or a color gradient.
    - Solid color
    - Horizontal gradient
    - Vertical gradient
  - **Desktop Color:** Select a background color if you have not selected an image.
  - **2nd Desktop Color:** Select a second background color if you have not selected an image.
  - **Custom Wallpaper Download:**
    - You can provide a user-specific background image on a download server.
  - **Custom Wallpaper file:** Give a name for the background image file.
- Specify the download server under **Desktop > Background > Custom Wallpaper Server**.

If you have already defined a server for the system update files, you can use the same server setting for downloading the background image.

The user-specific background image will be downloaded from the specified server if the function was enabled and if requested manually (Update Background Image). The download can also be launched from the *IGEL Universal Management Suite* via **Update desktop changes**.

A user-specific boot image can be provided on a download server. The file types BMP, JPG, GIF, TIF, PNG and SVG are supported for an **own background image** and **bootsplash**. A total storage area of 25 MB is available for all user-specific images.

## Custom Wallpaper Server

Menu path: **Setup > User Interface > Desktop > Background > Custom Wallpaper Server**

In this area, you can configure the download server for your own background images.

- **Use firmware update server location**
  - The same server and path configuration is used as for the firmware update.
  - An own server location is used. (default)
- **Protocol:** Determines the protocol that is to be used. The following are available to choose from:



- [HTTP](#)
- [HTTPS](#)
- [FTP](#)
- [SecureFTP](#)
- [FTPS](#)
- [File](#)
- **Server Name:** Name or IP address of the server used.
- **Server Path:** Directory in which you saved the background image.
- **Port:** Port used (default: [80](#))
- **User name:** Name of the user account on the server
- **Password:** Password for this account
- **Wallpaper update:** Refreshes the background image.

## Taskbar

Menu path: **Setup > User Interface > Desktop > Taskbar**

In this area, you can enable and configure the taskbar.

You can change the following settings:

- **Use Taskbar:**  
 The taskbar is displayed and the following taskbar settings options are available.
- **Taskbar Position:** Specifies the position in which the taskbar is displayed.  
Possible values:
  - [Bottom](#)
  - [Top](#)
  - [Left](#)
  - [Right](#)
- **Vertical Taskbar Mode:** Specifies how items are shown in the taskbar. This parameter is available if **Taskbar Position** is set to **Left** or **Right**.  
Possible values:
  - Vertical: The session texts are rotated by 90°.
  - [Deskbar](#): The session texts are not shown.
- **Taskbar Height/Width:** Specifies the height of the taskbar in pixels (default [40](#)).



If **Maximum number of rows/columns in window button list** is set to **Automatic**, the window buttons as well as the icons in the Quick Start Panel will be shown in a number of rows depending on the height of the taskbar. The number of rows increases in increments of 55 pixels:

- 1 - 55 pixels: One row
- 56 - 110 pixels: Two rows
- 111 - 165 pixels: Three rows
- 166 - 220 pixels: Four rows
- 221 - 275 pixels: Five rows
- 276 or more pixels: Six rows

The **Maximum number of rows/columns in window button list** parameter is described under [Taskbar Items<sup>302</sup>](#).

- **Number of rows/columns in taskbar:** Specifies the number of rows for the Quick Start Panel. The following taskbar items can be broken down into a number of rows and columns: Icons in the Quick Start Panel, window buttons. Possible values:
  - Automatic: The number of rows for the Quick Start Panel depends on the height and width of the taskbar.
  - Numeric value: The chosen value specifies the number of rows for the Quick Start Panel.
- **Multi Monitor Taskbar Size:** Specifies whether the taskbar is expanded across a number of monitors or restricted to one monitor. Possible values:
  - Restrict taskbar to one monitor
  - Extend taskbar to all monitors
- **Monitor:** Specifies the screen on which the taskbar is shown. This parameter is available if **Taskbar size in Multi Monitor** is set to **Restrict taskbar to one monitor** (default: 1st monitor).
- **Taskbar on top of all windows:**
  - The taskbar is accessible on all screens, even in sessions with a full-screen window.
- **Taskbar Auto Hide:**
  - The taskbar is hidden and will only be shown if the mouse pointer is moved to the position of the taskbar at the edge of the screen.
- **Auto Hide Behavior:** Specifies when the taskbar is automatically hidden. Possible values:
  - Intelligent: The taskbar is shown as standard. The taskbar will be hidden if the space is needed by a window, e. g. a window in full-screen mode.
  - Continuous: The taskbar is hidden as standard. The taskbar will be shown if the mouse pointer is moved to the edge of the screen.
- **Taskbar Show Delay:** Time interval in milliseconds before the taskbar is shown. The mouse pointer must be at the edge of the screen constantly during this time interval. This setting is only effective if **Taskbar Auto Hide** is enabled (default: 600).

<sup>302</sup> <https://kb.igel.com/display/igelos/Taskbar+Items>



With the show delay, you can prevent the taskbar for a full-screen session being covered by the thin client's taskbar. A show delay is necessary if the taskbar for the full-screen session is set to be shown automatically and both taskbars are positioned at the same screen edge. If no show delay is set and the user brings up the taskbar for the full-screen session, this will immediately be covered by the thin client's taskbar. During the show delay time interval, the user has time to move the mouse pointer away from the edge of the screen.

- **Taskbar Hide Delay:** Time interval in milliseconds before the taskbar is hidden. This setting is only effective if **Automatically hide taskbar** is enabled (default: 400).  
Further settings options can be found under [Screensaver and Screenlock](#)<sup>303</sup>.

## Taskbar Background

Menu path: **Setup > User Interface > Desktop > Taskbar Background**

You can specify the background style for the taskbar here.

- **Background Style:**

Possible values:

- [System preset](#)
- Solid color
- Color gradient
- Background image

Depending of the above selection you can define following features:

- **Taskbar Color:** Choose the color for the taskbar.
- **2nd Taskbar Color:** Choose the 2nd color for the taskbar if you want to create gradient colors.
- **Reverse Gradient**
  - The color gradient is reverse.
  - The color gradient is normal. (default)
- **Background Image Path:** Path of your background image

## Taskbar Items

Menu path: **Setup > User Interface > Desktop > Taskbar Items**

- **Taskbar clock:**

A clock is shown in the taskbar.

- **Sorting order in window button bar:** Specifies the criteria according to which the window buttons are sorted.

Possible values:

- [Time stamp](#): The window buttons are sorted in the chronological order in which the windows were opened.

---

<sup>303</sup> <https://kb.igel.com/pages/viewpage.action?pageId=23503671>



- Group and time stamp: The window buttons are grouped according to the type of application. If for example a number of setup applications are open, all associated window buttons will be arranged next to each other. Within the group, the window buttons are sorted chronologically.
- Window title: The window buttons are sorted alphabetically.
- Group and window title: The window buttons are grouped according to type. If for example a number of setup applications are open, all associated window buttons will be arranged next to each other. Within the group, the window buttons are sorted alphabetically.
- Drag and drop: You can order the buttons as you wish using drag and drop. You must drag a button over at least half of the button to be skipped.
- **Maximum number of rows/columns in window button bar:** Specifies the maximum number of rows available for window buttons.  
Possible values:
  - Automatic: The number of rows depends on the **Taskbar height/width** and **Number of rows/columns in taskbar** parameters, see [Taskbar<sup>304</sup>](#).
  - Numeric values: This value specifies the maximum number of rows.
- **Show labels in window button bar:**
  - The names of the ongoing sessions are displayed in the associated window buttons. (default)
  - Only the icons are displayed.
- **Taskbar system tray:**
  - The system tray is shown in the taskbar. (default)
- **Size of icons in system tray:** Specifies the size of system tray icons (volume, network connection etc.).

You can choose a pre-defined value or enter a numeric value between 1 and 64.

Predefined values:

- Automatic: The size is adjusted to the height and width of the taskbar.
- Small: 20 pixels
- Medium: 40 pixels
- Large: 60 pixels

Further settings options can be found under [On-screen Keyboard<sup>305</sup>](#), [Keyboard<sup>306</sup>](#) and [Additional Keyboard Layouts<sup>307</sup>](#) and [Screensaver and Screenlock<sup>308</sup>](#).

## Pager

Menu path: **Setup > User Interface > Desktop > Pager**

In this area, you can enable the use of a number of virtual workstations.

The **Pager** is a tool with virtual desktops which can be used as an easy way of switching between open applications. This window is shown at the right of the taskbar. You can use up to 25 virtual desktops. If you use a **Pager**, you can switch between full-screen applications for example at the click of a mouse.

---

<sup>304</sup> <https://kb.igel.com/display/igelos1005/Taskbar>

<sup>305</sup> <https://kb.igel.com/display/igelos/Bildschirmtastatur>

<sup>306</sup> <https://kb.igel.com/pages/viewpage.action?pageId=23501728>

<sup>307</sup> <https://kb.igel.com/display/igelos/Additional+Keyboard+Layouts>

<sup>308</sup> <https://kb.igel.com/pages/viewpage.action?pageId=23503671>



Instead of minimizing/maximizing sessions or switching between them using key combinations, you simply click on the desired screen using the mouse. The screen is then shown as it was when you closed it (unless you restarted the system beforehand).

- **Use Pager**

- Several virtual desktops may be used.
- Pager is not used. (default)

- **Number of Screens - Horizontal:** Specifies how many pages will be shown next to each other.

- **Number of Screens - Vertical:** Specifies how many pages will be shown above each other.

- **Names of the workspaces:** Give names for the individual desktops.

- **Paging Resistance:** Specifies how many pixels the cursor needs to be moved over the edge of the screen before it triggers a switch of desktop. You only need to make this setting if you enable at least one of the following options:

- **Wrap workspaces while dragging a window:** The desktop is switched as soon as a window is dragged out of view.
- **Wrap workspaces with pointer:** The desktop is switched as soon as the mouse reaches the edge of the screen.

## Start Menu

Menu path: **Setup > User Interface > Desktop > Start Menu**

In this area, you can configure the desktop start menu:

- **Start menu type:**

- **Auto:** A default setting that automatically selects the advanced or legacy type of the start menu depending on the processor.
- **Advanced:** An expanded start menu featuring a search function and a more attractive design. It requires more resources, which is particularly noticeable on slow devices.
- **Legacy:** A start menu resembles the one from Windows 95 – a list of available sessions and options.

## Options in Start Menu

Select which options are to be shown in the start menu:

- **Screenlock**

- **Logout**

- **Reboot**

- **Shutdown**

- **System tab**

- **About**

- **Show current user name in About, Application Launcher and start menu**

- The current user will be shown at the top edge of the relevant window.

- The current user will not be shown.



In order for user names to be recognized and passed on, you must configure two settings beforehand:

- Enable Active Directory/Kerberos: **Security > Active Directory/Kerberos**
- Enable local logon: **Security > Logon > Active Directory/Kerberos**

## In-Session Control Bar

Menu path: **Setup > User Interface > Desktop > In-Session Control Bar**

In a full-screen session, the in-session control bar allows you

- to eject a USB drive,
- to start the wireless manager (only available in Appliance Mode),
- to start the Mobile Device Access USB tool (only available if the Mobile Device Access USB feature is enabled),
- to minimize the session view (not available in Appliance Mode),
- to end the session.

### Use in-session control bar in all supported sessions

The in-session control bar is shown. Depending on the configuration, the in-session control bar will be permanently visible or will be shown as soon as you move the cursor to the top edge of the screen.

In-session control bar is not used. (default)

The in-session control bar is available for the following session types:

- **RDP** - see [RDP Global](#)(see page 811)
- **Citrix** - see [Citrix Global](#)(see page 776)
- **ThinLinc** - see [ThinLinc](#)(see page 933)
- **NX** - see [NX](#)(see page 887)
- **Parallel 2X Client** - see [Parallel 2X Client](#)(see page 907)

To use the in-session control bar, proceed as follows:

- ▶ To eject a USB device, click .
- ▶ To start the wireless manager, click  (only available in Appliance Mode).
- ▶ To start the Mobile Device Access USB tool, click  (only available if the Mobile Device Access USB feature is enabled).
- ▶ To minimize the session view, click .
- ▶ To end the session, click .
- ▶ To make the in-session control bar permanently visible, click .



### 3.10.3 Language

Menu path: **Setup > User Interface > Language**

In this area, you can configure the country-specific language settings.

- **Language:** The language of the user interface.
- **Keyboard layout:** When the language is changed for the first time, the keyboard layout is automatically set to the same language.
- **Show indicator in taskbar**
  - Shows a country abbreviation for the keyboard layout in the taskbar.
  - No indicator is shown (default)
- **Input language:** The keyboard layout is used by default.
- **Standards and formats:** Specifies how country-specific formats for the time and currency for example are displayed. The default setting is geared to the input language selected.

### 3.10.4 Screenlock / Screensaver

Menu path: **User Interface > Desktop > Screen Lock/Saver**

You can set up the screen saver so that it is activated automatically after a time limit expires, via a button or in response to a key combination (hotkey). You can also select a password option. The look of the taskbar can be configured separately for the logon dialog and the locked screen.

The screen can be locked via icons in the Quick Start Panel and on the desktop or via the hotkey [Ctrl-Shift-L].

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Starting Methods for Session

##### Start menu

The session can be launched from the start menu.

##### Application Launcher

The session can be launched with the Application Launcher.

##### Desktop

The session can be launched with a program launcher on the desktop.

##### Quick start panel

The session can be launched with the quick start panel.

##### Start menu's system tab

The session can be launched with the start menu's system tab.

##### Application Launcher's system tab



- The session can be launched with the Application Launcher's system tab.

#### Desktop context menu

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey



To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

## Autostart

- The session will be launched automatically when the device boots.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

- For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode\(see page 869\)](#).

- The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

- 
- [Options\(see page 1157\)](#)
  - [Taskbar\(see page 1159\)](#)
  - [Screensaver\(see page 1160\)](#)

## Options

Menu path: **Setup > User Interface > Screenlock / Screensaver > Options**

### Start automatically

- The screenlock or screensaver starts automatically if there is no activity on the endpoint device within this time limit. The screen can be unlocked by the user or, if the **Allow administrator password** is not disabled, the administrator with the relevant password (see: [Password\(see page 1236\)](#)). (Default)

**Timeout:** Period of time in minutes before the screenlock or the screensaver starts. (Default: 5)

### Screenlock Password

- **None:** No password is set. A screenlock cannot be set up.



- **User password:** A user password is deployed to unlock the screen, see [Password<sup>309</sup>](#). If the user is [logged in via Active Directory \(AD\)](#)(see page 1242), the AD credentials are used instead of the user password to unlock the screen.
- **Local user password:** A separate password specified under **Set** is deployed to unlock the screen. This password is also used for **Security > Logon > Local User > Login with local user password**, see [Local User](#)(see page 1246). If the user is [logged in via Active Directory \(AD\)](#)(see page 1242), the AD credentials are used instead of the local user password to unlock the screen.

#### Different screenlock timeout

- You can specify a time limit of your own for the screenlock. (Default)
- The same time limit will be used for the screenlock as for the screensaver. This means that after the set time the screen will be locked and then the screensaver will appear.

**Screenlock timeout:** Period of time in minutes before the screenlock starts. (Default: 5)

#### Allow administrator password

- Access is allowed for the user and the administrator, see [Password<sup>310</sup>](#). (Default)
- Access is allowed for the user only.

**Countdown duration in seconds:** Countdown time with which the screenlock is initiated. If the value is 0, the screen is locked without a countdown. (Default: 0)

The appearance of the digits for the countdown is specified together with the settings for the clock display under **Setup > User Interface > Screenlock / Screensaver > Screensaver**; see [Screensaver](#)(see page 1160). The following parameters are relevant for the countdown:

- **Clock display monitor**
- **Show seconds**
- **Horizontal clock position**
- **Vertical clock position**
- **Clock background color**
- **Clock foreground color**

**Countdown visual effect:** While the countdown is running, a current screenshot is displayed in the background.

This parameter determines the visual effect that the screenshot will be displayed with.

Possible options:

- Dark screenshot
- Gray screenshot

**Countdown background image:** Path and file name of an image file, which is displayed in the background while the countdown is running. This background image is displayed instead of the screenshot, if the path and file name are valid; if the field is empty, the screenshot is displayed. Supported file formats: JPEG, PNG, GIF. Example: /images/image.jpg

<sup>309</sup> <https://kb.igel.com/display/ENLITEOS/.Password+v10.05>

<sup>310</sup> <https://kb.igel.com/display/ENLITEOS/.Password+v10.05>



## Taskbar

Menu path: **Setup > User Interface > Desktop > Screenlock / Screensaver > Taskbar**

Taskbar settings for the login dialog

- Show taskbar in login screen. (Default)
- Show clock. (Default)
- Show keyboard layout switcher. (Default)
- Show on-screen keyboard button.
- Start on-screen keyboard automatically.
- Show reboot button.
- Show shutdown button. (Default)

Taskbar settings when the screenlock is active

- Show taskbar in screenlock. (Default)
- Show clock. (Default)
- Show keyboard layout switcher. (Default)
- Show on-screen keyboard button.
- Start on-screen keyboard automatically.
- Show reboot button.
- Show shutdown button.
- Show logoff button.

There is no separate option for enabling/disabling network connection icons in the login dialog and/or on the locked screen. With **Show taskbar in login screen** and **Show taskbar in screenlock** enabled, they appear automatically if the option **Enable tray icon** is activated under **Setup > Network > LAN Interfaces > Interface 1 (or Interface 2, Wireless)** and/or under **Setup > Network > Mobile Broadband** (and/or **VPN**).

The network connection icons in the login dialog and on the locked screen, with the exception of the Wi-Fi icon, serve for information purposes only and thus are inactive on clicking. The Wi-Fi icon invokes a [dialog for turning Wi-Fi on/off](#)(see page 1182) or the [Wireless Manager](#)(see page 1180) in case it is activated under **Setup > Network > LAN Interfaces > Wireless**.



## Screensaver

Menu path: **Setup > User Interface > Desktop > Screen Lock/Saver > Screensaver**

- **Screen background color:** Color palette for determining the background color of the screen.
  - **Enable image display**
    - An image will be shown as the screensaver. (default)
  - **File for screen saver logo:** Complete path for an individual image file or directory that contains an unlimited number of images. If no path is given, the IGEL logo will be used.
- If you enter a folder instead of a single image file as the source, all images in the folder will be displayed as a slide show, the **display time** for the images can be configured.
- **One image per monitor**
    - If a number of monitors are used, a different image will be shown on each one. (default)
    - Images will be distributed over the monitors.
  - **Image duration:** Time in seconds until the image is changed. (default: 10)
  - **Image display mode:** Type of display. The following are available to choose from:
    - Small-sized hopping - Small images are shown in changing positions.
    - Medium-sized hopping - Larger images are shown in changing positions.
    - Full-screen center cut-out - The images are shown in full-screen size. However, they may be clipped.
    - Full-screen letterbox - The images are shown as large as possible in relation to the screen size.
  - **Clock display monitor:** Selects the monitor on which the clock is to be shown. The following are available to choose from:
    - None
    - All
    - A specific monitor
  - **Show seconds:** Shows the seconds too in digital format.
  - **Clock display size:** The following sizes are available to choose from:
    - Tiny
    - Small
    - Medium
    - Large
    - Huge
  - **Horizontal clock position**
    - Left
    - Center
    - Right
  - **Vertical clock position**
    - Top
    - Center
    - Bottom
  - **Clock background color:** Color palette for determining the background color of the clock.
  - **Clock background opacity percentage:** 75% is preset.



- **Clock foreground color:** Color palette for determining the foreground color of the clock.

### 3.10.5 Input

Menu path: **Setup > User Interface > Input**

These setup pages allow you to set the keyboard layout and other input options.

The following input devices can be set up:

- [Keyboard](#)(see page 1161)
- [Additional Keyboard Layouts](#)(see page 1162)
- [Mouse](#)(see page 1162)
- [Touchpad](#)(see page 1163)
- [Touchscreen](#)(see page 1165)
- [Signature Pad](#)(see page 1167)

#### Keyboard

Menu path: **User Interface > Input > Keyboard**

In this area, you can configure the keyboard.

**Keyboard layout:** Specify the keyboard layout. The selected layout applies to all parts of the system including emulations, window sessions and X applications.

##### Enable dead keys

Dead keys can be used to enter special characters.

**Keyboard type:** Specifies the keyboard type.

Possible values:

- [Default](#): Automatically selects the keyboard type according to the computer type (Macbook, Chromebook or PC105 for all others).
- Standard PC keyboard (105 keys)
- IBM keyboard (122 keys)
- Trimodal keyboard
- Sun Type 6 keyboard
- Chromebook
- Macbook
- Macbook international
- Thinkpad

##### Show indicator in taskbar

Shows the language code for the keyboard in the taskbar.

#### Character Repeat

**Repeat delay:** Determines the delay (in milliseconds) before automatic repetition begins.



**Repeat rate:** Determines the number of times a character repeats per second.

#### Start with NumLock on

NumLock will be enabled automatically during the boot process.

#### Secure keyboard input with Cherry SECURE BOARD

A secure keyboard input mode will be enabled for the connected Cherry SECURE BOARD. In this mode, keyboard traffic between the keyboard and the endpoint is transmitted over a TLS 1.3 encrypted connection. The standard keyboard channel will be locked, which means that keyboard input devices without the secure mode will be blocked; see <https://www.cherry-world.com/cherry-secure-board-1-0.html>.

## Additional Keyboard Layouts

Menu path: **Setup > User Interface > Input > Additional Keyboard Layouts**

In this area, you can define additional keyboard layouts which can be selected by the user.

- **Enable this layout**
  - Keyboard layout is enabled and can be defined.
- **Keyboard layout:** Selects the language for the keyboard layout.
- **Enable dead keys:** Enable this function if the keyboard used supports dead keys for special characters.
- **Hotkey**
  - A hotkey allowing you to switch to this keyboard can be defined.
- **Key:** Select a key for the key combination.
- **Modifier:** If necessary, select an additional modifier.

Hotkey for default keyboard layout

- **Enable hotkey to switch to the default keyboard layout**
  - A hotkey which takes you back to the default keyboard layout can be defined. This is useful when a number of keyboard layouts are configured.

Hotkey for next keyboard layout

- **Enable hotkey to switch between a number of keyboard layouts**
    - A hotkey which switches to the next keyboard layout can be defined. This is useful when a number of keyboard layouts are configured.
- Further settings can be configured under [On-screen Keyboard](#)<sup>311</sup>.

## Mouse

Menu path: **Setup > User Interface > Input > Mouse**

In this area, you can configure the mouse.

- **Lefthand mode**
  - The mouse is switched to left-handed mode.

---

<sup>311</sup> <https://kb.igel.com/display/igelos1005/On-Screen+Keyboard>



- **Emulation 3 Button Mouse:** Enables/disables emulation of the third (middle) mouse button for mice with only two physical buttons. This third button is emulated by pressing both buttons at the same time. If 3-button emulation was enabled, the emulation time limit determines how long (in milliseconds) the driver waits before deciding whether two buttons were pressed at the same time.
- **Hide Cursor:** The mouse pointer will be hidden after the defined time limit.
- **Pointer Speed:** Determines the mouse resolution in counts per inch.
- **Double Click Interval:** Changes the maximum interval in milliseconds between two consecutive mouse clicks which are to be recognized as a double-click.
- **Double Click Distance:** Changes the maximum distance in pixels between two clicks which are to be recognized as a double-click. The object under the second click is double-clicked.

## Touchpad

Menu path: **Setup > User Interface > Input > Touchpad**

Here, you can configure touchpad settings.

The actual settings depend on the hardware supported by the particular touchpad.

- **Enable Touchpad**  Enable the touchpad
- **Hotkey** Each time you press the hotkey, you toggle the touchpad on or off.
  - **Modifiers:** Modifiers for the hotkey
  - **Key:** Key for the hotkey
- **Custom configuration**
  - Using the following options, adapt the touchpad to your needs.
  - No custom configuration (default)
- **Operation Mode:** Allows various touchpad modes.  
Possible values:
  - Enable touchpad
  - Switch off touchpad
  - Turn off tapping and scrolling only
- **Min speed:** Minimum speed of the pointer in seconds (default: 1.00)
- **Max speed:** Maximum speed of the pointer in seconds (default: 1.75)
- **Acceleration:** Acceleration from the minimum to the maximum speed in seconds (default: 0.01)

The following settings apply by default:

- **Top Left Action:** No action
- **Bottom Left Action:** No action
- **Top Right Action:** Middle mouse button
- **Bottom Right Action:** Right mouse button

With some touchpads, you can assign functions to the four corners. Specify which mouse button is clicked by tapping in the relevant corner:

- No action



- Left mouse button
- Middle mouse button
- Right mouse button

## Touchpad Scrolling

Define the properties for vertical and horizontal scrolling here.

### Vertical

- **Vertical scrolling:**
  - The right edge of the touchpad will be used as a vertical scrollbar. The vertical scroll speed can be set.
  - The right edge is not enabled as a scrollbar. (default)
- **Vertical scroll speed:** Specifies from what distance scrolling is recognized when moving in a vertical direction. (default: 25.00)
- **Scroll vertically with two fingers:**
  - Two-finger scrolling is enabled for vertical scrolling.
  - Two-finger scrolling is disabled.

### Horizontal

- **Horizontal scrolling:**
  - The bottom edge of the touchpad will be used as a horizontal scrollbar. The horizontal scroll speed can be set.
  - The bottom edge is not enabled as a scrollbar. (default)
- **Horizontal scroll speed:** Specifies from what distance scrolling is recognized when moving in a horizontal direction. (default: 25.00)
- **Scroll horizontally with two fingers:**
  - Two-finger scrolling is enabled for horizontal scrolling.
  - Two-finger scrolling is disabled.

## Touchpad Advanced

Further settings are possible here:

- **Corner coasting**
  - You can continue scrolling if your finger reaches the corner when scrolling vertically or horizontally along the touchpad edges.
- **Circular scrolling**
  - You can scroll in a circle. In the selection menu, specify where circular scrolling is to begin.
    - **Circular scrolling enabled at**
    - All Edges
    - Top Edge
    - Top Right Corner
    - Right Edge
    - Bottom Right Corner
    - Bottom Edge



Bottom Left Corner

Left Edge

Top Left Corner

- **Tap and drag gesture**

You can move items by tapping and dragging them.

- **Locked drags**

The tap and drag gesture ends only after an additional tap; it will otherwise end when you let go.

- **Palm detect**

Avoids triggering a function accidentally with the palm of your hand. The function must be supported by the device.

- **ClickPad**

ClickPads are permitted. These are touchpads with so-called integrated soft buttons on which physical clicks are possible.

## Touchscreen

Menu path: **Setup > User Interface > Input > Touchscreen**

Here, you can configure a touchscreen. To ensure that you can open the setup and navigate within it, the initial configuration should take place with a mouse and keyboard connected.

You will find an up-to-date list of the touchscreens supported by IGEL in the [IGEL Third Party Hardware Database<sup>312</sup>](#).

### Enable touchscreen

The touchscreen is enabled.

The touchscreen is disabled. (Default)

**Touchscreen type:** Selects the touchscreen driver which is to be used.

Possible options:

- "EvTouch (USB)"
- "eGalax"
- "Elo Multitouch (USB)"
- "Elo Singletouch (USB)"
- "TSharc"

You will find the complete list of supported devices in the [IGEL Hardware Database<sup>313</sup>](#).

### Touchscreen already calibrated

If you enable the touchscreen function, the touchscreen must be calibrated first.

Calibration starts automatically after each system boot. (Default)

Calibration does not start automatically after each system boot.

### Swap X and Y values

X values are interpreted as Y values and Y values as X values. Enable this option if the mouse pointer moves vertically when you move your finger in a horizontal direction.

<sup>312</sup> <https://www.igel.com/linux-3rd-party-hardware-database/>

<sup>313</sup> <https://www.igel.com/linux-3rd-party-hardware-database/>



X and Y values are not swapped. (Default)

**Minimal X/Y value:** These values are determined by the calibration tool. However, you can also change them manually. (Default: 0)

**Maximal X/Y value:** These values are determined by the calibration tool. However, you can also change them manually. (Default: 4000)

**Untouch delay:** The maximum permitted time (in milliseconds) between two instances of contact which are still registered as a single touch. When moving windows by drag & drop, for example, your contact with the screen may inadvertently be interrupted. Increasing this value prevents the thin client from recognizing two individual contacts if you let go in this way. (Default: 3)

**Report delay:** Determines how long (in milliseconds) the screen needs to be touched in order for the contact to be recognized. (Default: 2)

#### Emulate right button

A right-click is generated by touching the screen for a long time.

Touching the screen for a long time does not generate a right-click. (Default)

**Right button timeout:** Time (in milliseconds) after which a right-click is generated. (Default: 1000)

**Set driver-specific defaults:** Loads the preset for the driver currently selected under **Touchscreen type**. Click on this button once after changing the touchscreen type or to restore the default settings.

#### Multimonitor

**Graphic card:** Graphics card assigned to the selected touchscreen. A graphics card can have more outputs than are actually used. In order to ensure transparency, you may need to assign the graphics cards manually.

If “Automatic” is set for the **Touchscreen monitor** and no configurable monitor is found for the selected graphics card, the next available monitor will be used by another graphics card.

**Touchscreen monitor:** Assigns a monitor connection to the touchscreen. Example: **DisplayPort** (Default: Automatic)

To set up a touchscreen and on-screen keyboard, proceed as follows:

- ▶ Enable the on-screen keyboard for the touchscreen use under **IGEL Setup > Accessories > On-Screen Keyboard**; see [On-Screen Keyboard](#)(see page 1088).

The layout for the normal keyboard will also be used for the on-screen keyboard.

- ▶ Calibrate the touchscreen for optimum contact recognition. The **touchscreen calibration** application can be found under **Application Launcher > System**.

In the calibration program, you will see a pattern with calibration points which must be touched one after another.



## Signature Pad

Menu path: **Setup > User Interface > Input > Signature Pad**

You can connect signature pads from the following manufacturers here:

- StepOver;
- signotec.

### StepOver

- **Enable StepOver TCP Client**

- The StepOver TCP Client is enabled and you can use USB signature pads from this manufacturer in sessions.
- The StepOver TCP Client is not enabled. (Default)
- **Listening TCP port:** If necessary, you can change the TCP port. (Default: 8888)

### signotec

- **Enable signotec VCOM daemon**

- The signotec VCOM daemon is enabled and you can use USB signature pads from this manufacturer in sessions.
- The signotec VCOM daemon is not enabled. (Default)

See also the tip & trick [Connecting Signature Pads](#)(see page 681).

## 3.10.6 Hotkeys

Menu path: **Setup > User Interface > Hotkeys > Commands**

In order to make it easier to use your thin client, hotkeys are available for frequent operating routines. A hotkey is a combination of one or more modifiers and an alphanumeric key.

You can enable or disable hotkeys and change the keys used. For more information, see [Commands](#)(see page 1167).

- 
- [Commands](#)(see page 1167)

### Commands

Menu path: **Setup > User Interface > Hotkeys > Commands**

You can activate, deactivate and change the hotkeys that are available to the user.

#### Settings in the Dialog

##### Hotkey

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.



**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

## Available Hotkeys and their Default Settings

### Hide all windows and show desktop

Default:

- activated
- **Modifiers:** Ctrl | Mod4
- **Key:** d
- **Appliance Mode Access:** deactivated

### Mapping Ctrl+Alt+End to Ctrl+Alt+Del for Citrix sessions

Default:

- deactivated
- **Modifiers:** Ctrl | Alt + End
- **Key:** End
- **Appliance Mode Access:** deactivated



### Open start menu

Default:

- deactivated
- **Modifiers:** Shift + Super
- **Key:** Super\_L
- **Appliance Mode Access:** deactivated

### Open start menu (alternative):

Default:

- deactivated
- **Modifiers:** Shift + Super
- **Key:** Super\_L
- **Appliance Mode Access:** deactivated

### Screenshot of active window

Default:

- deactivated
- **Modifiers:** Ctrl|Alt
- **Key:** Print
- **Appliance Mode Access:** deactivated

### Screenshot of entire screen

Default:

- deactivated
- **Modifiers:** Ctrl|Shift
- **Key:** Print

### Switch between active windows using Task Switcher

Default:

- activated
- **Modifiers:** Ctrl|Alt
- **Key:** Tab
- **Appliance Mode Access:** deactivated

### Switch between active windows using Task Switcher (backwards)

Default:

- activated
- **Modifiers:** Ctrl|Alt|Shift
- **Key:** Tab
- **Appliance Mode Access:** deactivated

### Switch focus to next window

Default:

- activated
- **Modifiers:** Ctrl
- **Key:** Escape
- **Appliance Mode Access:** deactivated

**Switch focus to next window (alternative)**

Default:

- activated
- **Modifiers:** Ctrl|Alt
- **Key:** Up
- **Appliance Mode Access:** deactivated

**Switch focus to next window (reverse order)**

Default:

- activated
- **Modifiers:** Ctrl|Alt
- **Key:** Down
- **Appliance Mode Access:** deactivated

**Volume down (multimedia key)**

Default:

- activated
- **Modifiers:** (none)
- **Key:** XF86AudioLowerVolume

**Volume mute (multimedia key)**

Default:

- activated
- **Modifiers:** (none)
- **Key:** XF86AudioMute
- **Appliance Mode Access:** deactivated

**Volume up (multimedia key)**

Default:

- activated
- **Modifiers:** (none)
- **Key:** XF86AudioRaiseVolume
- **Appliance Mode Access:** deactivated

### 3.10.7 Font Services

Menu path: **Setup > User Interface > Font Services**

You can import further fonts in addition to the ones provided by IGEL:

- [XC Font Service](#)(see page 1170)
- [NFS Font Service](#)(see page 1171)

#### XC Font Service

Menüpfad: **Setup > User Interface > Font Services > XC Font Service**

In this area, you can configure the XC Font Service.



- **Enable XC Font Service**

- The XC Font Service is enabled.
- Der XC Font Service is not enabled. (Default)

Once you have enabled the XC Font Service, you can define the following settings:

- **XC Font Server:** The server on which the XC Font Service is running.
- **Port Number:** The port number on which the XC Font Service is available. (Default: 7100)
- **Prefer Local Fonts**
  - Local fonts are used before a request is sent to the font server.
  - Local fonts are not preferred. (Default)

## NFS Font Service

Menu path: **Setup > User Interface > Font Services > NFS Font Service**

Using the NFS font service is another way to import additional fonts. The NFS font service also offers the advantage that the mount point for the fonts can be configured. This is necessary for a number of remote applications that search for your fonts in a specific directory.

To define and enable an NFS font path entry in order to use the NFS font service, proceed as follows.

1. Click on **Add**  to open the dialog window:
  - **Local Path:** Defines the local directory for the mount point
  - **NFS Server:** Name or IP address of the server that makes available the font directories via NFS.
  - **Remote Path:** Path on the server under which the fonts are available.
  - **Prefer Local Fonts**
    - Local fonts are used before a request is sent to the font server.
2. Click on **OK** to enable the entry.
3. Export the font directory on the server via NFS read-only for the thin client.

## 3.11 Network

In this area, you can configure network connections of the endpoint device.

- [LAN Interfaces](#)(see page 1172)
- [Mobile Broadband](#)(see page 1186)
- [DHCP Client](#)(see page 1187)
- [VPN](#)(see page 1189)
- [SCEP Client \(NDES\)](#)(see page 1207)
- [Routing](#)(see page 1210)
- [Hosts](#)(see page 1211)
- [Network Drives](#)(see page 1212)
- [Proxy](#)(see page 1214)



### 3.11.1 LAN Interfaces

Menu path: **Setup > Network > LAN Interfaces**

Here, you can configure the LAN interfaces.

#### Predictable Network Interface Names (PNINs)

As of IGEL OS 11.06, the names of Ethernet and WLAN interfaces are predictable network interface names (PNINs), see [Predictable Network Interface Names](#)<sup>314</sup>. This ensures the stability of interface names on reboot and generally improves the reliability of associating configurations with interfaces.

- As "eth0", "eth1", and "wlan0" have been replaced by PNINs, configurations or custom scripts that include the old names of Ethernet and WLAN interfaces, e.g. eth0, eth2, wlan 0, have to be adjusted.

The following already existing configurations do NOT require manual adjustment since old names eth0, eth1, etc. will internally be replaced by the correct PNINs automatically:

- [Tcpdump](#)(see page 405)
- **Bind interface** under **Security > Smartcard > Services**, see [Services](#)(see page 1249)
- To view the PNINs and the order of the configured interfaces, you can use the following commands. The default interface is always listed first, the second interface is listed second, etc.
  - Ethernet (LAN):** cat /config/net/en-interfaces
  - WLAN:** cat /config/net/wl-interfaces

(Note: Only the first wireless interface (former wlan0) is supported. All other wireless interfaces will be ignored.)
- If you need to configure more than two Ethernet interfaces, go to **System > Registry > network.interfaces.ethernet.device%** and add an instance.  
To explicitly assign a configuration instance to a certain interface, enter the corresponding PNIN for the registry key **network.interfaces.ethernet.device%.ifname**.

#### Activate default interface (Ethernet)

The default interface is enabled. (Default)

The Ethernet interface is not enabled.

**Get IP from the DHCP server:** The IP address of the client will be obtained automatically using DHCP. (Default)

DHCP options can be specified under [DHCP Client](#)(see page 1187).

**Specify an IP address:** The IP address and the network mask are entered manually.

**IP address:** IP address of the device.

**Network mask:** Network mask of the device.

**Default gateway:** IP address of the default gateway.

**Enable**

<sup>314</sup> <https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/>



- Routing via the default gateway is enabled.  
 Routing via the default gateway is not enabled. (Default)

**Terminal name:** Local name of the device. If the field is empty, the default name combined of 'ITC' with a MAC address will be generated.

#### Enable DNS

- The manual DNS configuration will be used.  
 The DNS configuration will be carried out by DHCP or BOOTP. (Default)

**Default domain:** Usually the name of the local network.

**Name server:** IP address of the name server to be used.

**Name server:** IP address of an alternative name server.

#### Manually overwrite DHCP settings

- The default route, the domain name, and the DNS server will be overwritten by manual entries.  
 Manual entries will not overwrite DHCP settings. (Default)

#### Dynamic DNS registration:

- The terminal name will be registered dynamically via the DNS or DHCP server.  
 The terminal name will not be registered dynamically. (Default)

#### Dynamic DNS registration method

- DHCP: Updates the terminal name through DHCP option 81.
- DNS: Sends updates to the DNS server in accordance with RFC 2136.

**TSIG key file for additional DNS authentication:** Path to the private key if TSIG-based DDNS registration is used.

- 
- [Individual Interface](#)(see page 1173)
  - [Wireless](#)(see page 1178)

## Individual Interface

Menu path: **Setup > Network > LAN Interfaces > [Interface]**



### Predictable Network Interface Names (PNINs)

As of IGEL OS 11.06, the names of Ethernet and WLAN interfaces are predictable network interface names (PNINs), see [Predictable Network Interface Names](#)<sup>315</sup>. This ensures the stability of interface names on reboot and generally improves the reliability of associating configurations with interfaces.

- As "eth0", "eth1", and "wlan0" have been replaced by PNINs, configurations or custom scripts that include the old names of Ethernet and WLAN interfaces, e.g. eth0, eth2, wlan 0, have to be adjusted.

The following already existing configurations do NOT require manual adjustment since old names eth0, eth1, etc. will internally be replaced by the correct PNINs automatically:

- [Tcpcdump](#)(see page 405)
- **Bind interface under Security > Smartcard > Services**, see [Services](#)(see page 1249)
- To view the PNINs and the order of the configured interfaces, you can use the following commands. The default interface is always listed first, the second interface is listed second, etc.  
**Ethernet (LAN):** cat /config/net/en-interfaces  
**WLAN:** cat /config/net/wl-interfaces  
 (Note: Only the first wireless interface (former wlan0) is supported. All other wireless interfaces will be ignored.)
- If you need to configure more than two Ethernet interfaces, go to **System > Registry > network.interfaces.ethernet.device%** and add an instance.  
 To explicitly assign a configuration instance to a certain interface, enter the corresponding PNIN for the registry key **network.interfaces.ethernet.device%.ifname**.

### Activate default interface (Ethernet)

- The default interface will be enabled. (Default)  
 The Ethernet interface will not be enabled.

### Get IP from DHCP server

- The IP address of the client will be obtained automatically using DHCP. (Default)

DHCP options can be specified under [DHCP Client](#)(see page 1187).

**Specify an IP address:** The IP address and the network mask are entered manually.

**IP address:** IP address of the device.

**Network mask:** Network mask of the device.

### IPv6 Configuration

- Compatibility mode: Behavior of earlier firmware versions.
- Disabled: IPv6 completely disabled.
- Automatic: IPv6 auto configuration based on router advertisements (can include DHCPv6).  
 For further information, see [RFC 4861](#).<sup>316</sup>

<sup>315</sup> <https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/>

<sup>316</sup> <https://tools.ietf.org/html/rfc4861>



- DHCPv6: IPv6 configuration using DHCPv6 if router advertisements are not available.  
This is mentioned in [RFC 4862 Section 5.5.2](#).<sup>317</sup>

### **Network link type**

- [Auto sense](#)
- 1000 Mb/s full duplex
- 100 Mb/s full duplex
- 100 Mb/s half duplex
- 10 Mb/s full duplex
- 10 Mb/s half duplex

### **Force auto-negotiation**

With this option, problems with half/full duplex for specific switches that expect the auto-negotiation flag for fixed bandwidths can be addressed.

Automatic negotiation will not be forced. (Default)

### **Enable tray icon**

A tray icon for the network interface will be shown. (Default)

### **Enable context menu**

A context menu will be shown when you click on the tray icon. (Default)

### **Enable network info dialog**

A dialog window with information regarding the network connection will be shown when you click on the context menu. (Default)

- [Authentication](#)(see page 1175)
- [Wake-on-LAN](#)(see page 1177)

### Authentication

Menu path: **Setup > Network > LAN Interfaces > [Interface] > Authentication**

Here, you can enable and configure network port authentication.

#### **Enable IEEE-802.1x authentication**

Network port authentication is enabled.

Network port authentication is not enabled. (Default)

If you enable authentication, further options are available:

**EAP type:** Here, you can select the authentication procedure:

- [PEAP](#): Protected Extensible Authentication Protocol
- [TLS](#): Transport Layer Security with client certificate
- [TTLS](#): Tunneled Transport Layer Security
- [FAST](#): Flexible Authentication via Secure Tunneling

<sup>317</sup> <https://tools.ietf.org/html/rfc4862#section-5.5.2>



**Anonymous identity:** This identity is sent by authentication instead of the actual **Identity**. This prevents the disclosure of the actual identity of the user. The anonymous identity is relevant for any of the above-mentioned **EAP types**, except for "TLS".

**Auth method:** The following authentication methods are available:

- MSCHAPV2: Microsoft Challenge Handshake Authentication Protocol
- TLS: Transport Layer Security with client certificate
- GTC: Generic Token Card
- MD5: MD5-Challenge
- PAP: Password Authentication Protocol

#### Validate server certificate

The server's certificate is checked cryptographically. (Default)

**CA Root certificate:** The path to the CA root certificate file. This can be in PEM or DER format.

**Identity:** User name for RADIUS

**Password:** Password for network access

If you leave the **Identity** and **Password** fields empty, an entry mask for authentication purposes will be shown. However, this does not apply to the methods with a client certificate (TLS and PEAP-TLS) where these details are mandatory.

The following settings are relevant if you have selected "TLS" as **EAP type**:

#### Manage certificates with SCEP (NDES)

Client certificates will automatically be managed with [SCEP](#)(see page 1207).

Client certificates will not be managed with [SCEP](#)(see page 1207). (Default)

**Client certificate:** Path to the file with the certificate for client authentication in the PEM (base64) or DER format.

If a private key in the PKCS#12 format is used, leave this field empty.

**Private key:** Path to the file with the private key for the client certificate. The file can be in the PEM (base64), DER, or PFX format. The **Private key password** may be required for access.

**Identity:** User name for network access

**Private key password:** Password for the **Private key** for the client certificate

The following setting is relevant if you have selected "FAST" as **EAP type**:

**Automatic PAC provisioning:** Specifies how the PAC (Protected Access Credential) is delivered to the client. Possible options:

- "disabled": PAC files have to be transferred to the device manually, e.g. via UMS file transfer.
- "unauthenticated": An anonymous tunnel will be used for PAC provisioning.
- "authenticated": An authenticated tunnel will be used for PAC provisioning.



- "unrestricted": Both authenticated and unauthenticated PAC provisioning is allowed. PAC files are automatically created after the first successful authentication.

PAC files are stored in `/wfs/eap_fast_pacs/`.

PAC file names are automatically derived from the **Identity**, but are coded. In the case of the manual PAC provisioning, you can determine the PAC file names with the following script: `/bin/gen_pac_filename.sh`

In tests with hostapd, it has been necessary to disable TLS 1.2. To do that, enter the following command for **System > Registry**

```
> network.interfaces.ethernet.device% ieee8021x.phase1_direct: tls_disable_tls1_2=1
```

## Wake-on-LAN

Menu path: **Setup > Network > LAN Interfaces > [Interface] > Wake-On-LAN**

Select the packets or messages with which the endpoint device can be started via the network.

For further information on the Wake-on-LAN functionality of the UMS, see [Wake-on-LAN<sup>318</sup>](#).

### **Wake on magic packet**

The device can be started with a Wake-on-LAN magic packet. (Default)

### **Wake on ARP packet**

The device can be started with a Wake on ARP packet.

The device cannot be started with a Wake on ARP packet. (Default)

### **Wake on broadcast message**

The device can be started with a Wake on broadcast message.

The device cannot be started with a Wake on broadcast message. (Default)

### **Wake on multicast message**

The device can be started with a Wake on multicast message.

The device cannot be started with a Wake on multicast message. (Default)

### **Wake on physical activity**

The device can be started with a physical activity.

The device cannot be started with a physical activity. (Default)

### **Wake on unicast message**

The device can be started with a Wake on unicast message.

The device cannot be started with a Wake on unicast message. (Default)

---

<sup>318</sup> <https://kb.igel.com/display/endpointmgmt605/Wake-on-LAN>



## Wireless

Menu path: **Setup > Network > LAN Interfaces > Wireless**

In this area, you can configure everything relating to your wireless connections.

Configure the [wireless frequency range](#)(see page 1186) to ensure that your device meets the local regulations for wireless equipment.

You will find details of compatible wireless hardware in the [IGEL Linux 3rd Party Hardware Database](#)<sup>319</sup>.

### Predictable Network Interface Names (PNINs)

As of IGEL OS 11.06, the names of Ethernet and WLAN interfaces are predictable network interface names (PNINs), see [Predictable Network Interface Names](#)<sup>320</sup>. This ensures the stability of interface names on reboot and generally improves the reliability of associating configurations with interfaces.

- As "eth0", "eth1", and "wlan0" have been replaced by PNINs, configurations or custom scripts that include the old names of Ethernet and WLAN interfaces, e.g. eth0, eth2, wlan 0, have to be adjusted.

The following already existing configurations do NOT require manual adjustment since old names eth0, eth1, etc. will internally be replaced by the correct PNINs automatically:

- [Tcpcdump](#)(see page 405)
- **Bind interface** under **Security > Smartcard > Services**, see [Services](#)(see page 1249)
- To view the PNINs and the order of the configured interfaces, you can use the following commands. The default interface is always listed first, the second interface is listed second, etc.  
**Ethernet (LAN):** cat /config/net/en-interfaces  
**WLAN:** cat /config/net/wl-interfaces  
 (Note: Only the first wireless interface (former wlan0) is supported. All other wireless interfaces will be ignored.)
- If you need to configure more than two Ethernet interfaces, go to **System > Registry > network.interfaces.ethernet.device%** and add an instance.  
 To explicitly assign a configuration instance to a certain interface, enter the corresponding PNIN for the registry key **network.interfaces.ethernet.device%.ifname**.

### Activate wireless interface

The default interface is enabled.

The wireless interface is not enabled. (Default)

**Get IP from DHCP server:** The IP address of the endpoint device will be obtained automatically using DHCP. (Default)

DHCP options can be specified under [DHCP Client](#)(see page 1187).

<sup>319</sup> <https://www.igel.com/linux-3rd-party-hardware-database/>

<sup>320</sup> <https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/>



**Specify IP address:** The IP address and the network mask are entered manually

**IP address:** IP address of the endpoint device

**Network mask:** Network mask of the endpoint device

#### IPv6 configuration:

- Compatibility mode: Behavior of earlier firmware versions
- Disabled: IPv6 is completely disabled.
- Automatic: IPv6 auto-configuration is based on router advertisements (can include DHCPv6). You will find further information in [RFC 4861](#)<sup>321</sup>.
- DHCPv6: IPv6 configuration using DHCPv6 if router advertisements are not available. You will find further information in [RFC 4862 Section 5.5.2](#)<sup>322</sup>.

#### Enable tray icon

A tray icon for the wireless interface will be shown. (Default)

#### Enable context menu

A context menu will be shown when you click on the tray icon. (Default)

#### Enable network info dialog

A dialog window with information regarding the network connection will be shown when you click on the context menu. (Default)

#### Enable Wireless Manager

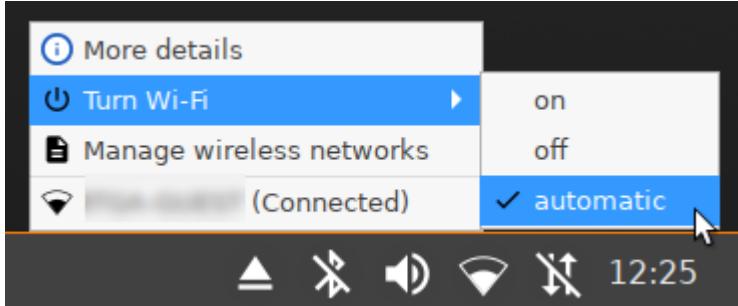
The [Wireless Manager](#)(see page 1180) is enabled. This tool allows the user to establish a connection to a wireless network quickly.

The Wireless Manager is disabled. (Default)

#### Enable Wi-Fi automatic switch

When a device is disconnected from the network cable, Wi-Fi is automatically turned on. When the device is connected again to the network cable, Wi-Fi is automatically turned off.

- If the registry key **System > Registry > network.applet.wireless.enable\_wifi\_switch** (see [Switch for the Wi-Fi Connection](#)(see page 1182)) is enabled, automatic mode is added to the Wi-Fi switch.



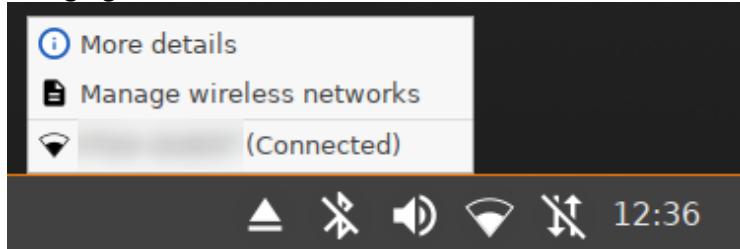
- If the registry key **System > Registry > network.applet.wireless.enable\_wifi\_switch** is disabled, Wi-Fi automatic switch functionality will work in the background. The option for

<sup>321</sup> <https://tools.ietf.org/html/rfc4861>

<sup>322</sup> <https://tools.ietf.org/html/rfc4862#section-5.5.2>



changing the Wi-Fi mode is not shown.



An automatic connection to a wireless network is disabled. (Default)

If you use wireless regularly, it is recommended to enable the following options: **Enable tray icon**, **Enable context menu**, and **Enable Wireless Manager**. Via the **Wireless Manager**, you can use [IGEL Café Wireless](#)(see page 1328).

If you have to frequently switch between LAN and WLAN networks, it is also useful to activate **Enable Wi-Fi automatic switch**.

- [Wireless Manager](#)(see page 1180)
- [Switch for the Wi-Fi Connection](#)(see page 1182)
- [Default Wi-Fi Network](#)(see page 1182)
- [Additional Wi-Fi Networks](#)(see page 1185)
- [Wireless Regulatory Domain](#)(see page 1186)

## Wireless Manager

The Wireless Manager tool allows the user to connect quickly to available wireless networks.

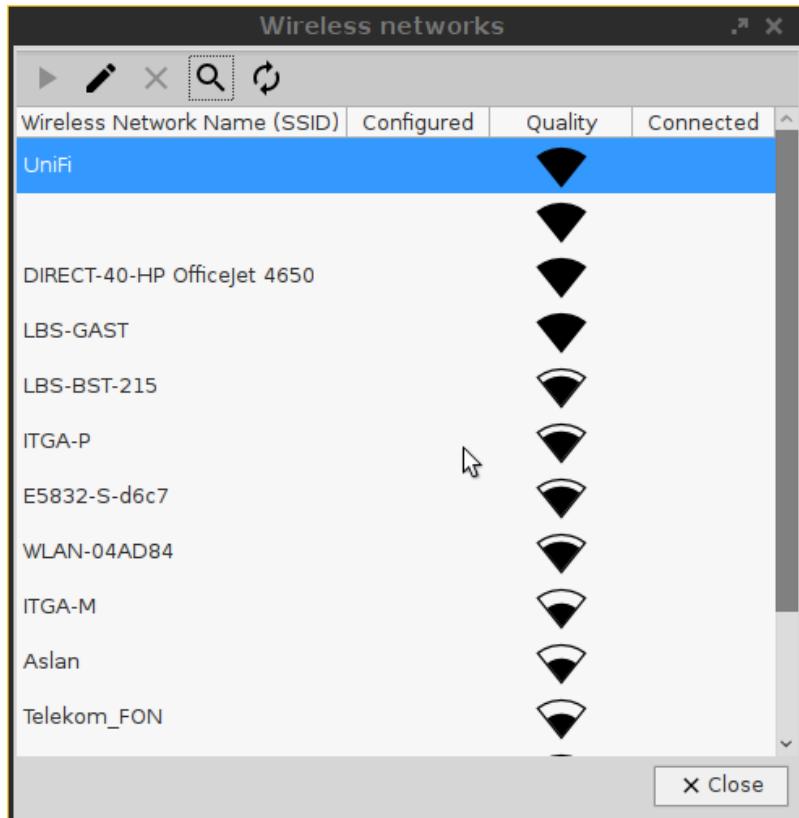
The Wireless Manager can be enabled under **Network > LAN Interfaces > Wireless**.

You can bring up the Wireless Manager from the tray icon for wireless:



See also [How to Launch the Wireless Manager within IGEL OS when the Taskbar Is Hidden](#)(see page 416).

1. Click on the tray icon for wireless and select **Manage wireless networks** from the context menu.



2. Search for available networks.

- The list of active networks is sorted according to the quality of their signal strength.
- Previously configured connections are flagged with a tick in the **Configured** column.
- The connection currently active is likewise flagged with a symbol under **Connected**.

3. Double-click on a network in the list in order to open the entry mask.

You can either **permanently save** the logon information or enter it each time you establish a connection to this network.

Click on the key symbol in order to display the key phrase while you are typing.

4. Click on the **Connect network** button in order to establish the previously configured connection:  
The tray icon will change to show the connection quality.

Hidden networks appear in the Wireless Manager with the network name empty or can be defined using the **Search for network** button.

In order to connect to a previously unknown hidden network, you must first enter the SSID before the access data are retrieved:

If you have configured the available connections, you will no longer need the Wireless Manager in order to establish a connection.

In the context menu for the tray icon, all available networks are listed and can be brought up from here.



5. The IGEL Setup shows all connections configured by the local user under **Network > LAN Interfaces > Wireless > Additional Wi-Fi Networks**.

See also [Café Wireless \(Wi-Fi\)](#)(see page 1328).

#### Switch for the Wi-Fi Connection

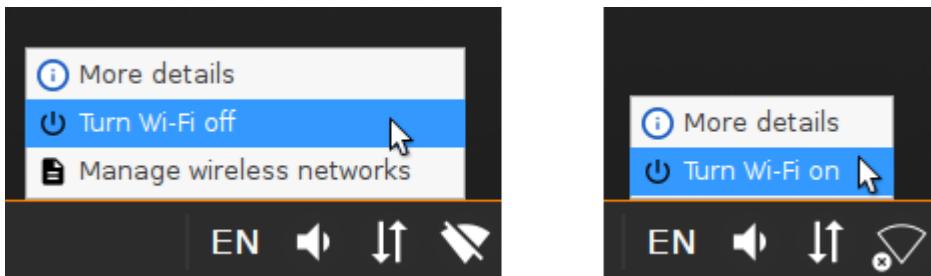
You can turn Wi-Fi off or on.

To use the switch for the Wi-Fi connection, **Enable Wi-Fi switch** under **Setup > System > Registry > Parameter > network > applet > wireless > enable\_wifi\_switch** must be activated. (Default)

#### Turning Wi-Fi Off or On

If You Are Logged In

- ▶ Select **Turn Wi-Fi off / Turn Wi-Fi on** from the context menu of the Wi-Fi tray icon.



If the Login Dialog Is Displayed or the Screen Is Locked

- ▶ To turn Wi-Fi off, click the tray icon and select **OK** in the **Turn Wi-Fi off** dialog. If the [Wireless Manager](#)(see page 1180) is activated, you can also use there the button .
- ▶ To turn Wi-Fi on, click and select **OK** in the **Turn Wi-Fi on** dialog.

#### Default Wi-Fi Network

Menu path: **Setup > Network > LAN Interfaces > Wireless > Default Wi-Fi network**

Here, you can configure wireless network connections.

**Disable Encryption:** No encryption will be used. (Default)

**Enable WEP Encryption:** WEP encryption will be used.

**Enable WPA Encryption:** WPA encryption will be used.

You will need to give further information depending on the encryption method chosen.

**Wireless Network Name (SSID):** Name of the wireless network (SSID)



For WEP Encryption

**Transmit key ID:** Choose from a maximum of four configurable keys. (Default: 1)

**Key Format:**

- ASCII
- Hexadecimal

**Key [1-4]:** Enter the key here.

Characters to be entered for WEP keys:

- For 64-bit encryption, 5 characters (ASCII) or 10 hex digits (hexadecimal)
- For 128-bit encryption, 13 characters (ASCII) or 26 hex digits (hexadecimal)

For WPA/WPA2/WPA3 Personal Encryption

**Network authentication**

- WPA Personal: Wi-Fi Protected Access Pre-Shared Key (WPA / IEEE 802.11i/D3.0)
- WPA2 Personal: Wi-Fi Protected Access Pre-Shared Key (WPA2 / IEEE 802.11i/RSN)
- WPA3 Personal: Wi-Fi Protected Access SAE (Simultaneous Authentication of Equals)

**Network key:** WPA network key/passphrase as set at the dial-in point. This is either an ASCII character string with a length of 8...63 or exactly 64 hexadecimal digits.

**Data encryption:**

- Default: The default value depends on which network authentication method is selected - TKIP for WPA, AES (CCMP) for WPA2.
- TKIP: Temporal Key Integrity Protocol (IEEE 802.11i/D7.0)
- AES (CCMP): AES in Counter mode with CBC-MAC (RFC 3610, IEEE 802.11i/D7.0)
- AES (CCMP) + TKIP: One of two encryption methods is selected by the access point.
- Automatic: The access point can choose the encryption method freely – nothing is stipulated.

**AP Scan mode:** Scan mode for access points

- Default
- Broadcast: Alternative for access points which allow the SSID broadcast
- No broadcast: Alternative for access points which refuse the SSID broadcast (hidden access points)

For WPA/WPA2 Enterprise Encryption

**Network authentication:**

- WPA Enterprise: Wi-Fi Protected Access with 802.1X authentication (WPA / IEEE 802.11i/D3.0)
- WPA2 Enterprise: Wi-Fi Protected Access with 802.1X authentication (WPA2/IEEE 802.11i/RSN)

**Data encryption:**

- Default: The default value depends on which network authentication method is selected - TKIP for WPA, AES (CCMP) for WPA2.
- TKIP: Temporal Key Integrity Protocol (IEEE 802.11i/D7.0)



- AES (CCMP): AES in Counter mode with CBC-MAC (RFC 3610, IEEE 802.11i/D7.0)
- AES (CCMP) + TKIP: One of two encryption methods is selected by the access point.
- Automatic: The access point can choose the encryption method freely – nothing is stipulated.

**AP Scan mode:** Scan mode for access points

- Default
- Broadcast: Alternative for access points which allow the SSID broadcast
- No broadcast: Alternative for access points which refuse the SSID broadcast (hidden access points)

#### EAP Type

- PEAP: Protected Extensible Authentication Protocol
- TLS: Transport Layer Security with client certificate
- TTLS: Tunneled Transport Layer Security
- FAST: Flexible Authentication via Secure Tunneling

**Anonymous identity:** This identity is sent by authentication instead of the actual **Identity**. This prevents the disclosure of the actual identity of the user. The anonymous identity is relevant for any of the above-mentioned **EAP types**, except for "TLS".

**Auth Method:** Method for authentication that is available for the selected EAP type  
Possible options:

- MSCHAPv2: Microsoft Challenge Handshake Authentication Protocol
- TLS: Transport Layer Security with client certificate
- GTC: Generic Token Card
- MD5: MD5-Challenge
- PAP: Password Authentication Protocol

#### Validate Server Certificate

The endpoint device validates the authenticity of the authentication server against the certificate file. This certificate file is stored under the path defined by **CA Root Certificate**.

The authenticity of the authentication server is not validated.

**CA Root Certificate:** Path and file name of the file that contains the certificates with which the authentication server authenticates itself.

**Identity:** User name that is stored at the authentication server

**Password:** Password relevant to the user name

The following settings are relevant if you have selected "TLS" as **EAP type**:

#### Manage certificates with SCEP (NDES)

- Client certificates will automatically be managed with [SCEP](#)(see page 1207).
- Client certificates will not be managed with [SCEP](#)(see page 1207). (Default)

**Client certificate:** Path to the file with the certificate for client authentication in the PEM (base64) or DER format.

If a private key in the PKCS#12 format is used, leave this field empty.



**Private key:** Path to the file with the private key for the client certificate. The file can be in the PEM (base64), DER, or PFX format. The **Private key password** may be required for access.

**Identity:** User name for network access

**Private key password:** Password for the **Private key** for the client certificate

Learn more from the how-to [Using WPA Enterprise / WPA2 Enterprise with TLS Client Certificates](#)(see page 399).

The following setting is relevant if you have selected "FAST" as **EAP type**:

**Automatic PAC provisioning:** Specifies how the PAC (Protected Access Credential) is delivered to the client. Possible options:

- "disabled": PAC files have to be transferred to the device manually, e.g. via UMS file transfer.
- "unauthenticated": An anonymous tunnel will be used for PAC provisioning.
- "authenticated": An authenticated tunnel will be used for PAC provisioning.
- "unrestricted

PAC files are stored in `/wfs/eap_fast_pacs/`.

PAC file names are automatically derived from the **Identity**, but are coded. In the case of the manual PAC provisioning, you can determine the PAC file names with the following script: `/bin/gen_pac_filename.sh`

In tests with hostapd, it has been necessary to disable TLS 1.2. To do that, enter the command `tls_disable_tls1_2=1` for the following registry keys:

- **System > Registry > network.interfaces.wirelesslan.device0.wpa.phase1\_direct**
- **System > Registry > network.interfaces.wirelesslan.device0.alt\_ssid%.wpa.phase1\_direct**

## Additional Wi-Fi Networks

Menu path: **Setup > Network > LAN Interfaces > Wireless > Additional Wi-Fi Networks**

You can add other wireless networks here. The settings options per wireless network correspond to those for the **Default Wi-Fi Network**(see page 1182).

To edit the wireless network list, proceed as follows:

- ▶ Click to create a new entry.
- ▶ Click to remove the selected entry.
- ▶ Click to edit the selected entry.
- ▶ Click to copy the selected entry.



## Wireless Regulatory Domain

Menu path: **Setup > Network > LAN Interfaces > Wireless > Wireless Regulatory Domain**

This page allows you to set the wireless device in accordance with local regulations.

**Wireless regulatory domains:** Select the area in which the device is located.

- Not configured
- Africa
- Arctic
- Asia
- Australia
- Europe
- North America
- South America
- World

**Location:** Select the country in which the device is located.

- Not configured
- Albania
- Armenia
- [...]
- Cyprus
- Austria

The list below sets out the technical requirements for the selected location for your information.

## 3.11.2 Mobile Broadband

Menu path: **Setup > Network > Mobile Broadband Network**

Here, you can change the settings for a modem or a surf stick. This function is available from IGEL Linux Version 10.03.100.

Ensure that data traffic is adequately secured. You can do this in the following ways:

- Use a private APN.
- Use OpenVPN and block traffic that would circumvent VPN with firewall rules.

If the device is already inserted and has been configured, the network connection will be established after the thin client boots. It can take between a few seconds and around 1 minute to establish a connection. The network connection will remain in place until the surf stick is removed or the thin client is put on standby or shut down.

The status of the network connection is shown in the system tray:

- The network connection is established; the thin client is online. This symbol is only shown if "Modem" is selected as the device type. If "Router" is selected as the device type, the symbol for a LAN connection will be shown.



- The network connection was interrupted; the thin client is offline. This symbol is only shown if "Modem" is selected as the device type. If "Router" is selected as the device type, the corresponding symbol for a LAN connection will be shown.

You can change the following settings:

- Enable mobile broadband**

- The mobile broadband network can be used if a supported modem is connected.
- The mobile broadband network cannot be used. (default)

- Device type**

Possible options:

- **Modem:** The device will be operated as a modem. The access data can be changed with the parameters **number**, **user name**, **password**, **APN**, **network ID** and **PIN**.
- Router: The device will be operated as a router. The device must be configured in advance in such a way that it is ready for use when it is inserted.

Select the "Router" device type if you use a device from Huawei in the HiLink mode; example: Huawei E3372.

- **Number:** Access number for your network connection. If you do not know the access number, ask your mobile communications operator for it.

- **User name:** User name for your network connection. If you do not know the user name, ask your mobile communications operator for it.

- **Password:** Password for your network connection. If you do not know the password, ask your mobile communications operator for it.

- **APN:** APN (Access Point Name) for your network connection. If you do not know the APN, ask your mobile communications operator for it.

- **Network ID:** Network ID for your network connection. If you do not know the network ID, ask your mobile communications operator for it.

- **PIN:** PIN for the SIM card used.

- Enable tray icon**

- The current status of the network connection is shown with the symbol ■ or ■!.
- The current status of the network connection is not shown with a symbol.

- Enable context menu**

- If you click on ■ or ■!, a context menu can be opened.
- No context menu can be opened.

- Enable network info dialog**

- Via the context menu, you can bring up detailed information regarding the network connection.
- No detailed information regarding the network connection can be brought up.

- Enable mobile broadband configuration dialog**

- Via the context menu, you can open a configuration dialog in order to change the access data.
- The configuration dialog cannot be opened.

### 3.11.3 DHCP Client

Menu path: **Setup > Network > DHCP Client**



Here, you can change the advanced settings for the firmware's built-in DHCP client.

- [Default Options](#)(see page 1188)
- [User-Defined Options](#)(see page 1188)

## Default Options

Menu path: **Setup > Network > DHCP Client > Default Options**

- **User Class:** A freely definable character string which can serve as a criterion for allocating specific settings for the DHCP server.
- **List of standard options:** Options with which the client can request information from the DHCP server.

You will find information regarding the various DHCP options in [RFC 2132 DHCP Options and BOOTP Vendor Extensions](#)<sup>323</sup>.

To edit the list, proceed as follows:

- Click on to create a new entry.
- Click on to remove the selected entry.
- Click on to edit the selected entry.
- Click on to copy the selected entry.

## User-Defined Options

Menu path: **Setup > Network > DHCP Client > User-Defined Options**

- To create a new entry, click on in the **List of custom options** area.

For more information regarding these options, see the manual for your DHCP server or your network components.

- **Enabled**  
 The option is enabled. (default)  
 The action is not enabled.
- **Option Name:** Add a prefix of your own in order to prevent a conflict with the default DHCP options. Example of the syntax: [YourPrefix]-[OptionName]. English letters, numbers and the special character “-” are allowed.
- **Code:** A number that is used by the DHCP server and DHCP client to reference an option. A number between 80 and 254 can be chosen. (default: 80)
- **Data Type:** Type of option. Possible values:  
 boolean  
 integer 8  
 integer 16

<sup>323</sup> <https://tools.ietf.org/html/rfc2132>



```

integer 32
signed integer 8
signed integer 16
signed integer 32
unsigned integer 8
unsigned integer 16
unsigned integer 32
ip address
text
string
  
```

### 3.11.4 VPN

Menu path: **Setup > Network > VPN**

Remote users securely access company networks via virtual private network protocols (VPN).

- **Enable tray icon**  
 A tray icon for the network interface will be shown. (default)
  - **Enable context menu**  
 A context menu will be shown when you click on the tray icon. (default)
  - **Enable network info dialog**  
 A dialog window with information regarding the network connection will be shown when you click on the context menu. (default)
- 

- OpenVPN(see page 1189)
- NCP VPN Client(see page 1197)
- OpenConnect VPN(see page 1199)
- genucard(see page 1202)

#### OpenVPN

Menu path: **Setup > Network > VPN > OpenVPN**

The *OpenVPN* client puts in place a virtual private network using TLS encryption and requires *OpenVPN* 2.x as a VPN server.

IGEL Linux 10.01.100 does not support the use of OpenVPN with smartcards and eTokens.

If problems with *OpenVPN* occur, read the `/tmp/journal.log` log file with the [System Log Viewer](#)(see page 1073) accessory.

- **Enable Autostart During Boot**



- Shows the **Auto** column in the list of OpenVPN sessions. Highlight the desired session and click on **Set Auto** to enable this connection to be established during the boot procedure.
- Autostart is disabled. (default)

- **Restart connection when disconnected:**

To manage the list of OpenVPN session, proceed as follows:

- ▶ Click to create a new entry.
- ▶ Click to remove the selected entry.
- ▶ Click to edit the selected entry.
- ▶ Click to copy the selected entry.

- [Session](#)(see page 1190)
- [Options](#)(see page 1192)
- [TLS Options for IGEL OS OpenVPN](#)(see page 1193)
- [Proxy](#)(see page 1194)
- [IPv4](#)(see page 1195)
- [Route](#)(see page 1195)
- [Desktop Integration](#)(see page 1195)

## Session

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > Session**

- **OpenVPN Server(s):** Name or public IP address of the OpenVPN server
- **Authentication type**
  - **TLS certificates:** Authentication with user certificate and private key
  - **Name/password:** Authentication with user name and password
  - **Name/password with TLS-certificates:** Combines name/password with user certificate.
  - **Static key:** Authentication with a private key. No PKI infrastructure is needed for this.

### TLS Certificates Authentication Type

Persistent storage of files is possible in the folder /wfs resp. subfolders of /wfs only.  
Files stored under other paths will be lost when the thin client is rebooted.

- **Client certificate file:** File with the client certificate. Enter a path relative to /wfs/OpenVPN or select using the file selection.
- **CA certificate file:** File with the CA certificate. Enter a path relative to /wfs/OpenVPN or select using the file selection.
- **Private key file:** File with the private key. Enter a path relative to /wfs/OpenVPN or select using the file selection.
- **Private key password:** Password in case one is set for the private key



If you have a PKCS#12 file which contains the client certificate, CA certificate and private key, always enter its name in the three file fields. The advantage lies in the fact that only a single file needs to be distributed.

For details of how to distribute certificates and keys securely to thin clients, see the [Securely Distributing Keys and Certificates](#)(see page 1190) How-To.

#### Name/Password Authentication Type

- **Username:** User name - if you leave this field empty, the user will be asked for it when establishing a connection.
- **Password required**  
 The user must enter a password. (default)
- **Password:** Password - if you leave this field empty, the user will be asked for it when establishing a connection.
- **CA certificate file:** File with the CA certificate. Enter a path relative to /wfs/OpenVPN or select using the file selection.

#### Name/Password with TLS-Certificates Authentication Type

- **Username:** User name - if you leave this field empty, the user will be asked for it when establishing a connection.
- **Password required**  
 The user must enter a password. (default)
- **Password:** Password - if you leave this field empty, the user will be asked for it when establishing a connection.
- **CA certificate file:** File with the CA certificate. Enter a path relative to /wfs/OpenVPN or select using the file selection.
- **Clientcertificate file:** File with the user certificate. Enter a path relative to /wfs/OpenVPN or select using the file selection.
- **CA certificate file:** File with the CA certificate. Enter a path relative to /wfs/OpenVPN or select using the file selection.
- **Private key file:** File with the private key. Enter a path relative to /wfs/OpenVPN or select using the file selection.
- **Private key password:** Password in case one is set for the private key

If you have a PKCS#12 file which contains the user certificate, CA certificate and private key, always enter its name in the three file fields. The advantage lies in the fact that only a single file needs to be distributed.

For details of how to distribute certificates and keys securely to thin clients, see the [Securely Distributing Keys and Certificates](#)(see page 1190) how-to.



## Static Key Authentication Type

- **Private key file:** File with the static key. Enter a path relative to /wfs/OpenVPN or select using the file selection.
- **Key direction:**
  - None: No key direction
  - 0: If the default option is not used, one side of the connection should use Direction 0 and the other Direction 1.
  - 1: If the default option is not used, one side of the connection should use Direction 0 and the other Direction 1.
- **Remote IP address:** The VPN IP address of the server
- **Local IP address:** The VPN IP address of the client

## Options

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > Options**

Here, you can configure the options for the OpenVPN client in order to ensure interaction with the server.

Further information regarding the options can be found in the [OpenVPN documentation<sup>324</sup>](#) which is maintained by the OpenVPN project.

- **Gateway port:** Local gateway port (default: 1194)
- **Custom renegotiation interval:** Renegotiate data channel key after given number of seconds (default: 0)
- **Use LZO data compression**
  - The client will use LZO compression. Necessary if the server uses compression.
  - The client will not use LZO compression. (default)
- **Protocol used for communication to the host**
  - udp: UDP will be used.
  - tcp-client: TCP will be used.

If you use a proxy, select **tcp-client**.

- **Virtual network type**
  - tun: Routing will be used
  - tap: Bridging will be used.
- **Use custom tunnel maximum transmission unit (MTU):** The MTU of the TUN device will be used as a given value. The MTU of the interface will be derived from it.
- **UDP fragment size:** Allow internal data fragmenting up to this size in bytes. Leave this field empty to keep the default value.
- **Restrict tunnel TCP maximum segment size (MSS)**
  - The TCP segment size (MSS) of the tunnel will be restricted.
  - The TCP segment size (MSS) will not be restricted. (default)
- **Randomize remote hosts**
  - The remote gateways will be ordered randomly as a simple type of load balancing.

<sup>324</sup> <https://openvpn.net/index.php/open-source/documentation.html>



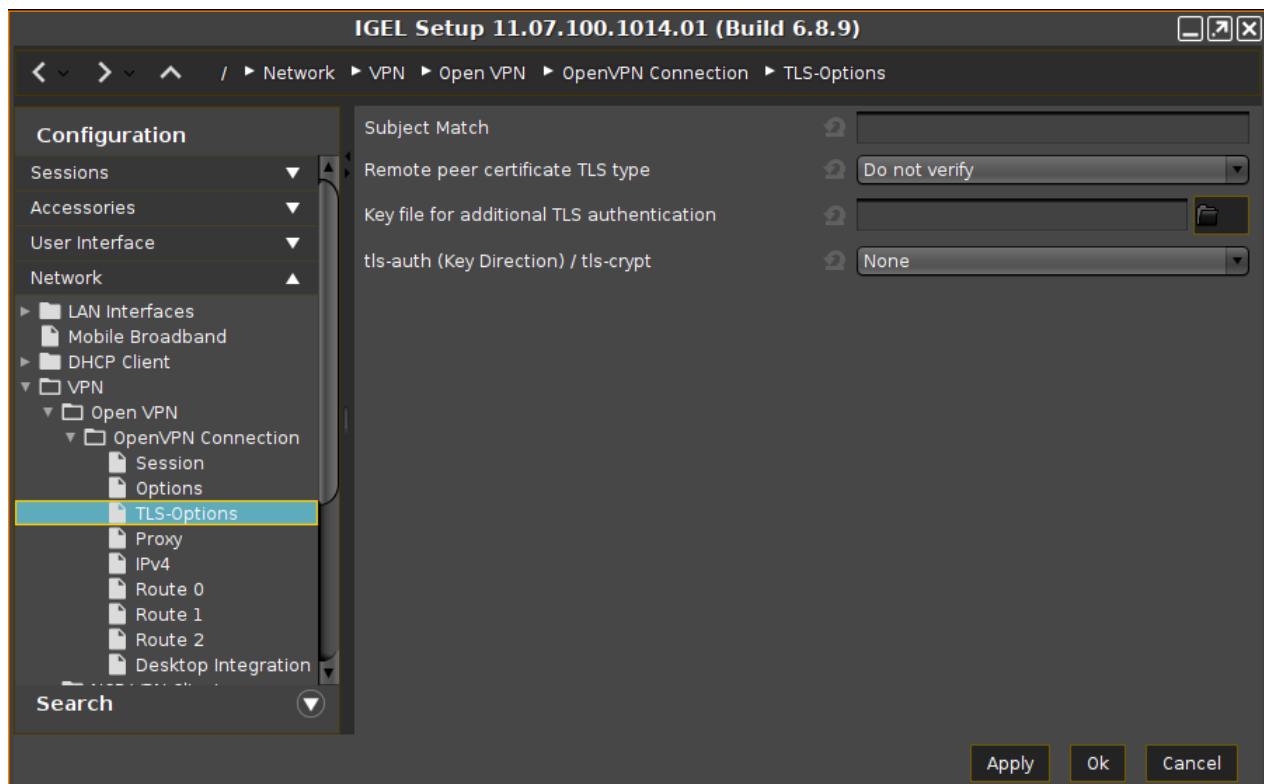
- The remote computers will not be ordered randomly. (default)
- **Cipher:** Encryption algorithm for data packets. (default: BF-CBC - Blowfish in the Cipher Block Chaining mode)
- **HMAC authentication:** Hashing algorithm for packet authentication (default: SHA1)

### TLS Options for IGEL OS OpenVPN

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > TLS Options**

This article shows how to define the TLS options for the OpenVPN client in IGEL OS. Under Transport Layer Security Options, you can customize the options for the OpenVPN protocol (tunnel). TLS is the successor to SSL (Secure Sockets Layer). It is a standard consisting of several protocols that can transmit encrypted data between authenticated communication partners over potentially insecure IP networks such as the Internet.

TLS Option for OpenVPN client in IGEL OS:



Subject match:

The computer will only accept connections from a computer whose X.509 name or name matches the one entered. If you leave this field empty, no check will take place.

Remote peer certificate TLS type:

- **Do not verify\***
- **Check for server certificate**



- **Check for client certificate**

Key file for additional TLS authentication:

As the path, enter relative to /wfs/OpenVPN or select using the file selection. This adds an additional HMAC legitimization level above the TLS control channel in order to prevent DDOS attacks.

tls-auth (Key Direction) / tls-crypt:

- **None\***: No key direction
- **tls-auth 0**: If the default option is not used, one side of the connection should use Direction 0 and the other Direction 1.
- **tls-auth 1**: If the default option is not used, one side of the connection should use Direction 0 and the other Direction 1.
- **tls-crypt**: In contrast to tls-auth, setting a key direction is not required. Use this option if the version of the OpenVPN server is 2.4 or higher. For more information on tls-crypt, see e.g. [Reference manual for OpenVPN 2.4](#)<sup>325</sup>.

\*IGEL OS system defaults

## Proxy

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > Proxy**

Here, you can set up an optional proxy server for the VPN connection.

If you use a proxy, select the value **tcp-client** under **Options > Communication protocol to the host**.

- **Proxy type**

- **None**: Direct connection to the Internet.
- **HTTP**: HTTP proxy will be used.
- **SOCKS**: SOCKS proxy will be used.

### Details for HTTP proxy

- **Proxy address**: Name or IP address of the proxy server
- **Proxy port**: Port on which the proxy service is available
- **Retry indefinitely when errors occur**
  - In the event of errors, repeated attempts to establish a connection via proxy will be made.
  - No further attempts to establish a connection will be made (default).

### Credentials for HTTP

- **Proxy username**: User name for the proxy server
- **Proxy password**: Password for the proxy server

<sup>325</sup> <https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/>



## IPv4

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > IPv4**

By default, OpenVPN uses the server's DNS and routing settings. Here, you can change these settings.

- **Automatic DNS:**
  - The name server(s) will be carried over by the OpenVPN server. (default)
  - Extra name servers (see below) will be used.
- **Extra name server(s):** One or more name servers, IP addresses separated by commas.
- **Extra search domain(s):** One or more search domains, separated by commas.
- **Automatic routes**
  - The routing table will be carried over by the OpenVPN server. (default)
  - Extra routes will be configured.
- **VPN is the default route**
  - The default route leads to the VPN. (default)
  - Extra routes will be configured.

## Route

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > Route [0,1,2]**

Here, you can configure extra routes.

- **Enable**
  - This route is enabled.
  - This route is not enabled. (default)
- **Network route / host route:** Type of route
  - **Network route:** The routing relates to a (sub) network
  - Host route: The routing relates to the address of a computer
- **Network / host IP:** The address of the network (for a network route) or the IP address or the name of the host (for a host route)
- **Network mask:** Mask for the desired IP range, e.g. 255.255.255.0
- **Gateway:** Gateway that routes the packets to the target network
- **Metric:** Here, you can enter a numerical quality assessment for routing decisions, 0 is the best value.

## Desktop Integration

Menu path: **Network > VPN > OpenVPN > [OpenVPN Connection] > Desktop Integration**

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start menu



- The session can be launched from the start menu.

#### **Application Launcher**

- The session can be launched with the Application Launcher.

#### **Desktop**

- The session can be launched with a program launcher on the desktop.

#### **Quick start panel**

- The session can be launched with the quick start panel.

#### **Start menu's system tab**

- The session can be launched with the start menu's system tab.

#### **Application Launcher's system tab**

- The session can be launched with the Application Launcher's system tab.

#### **Desktop context menu**

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### **Hotkey**

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None



- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

## NCP VPN Client

Menu path: **Network > VPN > NCP VPN Client**

NCP offers a 30-days trial period for IGEL customers.

The configuration parameters for the NCP Client are configured exclusively via the client program interface itself.

You will find the documentation regarding the NCP Secure Enterprise Client at <https://www.ncp-e.com/en/service-resources/library/>.

► Click to add an NCP VPN client session and configure the start methods.

**Session name:** Name for the session.



The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### **Start menu**

The session can be launched from the start menu.

### **Application Launcher**

The session can be launched with the Application Launcher.

### **Desktop**

The session can be launched with a program launcher on the desktop.

### **Desktop context menu**

The session can be launched with the desktop context menu.

### **Hotkey**

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
- [Ctrl] = Ctrl
-  = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super\_L

**Key:** Key for the hotkey



To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

### **Autostart**

- The session will be launched automatically when the device boots.

### **Restart**

- The session will be restarted automatically after the termination.

## OpenConnect VPN

Menu Path: **Setup > Network > VPN > OpenConnect VPN**

### **Feature Not Available on IZ Devices**

This feature is not available on IGEL IZ devices (IGEL Zero HDX, IGEL Zero RFX, or IGEL Zero Horizon).

The OpenConnect VPN Client puts in place a virtual private network using TLS encryption. This feature is available from *IGEL Linux 10.04.100* onwards.

**Feature with limited support** The OpenConnect VPN Client feature comes with limited support and without any warranty. Any support for this feature is provided on a non-binding, “best effort” basis.

The OpenConnect VPN Client feature needs to be enabled manually before you can use it, see [Enabling the OpenConnect VPN Client](#)(see page 1202).

- **Enable autostart during boot**

- Autostart is enabled.
- Autostart is disabled. (Default)

- **Restart connection when disconnected**

- Reconnect automatically when a disconnect occurs.
- Do not reconnect automatically when a disconnect occurs. (Default)

To manage the list of *OpenConnect VPN* sessions, proceed as follows:

- ▶ Click to create a new entry.
- ▶ Click to remove the selected entry.
- ▶ Click to edit the selected entry.
- ▶ Click to copy the selected entry.



- [Session](#)(see page 1200)
- [Desktop Integration](#)(see page 1200)
- [Enabling the OpenConnect VPN Client](#)(see page 1202)

## Session

Menu path: **Setup > Network > VPN > OpenConnect VPN > [session name] > Session**

- **Gateway:** IP address, hostname or Fully Qualified Domain Name (FQDN) of the VPN gateway
- **Connect to Juniper Networks VPN**
  - The protocol of Juniper Networks VPN is used.
  - The protocol of Juniper Networks VPN is not used. (Default)
- **Name/Password Authentication**
  - User name and password are used for authentication.
  - User name and password are not used for authentication. (Default)
- **User name:** User name used for authentication
- **Password:** Password used for authentication
- **CA Certificate:** Path to the CA certificate
- **User Certificate:** Path to the user certificate

The certificates should be stored in the directory /wfs/OpenVPN/ if possible, then they will certainly be found after a reboot.

- **Private Key:** Path to the private key
- **Private Key password:** Password of the private key

## Desktop Integration

Menüpfad: **Setup > Network > VPN > OpenConnect VPN > [session name] > Desktop Integration**

**Session Name:** Name for the session

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

## Starting Methods for Session

### Start Menu

The session can be started from the start menu. (Default)

### Application Launcher

The session can be started with the application launcher. (Default)

### Desktop:

The session icon will appear on the desktop. (Default)

### Quick Start Panel

The session can be started from the quick start panel.

The session cannot be started from the quick start panel. (Default)



### Desktop Context Menu

- The session can be started from the desktop context menu.
- The session cannot be started from the desktop context menu. (Default)

### Application Launcher folder:

Path to the application launcher folder

**Password Protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- Administrator: The administrator password is requested when launching the session.
- User: The user password is requested when launching the session.
- Setup User: The setup user's password is requested when launching the session.

### Hotkey:

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

### Key:

Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).



The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

#### Enabling the OpenConnect VPN Client

To enable the OpenConnect VPN Client, proceed as follows:

1. Ensure that the settings under **System > Update > Firmware Update** are correct. The **Server Path** must point to the firmware version that is currently installed. This is required because the software package for the OpenConnect VPN client must be downloaded in order to deploy the feature.
2. Go to **System > Firmware Customization > Features** and activate **VPN OpenConnect (Limited support - functionality "as is", see product documentation for details)**.
3. Confirm the warning dialog with **Ok**.
4. Click **Ok** in the main window.
5. Reboot the thin client.  
On reboot, the client downloads and installs the software package for the OpenConnect VPN Client feature.

#### genucard

Menu path: **Network > VPN > genucard**

The *genucard* VPN hardware offers a choice of preconfigured Internet and VPN connections.

The settings for launching the session are described below.

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

#### Starting Methods for Session

##### Start menu

The session can be launched from the start menu.

##### Application Launcher

The session can be launched with the Application Launcher.

##### Desktop

The session can be launched with a program launcher on the desktop.

##### Quick start panel



- The session can be launched with the quick start panel.

#### Start menu's system tab

- The session can be launched with the start menu's system tab.

#### Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

#### Desktop context menu

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. **Ctrl**.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
-  = Shift
-  = Ctrl
-  = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

-  = Alt



Key combinations are formed as follows with |:

- Ctrl + = Ctrl|Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

- “**Connections**” Window(see page 1204)
- Options(see page 1205)
- Desktop Integration(see page 1205)
- Administrator Session(see page 1207)

### “Connections” Window

The **Connections** window opens as soon as the *genucard* session is launched. You will find the following menu points there:

- **File**
  - **Change PIN:** Enter your previous PIN as well as your chosen new PIN twice.
  - **Rekeying:** Enter your PIN to generate a new key.
- **Wifi:** Opens the **Wifi** dialog which allows you to configure wireless access for the *genucard*.
  - Select a wireless network from the list. **Scan** updates the list (this can take up to a minute).
  - **Password:** The password for the selected wireless network. **Show** shows the entry in plain text.
  - **Save:** Saves the connection data entered along with the password on the *genucard*.
  - **Saved connections:** Select one of the previously saved connections.
  - **Delete:** Deletes the selected connection.
  - **Edit:** Changes the password for the selected connection.
- **Log:** Allows you to view the log
- **Network connection:** Select one of the network connections preconfigured on the *genucard*, for example LAN or WiFi.



The network connections listed here have been configured using a *genucard* administration session or the *genucenter*. Connections configured with the *genucenter* are marked with "(GCE)".

- ▶ To start the selected network connection, click **Connect**.

- **VPN connection:** Select one of the VPN connections preconfigured on the *genucard*.

The VPN connections listed here have been configured using a *genucard* administration session or the *genucenter*. Connections configured with the *genucenter* are marked with "(GCE)".

- ▶ To start the selected VPN connection, click **Connect**.

## Options

Menu path: **Setup > Network > VPN > genucard > Options**

Here, you can prepopulate connection and user data for the *genucard*.

- **Autostart during boot**

The *genucard* application is launched during booting. This option increases the waiting time until the network is available.

If the user name, password, default Internet connection and the default VPN connection are set in the setup, automatic launching allows firmware updates via VPN too.

The *genucard* application is not launched during booting. (default)

- **Autostart after USB directory (requires restart)**

The *genucard* application is automatically launched as soon as the *genucard* is connected to the thin client. (default)

Launching the *genucard* can take up to 60 seconds.

- **Default Internet connection:** Name of an Internet connection configured on the *genucard*.
- **Default VPN connection:** Name of an Internet connection configured on the *genucard*.
- **User name:** User name for the *genucard* application
- **Password:** Password for the *genucard* application
- **Internet connection timeout:** Permitted waiting time in seconds (default: 120)
- **VPN connection timeout:** Permitted waiting time in seconds (default: 120)
- **File path for private keys for machine connection:** File path for the key file.

## Desktop Integration

Menu path: **Setup > VPN > genucard > Desktop Integration**

- **Session name:** Name for the session



The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

- **Start menu:**

- The session can be started with the start menu. (Default)
- The session cannot be found in the start menu.

- **Application Launcher:**

- The session can be started with the Application Launcher. (Default)
- The session cannot be found in the Application Launcher.

- **Desktop:**

- The session can be started with a program starter on the desktop. (Default)
- The session does not have a program starter on the desktop.

- **Quick start panel:**

- The session can be started with the quick start panel.
- The session cannot be found in the quick start panel. (Default)

- **Start menu's system tab:**

- The session can be started with the start menu's system tab.
- The session cannot be found in the start menu's system tab. (Default)

- **Application Launcher's system tab:**

- The session can be started with the Application Launcher's system tab.
- The session cannot be found in the Application Launcher's system tab. (Default)

- **Desktop context menu:**

- The session can be started with the desktop context menu.
- The session cannot be found in the desktop context menu. (Default)

- **Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

- **Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

- **Password protection:** Specifies which password will be requested when launching the session.  
Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

- **Hotkey:** A hotkey with which the session can be started is defined. It consists of modifiers and a key.

- **Modifiers:** One or two modifiers for the hotkey:

- None
- = Shift
- [Ctrl] = Ctrl
- = Super\_L
- [Alt] = Alt



Modifiers can be combined by using the pipe character | :

- [Ctrl] + = Ctrl|Super\_L
- **Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the character string for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

## Administrator Session

The genucard is configured and administered centrally via the genucenter management interface. While VPN profiles can only be configured via genucenter or other remote interfaces, Internet connection profiles can also be configured via a local administration session.

Further information is available from [www.genua.de](http://www.genua.de)<sup>326</sup>.

Optionally, an administrator session allowing the genucard Internet connection to be configured can be set up:

To configure an Internet connection profile via a local administration session, proceed as follows:

1. Click on **Add instance** under **System > Registry > Sessions > genucard%**.  
The genucard icon will appear on the desktop.
2. Click on the genucard icon.  
The genucard logon window will open.
3. Enter a **user name** and **password**.
4. Click on **Logon**.  
The Internet/VPN page will open.
5. In the **Internet** area, configure the connection with the help of the (Create), (Edit) and (Delete) buttons.

### 3.11.5 SCEP Client (NDES)

Menu path: **Setup > Network > SCEP Client (NDES)**

SCEP allows the automatic provision of client certificates via an SCEP server and a certification authority. This type of certificate is automatically renewed before it expires and can be used for purposes such as network authentication (e.g. IEEE 802.1x).

A Microsoft Windows Server (MSCEP, NDES) for example can serve as a queried counterpart (SCEP server and certification body). More information can be found at Microsoft, e.g. in the following Technet article: [Network Device Enrollment Service \(NDES\) in Active Directory Certificate Services \(AD CS\)](http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs.aspx)<sup>327</sup>

#### Manage certificates with SCEP

<sup>326</sup> <https://www.genua.de/en.html>

<sup>327</sup> <http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs.aspx>



- Certificate management via SCEP Client (NDES) is enabled. Now carry out the necessary configuration.
- Certificate management via SCEP Client (NDES) is not enabled. (Default)
- 

- [Certificate](#)(see page 1208)
- [Certification Authority](#)(see page 1209)
- [SCEP](#)(see page 1209)

## Certificate

Menu path: **Setup > Network > SCEP Client (NDES) > Certificate**

Here, you can specify the basic data for the certificate to be issued by the certification body.

**Type of CommonName/SubjectAltName:** The characteristic for linking the certificate to the device.

- IP address: The IP address of the device.
- DNS name: The DNS name of the device.
- IP address (auto): The IP address of the device (inserted automatically).
- DNS name (auto): The DNS name of the device (inserted automatically).
- Email address: An email address.
- DNS name as UPN (auto)

If the client automatically obtains its network name, **DNS Name (auto)** is a good type for the client certificate.

The following parameter is available if **Type of CommonName/SubjectAltName** is set to **IP address**, **DNS name**, or **Email address**:

**CommonName/SubjectAltName:** Give a designation which matches the **Type of CommonName/SubjectAltName**. For certain types, this occurs automatically. No entry is then required.

The following parameter is available if **Type of CommonName/SubjectAltName** is set to **IP address (auto)**, **DNS name (auto)**, or **DNS name as UPN (auto)**:

**CommonName/SubjectAltName Suffix:** Specifies a suffix that will be added to CommonName/SubjectAltName. Possible values:

- "none
- "dot + DNS domain (auto)": The system's current DNS domain name separated with a dot will be added. Example: .igel.local
- Free text entry: The manually entered suffix will be added. Take notice that the percent symbol "%" is used for introducing the escape sequence, and thus the following replacements take place automatically:
  - "%D is replaced by the system's DNS domain name at the time the certificate signing request (CSR) is created. Example: @%D will be changed into @igel.de if the system's current DNS



domain name is `igel.de`.

- `%%` will be replaced by `%`. Example: `A%%B` will be changed into `A%B`.
- Other combinations with `%` are currently discarded. Example: `A%BC` will be changed into `AC`.

If you have to specify the suffix manually, make sure you enter the separator.

**Organizational unit:** Stipulated by the certification authority.

**Organization:** A freely definable designation for the organization to which the client belongs.

**Locality:** Details regarding the device's locality. Example: "Augsburg".

**State:** Details regarding the device's locality. Example: "Bayern".

**Country:** Two-digit ISO 3166-1 country code. Example: "DE".

**RSA key length (bits):** Select a key length (one suited to the certification authority) for the certificate that is to be issued.

Possible values:

- "1024"
- "2048"
- "4096"

## Certification Authority

Menu path: **Setup > Network > SCEP Client (NDES) > Certification Authority**

The details for the following fields can be obtained from the certification authority:

**CA identifier**

**CA certificate fingerprint (MD5)**

## SCEP

Menu path: **Setup > Network > SCEP Client (NDES) > SCEP**

Here, you can give information regarding the SCEP server used.

Because of the need to enter a fingerprint (CA root certificate) and the **Challenge password** (SCEP server), the configuration process is somewhat complicated. Ideally, it should be set up in the UMS as a profile and distributed to the devices. At the same time, the certificate cannot yet be used for communication purposes.

**SCEP server URL:** Address of the SCEP server. Examples: `http://myserver.mydomain.com/certsrv/mscep/mscep.dll` (Windows Server 2019); `http://myserver.mydomain.com/certsrv/mscep` (before Windows Server 2019)

**Proxy server for SCEP requests:** Proxy server in the format `host:port`. If this field is empty, no proxy will be used.

**Challenge password:** Password for queries.



**Certificate renewal period (days):** Time interval before certificate expiry after which the certificate renewal procedure is started. (Default: 30)

**Certificate expiry check interval (days):** Specifies how often the certificate is checked against its expiry date. (Default: 1)

As an example, a certificate is valid until 31.12. of a year. If the period for renewal is set to 10 days, a new certificate will be requested for the first time on 21.12. of the same year.

For more information, see the how-to [Providing the SCEP Server Data](#)(see page 465). See also [Configuration of the SCEP Client](#)(see page 461).

### 3.11.6 Routing

Menu path: **Setup > Network > Routing**

Here, you can enter additional routes if necessary.

**Enable:** (default: disabled)

Routing is enabled.

**Default gateway:** Gateway that routes the packets to the target network

**Interface:** The network interface via which the route is to run



### Predictable Network Interface Names (PNINs)

As of IGEL OS 11.06, the names of Ethernet and WLAN interfaces are predictable network interface names (PNINs), see [Predictable Network Interface Names](#)<sup>328</sup>. This ensures the stability of interface names on reboot and generally improves the reliability of associating configurations with interfaces.

- As "eth0", "eth1", and "wlan0" have been replaced by PNINs, configurations or custom scripts that include the old names of Ethernet and WLAN interfaces, e.g. eth0, eth2, wlan 0, have to be adjusted.

The following already existing configurations do NOT require manual adjustment since old names eth0, eth1, etc. will internally be replaced by the correct PNINs automatically:

- [Tcpcdump](#)(see page 405)
- **Bind interface** under **Security > Smartcard > Services**, see [Services](#)(see page 1249)
- To view the PNINs and the order of the configured interfaces, you can use the following commands. The default interface is always listed first, the second interface is listed second, etc.  
**Ethernet (LAN):** cat /config/net/en-interfaces  
**WLAN:** cat /config/net/wl-interfaces  
 (Note: Only the first wireless interface (former wlan0) is supported. All other wireless interfaces will be ignored.)
- If you need to configure more than two Ethernet interfaces, go to **System > Registry > network.interfaces.ethernet.device%** and add an instance.  
 To explicitly assign a configuration instance to a certain interface, enter the corresponding PNIN for the registry key **network.interfaces.ethernet.device%.ifname**.

## Routing [1-5]

**Enable:** (default: disabled)

This route is enabled.

**Network route / host route:** Type of route

- **Network route:** The routing relates to a (sub) network
- **Host route:** The routing relates to the address of a computer

**Network / host IP or name:** The address of the network (for a network route) or the IP address or the name of the host (for a host route)

**Network mask:** Mask for the desired IP range, e.g. 255.255.255.0

**Gateway:** Gateway that routes the packets to the target network

**Interface:** The network interface via which the route is to run

## 3.11.7 Hosts

Menu path: **Setup > Network > Hosts**

---

<sup>328</sup> <https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/>



If no DNS (Domain Name Service) is used, you can specify a list with computers in order to allow translation between the fully qualified host name, the short host name and the IP address.

To manage the list of computers, proceed as follows:

- Click to create a new entry.
- Click to remove the selected entry.
- Click to edit the selected entry.
- Click to copy the selected entry.

## Add

- **IP address:** IP address of the host you would like to add
- **Fully qualified host name:** Host name along with the domain, e.g. mail.example.com
- **Short host name:** E.g. mail

### 3.11.8 Network Drives

Menu path: **Setup > Network > Network Drives**

Here, you can configure both the drives that are to be connected during booting and the associated login data.

---

- [NFS](#)(see page 1212)
- [Windows Drive](#)(see page 1213)

## NFS

Menu path: **Setup > Network > Network Drives > NFS**

In this area, you can integrate network drives using the Network File System (NFS).

You can find a sample configuration at the end of this page.

To manage the network drives, proceed as follows:

- Click to create a new entry.
- Click to remove the selected entry.
- Click to edit the selected entry.
- Click to copy the selected entry.

## Add

- **Enabled:** Here, you can enable and disable configured entries.  
 The network drive will be integrated. (default)
- **Local Mount Point:** The local directory under which the server directory is to be visible (default: /nfsmount)



- **Server:** NFS server that exports the directory

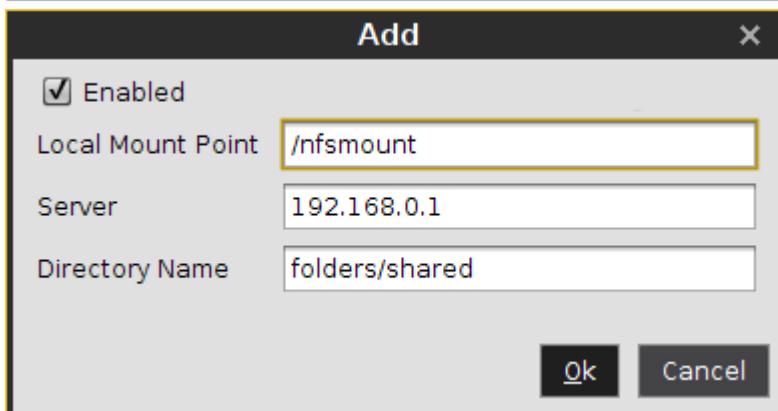
For **Server**, you can provide an IP address, a hostname or a Fully-Qualified Domain Name (FQDN).

- **Directory name:** Path under which the NFS server exports the directory

#### Sample configuration entry

The picture below shows a sample configuration entry.

In both the **Local Mount Point** and **Directory Name** only / (Linux/Unix-style forward slash) is permitted as a path separator.



#### Windows Drive

Menu path: **Setup > Network > Network Drives > Windows Drive**

In this area, you can integrate network drives shared by Windows as well as those from Linux/Unix servers via the SMB protocol (Samba).

You can find a sample configuration at the end of this page.

To manage the drive list, proceed as follows:

- Click to create a new entry.
- Click to remove the selected entry.
- Click to edit the selected entry.
- Click to copy the selected entry.

Clicking will bring up the **Add** dialogue, where you can define the following settings:

- **Enabled:** Defines whether the configuration entry will be applied.  
 The network drive will be integrated.



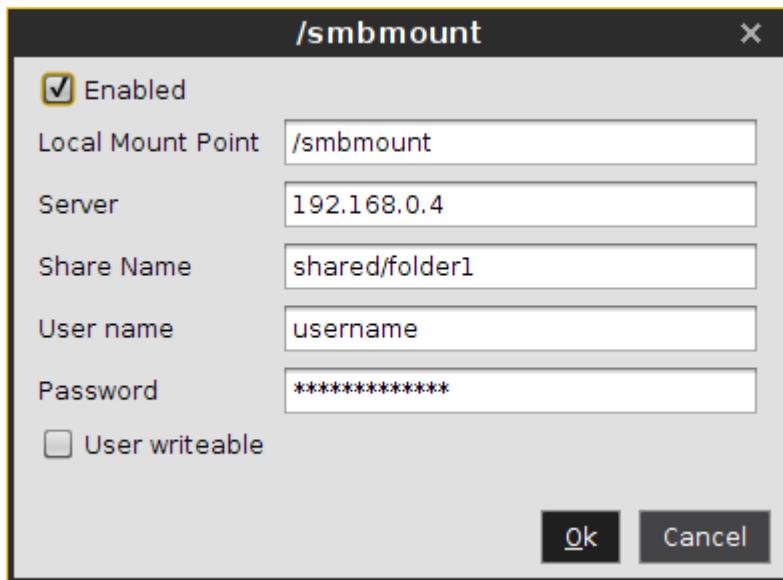
- **Local Mount Point:** The local directory under which the server directory is to be visible (default: /smbmount)
- **Server:** The IP address, Fully-Qualified Domain Name (FQDN) or NetBIOS name of the server.
- **Share Name:** Path name as exported by the Windows or Unix Samba host.
- **User name:** User name for your user account on the Windows or Unix Samba host.
- **Password:** Password for your user account on the Windows or Unix Samba host.
- **User writable**
  - The user can not only read but also write directory contents. Otherwise, only the local root user is able to do this.
  - The user can only read directory contents. (default)

Sample configuration entry

The following picture shows a sample configuration entry.

If a NetBIOS name is provided for **Server**, make sure it is not preceded by slashes, e.g. \\myComputer (wrong) vs. myComputer (correct).

For **Local Mount Point**, only / (Linux/Unix-style forward slash) can be used as a path separator. Note that if you enter, for example, \smbmount as a mount point, a directory called \smbmount will be created, because \ is a legal character in Linux directory names. For **Share Name**, however, / (Linux/Unix-style forward slash) or \ (Windows-style backward slash) can be used as a path separator.



### 3.11.9 Proxy

Menu path: **Setup > Network > Proxy**



Here, you can select the communication protocols for which a system-wide proxy server is to be used.

**Direct connection to the Internet:** The endpoint device is directly connected to the Internet. No proxy is used.

**Manual proxy configuration:** You can configure one or more proxies in the fields from **FTP proxy** up to **SOCKS protocol version**.

**Automatic proxy configuration:** The proxy settings are dynamically retrieved via a PAC file (Proxy Auto Config) that you specify under **URL**. For more information on PAC, see e.g. [https://en.wikipedia.org/wiki/Proxy\\_auto-config](https://en.wikipedia.org/wiki/Proxy_auto-config).

**FTP proxy / port:** FTP proxy server and port

**HTTP proxy / port:** HTTP proxy server and port

**SSL proxy / port:** SSL proxy server and port

**SOCKS host / port:** Socks proxy server and port

**SOCKS protocol version:** Selects the SOCKS protocol version. (Default: [SOCKS v5](#))

**URL:** URL of the PAC file for **Automatic proxy configuration**

**No proxy for:** List of computers to which the endpoint device is to connect directly, separated by commas (Default: [localhost, 127.0.0.1](#))

**Proxy realm for browser:** Area in which the browser authenticates itself for the proxy. Together with the user name and password, this information is necessary for authentication. See also [Browser Global Proxy](#)(see page 961)

#### Use passthrough authentication

The temporarily saved login information (user name and password) will be used to log in to the proxy server.

The login information entered under **User name** and **Password** will be used to log in to the proxy server. (Default)

**User name:** User name for the proxy login

**Password:** Password for the proxy login

#### Enable client-side NTLM authenticating proxy

Client-side proxy is enabled. It stands between the application and the corporate proxy, adding NTLM authentication at the corporate proxy. The credentials specified on this Setup page are used.

**Listening port:** Port for client-side proxy

## 3.12 Devices

Menu path: **Devices > Hardware Info**

► Click on **Hardware Info** to view the system information for your IGEL device.

In this area, you can make settings for the following options:

- [Printer](#)(see page 1216)
- [Storage Devices](#)(see page 1228)
- [Bluetooth](#)(see page 1231)
- [USB Access Control](#)(see page 1231)
- [Unified Communications](#)(see page 1233)



### 3.12.1 Printer

Menu path: **Devices > Printers**

You can set up a printer for the thin client here.

The printers must be set up under **Devices > Printer > CUPS > Printers** and must be enabled there for mapping in sessions.

Because the thin client merely places incoming print jobs in a queue, you need to install the printer on the server. Please note that you will need to be logged in as administrator to the terminal to which the printer is connected.

- [CUPS](#)(see page 1216)
- [LPD](#)(see page 1222)
- [TCP/IP](#)(see page 1222)
- [ThinPrint](#)(see page 1225)
- [PrinterLogic](#)(see page 1226)

### CUPS

Menu path: **Devices > Printers > CUPS**

The Common UNIX Printing System<sup>TM</sup> (or CUPS) is the software that allows you to print from within applications, e.g. from this web browser.

CUPS converts the page descriptions produced by the application, e.g. "Insert Paragraph", "Draw Line" etc., into data that can be read by the printer, and then sends this information to the printer.

With the appropriate configuration, CUPS can use printing devices via the following connections:

- Parallel (LPT 1, LPT 2)
- Serial (COM1, COM2, USB COM1, USB COM2 – with a USB-to-serial adapter)
- USB (1st and 2nd USB printer)
- Network (TCP/IP, LPD, IPP, SMB)

**Default Paper Size:** Specify a default paper size for print jobs.

Possible values:

- Letter
- Legal
- Executive
- A5
- A4
- A3
- Autodetect

Additional information on CUPS printers can be found under [CUPS: Mapping Local Printer to Citrix or RDP Sessions](#)(see page 712) and [Installing a Custom CUPS Driver](#)(see page 714).



- [Printers](#)(see page 1217)
- [IPP Printer Sharing](#)(see page 1221)

## Printers

Menu path: **Devices > Printer > CUPS > Printers**

Printers can be created and edited here.

- ▶ Click on to open the **Add** dialog.
- ▶ In the edit dialog, specify a **Printer name** which begins with a letter.

### General

**Printer port:** Interface type for locally connected printers or the network protocol for network printers.

Possible values:

- "Parallel port printer" (default)
- "Serial port printer"
- "USB printer"
- "USB class printer"
- "LPD network printer"
- "TCP network printer"
- "IPP network printer"
- "SMB network printer"

Depending on the chosen **Printer port** type, different parameters have to be configured, see [Settings to Be Configured for Each Printer Port Type](#)(see page 1218).

**Manufacturer:** List of possible printer manufacturers. When you select a manufacturer here, the relevant selection of models will be provided under **Printer names**. (Example: Generic)

**Printer names:** List of possible printer models. (Example: PostScript Printer)

**Default paper size:** Set the printer-specific paper size that you would like to use as a default.

Possible values:

- "Letter"
- "Legal"
- "Executive"
- "A5"
- "A4"
- "A3"
- "System setting"

### Share printer

You can access the printer via the network if you have enabled the print server under **IPP Printer Sharing**; see [IPP Printer Sharing](#)(see page 1221). (Default)



Mapping in sessions

#### **Map printer in NX sessions**

- The printer is available in NX sessions.  
 The printer is not available in NX sessions. (Default)

#### **Map printer in Parallels Client sessions**

- The printer is available in Parallels Client sessions.  
 The printer is not available in Parallels Client sessions. (Default)

#### **Map printer in ICA sessions**

- The printer is available in ICA sessions. (Default)

#### **Map printer in RDP sessions**

- The printer is available in RDP sessions. (Default)

#### **Map printer in AVD sessions**

- The printer is available in AVD sessions. (Default)  
 See also [CUPS Printer Redirection](#)(see page 1023) for AVD sessions.

#### **Use Windows driver name from list**

- A driver name from the following list will be used. (Default)

**Manufacturer:** List of possible printer manufacturers. (Example: Generic)

**Model:** List of possible models. (Example: Generic PostScript)

#### **Use custom Windows driver name**

- Enter the name of your driver here if it is not mentioned in the list above.

**Printer driver:** Windows driver name for the printer.

The name must not contain ";" or ":".

When printing in ICA and RDP sessions, the print data are normally prepared for the printer model by the Windows printer driver and are passed unchanged from the device to the printer. An exception is made when using the Windows driver in ICA sessions, **Manufacturer** is set to "Generic" and **Model** is set to "Generic PostScript." In this case, the print data are prepared on the device with the help of the printer driver defined above under **Printer** for the printer model. This requires device resources.

Settings to Be Configured for Each Printer Port Type

Menu path: **Devices > Printer > CUPS > Printers**

Here, you can find the parameters available for configuration for each **Printer Port** (**Devices > Printer > CUPS > Printers > Add > General > Printer port**).

Printer Port: "Parallel port printer"

**Parallel device:**

- LPT1



- "LPT2"

**Detect devices...:** Opens a dialog for selecting the available devices.

Printer Port: "Serial port printer"

**Serial device:**

- "COM1"
- "COM2"
- "USB COM1"
- "USB COM2"

**Detect devices...:** Opens a dialog for selecting the available devices.

**Baud rate:**

- "9600"
- "19200"
- "38400"
- "57600"
- "115200"

**Character size:**

- "5"
- "6"
- "7"
- "8"

**Parity:**

- "None"
- "Even"
- "Odd"

**Flow control:**

- "None"
- "XON/XOFF"
- "RTS/CTS"
- "DTR/DSR"

Printer Port: "USB printer"

**USB device:**

- "1st USB printer"
- "2nd USB printer"

**Detect devices...:** Opens a dialog for selecting the available devices.

Printer Port: "USB class printer"

If you use a lot of different printer models attached via USB, you can assign printer models to CUPS printers without specifying dependencies to a specific USB port. Instead, the USB printer is assigned by matching patterns specified under **Manufacturer pattern** and **Product pattern** with the specific model name. A single printer definition can thus work for a class of different USB printer models.

**Pattern matching mode:** Specifies the type of the search pattern.



- "pattern": Standard wildcards are used for pattern matching, e.g. "\*", "?". The matching is case sensitive. For detailed information on wildcards, see [man7.org](#)<sup>329</sup> and [tldp.org](#)<sup>330</sup>.
- "pattern, case insensitive": Standard wildcards are used for pattern matching, e.g. "\*", "?". The matching is case insensitive.
- "regular expression": Regular expressions are used for pattern matching. For detailed information on regular expressions, see [man7.org](#)<sup>331</sup> and [tldp.org](#)<sup>332</sup>.

**Manufacturer pattern:** Pattern matching the manufacturer name of the printer. If the pattern is empty, it is ignored.

**Product pattern:** Pattern matching the product name of the printer. If the pattern is empty, it is ignored.

Manufacturer and product names can be found in the accessories under **Devices > USB Devices > System Information**.

|              |                              |
|--------------|------------------------------|
| Product      | hp LaserJet 1015             |
| Manufacturer | Hewlett-Packard (www.hp.com) |
| Speed        | 12,00Mbit/s                  |
| Max Current  | 2mA                          |
| Misc         |                              |
| USB Version  | 1,00                         |
| Class        | 0x7                          |
| Vendor       | 0x3f0                        |
| Product ID   | 0xe17                        |
| Bus          | 1                            |

### Click to see examples...

Matching all printers whose product name contains "LaserJet":

**Pattern matching mode:** "pattern"

**Product pattern:** "\*LaserJet\*"

Matching all printers whose product name contains "LaserJet":

**Pattern matching mode:** "regular expression"

**Product pattern:** "LaserJet"

Matching all printers whose product name contains "LaserJet" or "DeskJet":

**Pattern matching mode:** "pattern"

**Product pattern:** "+(\*LaserJet\*|\*DeskJet\*)"

Matching all printers whose product name contains "LaserJet" or "DeskJet":

<sup>329</sup> <http://man7.org/linux/man-pages/man7/glob.7.html>

<sup>330</sup> <http://www.tldp.org/LDP/GNU-Linux-Tools-Summary/html/x11655.htm>

<sup>331</sup> <http://man7.org/linux/man-pages/man7/glob.7.html>

<sup>332</sup> <http://www.tldp.org/LDP/GNU-Linux-Tools-Summary/html/x11655.htm>



**Pattern matching mode:** "regular expression"

**Product pattern:** "LaserJet|DeskJet"

Printer Port: "LPD network printer"

**LPD print server:** Host name or IP address of the remote LPD printer.

**LPD queue name:** Name of the LPD printer queue.

Printer Port: "TCP network printer"

**TCP print server:** Host name or IP address of the remote TCP/JetDirect/Socket printer.

**TCP port:** TCP port number. (Default: 9100)

Printer Port: "IPP network printer"

**IPP URI:** URI of the IPP print server. Example: `ipp://myprinter.example.com/printers/printer1`

Printer Port: "SMB network printer"

**SMB server:** NetBIOS host name of the SMB server.

**SMB workgroup:** Workgroup or domain name. (Optional)

**SMB printer:** Share name of the printer.

**SMB port:** SMB port number. (Default: 0, which stands for standard ports 139 and 445)

#### Use Kerberos authentication

Kerberos credentials are used for authentication on condition that Active Directory/Kerberos Logon has been configured. See [Active Directory/Kerberos](#)(see page 1242).

Kerberos credentials are not used for authentication. (Default)

#### Use passthrough authentication

Single sign-on authentication is used on condition that Active Directory/Kerberos Logon or IGEL Shared Workplace have been configured. See [Active Directory/Kerberos](#)(see page 1242) and [Shared Workplace](#)(see page 1244).

Single sign-on authentication is not used. (Default)

**SMB user name:** User name used for authentication. (Optional)

**SMB password:** Password used for authentication. (Optional)

#### IPP Printer Sharing

Menu path: **Devices > Printer > CUPS > IPP Printer Sharing**

The IPP (Internet Printing Protocol) offers the following configuration options:

**Network or host for sharing local printers:** Access to the printer is possible from this network or host.

Possible options:

- "None"
- "Local network": Allows printing on the local device from the local network.

This can also be given in the form 192.0.2.\* or 192.0.2.0/24 or \*.domain.com or 192.0.2.1 or host.domain.com.

- "Global": Allows printing on the local device from the global network.



## LPD

Menu path: **Setup > Devices > Printers > LPD**

LPD printers are used by the BSD printing system and are also supported by *Windows* servers.

- **Enable LPD Print Server**

Local printers are provided in the network as LPD printers. The thin client is made the LPD print server. The CUPS printers defined under [Printers\(see page 1217\)](#) can be addressed under their printer name as a queue name via the LPD protocol. (default)

- **Print Filter:**

- Automatic: Attempts to automatically recognize whether or not the print data need to be prepared by the local printer driver.
- None: The print data are always forwarded unchanged to the printer.

- **Max. Concurrent Connections**: Limits the number of print jobs that can be accepted at the same time.

- Unlimited
- 1
- 2
- 3

- **Restrict LPD Access** - Specifies the sub-networks or hosts from which print jobs can be accepted.

► Click on to add an LPD network or a host to the list.

## TCP/IP

Menu path: **Setup > Devices > Printers > TCP/IP**

You can assign printers connected to your device to a TCP/IP port.

---

- [COM 1 / 2\(see page 1222\)](#)
- [Additional Serial Ports\(see page 1223\)](#)
- [LPT 1\(see page 1224\)](#)
- [USBLP 1\(see page 1225\)](#)

## COM 1 / 2

Menu path: **Setup > Devices > Printers > TCP/IP > COM 1**

- **Activate TCP/IP printers on this port**

Maps the interface defined below in a TCP/IP port.  
 Disabled (default)

- **TCP/IP port number**: Port on which the interface is to be mapped (default: 3004).

- **Poll criterion**: Criterion according to which the interfaces are mapped.

- Always: Maps constantly without polling.
- Online: Maps only if the printer is switched on.

- **Poll frequency**: Amount of time between polls (default: 1 sec)



- **Speed:** Input and output speed (default: 9600)
- **Parity:** Parity bits that are to be used. Possible values:
  - None
  - Even
  - Odd
- **Stop bits:** Use up to two stop bits. (default: 1)
- **Word width:** Sets the number of bits used per byte.
  - 5
  - 6
  - 7
  - 8
- **Use RTS/CTS flow control**
  - Hardware flow control will be used.
  - Not used (default)
- **Use XON/XOFF flow control**
  - Software flow control by sending start/stop signs will be used.
  - Not used (default)
- **Use DSR flow control**
  - Hardware flow control with DSR for output will be used.
  - Not used (default)

## Additional Serial Ports

Menu path: **Setup > Devices > Printers > TCP/IP > Additional Serial Ports**

### TCP/IP printers on additional serial ports

- ▶ Click on to add TCP/IP printers to the list.

A mask with the following settings options will open:

- **Activate TCP/IP printer on this interface**
  - Maps the interface defined below in a TCP/IP port.
  - Disabled (default)
- **Device name:** The printer can be connected to one of the following connections, provided that they are available on the device:
  - USB COM1
  - USB COM2
  - Perle COM1
  - Perle COM2

Data are forwarded bidirectionally at serial interfaces. This means that other serial devices such as barcode scanners or scales can be operated too.

- **Search for devices....:** Opens a dialog allowing you to select the device file. 3 device files are available for each device; the **Designation** column shows the type of device file:
  - (GENERIC) [device designation]: Generic type. The name of the device file ends in a consecutive number which depends on the boot procedure or the order of insertion.  
Example: /dev/ttyUSB0



- (BY PORT) [device designation]: According to USB port. The device file is in the /dev/usbserial/ directory. The name of the device file ends in the number of the USB port that the device is plugged into. Example: /dev/usbserial/ttyUSB\_P12
- (BY USBID) [device designation]: According to USB ID. The device file is in the /dev/usbserial/ directory. The name of the device file ends as follows: \_V[Vendor ID]\_P[Product ID]. Example: /dev/usbserial/ttyUSB\_V067b\_P2303
- **TCP/IP port number:** Port on which the interface is to be mapped (default: 9100).
- **Poll criterion:** Criterion according to which the interfaces are mapped.
  - Always: Maps constantly without polling.
  - DSR (M1): Maps only if the relevant line is set by the serial device.
  - DCD (M5): Maps only if the relevant line is set by the serial device.
- **Poll frequency:** Amount of time between polls (default: 1 sec)
- **Speed:** Input and output speed (default 9600 baud).
- **Parity:** Parity bits that are to be used. Possible values:
  - None
  - Even
  - Odd
- **Stop bits:** Use up to two stop bits. (default: 1)
- **Word width:** Sets the number of bits used per byte.
  - 5
  - 6
  - 7
  - 8
- **Use RTS/CTS flow control**
  - Hardware flow control will be used.
  - Not used (default)
- **Use XON/XOFF flow control**
  - Software flow control by sending start/stop signs will be used.
  - Not used (default)
- **Use DSR flow control**
  - Hardware flow control with DSR for output will be used.
  - Not used (default)

## LPT 1

Menu path: **Setup > Devices > Printers > TCP/IP > COM 1**

- **Activate TCP/IP printers on this interface**
  - Maps the interface defined below in a TCP/IP port.
  - Disabled (default)
- **TCP/IP port number:** Port on which the interface is to be mapped (default: 3004).
- **Poll criterion:** Criterion according to which the interfaces are mapped.
  - Always: Maps constantly without polling.
  - Online: Maps only if the printer is switched on.
- **Poll frequency:** Amount of time between polls (default: 1 sec)



## USBLP 1

Menu path: **Setup > Devices > Printers > TCP/IP > USBLP 1**

- **Activate TCP/IP Printers on this Port:**

- Maps the interface defined below in a TCP/IP port.
- Disabled (default)

- **TCP/IP Port Number:** Port on which the interface is to be mapped (default: 3004).

- **Poll Criterion:** Criterion according to which the interfaces are mapped.

- Always: Maps constantly without querying.

- Online: Maps only if the printer is switched on.

- **Poll Frequency:** Amount of time between status queries (default: 1 sec)

## ThinPrint

Menu path: **Devices > Printer > ThinPrint**

ThinPrint allows the bandwidth provided for the transfer of print jobs to be reduced depending on the resources available. The ThinPrint client prints either on printers connected to a local interface (serial, parallel or USB), on an LPD network printer or on a CUPS printer defined on the thin client.

In this area, you will find the following parameters:

**Port Number:** Port number via which the ThinPrint daemon will communicate (default: 4000).

Make sure that the port number on the ThinPrint client and the ThinPrint server is the same (communication will otherwise not be possible).

**Bandwidth:** A bandwidth value (in bits per second) which is lower than or equal to the value specified on the ThinPrint server. A higher value, the disabling of client control or no entry at all means that the ThinPrint server values will be used (default: 0).

**Open Printer Interval:** Maximum waiting time in seconds if a printer is unavailable (default: 165).

**Open Printer Tries:** Number of attempts to contact a printer in order to start a print job (default: 100).

- 
- [Printer](#)(see page 1225)
  - [Connection Service](#)(see page 1226)
  - [Encryption](#)(see page 1226)

## Printer

Menu path: **Devices > Printer > ThinPrint > Printer**

In this area, the **ThinPrint and ezeep Printers** are shown.

The page provides an overview of pre-configured ThinPrint printers.

► Click on to add a printer to the list.

A mask with the following settings options will open:

**Active:** Indicates whether or not the printer is visible.



**Printer Name:** Name under which the printer can be addressed.

**Printer Class Name:** Name of the printer class - optional, max. 7 characters without spaces

**Device:** A device file or the printer name, e.g. /dev/ttyS1 (COM2).

**Detect Devices...:** Opens a mask for selecting the available devices.

**Print Retries:** Number of attempts to contact a printer in order to start a print job (default: 10).

**Default:** Defines the selected device as the default printer.

## Connection Service

Menu path: **Setup > Devices > Printers > ThinPrint > Connection Service**

By default, the .print client waits for incoming connections from the print server. If the thin client is unavailable via the network from the print server, the connection can also be established from the thin client.

- **Connection Service Mode:**

- **Listen Mode:** Receive print jobs without Connection Service. The .print client heeds incoming connections.
- **Static Mode:** Use connection to receive print jobs. The .print client establishes a connection to the .print Connected Gateway.
- **Both:** Use both modes.
- **Connection Server Address:** IP address of the computer on which the connection service runs.
- **Connection Service Port number:** The client port of the .print Connected Gateway (default: 4001)
- **Client ID:** The ID of the client must be unique.
- **Connection Service Authentication key:** A value that is defined on the connection server.
- **Connection Service Retry Interval:** Waiting time in seconds until another connection attempt is made if the .print Connection Service is unavailable (default: 300)

## Encryption

Menu path: **Setup > Devices > Printers > ThinPrint > Encryption**

In this area, you can enable encryption for print jobs.

- **Enable SSL Encryption:**

- The client can receive print jobs via an encrypted connection.
- Disabled (default)

- **SSL Root Certificate:** Path name of the file that receives the root certificate in the .pem format.
- **SSL Client Certificate:** Path name of the file that receives the client certificate in the .pem format.
- **SSL Client Certificate Password**

## PrinterLogic

Menu path: **Setup > Devices > Printer > PrinterLogic**

If you are using PrinterLogic to provision printers, you are replacing the previous direct printer management from the Setup.



Instead, the administrator creates a website (on [printercloud.com](http://printercloud.com)<sup>333</sup>) with the respective printers of the location(s). The setup user/administrator can then select the desired printers via the browser.

#### Manage printers by Printer Installer client:

- The printers will be managed by the Printer Installer client and not by the IGEL CUPS functionality (**IGEL Setup > Devices > Printers > CUPS**).
- No Printer Installer client is activated. The printers will be managed by the IGEL CUPS functionality. (default)

#### HomeURL protocol

Possible options:

- <https://>
- <http://>

**HomeURL hostname:** The host name of the web server running the printer cloud. Default: `printercloud.com`

**Authorization code:** Authorization code for the printer cloud; generated by the administrator.



If you have successfully set up the printer cloud, this tray icon appears in the system tray.

Mapping in sessions

#### ICA sessions

- Include printers managed by PrinterLogic in ICA sessions. (default)

#### RDP sessions

- Include printers managed by PrinterLogic in RDP sessions. (default)

#### NX sessions

- Include printers managed by PrinterLogic in NX sessions.
- Don't printers managed by PrinterLogic in NX sessions. (default)

#### Parallels client sessions

- Include printers managed by PrinterLogic in Parallels client sessions.
- Don't include in Parallels client sessions. (default)

**Show CUPS printers:** Displays a list of installed printers that can be deleted.

The PrinterLogic menu



Right-click the icon to get the following options:

---

<sup>333</sup> <http://printercloud.com>



- **Add Printers...**: Opens the PrinterCloud in the browser. The installed printers are listed and can be installed via double-click.
- **Pull Printing...**: The print job is held and released by the user at each print device that supports this function.
  - **Print Job Management...**: Manages your print jobs.
  - **Secure Print Settings...**: Opens settings for secure printing.
- **Refresh Configurations**

### 3.12.2 Storage Devices

Menu path: **Setup > Devices > Storage Devices**

Configure your hotplug storage devices here.

**Show attached storage devices:** Shows a list with registered storage devices.

---

- [Storage Hotplug\(see page 1228\)](#)
- [Options\(see page 1230\)](#)
- [DriveLock\(see page 1231\)](#)

#### Storage Hotplug

Menu path: **Setup > Devices > Storage Devices > Storage Hotplug**

In this area you can set up the connection of hotplug storage devices to the device. These can be USB mass storage devices or MMC card readers for example.

Following file systems are officially supported:

|                    |                                         |
|--------------------|-----------------------------------------|
| ext2, ext3, ext4   | Standard Linux file systems             |
| squashfs           | a packed read-only file system          |
| vfat               | supports all FAT variants               |
| exFAT <sup>1</sup> | supports exFAT (found on SDXC SD-cards) |
| ISO 9660           | CDROM/DVD file systems                  |
| udf                | CDROM/DVD file systems                  |
| ntfs               | supported with ntfs-3g (Fuse)           |

<sup>1</sup> With Firmware 11.03.100 or newer

You can change the following settings:

#### Storage Hotplug

Hotplug storage devices will be mounted and unmounted automatically. When mounted, a hotplug storage device can be used in sessions like ICA, RDP, VMware Horizon, or in local applications like browser / PDF viewer or media player.



Before you unplug a hotplug storage device from the thin client, you must safely remove it. Otherwise, data on the hotplug storage device can be damaged. Depending on the configuration, there is one or several possibilities to safely remove a hotplug storage device:

- Click on in the task bar. The taskbar is not available in a fullscreen session.
- Click on in the in-session control bar. Depending on the configuration, the in-session control bar may be available in a fullscreen session. For further information, see [In-session Control Bar](#)(see page 1154).
- Function **Accessories > Disk Removal** with further starting possibilities; amongst other things, a hotkey can be defined here.  
If the following warning is displayed: **Volume(s) still in use. Dont' remove the device.**, then the hotplug storage device must not be removed. First, exit the program concerned or close all files or directories that reside on the hotplug storage device.

Hotplug storage devices will be mounted and unmounted automatically. (Default)

**Default permission:** Default access rights for hotplug storage devices.

Possible values:

- Read only
- Read/Write

**Client Drive Mapping:** Defines the creation of drives in ICA sessions, RDP sessions or Horizon sessions. The mounting of hotplug storage devices to the local file system is not influenced by this parameter.

Possible values:

- **Dynamic:** Drives are created automatically in a session when a hotplug storage device is connected to the device. When the device is removed, the corresponding drive is removed automatically.
- **Static:** The drives in a session are predefined by the parameters described under [Static Client Drive Mapping](#)(see page 1229).

Static Client Drive Mapping

**Private drive letter for each storage drive**

A drive letter is assigned to each hotplug storage device.

A single drive letter will be generated for all hotplug storage devices and each hotplug storage device will be assigned a sub-directory. (default)

**Number of drives:** The maximum number of hotplug storage devices that can be used simultaneously in the session.

When this number is reached, no additional hotplug storage devices will be assigned.

**Start storage drives with this drive letter:** Letter that is assigned to the first hotplug storage device if automatic drive mapping is enabled (default:A). Further hotplug storage devices are assigned the next letter alphabetically.



**ICA read access for storage hotplug devices:** Specifies whether read access to hotplug storage devices is allowed in an ICA session.

Possible values:

- Yes: Read access is allowed.
- No: Read access is not allowed.
- Ask user: Read access can be allowed on request.

**ICA write access for storage hotplug devices:** Specifies whether write access to hotplug storage devices is allowed in an ICA session.

Possible values:

- Yes: Write access is allowed.
- No: Write access is not allowed.
- Ask user: Write access can be allowed on request.

## Notification

### Hotplug beep

A signal tone will be heard when connecting and disconnecting hotplug storage devices. (Default)

### Hotplug message

Hotplug messages will be shown when connecting and disconnecting hotplug storage devices. (Default)

**Timeout:** Period of time in seconds after which the window with the hotplug messages is hidden. If the parameter is set to **No timeout**, the window will be shown until it is closed manually. (Default: 15)

You will find further settings options in the HDX / ICA Global setup area under [Drive mapping](#)(see page 781), in the RDP Global setup area under [Drive mapping](#)(see page 815), in the Devices area under [USB access control](#)(see page 1231) and in the Accessories area under [Disk Removal](#)(see page 1112).

## Options

Menu path: **Setup > Devices > Storage Devices > Options**

In this area, you can specify a directory in which external storage devices are accessible to the user. The devices are always mounted in the /media directory.

### User browse directory

The directory defined under **Browse directory** is linked to the /media directory. (Default)

**Browse directory:**/: Local directory in which the devices can be found. (Default: userhome/media)

### Support for built-in floppy drives

Built-in disk drives are active.

Built-in disk drives are disabled (default)

This option is only valid for drives which are not connected via USB.



## DriveLock

Menu path: **Devices > Storage Devices > DriveLock**

DriveLock allows the control of your USB devices and helps to prevent BadUSB attacks. For details, see <https://www.drivelock.com/>.

### Enable DriveLock agent

DriveLock agent is activated.

**DES server URL:** URL of the DriveLock Enterprise Service server used for the distribution of policies

**Tenant:** Name of the DES user group to which the policy should apply. (Default: root)

## 3.12.3 Bluetooth

Menu path: **Devices > Bluetooth**

In this area, you can set up a Bluetooth service.

### Bluetooth

The Bluetooth service is active. The Bluetooth Tool can be used.

The Bluetooth service is inactive. The Bluetooth Tool cannot be used. (Default)

### Tray Icon

A Bluetooth icon will be shown in the system tray. You can launch the Bluetooth Tool by double-clicking on the Bluetooth icon. Right-clicking on the Bluetooth icon will bring up an overview as to which Bluetooth devices are connected to the thin client and you can enable or disable Bluetooth.

A Bluetooth icon will not be shown in the system tray. (Default)

Details of the settings options for Bluetooth can be found under **Accessories > Bluetooth Tool**(see page 1100).

Here you can find information on the **Bluetooth Wizard**(see page 756).

## 3.12.4 USB Access Control

Menu path: **Devices > USB Access Control**

You can allow or prohibit the use of USB devices on your endpoint. Specific rules for individual devices or device classes are possible. For an example, see [How to Configure USB Access Control](#)(see page 706).

### Enable

USB access control is enabled and the following settings can be configured.

USB access control is inactive. (Default)



The activation of **USB Access Control** and setting the **Default rule** to **Deny** will block the use of USB devices locally and in the session and, thus, might disable devices needed for the users. Therefore, activate the USB access control only if your security policy requires that. In this case, set **Default rule** to **Deny** and configure **Allow** rules for the required USB devices and USB device classes.

It is recommended to make settings for **USB Access Control** as the last step in the device configuration. Before activating the USB access control, check that all your other settings for printers, Unified Communication, USB redirections, mapping settings for USB devices are working as expected.

Note that the USB access control is completely separate than USB redirection for remote sessions, see [When to Use USB Redirection](#)(see page 703).

Take also notice that the feature does not disable a USB port physically, i.e. power delivery will still work.

**Default rule:** Specifies whether the use of USB devices is allowed or prohibited.

- [Allow](#)
- [Deny](#)

**Default permission:** Default access rights for USB devices.

- [Read Only](#)
- [Read/Write](#)

## Class Rules

Class rules apply to USB device classes.

► Click on to create a new rule.

An input mask with the following options will open:

**Rule:** Specifies whether the use of the device class defined here is allowed or prohibited.

**Class ID:** Device class for which the rule should apply. (Examples: **Audio**, **Printers**, **Mass Storage**).

**Name:** Name of the rule

## Device Rules

Device rules apply to specific USB devices.

► Click on to create a new rule.

An input mask with the following options will open:

**Rule:** Specifies whether the use of the device defined here is allowed or prohibited.

**Vendor ID:** Hexadecimal ID of the device manufacturer

**Product ID:** Hexadecimal ID of the device

To find out the **Vendor ID** and **Product ID** of the connected USB device, use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal. You can also use the **System Information** tool, see [Using “System Information” Function](#)(see page 1108).



**Device uuid:** Universal Unique Identifier of the device

**Permission:** Authorizations for access to the device

Possible values:

- **Global setting:** The default setting for hotplug storage devices is used; see the **Default permission** parameter under **Devices > Storage Devices > Storage Hotplug**.
- Read only
- Read/Write

**Name:** Name of the rule

Further setting options can be found under [Storage Hotplug](#)(see page 1228).

### 3.12.5 Unified Communications

- [Jabra](#)(see page 1233)
- [EPOS Audio](#)(see page 1234)

#### Jabra

- [Jabra Xpress](#)(see page 1233)
- [Options](#)(see page 1234)

#### Jabra Xpress

Menu path: **Devices > Unified Communications > Jabra > Jabra Xpress**

Jabra Xpress is a solution for the remote mass-deployment of Jabra USB headsets that enables creating and deploying packages containing a configuration of settings, firmware updates, etc. for Jabra devices. For more information, see <https://www.jabra.com/supportpages/jabra-xpress#/>.

For detailed information on how to deploy a Jabra Xpress package, see [How to Deploy a Jabra Xpress Package](#)(see page 677).

**Device Dashboard URL:** URL of the dashboard server of the Jabra device.

**Package:** File name of the Jabra Xpress package. Example: `xpress_package_20190109_144111.zip`.

**Source URL:** URL to the directory containing the Xpress package. Example: `https://172.30.92.1:8443/ums_filetransfer/`

As a **Source URL**, you can specify any server, e.g. FTP(S) or HTTP(S), where you have placed the Xpress package downloaded from the Jabra Xpress portal.

If you want to use the UMS as a source location, your Jabra ZIP archive has to be registered as a file object in the UMS, see [Registering a File on the UMS Server](#)<sup>334</sup>. See also [UMS and Devices: File Transfer](#)<sup>335</sup>.

<sup>334</sup> <https://kb.igel.com/display/endpointmgmt606/Registering+a+file+on+the+UMS+server>

<sup>335</sup> <https://kb.igel.com/display/endpointmgmt606/UMS+and+Thin+Clients%3A+File+Transfer>



**Check SSL certificate:** Determines if the SSL certificate is checked. (Default: Enabled)

Disable SSL certificate checking if your HTTPS or FTPS server uses a self-signed certificate.

**User name:** User name for accessing the Xpress package that resides under the **Source URL**.

**Password:** Password for accessing the Xpress package that resides under the **Source URL**.

For the optimal performance of Jabra headsets (esp. relevant if Skype for Business is used), activate:

- in Citrix sessions: **HDX Realtime Media Engine** under **Sessions > Citrix > Citrix Global > Unified Communications > Skype for Business**;
- in VMware Horizon sessions: **Virtualization Pack Skype for Business** under **Sessions > Horizon Client > Horizon Client Global > Unified Communications > Skype for Business**;
- in RDP sessions: **Compression** under **Sessions > RDP > RDP Global > Performance**.

## Options

Menu path: **Devices > Unified Communications > Jabra > Options**

**Suspend on idle:** Determines if the wireless Jabra USB audio device is set to the offline state after 5 seconds of idle time. (Default)

## EPOS Audio

- [EPOS Connect](#)(see page 1234)

### EPOS Connect

Menu path: **Devices > Unified Communications > EPOS Audio > EPOS Connect**

Here you can set up EPOS Connect, a client application that connects with EPOS Manager and sends device information to it. EPOS Manager performs the following tasks for the EPOS devices that are connected to the endpoint:

- Firmware updates
- Remote asset management
- Remote configuration

### Enable EPOS Connect

The EPOS Connect client is enabled.

**Tenant ID:** The customer-specific system ID for your EPOS Manager installation.

**Backend Endpoint:** URL of EPOS Manager

**Proxy:** URL of the proxy that connects to EPOS Manager, if applicable. The proxy URL must be provided in the format [ADDRESS] : [PORT].



## 3.13 Security

Menu path: **Setup > Security**

In order to prevent unauthorized access to the thin client setup, it is important to set up an administrator password after the initial configuration. With an additional user password, you can allow the user to make limited changes to the configuration.

Further information can be found under [Password<sup>336</sup>](#).

---

- [Device Encryption](#)(see page 1235)
- [Password](#)(see page 1236)
- [Logon](#)(see page 1239)
- [Active Directory/Kerberos](#)(see page 1247)
- [Smartcard](#)(see page 1249)

### 3.13.1 Device Encryption

Menu path: **Security > Device Encryption**

#### **Device encryption mode**

Possible options:

- "Keep": If the device is encrypted, it stays encrypted. If it is not encrypted, it will not get encrypted.
- "Activate": The device will be encrypted when the user enters the password for the first time. The re-encryption may take about 10 to 60 seconds; the duration depends on the hardware performance and the size of the Custom Partition.
- "Deactivate": The device will be re-encrypted back to the default device encryption on the next boot. The re-encryption may take about 10 to 60 seconds.

**Change password:** Only applicable if device encryption is enabled. The user can change the password for device encryption.

#### **Authentication type**

Possible options:

- "PW": Password authentication. In this version of IGEL OS, this is the only available authentication type.

#### **Security level**

Possible options:

- "Auto, constant-time": The password aggregation function that fits best with the defined **Target time delay (ms)** is selected.
- "Auto, at least level": The security level will be at least as high as the value selected by **Password aggregation function**; if the **Target time delay (ms)** allows for a higher security level, the higher security level will be used.

---

<sup>336</sup> <https://kb.igel.com/display/igelos/Password>



- "Manual": The **Password aggregation function** can be set manually, irrespective of the delay time specified by **Target time delay (ms)**.

**Target time delay (ms):** Maximum time that should be consumed by the password aggregation function. This delay is effective when the user enters the device encryption password on boot or changes the device encryption password.

**Password aggregation function:** Security level of the encryption.

Possible options:

- "I: Argon2id, 8M/7 ops"
- "II: Argon2id, 128M/3 ops"
- "III: Argon2id, 256M/3 ops"
- "IV: Argon2id, 512M/3 ops"
- "V: Argon2id, 1024M/4 ops"
- "VI: Argon2id, 128M/4 ops"

**Minimum password length:** Minimum number of characters the password must be composed of

**Unwanted strings in password (comma separated):** Comma-separated list of strings that must not be contained in the password

**The password must contain:** Defines whether all of the subsequent minimum requirements (minimum amount of lower case letters etc.) must be fulfilled, or 2, or 3 of them.

- all
- 2 of
- 3 of

**Minimum amount of lower case letters**

**Minimum amount of upper case letters**

**Minimum amount of numbers**

**Minimum amount of special characters**

**Special characters allowed:** List of all non-alphanumeric characters that are allowed in the password, without separators

### 3.13.2 Password

Menu path: **Setup > Security > Password**

You can assign four different authorization levels:

**Administrator:** The administrator has full access to the IGEL Setup.



The assignment of the administrator password is a prerequisite for all other rights assignments. Even if the administrator wants to leave the administration of the Setup to the Setup administrator, the administrator password must be set.

An administrator password protects the following critical actions/areas from unauthorized access:

- the [reset to factory defaults](#)(see page 763) in the boot menu
- the [local terminal](#)(see page 1044)
- the [virtual console access](#)(see page 1144).

**Setup Administrator:** A user to whom rights are assigned for minor administrative tasks. You specify which pages the setup administrator can edit under **Accessories > Setup > Page Permissions Setup Administrator**.

**Setup User:** A user who can make some unlocked user settings in the Setup. You specify which pages the setup user can edit under **Accessories > Setup > Page Permissions Setup User**.

**User:** This user has no access to the Setup. A user password is required in the following cases:

- when logging on to the [terminal session](#)<sup>337</sup>
- when logging on to sessions (see Desktop Integration)
- for unlocking the [screenlock](#)<sup>338</sup>

If you have defined passwords for different authorization levels, a login window appears at the start of the Setup in which you can select an authorization level.

When entering a password, ensure that the correct [keyboard layout](#)(see page 1161) is enabled.

## Administrator

### Use password

- A password is needed to log in as administrator (root).
- A password is also needed for the user, the Setup user and the Setup administrator.
  - The password is set by clicking **Change password**.

No password is needed to log in as an administrator. Also, no password is needed for the user (user), the Setup user and the Setup administrator. (default)

**Change password:** Sets the password for the administrator (root).

<sup>337</sup> <https://kb.igel.com/display/igelos/Using+Local+Terminal>

<sup>338</sup> <https://kb.igel.com/pages/viewpage.action?pageId=23501723>



### Effects on local terminal access

Setting an administrator password has the following effects on the access to local terminals:

- For logging in as root, the administrator password must be entered.
- Logging in as user is no longer possible.

However, you can allow access for user by making the following settings:

- Enable the registry key `system.security.usershell` (Default: Disabled).
- Set a user password.

For logging in as user, the user password will have to be entered. (See the "User" section of this page).

## Setup Administrator

**Enable setup administrator access:** This option is relevant if an administrator password is set.

- The Setup administrator can access the areas of the Setup for which he has authorization.
- A password is needed to log in as Setup administrator.
  - The password is set by clicking **Change password**.
  - Further information can be found under [Page authorizations](#)<sup>339</sup>.
- Setup administrators cannot access the Setup. (default)

**Change password:** Sets a new password for Setup administrators.

## Setup User

**Enable user access:** This option is relevant if an administrator password is set.

- The user can access the areas of the Setup for which they have authorization. Further information can be found under [Page authorizations](#)<sup>340</sup>.
- A password is needed to log in as a setup user.
  - The password is set by clicking **Change password**.
- The user cannot access the *IGEL* setup. (default)

**Change password:** Sets the password for the setup user.

## User

**Use password:** This option is relevant if an administrator password is set.

- The user (user) needs a password in order to log in to the thin client via the local terminal. The password is set by clicking **Change password**.
- If an administrator password is set, the user (user) cannot log in to the thin client via the local terminal.

<sup>339</sup> <https://kb.igel.com/display/igelos/User+Page+Permissions>

<sup>340</sup> <https://kb.igel.com/display/igelos/User+Page+Permissions>



If no administrator password is set, the user (user) can log in to the thin client via the local terminal without a password. (default)

**Change password:** Sets the password for the user (user).

### User account for remote access

#### Enable login

The remote user (ruser) can log in to the thin client via SSH.

Further information can be found under [Remote access](#)<sup>341</sup>. (default)

Logging in via SSH is not possible.

#### Use password

A password is needed to log in via SSH.

No password is needed to log in via SSH. (default)

► By clicking **Change password**, set up a user password.

### 3.13.3 Logon

Menu path: **Setup > Security > Logon**

---

- [IGEL Smartcard](#)(see page 1239)
- [Taskbar](#)(see page 1240)
- [Active Directory/Kerberos](#)(see page 1242)
- [Shared Workplace](#)(see page 1244)
- [Local User](#)(see page 1246)

### IGEL Smartcard

Menu path: **Setup > Security > Logon > IGEL Smartcard**

#### Login with IGEL smartcard

You can log in to the device using a smartcard. Depending on the configuration, a password may also be needed. Sessions stored on the smartcard become available.

The desktop can be used without an IGEL smartcard. (Default)

#### Enable IGEL smartcard without locking desktop

Enables sessions stored on the smartcard after entering an optional password. The device is not locked – even without a smartcard.

The device will be locked after the removal of the smartcard. (Default)

---

<sup>341</sup> <https://kb.igel.com/display/igelos/Remote+Access>



### On smartcard removal, terminate

This parameter is available if **Enable IGEL smartcard without locking desktop** is activated.

Possible options:

- "All sessions": When the card is removed, all sessions are ended.
- "Sessions originating from smartcard": When the card is removed, all sessions stored on the card are ended. Other sessions are not affected.

**Company key:** A shared code for a smartcard and a device. The code entered must match the code stored on the IGEL smartcard. If two codes do not match, the IGEL smartcard cannot be used on this terminal.

Save the settings before starting to personalize the card.

### Start application to write IGEL smartcards:

**Smartcard personalization:** Opens a window where you can set a login password and add sessions to the card.

Session configurations are stored on the card's integrated circuit, and the session can be used on any IGEL device that reads the card.

Smartcard personalization is possible via the local Setup only. The option is not available via the UMS.

For further information about the smartcard personalization function, see [Using “Smartcard Personalization” function](#)(see page 1121).

For information on how to create IGEL smartcards via the UMS, see [Authentication with IGEL Smartcard](#)(see page 485).

See also [Smartcard Readers Supported by IGEL Smartcards](#)(see page 491).

## Taskbar

Menu path: **Setup > Security > Logon > Taskbar**

Taskbar settings for the login dialog

- **Show taskbar in login screen**
  - The taskbar will be shown during the login dialog. (Default)
  - The taskbar will not be shown during the login dialog.
- **Show clock**
  - The clock will be shown during the login dialog. (Default)
  - The clock will not be shown during the login dialog.
- **Show keyboard layout switcher**
  - The switch for the keyboard layout will be shown during the login dialog. (Default)
  - The switch for the keyboard layout will not be shown during the login dialog.
- **Show on-screen keyboard button**



- The button for opening the on-screen keyboard is shown during the login dialog.  
 The button for opening the on-screen keyboard is not shown during the login dialog. (Default)
- **Start on-screen keyboard automatically**  
 The on-screen keyboard is open during the login dialog.  
 The on-screen keyboard is not open during the login dialog. (Default)
- **Show reboot button**  
 The button for rebooting the thin client is shown during the login dialog.  
 The button for rebooting the thin client is not shown during the login dialog. (Default)
- **Show shutdown button**  
 The button for shutting down the thin client is shown during the login dialog. (Default)  
 The button for shutting down the thin client is not shown during the login dialog.

Taskbar settings when the screenlock is active

- **Show taskbar in screenlock**  
 The taskbar is shown while the screen is locked. (Default)  
 The taskbar is not shown while the screen is locked.
- **Show clock**  
 The clock is shown while the screen is locked. (Default)  
 The clock is not shown while the screen is locked.
- **Show keyboard layout switcher**  
 The switch for the keyboard layout is shown while the screen is locked. (Default)  
 The switch for the keyboard layout is not shown while the screen is locked.
- **Show on-screen keyboard button**  
 The button for opening the on-screen keyboard will be shown while the screen is locked.  
 The button for opening the on-screen keyboard will not be shown while the screen is locked. (Default)
- **Start on-screen keyboard automatically**  
 The on-screen keyboard will remain open while the screen is locked.  
 The on-screen keyboard is not open while the screen is locked. (Default)
- **Show reboot button**  
 The button for rebooting the thin client is shown while the screen is locked.  
 The button for rebooting the thin client is not shown while the screen is locked. (Default)
- **Show shutdown button**  
 The button for shutting down the thin client is shown while the screen is locked.  
 The button for shutting down the thin client is not shown while the screen is locked. (Default)
- **Show logoff button**  
 The button for logging off is shown while the screen is locked.  
 The button for logging off is not shown while the screen is locked. (Default)



There is no separate option for enabling/disabling network connection icons in the login dialog and/or on the locked screen. With **Show taskbar in login screen** and **Show taskbar in screenlock** enabled, they appear automatically if the option **Enable tray icon** is activated under **Setup > Network > LAN Interfaces > Interface 1 (or Interface 2, Wireless)** and/or under **Setup > Network > Mobile Broadband** (and/or **VPN**).

The network connection icons in the login dialog and on the locked screen, with the exception of the Wi-Fi icon, serve for information purposes only and thus are inactive on clicking.

The Wi-Fi icon invokes a [dialog for turning Wi-Fi on/off](#)(see page 1182) or the [Wireless Manager](#)(see page 1180) in case it is activated under **Setup > Network > LAN Interfaces > Wireless**.

## Active Directory/Kerberos

Menu path: **Setup > Security > Logon > Active Directory / Kerberos**

In this area, you can enable local login to the device via the Kerberos protocol. Active Directory/Kerberos must be configured, see [Active Directory/Kerberos](#)(see page 1247).

The login can be used for single sign-on in a number of session types (ICA, RDP).

- **Login to Active Directory domain**

- You can log in to the device via Active Directory.
- You cannot log in to the device via Active Directory. (Default)

### Login Methods

- **Explicit:**

- You can log in with a user name and password. (Default)
- You cannot log in with a user name and password. If logging in with a smartcard is set up, you can log in with a smartcard.

- **Remember last user name**

- The login dialog will be prepopulated with the last user name that logged on. **Explicit** must be enabled for this.
- The login dialog will not be prepopulated. (Default)

- **Smartcard**

- You can log in using a smartcard.
- You cannot log in using a smartcard. (Default)

Select the smartcard type under **Security > Smartcard > Middleware**.

- **Smartcard removal action:** Specifies what action is performed when the smartcard via which the user is logged in is removed.

Possible actions:



- Log out: The user is logged out from the device.
- Lock device: The screen is locked.

## Logout Shortcut Locations

The start options for the logoff function are specified here.

### **Start menu**

The session can be launched from the start menu.

### **Application Launcher**

The session can be launched with the Application Launcher.

### **Desktop**

The session can be launched with a program launcher on the desktop.

### **Quick start panel**

The session can be launched with the quick start panel.

### **Start menu's system tab**

The session can be launched with the start menu's system tab.

### **Application Launcher's system tab**

The session can be launched with the Application Launcher's system tab.

### **Desktop context menu**

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

### **Hotkey**

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. **Ctrl**.



Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

## Shared Workplace

Menu path: **Setup > Security > Logon > Shared Workplace**

- **Activate IGEL Shared Workplace**
  - You can log in to the thin client via IGEL Shared Workplace.
  - You cannot log in to the thin client via IGEL Shared Workplace. (Default)
- **Skip IGEL Shared Workplace login if UMS server is unavailable**
  - If the UMS server is not available, the user can log in via Active Directory/Kerberos. In order to do this, logging in via Active Directory/Kerberos must be configured; further information can be found under [Active Directory/Kerberos](#)(see page 1242).
  - Logging in is only possible if the UMS server is available. (Default)
- **Remember last user name**
  - The login dialog will be prepopulated with the last user name that logged on.
  - The login dialog will not be prepopulated. (Default)

## Logout Shortcut Locations

The start options for the logoff function are specified here.



- **Start menu:** If this option is enabled, the session can be launched from the start menu.
- **Application Launcher:** If this option is enabled, the session can be launched with the Application Launcher.
- **Desktop:** If this option is enabled, the session can be launched with a program launcher on the desktop.
- **Quick start panel:** If this option is enabled, the session can be launched with the quick start panel.
- **Start menu's system tab:** If this option is enabled, the session can be launched with the start menu's system tab.
- **Application Launcher's system tab:** If this option is enabled, the session can be launched with the Application Launcher's system tab.
- **Desktop context menu:** If this option is enabled, the session can be launched with the desktop context menu.
- **Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.
- **Path in the Application Launcher:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.
- **Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.
- **Password protection:** Specifies which password will be requested when launching the session.  
Possible values:
  - **None:** No password is requested when launching the session.
  - **Administrator:** The administrator password is requested when launching the session.
  - **User:** The user password is requested when launching the session.
  - **Setup user:** The setup user's password is requested when launching the session.
- **Hotkey:**
  - The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.
- **Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl. Here, you will find the available modifiers and the associated key symbols:
  - (No modifier) = None
  -  = Shift
  - [Ctrl] = Ctrl
  -  = Super\_L
  - [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super\_L
- **Key:** Key for the hotkey



To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field.  
Example: Tab in (`keysym 0xff09, Tab`)

## Local User

Menu path: **Setup > Security > Logon > Local User**

### Login with local user password

- Upon the start of the device, a login screen is shown and authentication with a local user password is enabled. A password specified under **Set password** is deployed to log in. This password will also be used for **User Interface > Screenlock / Screensaver > Options > Local user password** (previously called **Screenlock password**), see [Options](#)(see page 1157). If both **Active Directory (AD) login**(see page 1242) and login with local user password are enabled, you can choose on the login screen which login method you want to use.
- Authentication with a local user password upon device startup is disabled.

### Logout Shortcut Locations

#### Start menu

- The session can be launched from the start menu.

#### Application Launcher

- The session can be launched with the Application Launcher.

#### Desktop

- The session can be launched with a program launcher on the desktop.

#### Quick start panel

- The session can be launched with the quick start panel.

#### Start menu's system tab

- The session can be launched with the start menu's system tab.

#### Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

#### Desktop context menu

- The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.



**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

### 3.13.4 Active Directory/Kerberos

Menu path: **Setup > Security > Active Directory / Kerberos**

- **Enable**



- The Kerberos basic configuration will be carried out.  
 The Kerberos basic configuration will not be carried out. (default)
- **Default domain (Fully Qualified Domain Name):** This value must match the Windows domain on which the logon is to take place, e.g. EXAMPLE . COM.

The value must be entered in upper case letters.

- **DNS lookup for domain controller**

- In order to find the key distribution centers (KDCs, domain controllers) and other servers for a realm, DNS SRV records are used if they are not explicitly indicated. (default)
- The key distribution centers entered under **Setup > Security > Active Directory/Kerberos > Domain 1 ... Domain 4** will be used.

- **DNS lookup for domain**

- In order to determine the Kerberos realm of a host, DNS TXT records are used. (default)
- The details under **Setup > Security > Active Directory / Kerberos > Domain Realm Mapping** are used.

- **Obtain addressless tickets**

- The first Kerberos ticket is addressless. This may be necessary if the client is located behind an NAT device (Network Address Translation). (default)

- [Domain 1 ... Domain 4\(see page 1248\)](#)
- [Domain Realm Mapping\(see page 1248\)](#)

## Domain 1 ... Domain 4

Menu path: **Setup > Security > Active Directory/Kerberos > Domain 1 ... Domain 4**

Up to 4 domains where a login is possible can be configured here.

To configure a domain, proceed as follows:

1. Under **Domain name**, give the name of the domain (Kerberos realm).
  2. Click **[+]** to create a new entry.
  3. Under **Domain controller**, give the name or IP address of the domain controller (Kerberos key distribution center). A port number can be added to the host name; the port name must be preceded by a colon.
  4. Click on **Continue**.
- The domain controller will be added to the **Domain controller list**.

## Domain Realm Mapping

Menu path: **Setup > Security > Active Directory / Kerberos > Domain Realm Mapping**

With domain realm assignment, a host name is translated into the corresponding Kerberos realm name.

- **Use default DNS domain - Active Directory domain mapping**  
 The DNS name and Active Directory domain name match. (default)



DNS name and Active Directory domain name assignments must be set up.

To set up a DNS name to Active Directory domain name assignment proceed as follows:

1. Click  to create a new entry.
2. Under **DNS host or domain name**, enter the host name that is to be assigned to an Active Directory domain name.
3. Under **Active Directory domain name**, enter the Active Directory domain name that is to be assigned to the host name.
4. Click on **Continue**.

The data entered will be added to the **Domain realm mapping** list.

### 3.13.5 Smartcard

Menu path: **Setup > Security > Smartcard**

Here, you can define settings for logging on using a smartcard.

---

- Services(see page 1249)
- Middleware(see page 1250)

#### Services

Menu path: **Setup > Security > Smartcard > Services**

The PC/SC service enables the smartcard reader to connect to the device, so that the smartcard is available to an application. This can be a server-side application where the data are forwarded via an RDP or ICA connection or a local application, e.g. the browser.

##### Enable PC/SC daemon

- The PC/SC service is enabled. The card reader is available for applications. (Default)  
 The PC/SC service is disabled. The card reader is not available.

**Currently active PC/SC devices:** List of smartcard readers currently connected to the device. Internal smartcard readers and a variety of USB smartcard readers are supported.

You will find a list of supported smartcard readers in the [IGEL Hardware Database](#)<sup>342</sup>.

See also [Smartcard Readers Supported by IGEL Smartcards](#)(see page 491).

##### Cherry USB2LAN proxy

- The Cherry USB2LAN proxy is active and makes Cherry electronic health card devices available in the network via SICCT and HTTPS.  
 The Cherry USB2LAN proxy is disabled. (Default)

**Bind interface:** Network interface used for the proxy.

This parameter is available if **Cherry USB2LAN proxy** is enabled.

Possible options:

---

<sup>342</sup> <https://www.igel.com/linux-3rd-party-hardware-database/>



- "autoBind IP (see below) is set to "auto".
- "eth0": The Ethernet interface will be used.
- "wlan0": The WLAN interface will be used.
- Free text entry: The manually entered network interface will be used.

The Ethernet and WLAN interfaces can be configured under **Network > LAN Interfaces**. See [LAN Interfaces](#)(see page 1172).

**Bind IP:** The IP address used for the proxy.

Possible options:

- "autoBind interface is set to "auto".
- Free text entry: The manually entered IP address will be used instead of the network interface specified under **Bind interface**.

**HTTPS server port:** The TCP port for the HTTPS server. (Default: 443)

**SICCT announce IP:** The IP address to send the SICCT announce messages to.

Possible options:

- "broadcast
- Free text entry: SICCT announce messages are sent to the manually entered IP address.

**SICCT announce port:** UDP port for SICCT announce messages. (Default: 4742)

**SICCT announce interval:** Time interval in seconds for sending out SICCT announce messages.

Value range: 5 to 1800 (Default: 30)

#### USB fast mode

Faster connection to a Cherry eGK device is enabled.

Faster connection to a Cherry eGK device is disabled. (Default)

In order for the changes of this setting to be applied, the device must be unplugged and connected again.

#### Alternative initialization method for G87-1505

Alternative initialization method for Cherry eGK keyboard G87-1505 is enabled.

Alternative initialization method for Cherry eGK keyboard G87-1505 is disabled. (Default)

#### Middleware

Menu path: **Security > Smartcard > Middleware**

Here, select the middleware (PKCS#11 module) which matches your card or your token. The middleware selected here will be used for the following logins:

- Login to Citrix sessions; see [Citrix Global](#)(see page 776)



- Login to Citrix StoreFront; see [Citrix StoreFront](#)(see page 798)
- Login to thin client via Active Directory; see [Active Directory/Kerberos](#)(see page 1247)

The PKCS#11 module can be provided via a Custom Partition. For building a Custom Partition, see [Custom Partition Tutorial](#)(see page 529).

The following options are available:

**Gemalto SafeNet:** The middleware for Gemalto/SafeNet eToken, IDPrime smartcards and Token is used.

**cryptovision sc/interface:** The middleware for cryptovision smartcards is used.

**Gemalto IDPrime:** The middleware for Gemalto IDPrime smartcards is used.

Enable this Gemalto middleware when you want to operate Gemalto Common Criteria devices in unlinked mode.

**Athena IDProtect:** The middleware for Athena IDProtect smartcards is used.

**A.E.T. SafeSign:** The middleware for SafeSign smartcards is used.

**Secmaker Net iD:** The middleware for Net iD smartcards is used.

**Coolkey:** The middleware Coolkey is used.

**OpenSC:** The middleware OpenSC is used.

**90meter:** The 90meter middleware is used.

#### Licensed Feature

This feature requires an add-on license; see [Add-On Licenses](#)<sup>343</sup>. Please contact your IGEL sales representative.

**Custom PKCS#11 module:** The PKCS#11 module stored under the **Path to the library** is used. See also [Using a Custom PKCS#11 Library](#)(see page 588).

**Path to the library:** Path to the custom PKCS#11 module

## 3.14 System

Menu path: **Setup > System**

You can configure basic system settings here.

- [Time and Date](#)(see page 1252)
- [Update](#)(see page 1252)
- [Remote Management](#)(see page 1254)
- [Remote Access](#)(see page 1256)
- [Logging](#)(see page 1259)

<sup>343</sup> <https://kb.igel.com/display/licensesmoreigelos11/Add-on+Licenses>



- [Power Options](#)(see page 1261)
- [Firmware Customization](#)(see page 1264)
- [Registry](#)(see page 1282)

### 3.14.1 Time and Date

Menu path: **Setup > System > Time and Date**

- **Timezone Continent/Area:** Continent/Area for your location  
Possible values:
  - General: Under **Location**, you can select a time zone.
  - Africa... Pacific: Under **Location**, you can select a city for the selected continent/area.
- **Location:** Select your location or time zone.

Please note that the GMT time zones under Linux are usually in POSIX format. This means that you need to invert the actual time difference (e.g. for New York you select the zone "GMT+5" for "5 hours west of Greenwich" although the time in New York is actually 5 hours behind GMT). Defining the time zone by selecting a **Continent** and **Location** is therefore preferable.

- **Use NTP Time Server**  
 The system clock is set via NTP.  
 The system clock is not set via NTP. (default)
- **Use NTP Time Server:** IP or name of an NTP time server. If you would like to enter a list of NTP time servers for redundancy purposes, separate the servers with spaces.
- **Set time and date:** Carries over the time and date and sets the hardware clock.  
You will find further information regarding the updating of time zone information (e.g. summer time adjustments) in the [Updating Timezone Information \(Daylight Saving Time, DST\)](#)<sup>344</sup> FAQ.

### 3.14.2 Update

Menu path: **Setup > System > Update**

Here, you can configure settings for the system update.

- [Firmware Update](#)(see page 1252)
- [Buddy Update](#)(see page 1254)

#### Firmware Update

Menu path: **Setup > System > Update > Firmware Update**

Here, you can specify how the device obtains updates for its own firmware.

<sup>344</sup> <https://kb.igel.com/pages/viewpage.action?pageId=23501185>



### No Downgrade from IGEL OS 11.03

It is not possible to downgrade from IGEL OS 11.03 or higher to any version before IGEL OS 11.03, except IGEL OS 11.02.200. This is because, from IGEL OS 11.03 onwards, the system partitions are signed to guarantee their integrity; it is not possible to change from a system with signed partitions to a system with unsigned partitions. IGEL OS 11.02.200 is a special variant of IGEL OS 11.02 that has signed system partitions. IGEL OS 11.02.200 is only available from the IGEL Support Team.

### Update Can Be Canceled After Timeout

An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

- **Protocol:** Select the method for accessing the updates.

- HTTP: Download from a web server.
- HTTPS: Download from a TLS/SSL-secured web server.
- FTP: Download from an FTP server. (FTP passive mode is used)
- Secure FTP: Download via SSH-secured FTP.
- FTPS: Download from a TLS/SSL-secured FTP server.
- FILE: The update lies in the device file system, possibly as a shared NFS or Windows update.  
You can choose the location by selecting a file below.

- **Server name:** Name or IP address of the server.

- **Port:** Port of the server on which the service is provided.

- **Server path:** The path to the directory with the update files on the server.

- **User name:** User name on the server.

- **Password:** Password for the user account on the server.

- **Automatic update check on boot**

- The device will automatically search for and install an updated firmware version each time that it boots.
- The device will not automatically search for an updated firmware version. (Default)

- **Automatic update check on shutdown**

- The device will automatically search for and install an updated firmware version each time that it shuts down or it reboots.
- The device will not automatically search for an updated firmware version when it shuts down. (Default)

- **Automatic buddy detection**

- The device will automatically search for further devices in the local network that offer firmware updates as Buddy Servers.
- The device will not automatically search for Buddy Servers. (Default)



- **Update firmware:** Launches the update process. If you have made changes on this setup page earlier on, click on **Apply** first.

## Buddy Update

Menu path: **Setup > System > Update > Buddy Update**

Under **Buddy Update**, you can specify your thin client as an update server for other IGEL thin clients. If you use a thin client as an update server, only the FTP protocol can be used to update the firmware. A number of thin clients can be set up as buddy update servers within the network.

Thin clients without a specified update server search for available servers during the update. The first update server contacted then provides the update.

### No Downgrade from IGEL OS 11.03

It is not possible to downgrade from IGEL OS 11.03 or higher to any version before IGEL OS 11.03, except IGEL OS 11.02.200. This is because, from IGEL OS 11.03 onwards, the system partitions are signed to guarantee their integrity; it is not possible to change from a system with signed partitions to a system with unsigned partitions. IGEL OS 11.02.200 is a special variant of IGEL OS 11.02 that has signed system partitions. IGEL OS 11.02.200 is only available from the IGEL Support Team.

### Update Can Be Canceled After Timeout

An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

### Enable Update Server

- This thin client serves as an FTP firmware update server for other thin clients.
- This thin client does not serve as an FTP firmware update server for other thin clients. (default)

- **User Name:** User name for FTP access (default: anonymous)
- **Password:** Password for FTP access. The asterisk \* allows any password.
- **Max. Concurrent Logins:** Maximum number of simultaneous logons on the FTP server. (default: 10)

For further information, read the [Buddy Update\(see page 221\)](#) how-to.

## 3.14.3 Remote Management

Menu path: **Setup > System > Remote Management**

Here, you can configure settings relating to the remote administration of the device using the Universal Management Suite (UMS).



### Enable remote management

- The endpoint device can be managed via the UMS. (Default)
- Remote management is not allowed.

**Universal Management Suite:** If the device is registered on a UMS Server, its IP address or hostname will be shown in the list.

The list can contain more than one UMS instance. If the device cannot contact a UMS Server under the hostname `igelrmserver`, and the DHCP option 244 is not set, the device will go through the entries in the list until it can contact a UMS Server successfully.

To add another UMS instance, click on :

- **UMS Server:** Name or IP of the UMS Server
- **Port Number:** Port number of the UMS Server (Default: 30001)

**Display “Apply changes” dialog on boot:** If new settings were made in the UMS, the device may receive them during the boot procedure. Here you can decide whether the user can influence the application of the new settings.

During the boot procedure, the **Apply changes** dialog will be shown if new settings are available. The user can decide whether the new settings are applied immediately. If the user does not allow them to be applied immediately, they will automatically be applied when the system is next restarted.

The dialog will not be shown. The new settings will be automatically applied or ignored depending on the setting under **Default action on boot**.

**Timeout:** Number of seconds for which the **Apply changes** dialog is shown (Default: 20). If the timeout is exceeded, the received settings will be automatically applied.

Possible values:

- No timeout: The dialog is shown until the user clicks on a button.
- 1 ... 120 seconds

**Default action on boot:** Configure the action that is to be performed if the dialog exceeds the time limit or if it is disabled.

Possible values:

- Apply changed configuration immediately: New settings will become active immediately and programs that are running may be restarted.
- Ignore changed configuration: New settings will not be applied. The new configuration will be saved on the device.

### Prompt user on UMS actions

The user will be informed via a message window if the device receives new settings from the UMS or is shut down. (Default)

The user will not be informed if the device receives new settings from the UMS or is shut down.

**Timeout:** Number of seconds for which the notification window is shown

Possible values:

- No timeout: The dialog is shown until the user clicks on a button.
- 1 ... 120 seconds



**Structure tag:** You can define a structure tag in order to sort the device into a directory in accordance with the UMS directory rules.

**UMS Registration:** This button opens the [UMS Registration](#)(see page 1073) program from the accessories.

Further information regarding the use of structure tags can be found in the how-to [Using Structure Tags](#)<sup>345</sup>.

- [Options](#)(see page 1256)

## Options

Menu path: **Setup > System > Remote Management > Options**

- **Log login and logoff events**

Please note: For this option to work, in the UMS Console under **UMS Administration > Globale Configuration > Logging** the option **Log Events** must be enabled.

- If a user logs on or off via Citrix or Kerberos, details of this event will be sent to the UMS and can be used there, e.g. to process support queries.  
Logoffs from the Shared Workplace will also be logged (logons take place via the UMS anyway).  
(default)
- Logon and logoff events will not be relayed. (default)

The event logs can be found under the system information for the thin clients in the UMS.

- **Delay session start at boot time in order to apply new UMS settings:** If new settings were made in the UMS, the thin client may receive them during the boot procedure.

- The session start will be delayed until the settings have been transferred or the time limit has been exceeded.

- **Timeout:** Delay in seconds (default: 10)

Possible values:

- [No time limit](#): The dialog is shown until the user clicks on a button.
- 1 ... 120 seconds

## 3.14.4 Remote Access

Menu path: **Setup > System > Remote Access**

In order to allow central administration, the thin client can be configured in such a way that it can be accessed via the WAN.

- [SSH Access](#)(see page 1257)
- [Shadow](#)(see page 1258)
- [Secure Terminal](#)(see page 1259)

<sup>345</sup> <https://kb.igel.com/display/endpointmgmt605/Using+Structure+Tags>



## SSH Access

Menu path: **Setup > System > Remote Access > SSH Access**

Remote access to the local system via SSH is permitted by default. However, you can restrict remote access to a specific user from a specific host.

### Enable

The SSH service is enabled. (default)

### Permit empty passwords

Logging on without a password is allowed.

Logging on without a password is not allowed. (default)

### Permit administrator logon:

Logging on as an administrator is allowed.

Logging on as an administrator is not allowed (default)

**Port number:** Port number for SSH (default: 22)

## User access

**User name:** Permitted user

Possible values:

- root
- user
- ruser

For the **user name** "ruser" a password has to be assigned under **Security > Password**. The names "root" and "user" work also without passwords.

**Hostname:** Name of the host from which SSH access takes place (example: xterm.igel.de)

### Deny

Access is denied.

Access is allowed. (default)

### Permit X11 forwarding:

X11 forwarding is enabled.

X11 forwarding is disabled. (default)

Enable applications access for remote user "ruser"

**Command line:** Command that is allowed or prohibited for the remote user

### Enable application



- The application given under **command line** may be executed by the remote user. (default)
- The application given under **command line** may not be executed by the remote user.

## Shadow

Menu path: **Setup > System > Remote Access > Shadow**

For helpdesk purposes, you can observe the client through shadowing. This is possible via the IGEL UMS or another VNC client (e.g. TightVNC).

### For Remote Working, Use Secure Shadowing

If the endpoint device is in a mobile or work-from-home environment, it is highly recommended to use secure shadowing only. Regular shadowing without encryption poses a security risk.

The user can terminate the VNC connection at any time by clicking on the **End shadowing** button.

- **Allow remote shadowing:**

- Desktop content can be viewed from remote computers with VNC software.
- VNC shadowing is not allowed. (default)

You can change the following settings:

- **Secure mode**

- Communication will be secured via SSL/TLS and shadowing will only be possible for *UMS* administrators.
- Communication will not be secured via SSL/TLS. (default)

Further information regarding secure shadowing can be found in the [Secure Shadowing<sup>346</sup>](#) How-To.

- **Use password**

- The remote user must enter a password before shadowing can begin.
- The remote user does not require a password for shadowing. (default)

- **Password:** Password for the VNC connection

- **Prompt user to allow remote session**

- The local user will be asked for permission before shadowing. (default)
- The local user will not be asked for permission.

In a number of countries, for example Germany, unannounced shadowing is prohibited by law. Do not disable this option if you are in one of these countries!

- **Allow user to disconnect remote shadowing**

- A button with which the user can terminate the connection is shown. (default)

- **Allow input from remote**

- The remote user can make entries using the keyboard and mouse as if they were the local user. (default)

- **Scale frame buffer**

<sup>346</sup> <https://kb.igel.com/pages/viewpage.action?pageId=23500626>



- The screen content of the shadowed client is reduced or enlarged by the **scaling factor** before being transferred.

Further parameters for the VNC server on the client are accessible in the *IGEL* registry (**Setup > System > Registry > network.vncserver**).

- The screen content is transferred in the original size. (default)
- **Scale factor:** Factor by which the screen content of the shadowed client is enlarged or reduced (default: 1.0)

## Secure Terminal

Menu path: **Setup > System > Remote Access > Secure Terminal**

You can establish a secure terminal connection to a thin client.

The thin client must meet the following requirements:

- The firmware of the thin clients is *IGEL Linux Version 5.11.100* or higher or *IGEL Linux Version 10.01.100* or higher.

For IGEL Linux Version 5.11.100 and 10.03.100:

1. In the thin client setup, go to **System > Remote Access > Secure Terminal**
2. Enable **Secure Terminal**

For IGEL Linux Version 10.01.100 or newer:

- Enable the following options in the thin client registry:
  - **network > telnetd > enabled > allow telnet access**
  - **network > telnetd > secure\_mode > secure telnet**

You can allow access via the secure terminal for all registered thin clients. To do this, enable the **UMS Administration > Global Configuration > Remote Access > Enable Global Secure Terminal** option.

## 3.14.5 Logging

Menu path: **Setup > System > Logging**

Here you can configure local and remote logging for the device.

### Local logging

- The log messages are stored locally in `/var/log`. The format is human-readable. Log rotation is applied.
- The log messages are not stored locally.

**Persistent log partition:** This parameter is effective only when **Local logging** is activated.



The log messages are stored in a persistent partition on the device. This partition is encrypted.

The log messages are stored in temporary files that are deleted on reboot.

**Partition size in MB:** Size of the persistent log partition

#### Remote mode

Possible options:

- "Server": The device receives log messages from a remote client.
- "Client": The device sends its log messages to a remote server.
- "Off": The device does not send or receive any log messages.

### Remote Mode Switched to "Server"

You can configure the device to act as a syslog server. One or more other clients can send log files to this server; you can create a separate server configuration for each client.

**Template for log file storage:** Pattern from which the file path for storing the received log messages is created.

%HOSTNAME% is the name of the sender which is configured under **Name**.

**Server:** A syslog server can be added by clicking

**Local port:** Port on which the local server listens for log messages

**Transport protocol:** Protocol to be used for the transmission of log messages

**Name:** Hostname of the sender (optional). This is useful for filtering the log messages based on the clients that have sent them.

**Local address:** Optional parameter; on multihomed machines (i. e. machines with multiple addresses), this specifies to which local address rsyslog is bound. If no address is specified it defaults to 0.0.0.0, so that rsyslog listens on every network interface. For more information, see the official documentation at <https://www.rsyslog.com/doc/v8-stable/configuration/modules/imtcp.html>.

### Remote Mode Switched to "Client"

You can configure one or more clients, e.g. one server for kernel messages and another server for authentication messages.

**Clients:** A client can be added by clicking

**Remote address:** IP address or hostname of the remote server

**Remote port:** Port on which the server listens for log messages

**Transport protocol:** Protocol to be used for the transmission of log messages

**Syslog facility:** Type of program for which log messages are created

**Syslog level:** Severity level of the event

**Syslog style template:** Format in which the messages are sent

#### TLS enabled

TLS encryption for the transmission of log messages is enabled.

Transmitted log messages are not encrypted.



**CA certificate:** Path to the local CA root certificate file in PEM format which is used to verify the authenticity of the X.509 certificate of your log collector and analyzer. If the UMS is used to transfer the certificate file to devices (see [Logging and Log Evaluation](#)<sup>347</sup>), the same path and file name as in the UMS must be entered. Example: /wfs/ca-certs/ca.pem

### 3.14.6 Power Options

Menu path: **Setup > System > Power Options**

In this area, you will find the settings for energy management.

---

- [System](#)(see page 1261)
- [Battery](#)(see page 1262)
- [Screen](#)(see page 1263)
- [Shutdown](#)(see page 1263)

#### System

Menu path: **Setup > System > Power Options > System**

Here you can configure the settings for standby and for the CPU power plan.

**System suspend/shutdown on inactivity:** Specify how long the user can be inactive before the system switches to standby mode or shuts down, dependent on the option selected under **System action on inactivity**.

Possible values:

- [Never](#)
- After 1 minute
- ...
- After 24 hours

#### System action on inactivity

Possible options:

- Suspend: The system is set to standby mode after the timeout defined with **System suspend/shutdown on inactivity** has expired.
- Shutdown: The system is shut down after the timeout defined with **System suspend/shutdown on inactivity** has expired.

#### Without dialog

The user is not asked if the system is to be set to the standby mode.

The dialog will be shown. (Default).

**Dialog timeout:** Time in seconds, for which the dialog is to be displayed. (Default: [10 seconds](#))

**CPU Power Plan:** Specify here which CPU power plan (CPU Governor) the device is to use in battery mode and in AC mode.

---

<sup>347</sup> <https://kb.igel.com/display/securitysafety/Logging+and+Log+Evaluation>



- **On Battery:**

High Performance: full performance with maximum processor speed

Balanced (Smooth): slower regulation of performance in a balanced manner according to the demands of programs. Suitable for users who are bothered by the fan frequently running at high speed.

Balanced (Recommended): rapid regulation of performance according to the demands of programs.

Power Saver: lowest processor speed

- **Plugged in:**

High Performance

Balanced (Smooth)

Balanced (Recommended)

Power Saver

### Tray Icon

A CPU icon will be shown in the system tray. This makes it easy to switch between power plans.

No CPU icon will be shown. (Default)

## Battery

Menu path: **Setup > System > Power Options > Battery**

In this area, you can define the rechargeable battery messages.

### Battery Notification

- **Critical battery level (percentage):** Percentage of remaining battery charge deemed critical (default: 5)

- **Critical battery action:** Action to be taken in the event of a critical battery level Possible options:

- Do nothing
- Show warning
- Run command
- Run command in terminal

- **Critical command:** Command that is executed when a critical charge level is reached (example: Shutdown)

- **Low battery level (percentage):** Percentage of remaining battery charge deemed low (default: 10)

- **Low battery action:** Here you can specify what action is to be taken in the event of a low battery level.

Possible options:

- Do nothing
- Show warning
- Run command
- Run command in terminal

- **Low command:** Command that is executed when a low charge level is reached (example: Shutdown)



## Battery Tray Icon

- **Display percentage:**
  - The percentage of remaining energy is shown in the taskbar. (default)
- **Display time**
  - The estimated remaining battery life is shown in the taskbar.
  - The estimated remaining battery life is not shown. (default)

## Screen

Menu path: **Setup > System > Power Options > Display**

In this area, you can configure screen settings which can help to reduce energy consumption.

### Display Power Management Settings

- **Handle Display Power Management:**
  - You can configure energy saving settings separately for battery or AC operation. (default)
  - You cannot configure energy saving settings.
- **Standby Time:** Number of minutes after which the screen switches to standby mode if the user is inactive. (default: 6 minutes)
- **Suspend time:** Number of minutes after which the screen switches to suspend mode if the user is inactive. (default: 8 minutes)
- **Off Time:** Number of minutes after which the screen switches off if the user is inactive. (default: 10 minutes)

### Brightness Reduction

The brightness reduction controls have been added specifically for use of laptops. They have no effect on other devices connected to the power supply.

- **On inactivity reduce to:** Specify to how many percent the screen brightness should be reduced if you are not using the device for battery and AC operation. (default for battery: 20%, default for AC operation: 80%)
- **Reduce after:** Specify a time between 10 and 120 seconds after which the screen brightness will be reduced for battery and AC operation. (default: Never)

## Shutdown

Menu path: **Setup > System > Power Options > Shutdown**

Here, you can change the behavior when the device shuts down manually or automatically.

### Allow system shutdown

- The device can be shut down by the user. (Default)
- The device cannot be shut down by the user.



### Allow system suspend

- The device can be suspended by the user. (Default)  
 The device cannot be suspended by the user.

### Allow canceling of shutdown process

- The user can cancel the procedure via a button. (Default)  
 The user cannot cancel the procedure.

**Default action:** Action that is carried out when the time is set under **Dialog timeout**.

Possible options:

- Shutdown
- Suspend
- Cancel: No action will be carried out after the time set under **Dialog timeout** expires, see **Allow canceling of shutdown process** parameter.
- Nothing: No action will be carried out after the time set under **Dialog timeout** expires.

### Without dialog

- The dialog will not be shown. The action selected under **Default action** will be carried out.  
 The dialog will be shown. (Default)

**Dialog timeout:** After the time (in seconds) set here expires, the dialog will close and the action specified under **Default action** will be carried out. If the value is set to 0, the dialog will be shown until the user selects one of the possible actions. (Default: 10)

## 3.14.7 Firmware Customization

Menu path: **Setup > System > Firmware Customization**

You can configure the firmware according to your needs.

- [Custom Partition](#)(see page 1264)
- [Custom Application](#)(see page 1267)
- [Custom Commands](#)(see page 1272)
- [Corporate Design](#)(see page 1275)
- [Environment Variables](#)(see page 1280)
- [Features](#)(see page 1281)

### Custom Partition

Menu path: **Setup > System > Firmware Customization > Custom Partition**

In IGEL OS, a custom data partition is available for use as required. A download/update function that loads data from a server and, where appropriate, updates them can be set up for this custom storage area.

The IGEL Support Team offers support for the deployment of Custom Partitions. However, it is not possible to offer support for any third-party software that is installed on a Custom Partition.



If the device is reset to the default settings (factory reset), the custom partition and all data stored on it will be deleted.

- [Partition](#)(see page 1265)
- [Download](#)(see page 1266)

## Partition

Menu path: **Setup > System > Firmware Configuration > Custom Partition > Partition**

Here, you can create a partition of your own.

- **Enable partition**
  - The customer partition is enabled in the *IGEL* Setup of the thin client or with the *IGEL Universal Management Suite* via the setup path.
  - The customer partition is not enabled. (default)
- **Size:** Size of the partition in bytes. The value can have the following multiplicative endings:  
 k for kilobytes  
 K for kibibytes  
 m for megabytes  
 M for mebibytes  
 g for gigabytes  
 G for gibibytes

Sensible figures are for example 100 K (for 100 KiB = 100 \* 1024 bytes) or 100 M (for 100 MiB = 100 \* 1024 \* 1024 bytes). The size of the partition should be set to at least 100 KiB.

However, no more than 300 MiB should be reserved for the customer-specific partition (based on the 1 GB standard CF used in *IGEL Linux* thin clients). This is because subsequent firmware updates may require more storage space than the current version.

- **Mount point:** Path on which the partition is to be mounted. (default: /custom)
- **Partitions parameters:** From *IGEL OS Version 10.03.100*, you can enter name value pairs which are passed on to the custom partition for further processing.

To manage the list, proceed as follows:

- Click to create a new parameter.
- Click to remove the selected parameter.
- Click to edit the selected parameter.
- Click to copy the selected parameter.

## Add

- **Name:** Name of the parameter
- **Value:** Value of the parameter



## Download

Menu path: **Setup > System > Firmware Configuration > Custom Partition > Download**

### Sources for partition data

In order to load data onto the custom partition, at least one source for partition data must be set up here.

To manage the list, proceed as follows:

- Click to create a new source.
- Click to remove the selected source.
- Click to edit the selected source.
- Click to copy the selected source.

## Add

- **Automatic update**  
 The contents from this source will be updated automatically.  
 The contents from this source will not be updated automatically. (default)
- **URL:** URL of the web server
- **User name:** User name for access to the web server
- **Password:** Password for access to the web server
- **Initialization action:** Action which is performed after mounting the partition (program or script with absolute path). For example, a program downloaded to the partition can be launched.
- **Finalizing action:** Action which is performed before mounting the partition (program or script with absolute path). For example, a program downloaded to the partition can be ended.

The transfer protocols are the same as the ones for updating the firmware, e.g. HTTP and HTTPS. An INF file which in turn references a tar archive zipped using bzip2 must be referenced as the target.

The structure of the INF file is as follows:

|                     |                                                                                            |
|---------------------|--------------------------------------------------------------------------------------------|
| [INFO] , [PART]     | Header information                                                                         |
| file="test.tar.bz2" | File name of the compressed tar archive                                                    |
| version="1"         | Version number - a higher version results in an update if Update automatically is enabled. |

The files to be transferred must therefore be zipped in a tar archive which is then compressed using bzip2. This file is referenced in the INF file which is the target of the URL.

The tar archive can be created under Windows, e.g. with the open source program 7-Zip ([www.7-zip.de](http://www.7-zip.de)<sup>348</sup>). This program also allows bzip2 compression. Under Linux, tar and bz2 files can be created using onboard resources.

<sup>348</sup> <http://www.7-zip.de>



The procedure makes it possible to replace the file(s) on the server with a new version which the thin client loads the next time it is booted. The Version parameter in the INF file must be increased for this purpose.

## Custom Application

Menu path: **System > Firmware Customization > Custom Application**

Applications that were loaded onto a customer partition for example can be launched via the Application Launcher or an icon on the desktop once they have been defined as custom applications. In order for this to be possible, a command to call up the application must be entered under [Settings](#)(see page 1269).

- ▶ Click on **[+]** to define a custom application.
- ▶ Specify the launch options:

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )

### Starting Methods for Session

#### Start menu

The session can be launched from the start menu.

#### Application Launcher

The session can be launched with the Application Launcher.

#### Desktop

The session can be launched with a program launcher on the desktop.

#### Quick start panel

The session can be launched with the quick start panel.

#### Start menu's system tab

The session can be launched with the start menu's system tab.

#### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

#### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.



**Password protection:** Specifies which password will be requested when launching the session.  
Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

#### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- = Alt

Key combinations are formed as follows with |:

- + = Ctrl | Super\_L

#### Key: Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (`keysym 0xff09, Tab`)

#### Autostart

The session will be launched automatically when the device boots.

#### Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.



**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

- For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.
- No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

#### Autostart requires network

- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode\(see page 869\)](#).

- The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

- The session cannot be started in appliance mode.

- 
- [Settings\(see page 1269\)](#)
  - [Desktop Integration\(see page 1269\)](#)

#### Settings

Menu path: **System > Firmware Customization> Custom Application > [Session Name] > Settings**

Enter the command for calling up an application here:

**Icon name:** Select an icon provided. (default: applications-other).

**Command:** Give the name and path of the application. (Example: /usr/bin/gpicview).

Only the desktop icon of a session is customizable. The taskbar icon of a session cannot be customized and will remain the default icon. Complete customization is not possible.

#### Desktop Integration

Menu path: **System > Firmware Customization > Custom Application > [Session Name] > Desktop Integration**

**Session name:** Name for the session.

The session name must not contain any of these characters: \ / : \* ? “ < > | [ ] { } ( )



## Starting Methods for Session

### Start menu

The session can be launched from the start menu.

### Application Launcher

The session can be launched with the Application Launcher.

### Desktop

The session can be launched with a program launcher on the desktop.

### Quick start panel

The session can be launched with the quick start panel.

### Start menu's system tab

The session can be launched with the start menu's system tab.

### Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

### Desktop context menu

The session can be launched with the desktop context menu.

**Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

**Application Launcher folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

**Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

**Password protection:** Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

### Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

**Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol / combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. Ctrl.

Do not use [AltGr] as a modifier (represented as Mod5). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".



These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = None
- = Shift
- [Ctrl] = Ctrl
- = Mod4

When this keyboard key is used as a modifier, it is represented as Mod4; when it is used as a key, it is represented as Super\_L.

- [Alt] = Alt

Key combinations are formed as follows with | :

- Ctrl + = Ctrl | Super\_L

**Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard. Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

#### Autostart

The session will be launched automatically when the device boots.

#### Restart

The session will be relaunched automatically after the termination.

**Autostart delay:** Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

**Autostart notification:** This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

#### Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

**Appliance mode access:** Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 869).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)



- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

## Custom Commands

Menu path: **Setup > System > Firmware Customization > Custom Commands**

You can define custom commands for specific points in time when the system is starting. You can use configured [environment variables](#)(see page 1280) in the commands.

---

- [Post Session](#)(see page 1272)
- [Base](#)(see page 1273)
- [Network](#)(see page 1274)
- [Desktop](#)(see page 1275)
- [Reconfiguration](#)(see page 1275)

### Post Session

Menu path: **System > Firmware Customization > Custom Commands > Post Session**

For a specific session type, you can define an action that is performed when the last session of this type is ended. The defined post-session command can also be used for multiple session types.

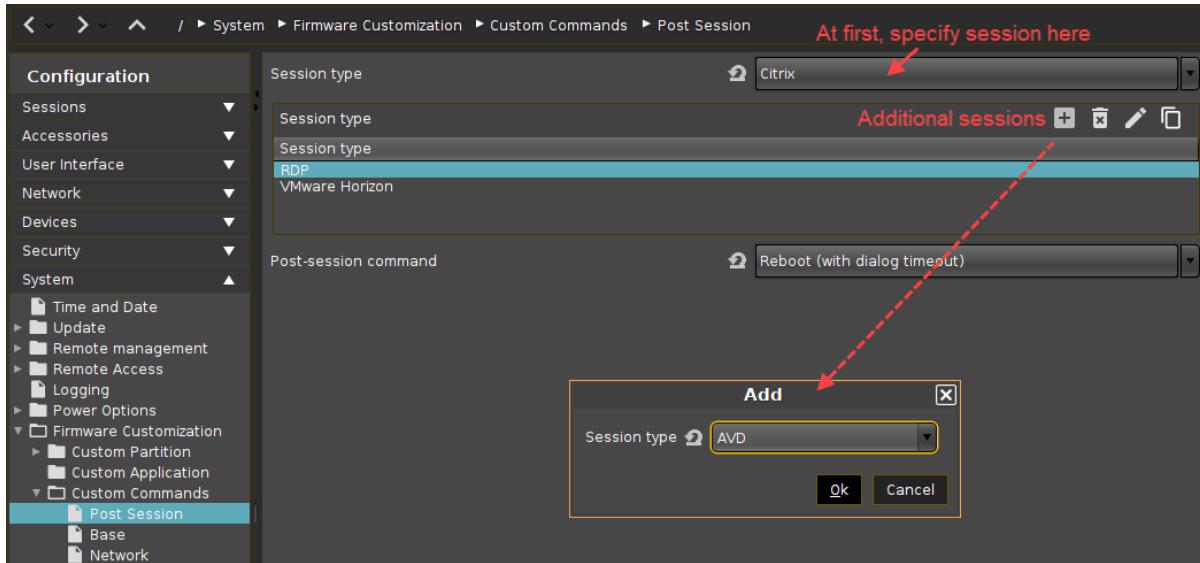
**Session type:** Session type for which the action is performed

Possible values:

- No post-session command
- Citrix
- Citrix via Browser
- RDP (with login dialog)
- RDP
- VMware Horizon
- Browser
- NoMachine NX
- Parallels Client
- PowerTerm terminal emulation
- ThinLinc
- X session
- IBM iAccess
- Media player
- VNC viewer
- AVD



- If a post-session command has to be applied to multiple sessions, specify the main session in the above **Session type** field and use **[+]** to add additional sessions.



**Post-session command:** Action that is carried out after the end of the session(s) selected above  
Possible options:

- "Logoff": The user is automatically logged off; a login method must be defined for this purpose.  
Further information can be found under [IGEL Smartcard](#)(see page 1239), [Active Directory / Kerberos](#)(see page 1242) and [Smartcard](#)(see page 1249).

The “Logoff” option cannot be used if the Appliance Mode is in use. Further information can be found under [Appliance Mode](#)(see page 869).

- "Shutdown/suspend (system default action)": The device will be shut down or placed in a standby mode depending on the setting under **System > Power Options > Shutdown > Default action** selection. A dialog allowing the user to cancel the procedure will be shown in the process. Further information can be found under [Shutdown](#)(see page 1263).
- "Shutdown/suspend (system default action without dialog)": The device will be shut down or placed in a standby mode depending on the setting under **System > Power Options > Shutdown > Default action** selection. The user cannot cancel the procedure.
- "Reboot (with dialog timeout)": The device will reboot. A dialog allowing the user to cancel the procedure will be shown in the process.
- "Reboot (without dialog)": The device will reboot. The user cannot cancel the procedure.
- "Enter custom command here": Command to be executed

## Base

Menu path: **Setup > System > Firmware Customization > Custom Commands > Base**

The commands defined here are executed on a one-off basis during the boot procedure. You can define commands for the execution times described below:



- **Initialization**
  - Not all drivers loaded, not all devices available
  - Network scripts not launched, network not available
  - Partitions available except *firefox profile, scim data, ncp data, custom partition*
- **Before session configuration**
  - Not all drivers loaded, not all devices available
  - Network scripts launched, network not available
  - Partitions available except *firefox profile, scim data, ncp data, custom partition*
  - Sessions not configured
- **After session configuration**
  - All drivers loaded, all devices available
  - Network available
  - Partitions available except *custom partition*
  - System daemons not launched (CUPS, ThinPrint etc.)
  - Sessions configured
  - UMS settings retrieved but not yet effective
- **Final initialization command**
  - All partitions available
  - All system daemons launched
  - UMS settings effective

## Network

Menu path: **Setup > System > Firmware Customization > Custom Commands > Network**

You can define commands for the execution times described below:

### Network initialization

- The commands defined here are executed at the beginning of the network configuration.

The commands in the below fields are executed each time the relevant network interface starts. The `INTERFACE` environment variable contains the name of the network interface started.

### After network DNS

- Runs after each change in the IP address or host name
- IP address / name server settings used (e.g. via DHCP)

### Before network services

- IP address / name server settings used
- VPN connected (if VPN autostart was enabled in the setup)
- No network / host routing settings used

### Final network command

- Network / host routing settings used
- NFS and SMB drives available
- System time synchronized with time server
- UMS settings retrieved but not effective yet



## Desktop

Menu path: **Setup > System > Firmware Customization > Custom Commands > Desktop**

The commands defined here are executed when the X server is launched. You can define commands for the execution times described below:

- **Desktop initialization**

- Runs once during the boot procedure
- Desktop environment configured but not launched
- User not logged on (Kerberos, smartcard etc.)

- **Before desktop start**

- Runs once during the boot procedure
- Desktop environment launched
- Message service launched
- Session D-Bus launched
- User not logged on (Kerberos, smartcard etc.)

- **Final desktop command**

- Runs after each user logon and desktop restart
- User logged on (Kerberos, smartcard etc.)
- User desktop launched

## Reconfiguration

Menu path: **Setup > System > Firmware Customization > Custom Commands > Reconfiguration**

The commands defined here are executed after settings relating to the local setup or the UMS have been changed. You can define commands for the execution time described below.

- **After reconfiguration:** Runs after an effective change in the endpoint device settings (local setup, UMS)

## Corporate Design

Menu path: **Setup > System > Firmware Customization > Corporate Design**

In this area, settings options allowing you to adapt the user interface to your company layout are grouped together.

You can place your own logo in the following places:

- [Custom Bootsplash](#)(see page 1275)
- [Background \(1st Monitor\)](#)(see page 1277)
- [Company Logos](#)(see page 1279)

Please also see our [Customizing IGEL Linux Desktop](#)<sup>349</sup> How-To.

## Custom Bootsplash

Menu path: **Setup > System > Firmware Configuration > Corporate Design > Custom Bootsplash**

---

<sup>349</sup> <https://kb.igel.com/display/igelos/Customizing+IGEL+Linux+Desktop>



With a bootsplash, you can show your company logo or a specific image during the booting procedure. The bootsplash will be shown instead of the console messages.

Please note: You need to provide an image file for your custom bootsplash on a download server.

The file types BMP, JPG, GIF, TIF, PNG and SVG are supported for a bootsplash. A total storage area of 25 MB is available for all user-specific images. The image is 800 x 600 pixels in size (aspect ratio remains unchanged). It can be positioned vertically and horizontally.

## Custom bootsplash

- **Enable custom bootsplash**

- You can make the following settings in order to configure a custom bootsplash.
- No custom bootsplash is configured. (default)

## Custom bootsplash - Server Location

- **Use firmware update server location**

- The server configuration will be carried over from the [firmware update](#)(see page 1252).
- You can carry out a custom configuration below. (default)

- **Protocol:** Access method for the image

- HTTP: Download from a web server.
- HTTPS: Download from a TLS/SSL-secured web server.
- FTP: Download from an FTP server.
- Secure FTP: Download via SSH-secured FTP.
- FTPS: Download from a TLS/SSL-secured FTP server.
- FILE: The image file lies in the thin client file system, possibly as a shared NFS or Windows update. You can choose the location simply by selecting a file below.

- **Server name:** Name or IP address of the server

- **Port:** Port of the server on which the service is provided

- **Server path:** Path to the directory with the image file on the server

- **User name:** User name on the server

- **Password:** Password for the user account on the server

## Custom Bootsplash - Settings

- **Custom bootsplash file:** File name of the custom image

As regards positioning, the following applies: 0 = left-justified, 50 = centered, 100 = right-justified

- **Custom Bootsplash Style:**

- Original
- Stretched
- Scaled
- Zoomed

- **Background color:** Use the color picker to choose.

- **Horizontal position of the bootsplash image** (default: 50)

- **Vertical position of the bootsplash image** (default: 50)



- **Size of progress indicator** (default [72](#))
- **Horizontal position of the progress indicator** (default: [90](#))
- **Vertical position of the progress indictaor** (default: [90](#))
- **Bootsplash update:** The user-specific bootsplash will be downloaded from the given server.

If you change the image file or even just one of the settings for an existing bootsplash, be sure to click on **Bootsplash update** in order to regenerate the system files used and then on **Apply** or **OK**.

## Background (1st Monitor)

Menu path: **Setup > System > Firmware Customization > Corporate Design > Background (1st Monitor)**

Decorate the desktop background with predefined IGEL backgrounds, a fill color or a color gradient or define a custom background image. You can set up a separate background image for each monitor that is connected to the thin client.

Prerequisite: You have provided a custom background image on a server; see [Background Image Server](#)(see page 1278).

The file types BMP, JPG, GIF, TIF, PNG and SVG are supported for a background image. A total storage area of 25 MB is available for firmware customization images.

From IGEL Linux Version 10.03.500 both background images and background image server can be defined user-customized via Shared Workplace. Please note the following for this:

- All user-customized background images will be saved on the thin client and therefore require a part of the available 25 MB storage space. Ensure that this storage limit is not exceeded. (When the storage limit is reached, all images except the one currently used will be deleted; with a new logon via Shared Workplace, the previously deleted images will be downloaded again until the storage limit is reached.)

You will find further information on Shared Workplace and background images here:

- IGEL Linux user manual: [Shared Workplace](#)(see page 1244)
- IGEL UMS user manual: Shared Workplace
- How-To: Creating your own Wallpaper in the How-To Customizing the IGEL Linux Desktop

- **Wallpaper:** Select one of the predefined background images from the following list:

- neutral
- disabled
- black (4x3)
- [blue \(4x3\)](#)
- gray (4x3)
- orange (4x3)



- green
- black (16x9)
- blue (16x9)
- gray (16x9)
- orange (16x9)
- **Wallpaper Style:** If you have set a custom background image, you can display it in a number of ways.  
Possible options:
  - Automatic
  - Centered
  - Tiled
  - Spread
  - Scaled
  - Zoomed
- **Color Style:** If you have chosen two different colors as the desktop background color, you can define color gradients here. Possible values:  
Possible options:
  - Solid color
  - Horizontal gradient
  - Vertical gradient
- **Desktop Color:** Click on **Choose color** to specify a custom background color for your desktop if you have not chosen a background image.
- **2nd Desktop Color:** Click on **Choose color** to specify a second background color for your desktop.
- **Custom wallpaper download**  
 You can set up a custom background image.  
 No custom background image will be used. (Default)
- **Custom Wallpaper file:** Name of the background image file

If you would like to use a custom background image, you need to specify the download server under **System > Firmware Customization > Corporate Design > Background (1st Monitor) > Custom Wallpaper Server**(see page 1278). If you have already defined a server for the system update files, you can use the same server settings for downloading the background image.

## Background Image Server

Menu path: **Setup > System > Firmware Customization > Corporate Design > Background (1st Monitor) > Custom Wallpaper Server**

### Custom Wallpaper - Server Configuration

- **Use firmware update server location**  
 The server configuration will be carried over from the [firmware update](#)(see page 1252).  
 You can carry out a custom configuration below. (default)
- **Protocol:** Select the method for accessing the image.
  - HTTP: Download from a web server.
  - HTTPS: Download from a TLS/SSL-secured web server.



- **FTP:** Download from an FTP server.
- **Secure FTP:** Download via SSH-secured FTP.
- **FTPS:** Download from a TLS/SSL-secured FTP server.
- **FILE:** The image lies in the thin client file system, possibly as a shared NFS or Windows file. You can choose the location simply by selecting a file below.
- **Server name:** Name or IP address of the server.
- **Port:** Port of the server on which the service is provided.
- **Server path:** The path to the directory with the image file on the server
- **User name:** User name on the server
- **Password:** Password for the user account on the server
- **Wallpaper update:** The user-specific background image will be downloaded from the given server.

## Company Logos

Menu path: **Setup > System > Firmware Customization > Corporate Design > Company Logos**

You can show your company logo in the screensaver and in the start menu.

## Screensaver

- **Enable image display**  
 The image defined below will be shown as the screensaver. (default)
- **File for screen saver logo:** Complete path for an image file or a directory that contains a number of image files.

If you enter a folder instead of a single image file as the source, all images in the folder will be displayed as a slide show. The **image display time** for the images can be configured. If you do not specify a file of your own, the *IGEL* logo will be used.

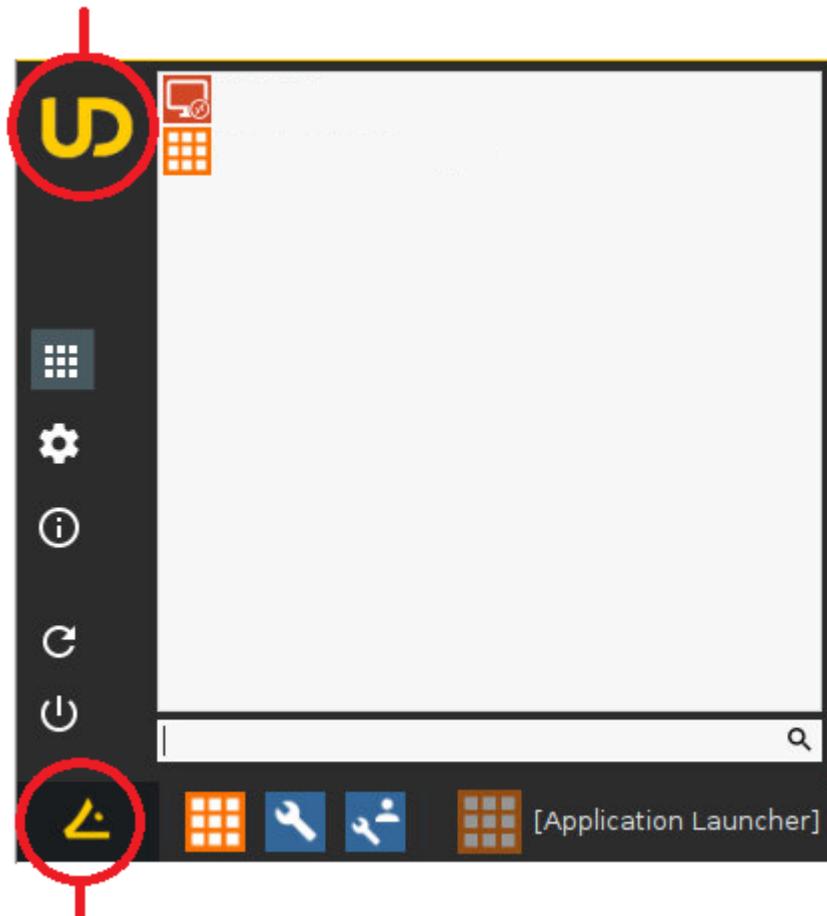
- **One image per monitor**  
 The image will be shown on each individual monitor rather than one image across all monitors. (default)
- **Image duration:** Time in seconds until the image changes (default: 10)
- **Image display mode**
  - **Small-sized hopping:** small image that jumps across the screen
  - Medium-sized hopping: larger image that jumps across the screen
  - Full screen center cut out: Image is displayed across whole screen, edges can be cut off.
  - Full screen letterbox: Complete image is shown. A black edge may be visible depending on the format.

## Start menu

- **Start button icon:** File name with full path to select your logo as the icon for the start menu in the taskbar. Size: 32x32 pixels
- **Company logo in start menu:** File name with full path to show your company logo in the start menu window. Size: 64x64 pixels

In order to see the company logo in the start menu window, you must set the start menu type to **Advanced**. To do this, click on **User Interface > Desktop > Start Menu**.

### Logo in Start Menü



### Start Button Icon

## Environment Variables

Menu path: **System > Firmware Customization > Environment Variables**

Environment variables allow you to use dynamic parameter values for a number of session types, e.g. so as not to have to enter ICA or RDP servers for every session.

Predefined variables can also be allocated and distributed via the IGEL UMS. Additionally, defined variables can only be used locally on the thin client and may be overwritten by a UMS configuration.

**Enable variable substitution in session:** (default: disabled)

The use of variables in sessions such as ICA and RDP is enabled. If specific parameters contain a \$, shell substitution will be carried out.



- The use of variables in sessions is not enabled. (default)

The environment variables are available in the setup under [Custom Commands](#)(see page 1272).

In addition, the following session parameters can be updated through variables:

- Legacy ICA sessions: Citrix Server or published application
  - Legacy ICA sessions: User
  - RDP session: Server
  - RDP session: User
- 

- [Predefined](#)(see page 1281)
- [Additional](#)(see page 1281)

#### Predefined

Menu path: **System > Firmware Customization > Environment Variables > Predefined**

- **Variable name:** Name for the variable
- **Value:** Value for the variable

To use environment variables in sessions, proceed as follows:

1. Enable environment variables under **System > Firmware Customization > Environment Variables > Enable variable substitution in session.**
2. Define the variable name and content, e.g.
  - **Variable name:** SERVERNAME
  - **Value:** testServer
3. Enter the variable name in the parameter field of the session with the \$ symbol before it. Example: \$SERVERNAME

In the case of RDP and ICA sessions, the value is entered in the session file after saving.  
With XenApp, the setting is not implemented until a session starts and is running.

#### Additional

Menu path: **System > Firmware Customization > Environment Variables > Additional**

You can define other variables in addition to the 10 predefined ones.

- **Variable name:** Name for the variable
- **Value:** Value for the variable

#### Features

Menu path: **System > Firmware Customization > Features**

Using this list of available services, you can quickly enable or disable firmware components such as Media Player, Extra Font Services, etc. By deactivating e.g. unused features, you can save storage space.



If a service was disabled, the associated session type will no longer be available when the system is restarted. Existing sessions will no longer be shown but will not be deleted either.

For further information, see [Disabling Features to Reduce Firmware Size](#)(see page 376).

A disabled session type will not be updated during a firmware update. Therefore, you should disable unused services in order to speed up update processes.

#### Features with Limited Support

A number of products feature functions with “limited support”. These functions are offered ‘as is’ without any warranty. Any support for these functions is provided on a non-binding, “best effort” basis.

### 3.14.8 Registry

Menu path: **System > Registry**

In the registry, you can change virtually any firmware parameter. You will find information on the individual items in the tooltips.

Changes to the registry should only be made by experienced administrators. Incorrect parameter settings can easily destroy the configuration and cause the system to crash. In cases like these, the only way to restore the functionality is to reset the device to the factory defaults!

**Search parameter....:** Search for setup parameters in the registry.

- **Search criterion:** Criterion for searching.

The following can be selected:

- Parameter name

- **Parameter name:** Any search term.

- Logical search restriction:

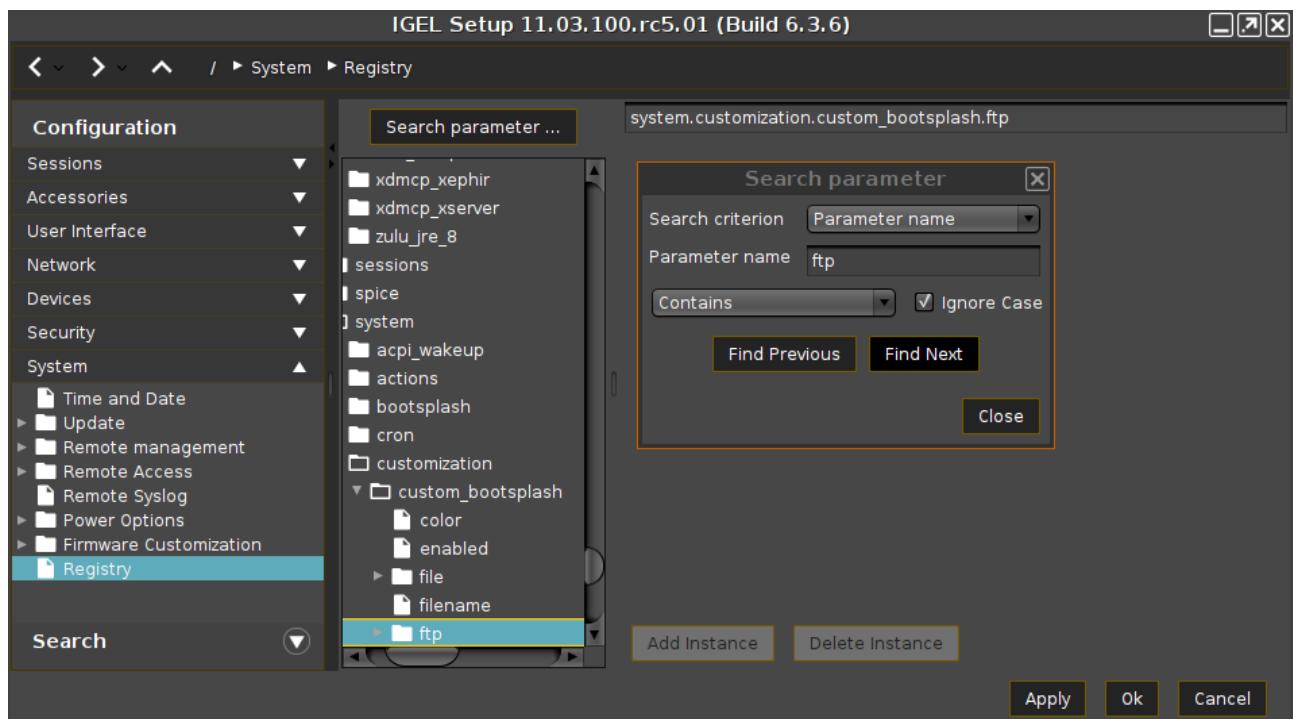
- Contains
- Exact match
- Use regular expressions

- **Ignore case**

- **Find previous:** Go back if there are a number of hits.

- **Find next:** Go forwards if there are a number of hits.

Example: If you would like to find the FTP settings for updating the Linux firmware, you can search for the parameter name `ftp`. The parameter found in the registry structure is highlighted. Click on **Find next** until you find your desired parameter:



**Add instance:** Adds instances. This is possible with parameters which have a percent sign as their last character, e.g. nfymount%. The new instances are numbered consecutively: nfymount1, nfymount2 etc.

**Delete instance:** Deletes a previously added instance.



## 4 UD Pocket (UDP) Reference Manual

This reference manual applies to **UD Pocket<sup>350</sup>** and **UD Pocket2<sup>351</sup>**.

- General Information(see page 1284)
- Devices Supported by OSC and UD Pocket(see page 1284)
- Setup and Startup(see page 1291)

### 4.1 IGEL TechChannel



Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:

<https://www.youtube.com/watch?v=iURhgESSn6k>

### 4.2 General Information

UD Pocket boots IGEL OS on your computer. However, it does not make any changes to the operating system already installed on the hard disk, SSD or flash storage - UD Pocket runs entirely from the USB stick.

UD Pocket has a partition which contains this manual and is readable under Windows.

UD Pocket, like all IGEL operating systems, can be managed centrally using the Universal Management Suite (UMS).

This document describes setting up and starting UD Pocket on your computer.

UD Pocket uses IGEL OS, which is described in detail in the [IGEL OS Reference Manual](#)(see page 750).

### 4.3 Devices Supported by OSC and UD Pocket

#### 4.3.1 Core Requirements

- CPU with 64-bit support
- CPU speed ≥ 1 GHz
- ≥ 2 GB memory (RAM)

With devices that have 2 GB RAM and shared video memory, a maximum of 512 MB may be used as video memory.

<sup>350</sup> <https://kb.igel.com/display/hardware/Technical+Specification+UD+Pocket>

<sup>351</sup> <https://kb.igel.com/display/hardware/Technical+Specification+UD+Pocket2>



- Recommended: ≥ 4 GB; minimum 2 GB storage

**Storage Requirements for IGEL OS 11.04 or Higher**

IGEL OS 11.04.100 or higher requires at least 2.4 GB storage if the full feature set is applied. Thus, the feature set must be modified accordingly; for more information, see Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher(see page 231).

- No VIA graphic adapter; VIA graphics support is discontinued in IGEL OS.
- Legacy Bios and EFI/UEFI are supported.

### 4.3.2 Devices Officially Supported by OSC and UD Pocket with IGEL OS 11

The following list only includes those devices that are **tested by IGEL** (with each major release of IGEL OS). By no means it implies that the devices which are not included in this list but meet the [core requirements](#)(see page 1284) will not function with IGEL OS.

Further supported devices can be found on the [IGEL Ready](#)<sup>352</sup> Showcase at <https://www.igel.com/ready/showcase-categories/endpoints/>.

Integrated drivers and supported peripherals are listed in the [Third-Party Hardware Database](#)<sup>353</sup>. For more solutions compatible with IGEL OS, see [Partner Solutions](#)<sup>354</sup>.

For some of the devices listed here, Flash memory must be extended to ≥ 2 GB. For these devices, an appropriate note is added.

#### ADS-Tec

| Name    | Endpoint Type              | Memory (RAM) | Storage    | Processor            | Supported from IGEL OS Version |
|---------|----------------------------|--------------|------------|----------------------|--------------------------------|
| VMT9000 | Industrial PC/<br>Terminal | 4 GB<br>8 GB | 64 GB eMMC | Intel Atom® x7-E3950 | 11.02.100                      |

<sup>352</sup> <https://www.igel.com/technology-partners/>

<sup>353</sup> <https://www.igel.com/linux-3rd-party-hardware-database/>

<sup>354</sup> <https://kb.igel.com/display/igelos1105/Partner+Solutions>



## Advantech

| Name                      | Endpoint Type      | Memory (RAM) | Storage | Processor                     | Supported from IGEL OS Version |
|---------------------------|--------------------|--------------|---------|-------------------------------|--------------------------------|
| POC-W213L                 | Medical All in One | 4 GB         | 128 GB  | Intel Core i7-7300U           | 11.01.100                      |
| POC-W243L*(see page 1291) | Medical All in One | 4 GB         | 32 GB   | Intel Kaby Lake Core i5-7300U | 11.01.110                      |
| POC-W243L*(see page 1291) | Medical All in One | 4 GB         | 128 GB  | Intel Core i7-7300U           | 11.01.100                      |

## Advantech-DLoG

| Name        | Endpoint Type          | Memory (RAM) | Storage | Processor        | Supported from IGEL OS Version |
|-------------|------------------------|--------------|---------|------------------|--------------------------------|
| DLT-V6210   | Industrial PC/Terminal | 4 GB         | 32 GB   | Intel Atom       | 11.01.100                      |
| DLT-V7210 K | Industrial PC/Terminal | 4 GB         | 4 GB    | Intel Atom E3845 | 11.01.100                      |

## Dell / Wyse

| Name              | Endpoint Type   | Memory (RAM) | Storage | Processor            | Supported from IGEL OS Version |
|-------------------|-----------------|--------------|---------|----------------------|--------------------------------|
| (AiO) 5040 / 5212 | All in One      | 2 GB         | 2 GB    | AMD G-T48E           | 11.01.100                      |
| 3040              | Thin Client     | 2 GB         | 8 GB    | Intel Atom x5-Z8350  | 11.01.100                      |
| 5020              | Thin Client     | 2 GB         | 8 GB    | AMD G-Series SoC     | 11.02.140                      |
| 5060              | Thin Client     | 4 GB         | 8 GB    | AMD GX-424CC         | 11.01.100                      |
| 5070              | Thin Client     | 8 GB         | 32 GB   | Intel Celeron J4105  | 11.01.100                      |
| Latitude 5510     | Laptop/Notebook | 8 GB         | 256 GB  | Intel Core i5-10210U | 11.05.100                      |



## Elo

| Name                              | Endpoint Type | Memory (RAM) | Storage | Processor           | Supported from IGEL OS Version |
|-----------------------------------|---------------|--------------|---------|---------------------|--------------------------------|
| (AiO) i2 Touch (15 and 22 inches) | All in One    | 8 GB         | 128 GB  | Intel Core i3-8100T | 11.05.100                      |

## Fujitsu

| Name       | Endpoint Type | Memory (RAM) | Storage | Processor           | Supported from IGEL OS Version |
|------------|---------------|--------------|---------|---------------------|--------------------------------|
| Q957       | Desktop PC    | 8 GB         | 500 GB  | Intel Core i3-6100  | 11.02.100                      |
| FUTRO S740 | Thin Client   | 4 GB         | 8 GB    | Intel Celeron J4105 | 11.04.100                      |

## HP

| Name | Endpoint Type | Memory (RAM) | Storage | Processor                      | Supported from IGEL OS Version |
|------|---------------|--------------|---------|--------------------------------|--------------------------------|
| t420 | Thin Client   | 2 GB         | 8 GB    | AMD Embedded G-Series GX-209JA | 11.02.100                      |
| t430 | Thin Client   | 2 GB         | 16 GB   | Intel® Celeron® N4000          | 11.01.110                      |
| t530 | Thin Client   | 4 GB         | 8 GB    | AMD GX-215JJ Dual-Core         | 11.01.100                      |
| t630 | Thin Client   | 4 GB         | 8 GB    | AMD GX-420GI                   | 11.01.100                      |
| t730 | Thin Client   | 16 GB        | 8 GB    | AMD RX-427BB APU               | 11.01.100                      |
| t820 | Thin Client   | 16 GB        | 16 GB   | Intel Core i5-4570S            | 11.01.100                      |
| t640 | Thin Client   | 4 GB         | 16 GB   | AMD Ryzen R1505G               | 11.04.100                      |
| t540 | Thin Client   | 16 GB        | 16 GB   | AMD Ryzen Embedded R1305G      | 11.06.100                      |



## Intel

| Name        | Endpoint Type | Memory (RAM) | Storage | Processor           | Supported from IGEL OS Version |
|-------------|---------------|--------------|---------|---------------------|--------------------------------|
| NUC 5i5MYHE | Desktop PC    | 2 GB         | 32 GB   | Intel i5-5300U      | 11.01.100                      |
| NUC 5i3RYH  | Desktop PC    | 2 GB         | 2 GB    | Intel i3-5010U      | 11.01.100                      |
| NUC 7CJYH   | Desktop PC    | 2 GB         | 4 GB    | Intel Celeron J4005 | 11.01.100                      |

## Lenovo

| Name              | Endpoint Type   | Memory (RAM) | Storage | Processor                 | Supported from IGEL OS Version |
|-------------------|-----------------|--------------|---------|---------------------------|--------------------------------|
| ThinkCentre M625q | Desktop PC      | 4 GB         | 32 GB   | AMD E2-9000e              | 11.04.100                      |
| ThinkCentre M75n  | Desktop PC      | 8 GB         | 128 GB  | AMD Ryzen 3 Pro 3300U     | 11.05.100                      |
| ThinkCentre M70q  | Desktop PC      | 8 GB         | 500 GB  | Intel Pentium Gold G6400T | 11.05.100                      |
| L14               | Laptop/Notebook | 64 GB        | 1000 GB | AMD Ryzen 7 Pro 4750      | 11.05.100                      |
| 14w               | Laptop/Notebook | 8 GB         | 128 GB  | AMD A6                    | 11.05.100                      |

## LG

| Name                                | Endpoint Type | Memory (RAM) | Storage | Processor             | Supported from IGEL OS Version |
|-------------------------------------|---------------|--------------|---------|-----------------------|--------------------------------|
| (AiO) 24CK550N<br>**(see page 1291) | All in One    | 4 GB         | 32 GB   | AMD G-Series GX-212JJ | 11.01.100                      |
| (AiO) 24CK550W<br>**(see page 1291) | All in One    | 4 GB         | 32 GB   | AMD G-Series GX-212JJ | 11.01.100                      |
| (AiO) 24CK560N<br>**(see page 1291) | All in One    | 4 GB         | 32 GB   | AMD G-Series GX-212JJ | 11.01.100                      |
| CK500W                              | Thin Client   | 4 GB         | 32 GB   | AMD G-Series GX-212JJ | 11.01.100                      |



| Name           | Endpoint Type | Memory (RAM) | Storage | Processor            | Supported from IGEL OS Version |
|----------------|---------------|--------------|---------|----------------------|--------------------------------|
| (AiO) 38CK950N | All in One    | 8 GB         | 128 GB  | AMD Ryzen 3          | 11.02.100                      |
| (AiO) 38CK900N | All in One    | 8 GB         | 128 GB  | AMD Ryzen 3          | 11.02.100                      |
| CL600N         | Thin Client   | 4 GB         | 16 GB   | Intel® Celeron J4105 | 11.03.100                      |
| CL600W         | Thin Client   | 8 GB         | 128 GB  | Intel® Celeron J4105 | 11.03.100                      |
| (AiO) 34CN650N | All in One    | 4 GB         | 16 GB   | Intel® Celeron J4105 | 11.05.100                      |

### OnLogic

| Name       | Endpoint Type          | Memory (RAM) | Storage | Processor           | Supported from IGEL OS Version |
|------------|------------------------|--------------|---------|---------------------|--------------------------------|
| CL210G-10  | Industrial PC/Terminal | 4 GB         | 32 GB   | Intel Celeron N3350 | 11.04.100                      |
| KARBON 300 | Desktop PC             | 4 GB         | 32 GB   | Intel Atom x5-E3930 | 11.04.100                      |

### Onyx Healthcare

| Name      | Endpoint Type      | Memory (RAM) | Storage | Processor             | Supported from IGEL OS Version |
|-----------|--------------------|--------------|---------|-----------------------|--------------------------------|
| Venus 223 | Medical All in One | 4 GB         | 128 GB  | Intel Quad-Core J1900 | 11.01.100                      |

### Rein Medical

| Name            | Endpoint Type      | Memory (RAM) | Storage | Processor                        | Supported from IGEL OS Version |
|-----------------|--------------------|--------------|---------|----------------------------------|--------------------------------|
| Silenio C122    | All in One         | 8 GB         | 128 GB  | Intel® Core™ i5 – 6th Generation | 11.01.110                      |
| Silenio C124    | All in One         | 8 GB         | 128 GB  | Intel® Core™ i5 – 6th Generation | 11.01.110                      |
| Clinio S 522TCT | Medical All in One | 8 GB         | 16 GB   | Intel® Pentium® Silver J5005     | 11.04.100                      |



| Name            | Endpoint Type      | Memory (RAM) | Storage | Processor                    | Supported from IGEL OS Version |
|-----------------|--------------------|--------------|---------|------------------------------|--------------------------------|
| Clinio S 524TCT | Medical All in One | 8 GB         | 16 GB   | Intel® Pentium® Silver J5005 | 11.04.100                      |

## Secunet

| Name                                | Endpoint Type | Memory (RAM) | Storage | Processor          | Supported from IGEL OS Version |
|-------------------------------------|---------------|--------------|---------|--------------------|--------------------------------|
| SINA Workstation S EliteDesk 800 G2 | Workstation   | 16 GB        | 256 GB  | Intel Core i7-6700 | 11.01.100                      |

## Toshiba

| Name           | Endpoint Type   | Memory (RAM) | Storage | Processor           | Supported from IGEL OS Version |
|----------------|-----------------|--------------|---------|---------------------|--------------------------------|
| Portégé X20W-D | Laptop/Notebook | 8 GB         | 256 GB  | Intel Core i5-7200U | 11.01.100                      |
| Portégé X30-D  | Laptop/Notebook | 8 GB         | 256 GB  | Intel Core i5-7300U | 11.01.100                      |
| Tecra C50      | Laptop/Notebook | 4 GB         | 500 GB  | Intel i5-4210U      | 11.01.100                      |
| Tecra Z50-D    | Laptop/Notebook | 8 GB         | 256 GB  | Intel Core i5-7200U | 11.01.100                      |
| SATELLITE R50  | Laptop/Notebook | 4 GB         | 500 GB  | Intel i3-6006U      | 11.01.100                      |

## 4.3.3 USB Memory Sticks That Can Be Used as Alternative UD Pocket Hardware

## DIGITTRADE

| Name        | Storage | Supported from IGEL OS Version |
|-------------|---------|--------------------------------|
| Kobra Stick | ≥ 4GB   | 11.05.133                      |



#### 4.3.4 Officially Supported Virtual Environments

- Tested with Ubuntu (64-bit) and default settings

Note that the use of a UD Pocket within a virtual machine is **not** supported by IGEL.

| Name                 | Memory (RAM) | Storage | Type  | Supported from IGEL OS Version |
|----------------------|--------------|---------|-------|--------------------------------|
| Oracle VM VirtualBox | ≥ 2 GB       | ≥ 4 GB  | Linux | 11.04.100                      |
| VMware Workstation   | ≥ 2 GB       | ≥ 4 GB  | Linux | 11.04.100                      |

\* Delock Adapter DP 1.2 to DVI does not work.

\*\* When using an additional 4k screen with this device, please edit the BIOS settings as follows:

1. Go to the **Chipset** screen.
2. Set **Integrated Graphics** to “Force”.
3. Set **UMA Frame Buffer Size** to “256M” or higher.

### 4.4 Setup and Startup

- Requirements(see page 1291)
- Boot Settings(see page 1291)
- Starting Your UD Pocket(see page 1292)

#### 4.4.1 Requirements

In order to use UD Pocket, your computer must meet the following requirements:

- 64-bit-capable CPU
- At least 2 GB RAM
- Intel, ATI/AMD or Nvidia graphics chip
- USB 3.0 or 2.0 port from which the computer can boot
- Ethernet or wireless adapter

You will find a detailed list of supported graphics and network chips in the [IGEL Linux 3rd Party Hardware Database](#)<sup>355</sup>

#### 4.4.2 Boot Settings

UD Pocket works on systems with BIOS and UEFI.

---

<sup>355</sup> <https://www.igel.com/linux-3rd-party-hardware-database/>



It is essential that your system supports booting from USB storage media. This may already be enabled, or you may have to enable it yourself. The required key presses for this may vary from vendor to vendor. However, here are some hints:

- ▶ While the device is booting, try pressing [F12] (in general), [F10] (Intel devices) or [F9] (Hewlett-Packard devices) in order to access a list of boot devices and select UD Pocket.
- ▶ If the above does not work, access the BIOS settings via pressing [Del], [F1] or [F2] during boot and activate booting from USB storage media and/or change the boot order.
- ▶ See the BIOS/UEFI documentation for your system for details of how to boot from USB storage media.

IGEL OS supports UEFI Secure Boot. Refer to the manual of your device's manufacturer to learn whether your device supports Secure Boot and how to enable it. Enabling Secure Boot often consists of two steps. First, the boot mode has to be changed to UEFI Boot in the BIOS; after that, Secure Boot can be activated, also in the BIOS. How to check whether Secure Boot has been properly enabled you can learn [here](#).

If UD Pocket fails to boot in UEFI mode, try it in legacy/BIOS mode.

Do not remove UD Pocket from the computer until you have shut down the IGEL OS contained on it. Otherwise, you can damage the operating system on UD Pocket and lose your settings as well as data on other removable media.

#### 4.4.3 Starting Your UD Pocket

##### The First Boot Procedure

1. Plug the UD Pocket into a free USB slot of your device.
2. Turn on your device; if the device is already switched on, restart it.

##### Should the UD Pocket Boot-Up Fail

- ▶ If the device does not boot into UD Pocket, but into its pre-installed operating system instead, change the boot settings appropriately. For further information, see [Boot Settings](#)(see page 1291).

##### After the First Boot-Up

The Setup Assistant guides you through the basic configuration. For a detailed description of each step, see the [Setup Assistant](#)(see page 757) chapter in the IGEL OS manual.



## 5 IGEL OS Creator

- [IGEL OS Creator Manual](#)(see page 1293)
- [IGEL OS Creator Articles](#)(see page 1328)

### 5.1 IGEL OS Creator Manual

With the IGEL OS Creator, you can install IGEL OS 11 on any device that supports it. Moreover, you can use the IGEL OS Creator for recovering a broken installation of IGEL OS which is not able to boot anymore.

For rolling out IGEL OS via the IGEL OS Deployment Appliance, you need to have installed IGEL OS Deployment Appliance 11.0.

- [General Information](#)(see page 1293)
- [Devices Supported by IGEL OS 11](#)(see page 1293)
- [Licensing](#)(see page 1295)
- [Installation](#)(see page 1295)

#### 5.1.1 General Information

The IGEL OS Creator (OSC) software allows the migration of existing hardware to create a functionally standardized IGEL Workspace infrastructure. In the process, the existing operating system is replaced by IGEL OS. The devices can then be administered via the IGEL Universal Management Suite (UMS).

Installing the IGEL OS operating system via OSC destroys all data on the target device's mass storage device (hard disk, flash memory, SSD).

This manual describes the installation of IGEL OS 11 using OSC.

#### 5.1.2 Devices Supported by IGEL OS 11

##### IGEL Devices

##### IGEL UD (Universal Desktop)

| Product Line | Device Type | Hardware ID | 64 Bit | Memory | Storage | HW Video Acceleration |
|--------------|-------------|-------------|--------|--------|---------|-----------------------|
| UD2          | D220        | 40          | Yes    | 2 GB   | 4 GB    | Yes                   |
| UD2          | M250C       | 50          | Yes    | 2 GB   | 4 GB    | Yes                   |
| UD2          | M250C       | 51/52       | Yes    | 2 GB   | 8 GB    | Yes                   |



| Product Line          | Device Type | Hardware ID     | 64 Bit | Memory | Storage | HW Video Acceleration |
|-----------------------|-------------|-----------------|--------|--------|---------|-----------------------|
| UD3*(see page 1294)   | M340C       | 50              | Yes    | 2 GB   | 4 GB    | Yes                   |
| UD3                   | M340C       | 51              | Yes    | 2 GB   | 4 GB    | Yes                   |
| UD3                   | M350C       | 60              | Yes    | 4 GB   | 8 GB    | Yes                   |
| UD5                   | H830C       | 50              | Yes    | 2 GB   | 4 GB    | Yes                   |
| UD6                   | H830C       | 51              | Yes    | 2 GB   | 4 GB    | Yes                   |
| UD7                   | H850C       | 10              | Yes    | 4 GB   | 4 GB    | Yes                   |
| UD7***(see page 1294) | H850C       | 11              | Yes    | 4 GB   | 4 GB    | Yes                   |
| UD7                   | H860C       | 20              | Yes    | 8 GB   | 8 GB    | Yes                   |
| UD9                   | TC215B      | 40 / 41 (Touch) | Yes    | 2 GB   | 4 GB    | Yes                   |

\* IGEL UD3-LX 50 is officially supported up to IGEL OS 11.05, incl. private builds.

\*\*As of December 2019, IGEL UD7 model H850C is equipped with the AMD Secure Processor<sup>356</sup>; for further information, see [UD7 Model H850C](#)<sup>357</sup>.

## IGEL Zero

### Note on IZ Devices

The IZ devices listed below can be upgraded to IGEL OS 11. To upgrade your IZ devices to IGEL OS 11, please contact your IGEL sales representative. See also <https://www.igel.com/tradeup/> and [The IGEL OS 11 Trade-Up](#)<sup>358</sup>.

| Product Line | Device Type | Hardware ID | 64 Bit | Memory | Storage | UEFI Secure Boot Support | HW Video Acceleration |
|--------------|-------------|-------------|--------|--------|---------|--------------------------|-----------------------|
| IZ2          | D220        | 40          | Yes    | 2 GB   | 4 GB    | Yes                      | Yes                   |
| IZ3          | M340C       | 50          | Yes    | 2 GB   | 4 GB    | Yes                      | Yes                   |
| IZ3          | M340C       | 51          | Yes    | 2 GB   | 4 GB    | Yes                      | Yes                   |

<sup>356</sup> <https://kb.igel.com/display/securitysafety/AMD+Secure+Processor>

<sup>357</sup> <https://kb.igel.com/display/securitysafety/UD7+Model+H850C>

<sup>358</sup> <https://kb.igel.com/display/licensesmoreigelos11/The+IGEL+OS+11+Trade+up>



## Third-Party Devices

For an up-to-date list, see <https://kb.igel.com/os11-supported-hardware>.

### 5.1.3 Licensing

For information on licensing, see [IGEL Software License Overview<sup>359</sup>](#) and [Deploying Licenses<sup>360</sup>](#).

### 5.1.4 Installation

- [Create USB installation medium \(Windows\)](#)(see page 1295)
- [Create USB installation medium \(Linux\)](#)(see page 1298)
- [Create DVD installation medium](#)(see page 1299)
- [Boot Settings](#)(see page 1299)
- [Installation Procedure](#)(see page 1302)
- [Installation Procedure for Factory Images](#)(see page 1314)

#### Create USB installation medium (Windows)

1. Download the ZIP archive for OSC from our [download server<sup>361</sup>](#).
  - For new devices, use the standard installer (e. g. OSC\_11.01.100.zip).
  - For older devices or if you haven't been able to boot the installer at all, use the legacy installer (e. g. OSC\_11.01.100\_legacy.zip).
2. Unzip the contents into a local directory.
3. Connect a USB memory stick with at least 4 GB capacity to the computer.

All existing data on the USB memory stick will be destroyed.

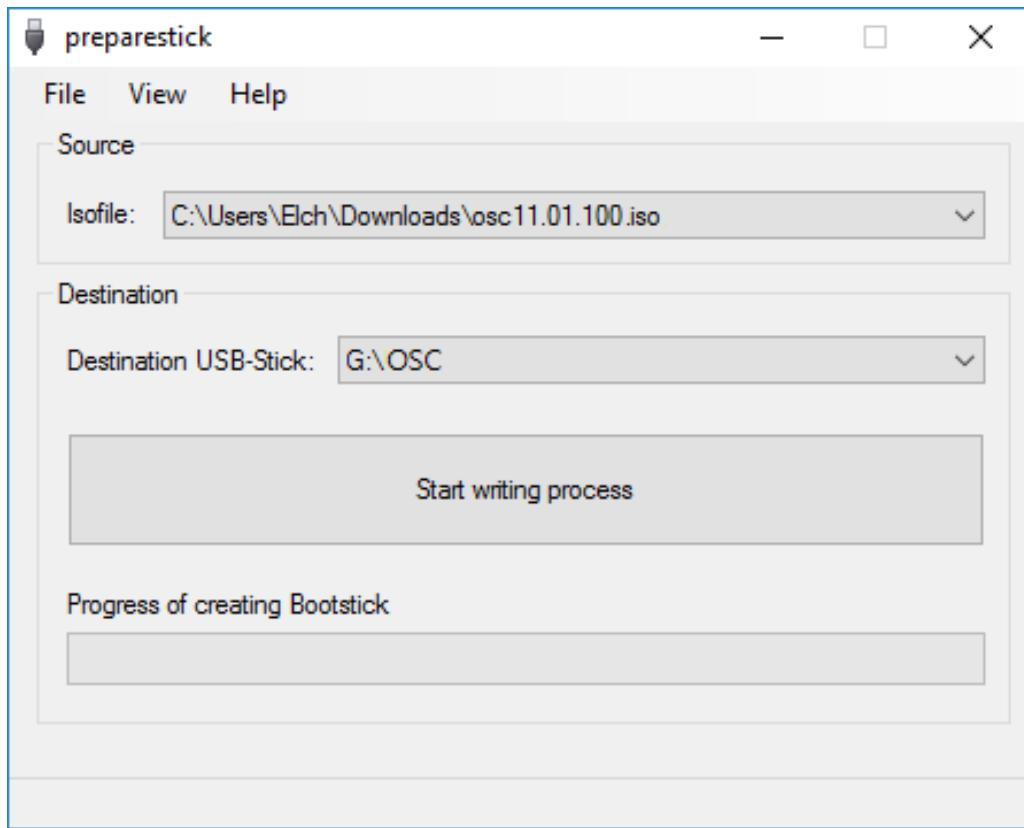
4. Double-click the preparestick.exe file from the unzipped directory.

If you are in the "administrators" group, the program will start after you have confirmed a dialog. If you are not in the "administrators" group, you must enter the administrator password to start the program.

<sup>359</sup> <https://kb.igel.com/display/licensesmoreigelos11/IGEL+Software+License+Overview>

<sup>360</sup> <https://kb.igel.com/display/licensesmoreigelos11/Deploying+Licenses>

<sup>361</sup> <https://www.igel.com/software-downloads/>



The dropdown menu **Isofile** shows the ISO files contained in the unzipped directory.

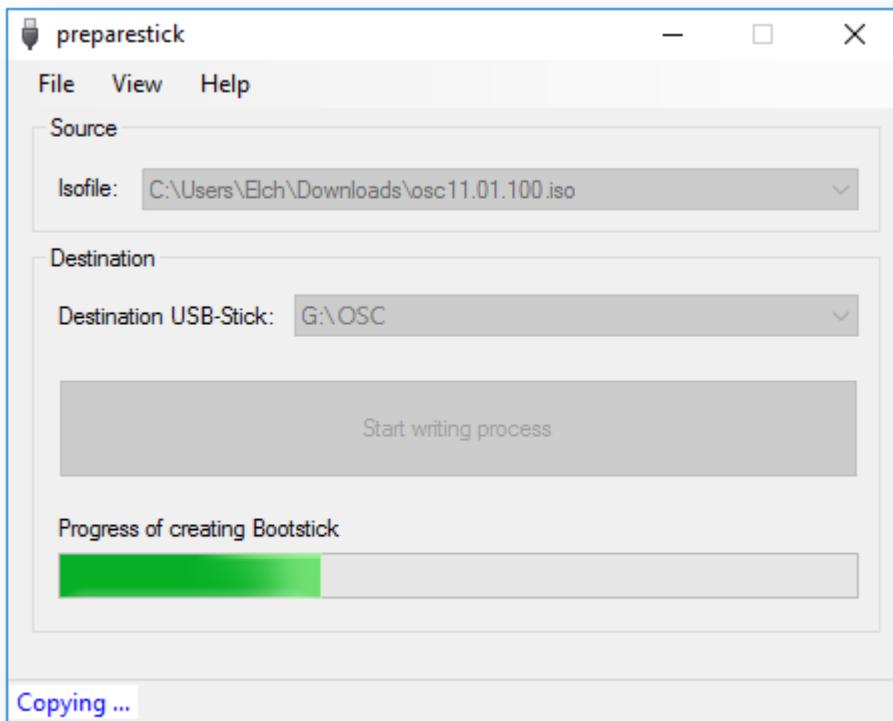
5. Under **Isofile**, select the appropriate ISO file, e. g. osc11.01.100.iso
6. Under **Destination USB stick**, select the USB storage medium on which you would like to save the installation data.

It is recommended that you only have one USB storage medium connected during this procedure. If you accidentally select the wrong medium, all data on it will be lost.

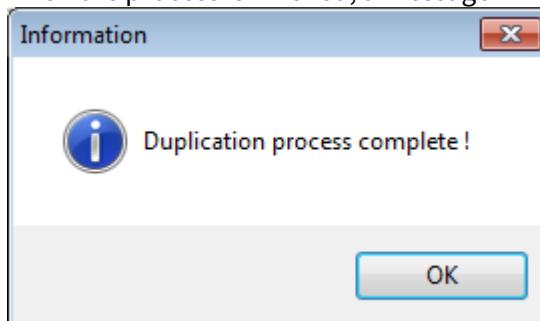
Generally speaking, the list of available USB storage media is refreshed automatically. If, however, you would like to refresh it manually, click on **View > Refresh USB Device List**.

7. Click on **Start writing process**.

In the program window, the progress of the process is shown.



When the process is finished, a message window is displayed.



8. Close the message window and the program.
9. After about 3 seconds, remove the USB memory stick.

If you remove the USB memory stick immediately, there is a possibility that the writing process has not been completed. In this case, the data on the memory stick gets corrupted.



## Create USB installation medium (Linux)

1. Download the ZIP archive for OSC from our [download server](#)<sup>362</sup>:
  - For new devices, use the standard installer (e. g. OSC\_11.01.100.zip).
  - For older devices or if you haven't been able to boot the installer at all, use the legacy installer (e. g. OSC\_11.01.100\_legacy.zip).
2. Unzip the contents into a local directory.
3. From this directory, you will need the ISO file (e. g. osc11.01.100.iso or osc11.01.100\_legacy.iso) to create a bootable medium.
4. Connect a USB memory stick with at least 4 GB capacity to the computer.

All existing data on the USB memory stick will be destroyed.

5. Open a terminal emulator and enter the command dmesg to determine the device name of the USB memory stick.

Example output:

```
[...]
[19514.742229] scsi 3:0:0:0: Direct-Access JetFlash Transcend 8GB 1100 PQ: 0
ANSI: 6
[19514.742805] sd 3:0:0:0: Attached scsi generic sg1 type 0
[19514.744688] sd 3:0:0:0: [sdb] 15425536 512-byte logical blocks: (7.89 GB/
7.35 GiB)
[19514.745370] sd 3:0:0:0: [sdb] Write Protect is off
[19514.745376] sd 3:0:0:0: [sdb] Mode Sense: 43 (0) 00 00 00
[19514.746040] sd 3:0:0:0: [sdb] Write cache: enabled, read cache: enabled,
doesn't support DPO or FUA
[19514.752438] sdb: sdb1
```

In this example, the device name searched for is /dev/sdb.

Ensure that you have determined the correct device name. Use of the dd command in the next step can destroy your operating system if you use the wrong device name.

6. The following command writes the installation data to the USB memory stick:  
`dd if=osc11.01.100.iso of=/dev/sdX bs=1M oflag=direct`  
 Replace sdX with the device name of the USB memory stick that you have determined.  
 When the dd command has terminated, you can see the terminal emulator input prompt again.
7. Wait for about 3 seconds after the dd command has terminated, and remove the USB memory stick.

If you remove the USB memory stick immediately, there is a possibility that the writing process has not been completed. In this case, the data on the memory stick gets corrupted.

<sup>362</sup> <https://www.igel.com/software-downloads/>



The USB memory stick for OSC installation is ready for use.

## Create DVD installation medium

The ISO file in the installation directory for OSC is a so-called hybrid image. It can not only be copied onto USB storage devices but can also be used to create a bootable DVD.

### Burn ISO Image (Windows)

1. In Explorer, open the directory that contains the ISO file.
2. Right-click on the ISO file.
3. Select **Burn disc image**.

### Burn ISO Image (Linux)

Under Linux, various burning programs with a graphical user interface or for the command line are available.

The [Ubuntu Wiki<sup>363</sup>](#) explains how to burn an ISO image onto a DVD using a number of programs.

## Boot Settings

OSC works on systems with BIOS and UEFI.

It is essential that your system supports booting from USB storage media or from DVD. This may already be enabled, or you may have to enable it yourself.

IGEL OS 11 supports UEFI Secure Boot. Refer to the manual of your device's manufacturer to learn whether your device supports Secure Boot and how to enable it. Enabling Secure Boot often consists of two steps. First, the boot mode has to be changed to UEFI Boot in the BIOS; after that, Secure Boot can be activated, also in the BIOS.

If IGEL OS fails to boot in UEFI mode, try it in legacy/BIOS mode. IGEL OS will then be installed in legacy/BIOS mode.

For older devices or if you haven't been able to boot the installer at all, use the legacy installer under <https://www.igel.com/software-downloads/workspace-edition/> > **OS 11 > OS CREATOR > LEGACY**.

## Third-Party Devices

The required key presses for this may vary from vendor to vendor. However, here are some hints:

- While the device is booting, try pressing [F12] (in general), [F10] (Intel devices) or [F9] (Hewlett-Packard devices) in order to access a list of boot devices and select UD Pocket.

<sup>363</sup> [https://help.ubuntu.com/community/BurningIsoHowto#Burning\\_from\\_Ubuntu](https://help.ubuntu.com/community/BurningIsoHowto#Burning_from_Ubuntu)



- ▶ If the above does not work, access the BIOS settings via pressing [Del], [F1] or [F2] during boot and activate booting from USB storage media and/or change the boot order.
- ▶ See the BIOS/UEFI documentation for your system for details of how to boot from USB storage media.

## IGEL Devices

### UD7 (H850C and H860C)

1. Power up the device while pressing the [Del] button repeatedly in rapid succession.
2. If a password prompt is shown, enter the BIOS password.
3. Select **Setup Utility**.
4. Select the **Boot** tab.
5. Set **USB Boot** to <ENABLED>.
6. Save the settings and exit.
7. Connect the USB stick to the device.
8. Reboot the device while pressing the [Del] button repeatedly in rapid succession.
9. Select **Boot Manager**.
10. Select the USB stick as the boot medium and press **Enter**.
11. You can continue with the [installation procedure](#)(see page 1302).

### UD6 (H830C)

1. Power up the device while pressing the [Del] button repeatedly in rapid succession.
2. Select **SCU**.
3. If a password prompt is shown, enter the BIOS password.
4. Select the **Boot** tab.
5. Set **USB Boot** to <ENABLED>.
6. Save the settings and exit.
7. Connect the USB stick to the device.
8. Reboot the device while pressing the [Del] button repeatedly in rapid succession.
9. Select **Boot Manager**.
10. Select the USB stick as the boot medium and press **Enter**.
11. You can continue with the [installation procedure](#)(see page 1302).

### UD5 (H830C)

1. Power up the device while pressing the [Del] button repeatedly in rapid succession.
2. If a password prompt is shown, enter the BIOS password.
3. Select the **Boot** tab.
4. Select **Boot Options Priorities**.
5. Select the entry for the USB stick and move it to the first position using the [+] key.
6. Save the settings and exit.
7. You can continue with the [installation procedure](#)(see page 1302).



## UD3 (M350C)

1. Power up the device while pressing the [Del] button repeatedly in rapid succession.
2. If a password prompt is shown, enter the BIOS password.
3. Select **Setup Utility**.
4. Select the **Boot** tab.
5. Set **USB Boot** to <ENABLED>.
6. Save the settings and exit.
7. Connect the USB stick to the device.
8. Reboot the device while pressing the [Del] button repeatedly in rapid succession.
9. Select **Boot Manager**.
10. Select the USB stick as the boot medium and press **Enter**.
11. You can continue with the [installation procedure](#)(see page 1302).

## UD3 (M340C)

1. Power up the device while pressing the [Del] button repeatedly in rapid succession.
2. If a password prompt is shown, enter the BIOS password.
3. Select the **Boot** tab.
4. Set **USB Boot** to <ENABLED>.
5. Select **Legacy > Boot Type Order**.
6. Select **USB** and move it to the first position using the [+] key.
7. Save the settings and exit.
8. You can continue with the [installation procedure](#)(see page 1302).

## UD2 (M250C)

1. Power up the device while pressing [Del] button repeatedly in rapid succession.
2. Select **SCU**.
3. If a password prompt is shown, enter the BIOS password.
4. Select the **Boot** tab.
5. Set **USB Boot** to <ENABLED>.
6. Save the settings and exit.
7. Connect the USB stick to the device.
8. Reboot the device while pressing the [Del] button repeatedly in rapid succession.
9. Select **Boot Manager**.
10. Select the USB stick as the boot medium and press **Enter**.
11. You can continue with the [installation procedure](#)(see page 1302).

## UD2 (D220)

1. Power up the device while pressing the [F2] (older devices) or [Del] (newer devices) button repeatedly in rapid succession.
2. Select **SCU**.
3. If a password prompt is shown, enter the BIOS password.
4. Select the **Boot** tab.
5. Set **USB Boot** to <ENABLED>.



6. Save the settings and exit.
7. Connect the USB stick to the device.
8. Reboot the device while pressing the [F2] or [Del] (newer devices) button repeatedly in rapid succession.
9. Select **Boot Manager**.
10. Select the USB stick as the boot medium and press **Enter**.
11. You can continue with the [installation procedure](#)(see page 1302).

#### UD9 (TC215B)

1. Power up the device while pressing the [F2] button repeatedly in rapid succession.
2. If a password prompt is shown, enter the BIOS password.
3. Select the **Boot** tab.
4. Select **Boot Option Priorities**.
5. Select the entry for the USB stick and move it to the first position using the [+] key.
6. Save the settings and exit.
7. You can continue with the [installation procedure](#)(see page 1302).

### Installation Procedure

This article describes the regular installation procedure for single devices with the IGEL OS Creator (OSC). If you are an IGEL third-party endpoint partner (i.e. hardware manufacturer, independent hardware vendor, reseller) that has a factory ID from IGEL, please refer to [Installation Procedure for Factory Images](#)(see page 1314).

The installation will overwrite all existing data on the target drive.

1. Connect the prepared USB memory stick to the target device and switch the target device on.



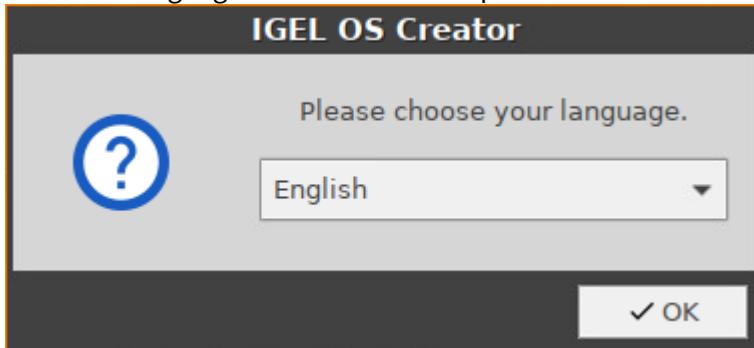
2. Select one of the following options from the boot menu:



- **Standard Installation + Recovery:** Boots the system with just a few messages from the USB memory stick and launches the installation program. (Default)
- **Verbose Installation + Recovery:** Boots the system from the USB memory stick and shows the Linux boot messages in the process.
- **Failsafe Installation + Recovery:** Fallback mode to be used if the graphical boot screen cannot be displayed.
- **Memory Test:** Memory test, only available in legacy/BIOS mode. This option does not carry out an installation.
- **EFI Debug Shell:** Available only in UEFI boot mode. If the hardware in use is EFI-capable, boot problems can be analyzed with that.

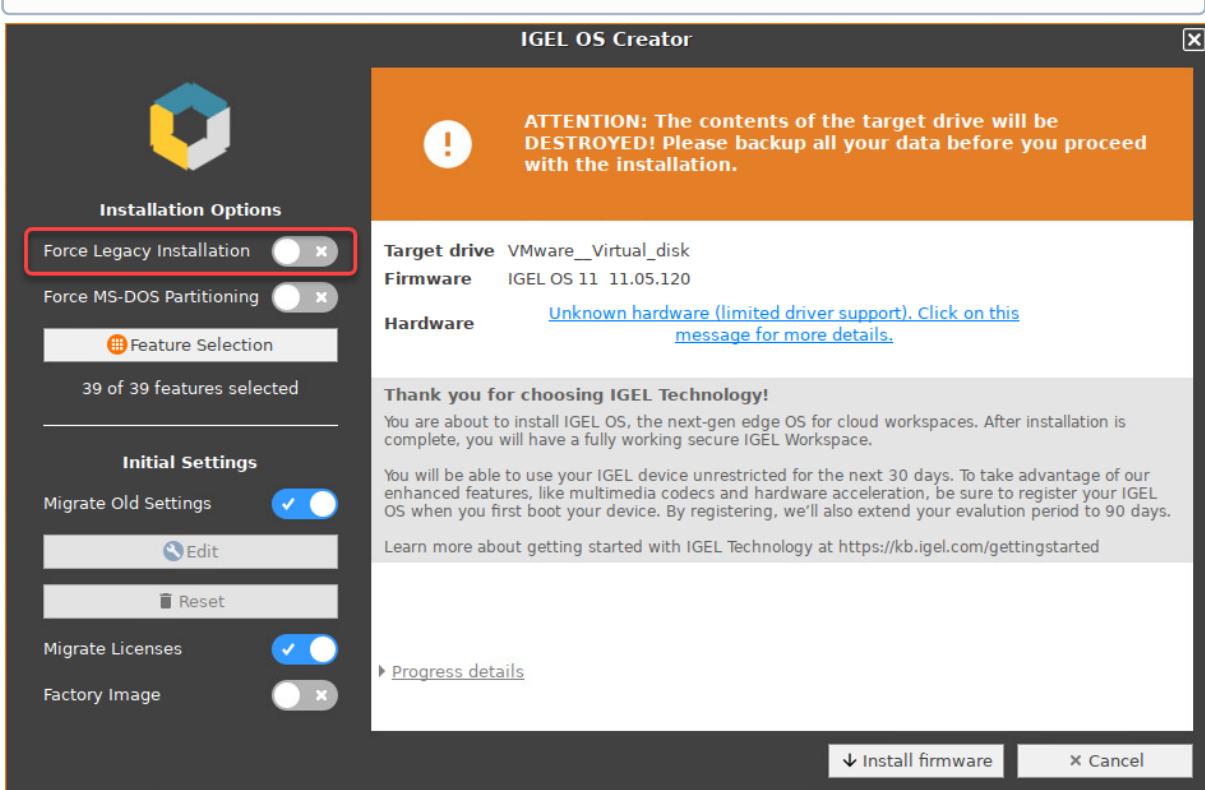


3. Select the language for the installation process.



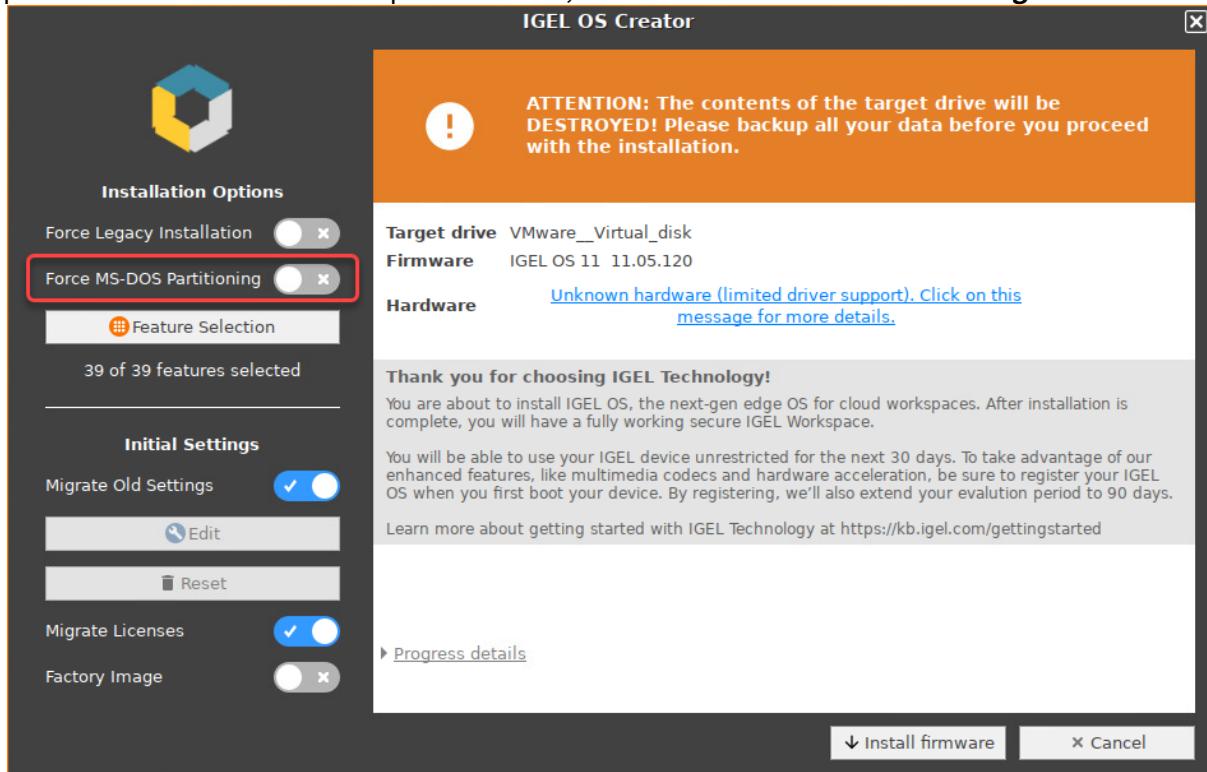
4. Optional, only available if your device has booted in UEFI mode: If you want to install the legacy/BIOS version of IGEL OS 11, activate **Force Legacy Installation**.

If you have activated **Force Legacy Installation**, remember to set the system to legacy/BIOS mode after installation.



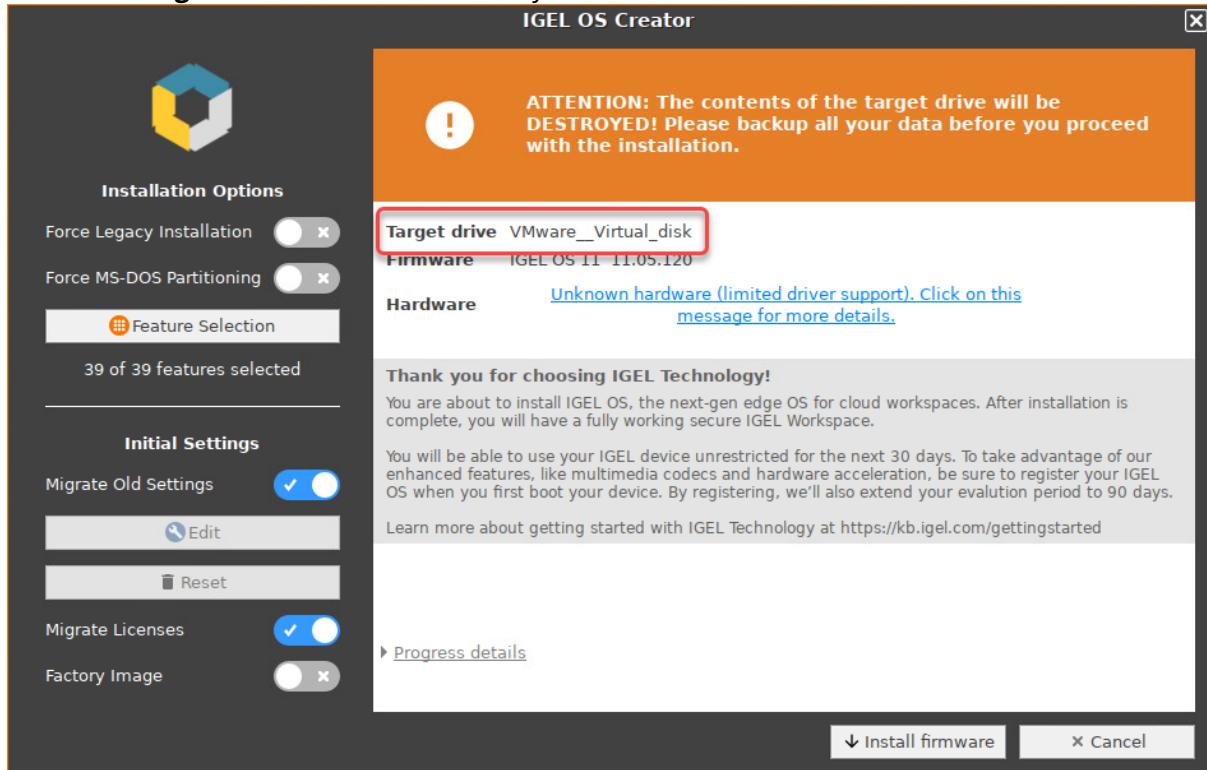


5. Optional, only available if your device has booted in UEFI mode: If you want to use an MS-DOS partition table instead of a GPT partition table, activate **Force MS-DOS Partitioning**.

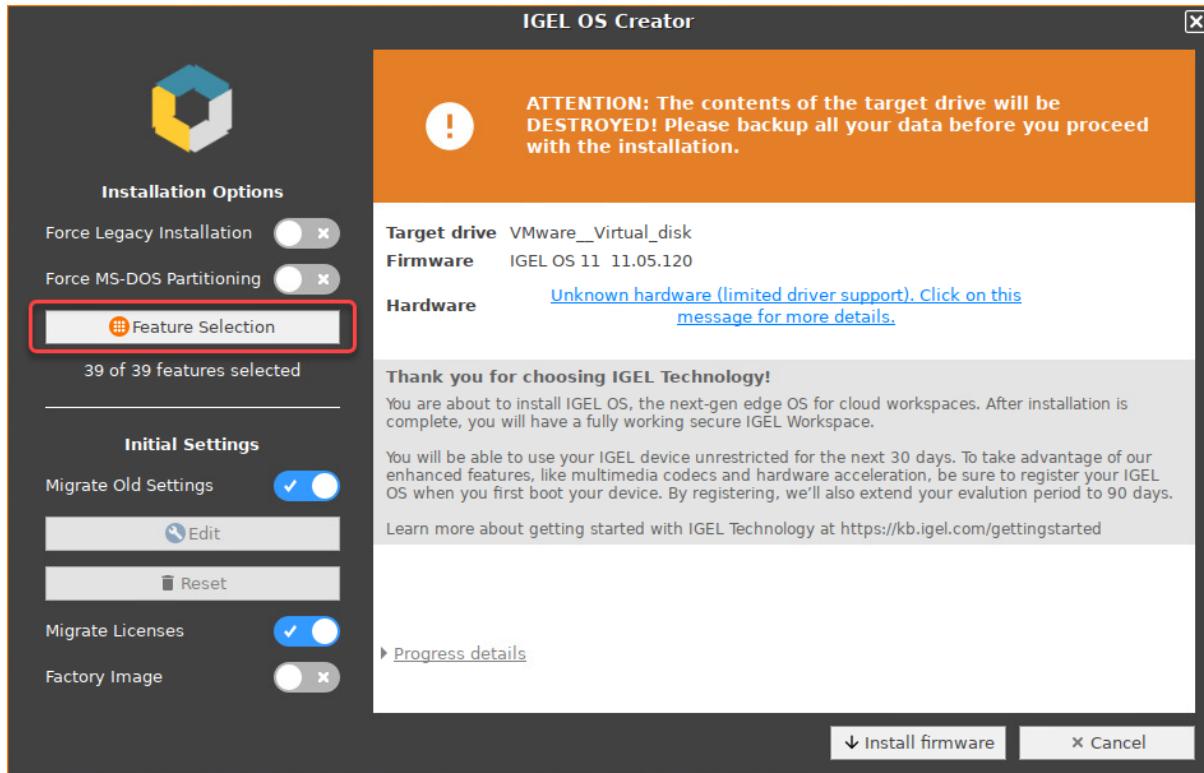




6. Check the **Target drive** to ensure that the system is installed on the desired drive.



7. If you want to exclude features of IGEL OS, e.g. to save storage space, click **Feature Selection** and edit the settings as required.





**Feature Selection**

Disk size 17.2 GB, firmware size 2.7 GB

Select the set of features to be installed on the target device.

All      None      Total size of all features: 1.9 GB

| Install                             | Feature                              | Size     |
|-------------------------------------|--------------------------------------|----------|
| <input checked="" type="checkbox"/> | Citrix ICA                           | 301.7 MB |
| <input checked="" type="checkbox"/> | Imprivata                            | 273.4 MB |
| <input checked="" type="checkbox"/> | Local browser (Chromium)             | 198.7 MB |
| <input checked="" type="checkbox"/> | VMware Horizon                       | 137.6 MB |
| <input checked="" type="checkbox"/> | Local Browser (Firefox)              | 133.7 MB |
| <input checked="" type="checkbox"/> | NVIDIA graphics driver               | 132.9 MB |
| <input checked="" type="checkbox"/> | Windows Virtual Desktop Client (WVD) | 93.6 MB  |
| <input checked="" type="checkbox"/> | IBM i Access Client Solutions        | 76.0 MB  |
| <input checked="" type="checkbox"/> | VirtualBox                           | 66.8 MB  |
| <input checked="" type="checkbox"/> | Cisco JVDI client                    | 64.7 MB  |
| <input checked="" type="checkbox"/> | Zoom VDI                             | 49.5 MB  |
| <input checked="" type="checkbox"/> | Cisco Webex Teams VDI                | 45.9 MB  |

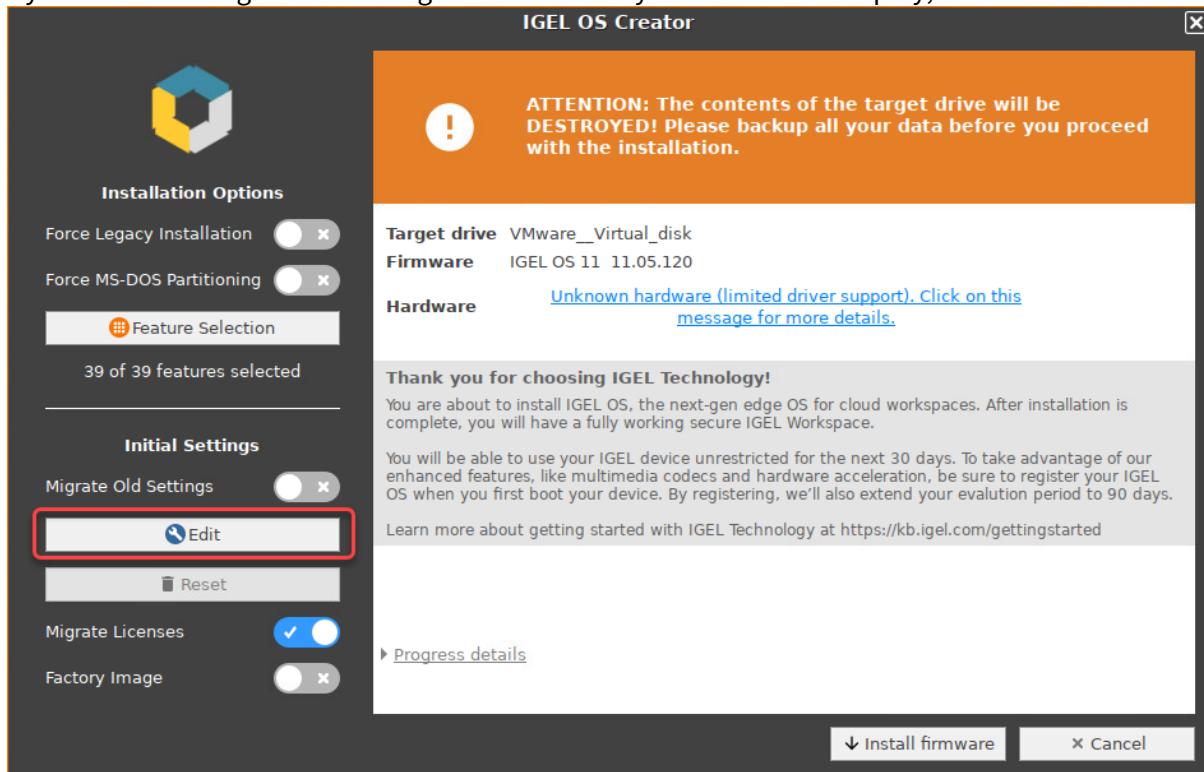
✓ OK

A screenshot of a software window titled "Feature Selection". It displays a message about disk and firmware sizes, a note to select features for installation, and two buttons ("All" and "None"). Below is a table listing installed features with their sizes. The table has columns for "Install" (checkboxes), "Feature" (list items), and "Size" (MB values). A "Total size of all features: 1.9 GB" summary is shown at the top right. An "OK" button is at the bottom right.

- **All:** Select all features
- **None:** Select no feature
- **Feature:** Sort the list alphabetically
- **Size:** Sort the list by the memory requirements of the features



8. If you want to change initial settings for the devices you are about to deploy, click **Edit**.

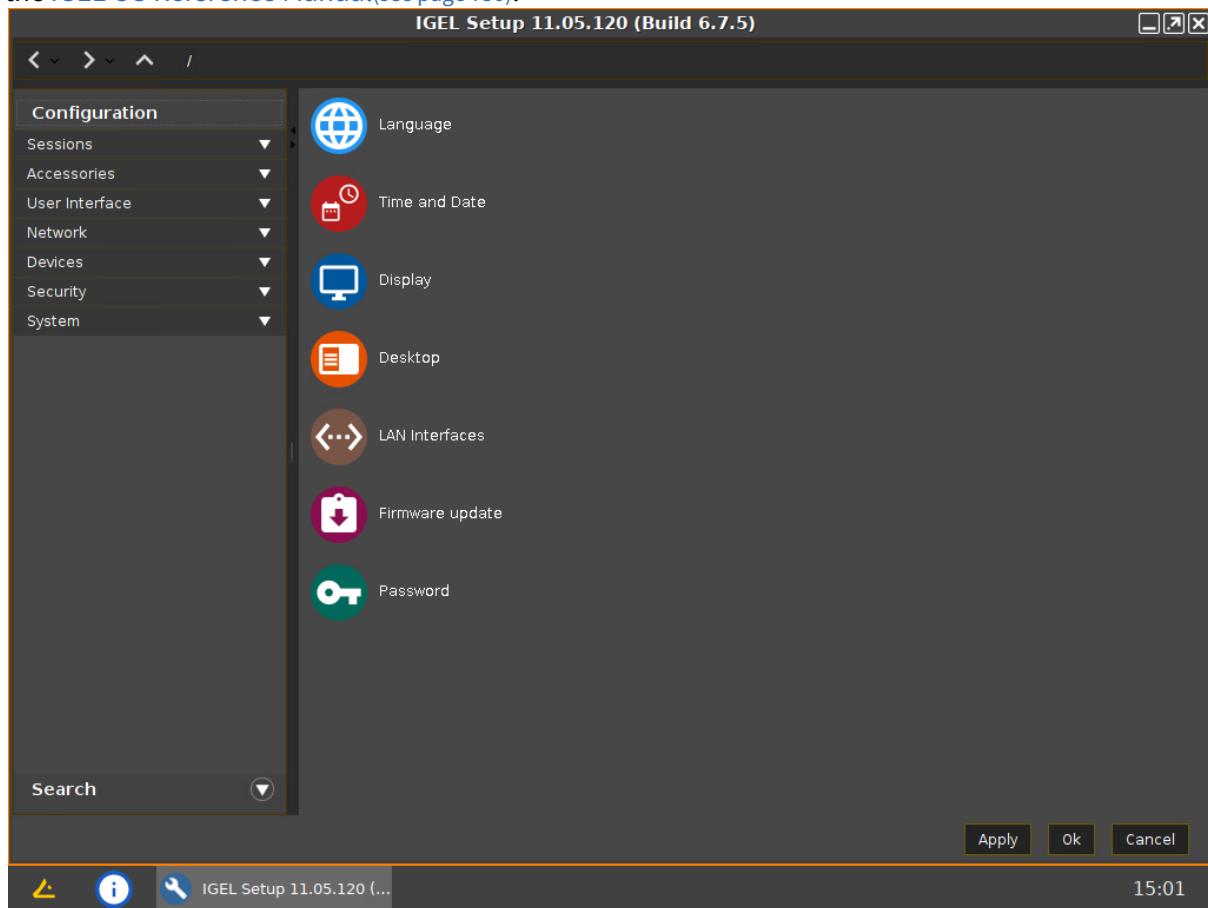


The IGEL Setup opens, enabling you to change the settings in the same way as with a regular IGEL OS installation.

The changes are stored on the USB memory stick from which the IGEL OS Creator (OSC) is executed. When you use this USB memory stick for subsequent OSC installations, your custom settings will be re-used. This allows you to easily create a number of IGEL OS installations with custom settings.

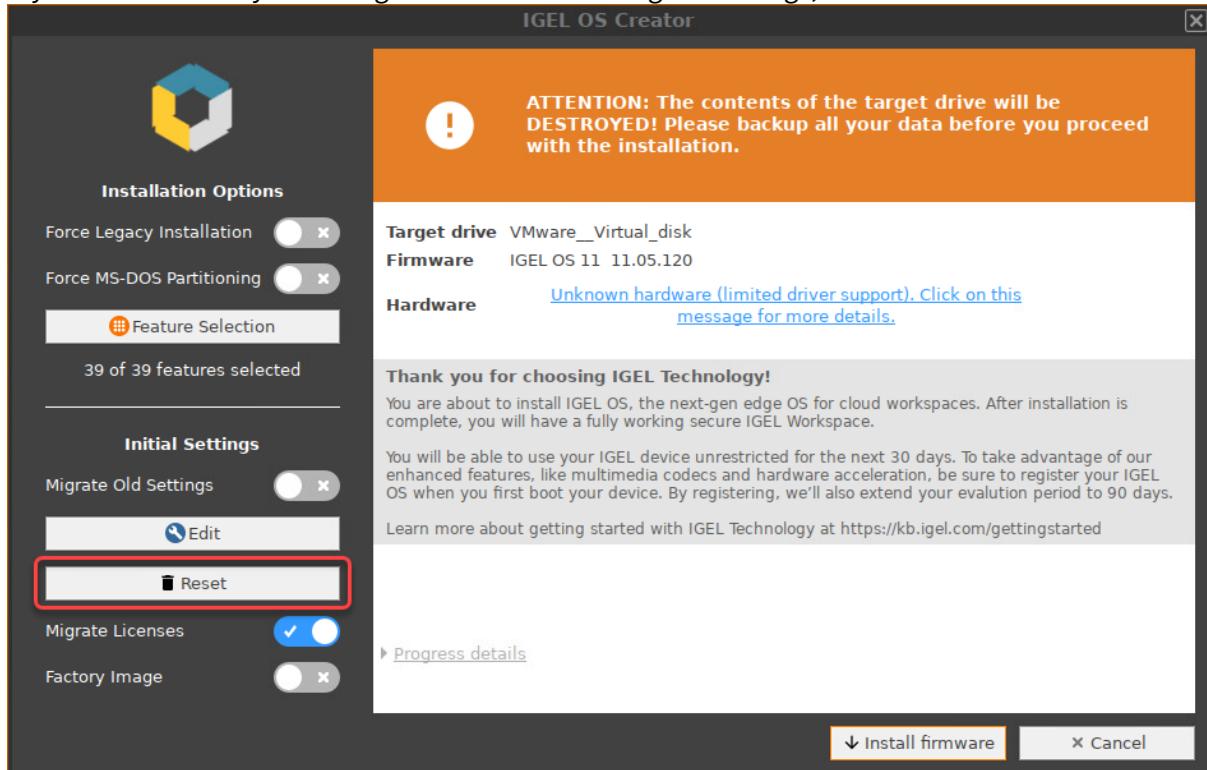


For details about the settings, see the chapters [Setup](#)(see page 772) and the subsequent chapters in the [IGEL OS Reference Manual](#)(see page 750).

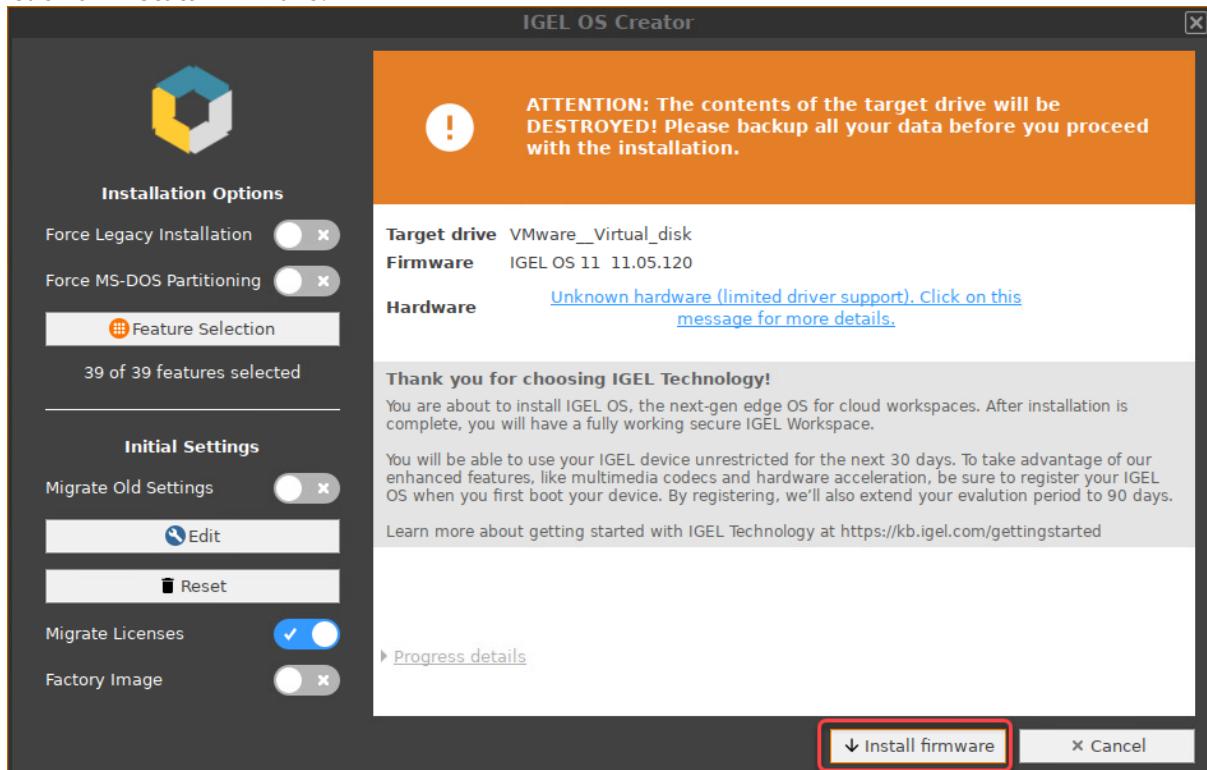




9. If you want to undo your changes and restore the original settings, click **Reset**.

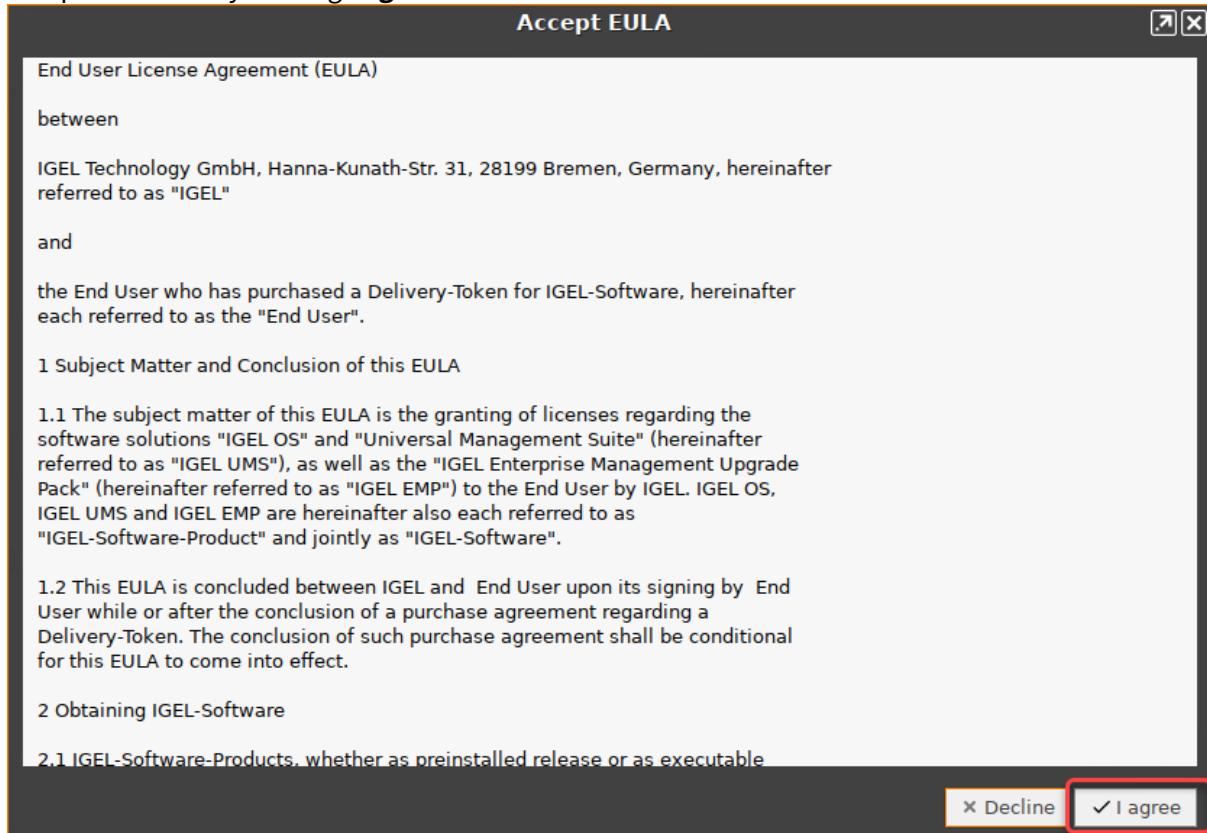


10. Click on **Install firmware**.

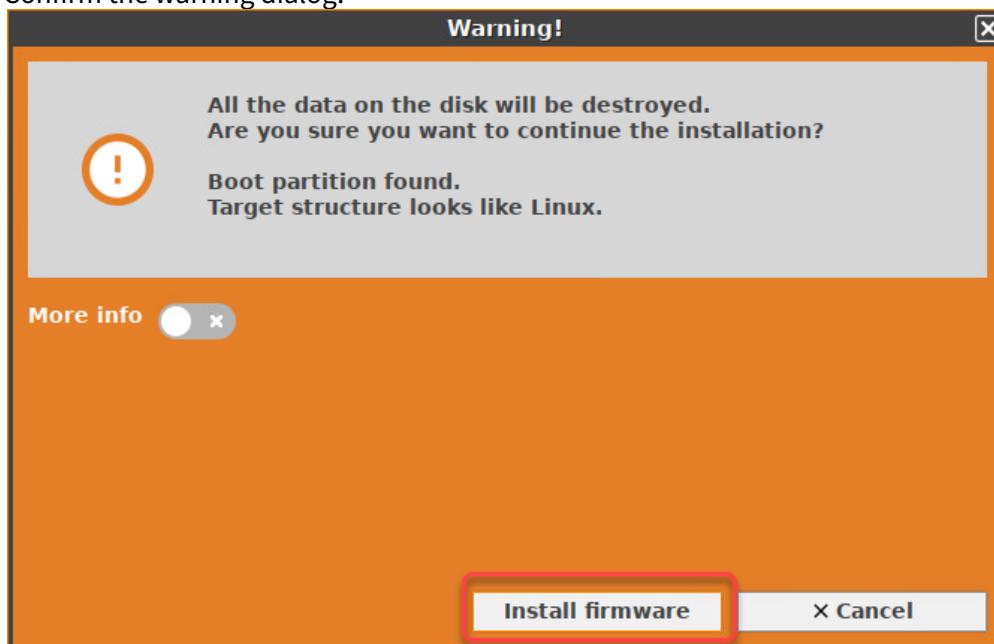




11. Accept the **EULA** by clicking **I agree**.



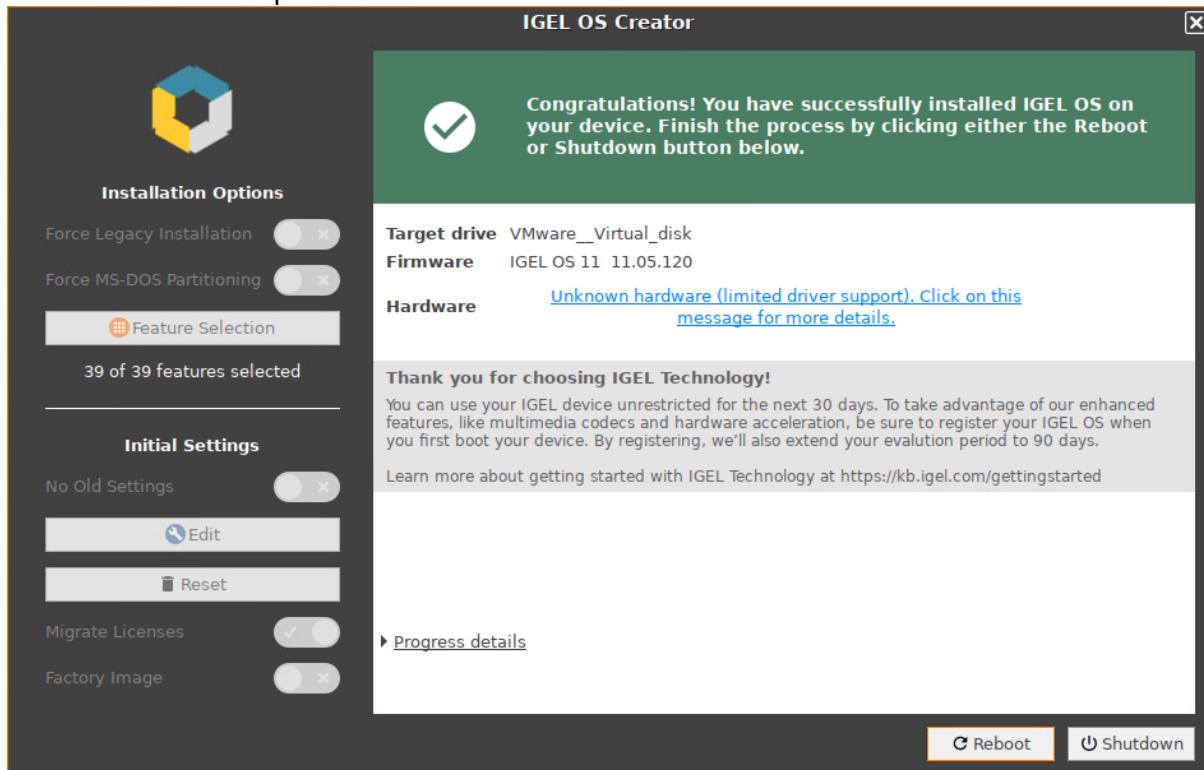
12. Confirm the warning dialog.



The installation program will install IGEL OS 11 on the target drive. If you see the success message,



the installation is complete.

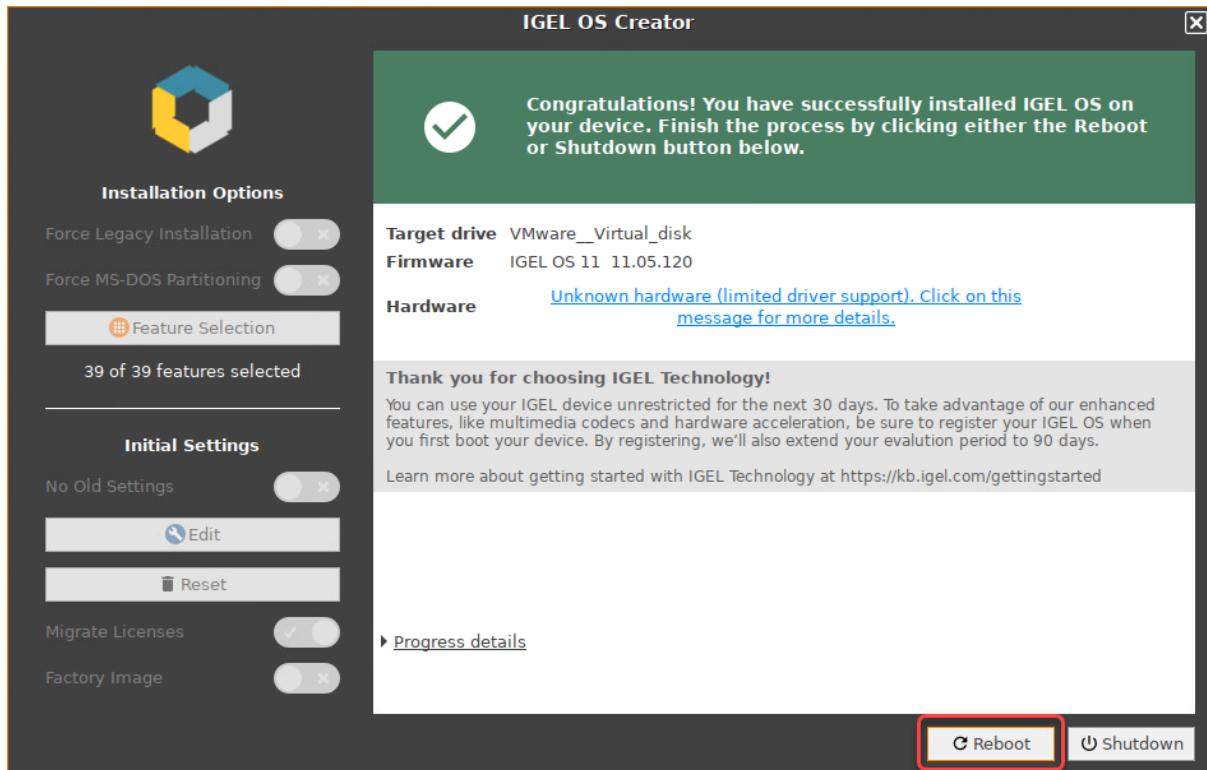


13. Detach any external network adapters from the device.

In this way, you ensure that the unit ID for the device is derived from the built-in network adapter. The unit ID will be saved on the device persistently, regardless of any external network adapter that may be used in the future. This is important for licensing.

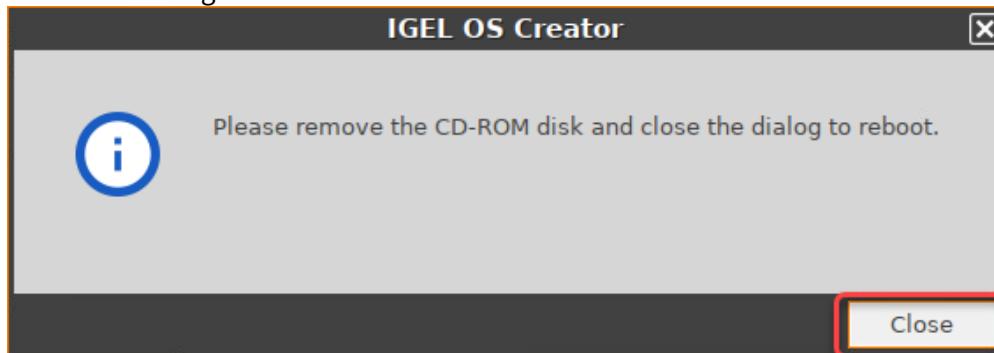


**14. Click on Reboot.**



15. Remove the USB memory stick.

16. Close the message window.



The system will shut down and then boot IGEL OS 11.

### Installation Procedure for Factory Images

The installation will overwrite all existing data on the target drive.

#### Preparing the Image

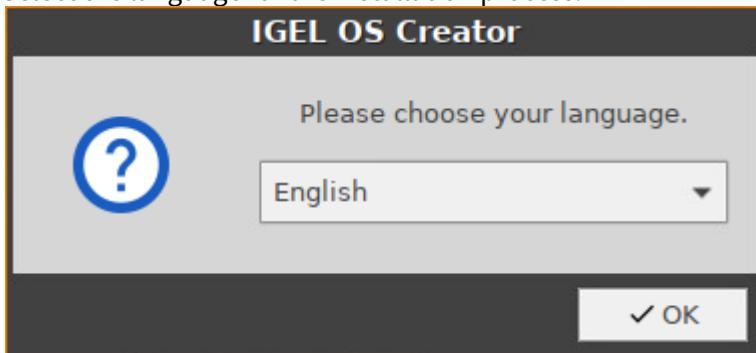
1. Connect the prepared USB memory stick to the target device and switch on the target device.



2. Select **Standard Installation + Recovery** or **Verbose Installation + Recovery**.



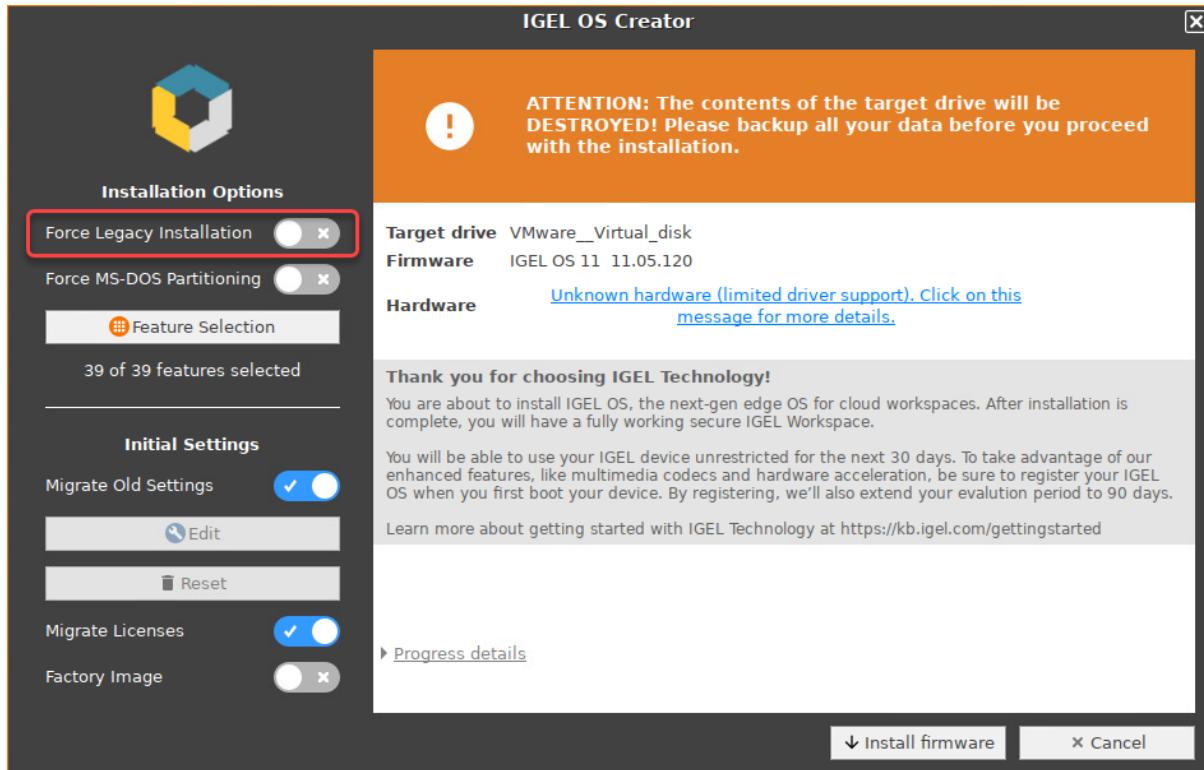
3. Select the language for the installation process.



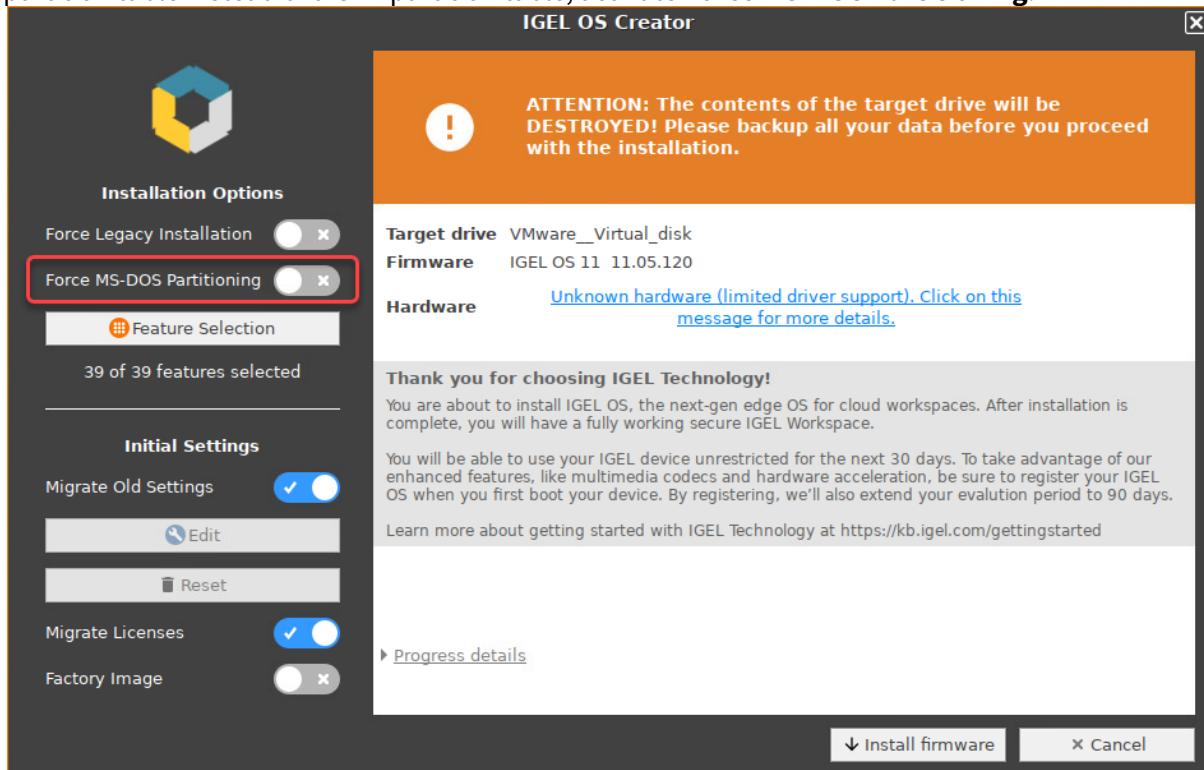
The installation program **IGEL OS Creator** opens. Here, you can configure settings for the installation process and start it.

4. Optional; only available if your device has booted in UEFI mode: If you want to install the legacy/BIOS version of IGEL OS 11, activate **Force Legacy Installation**.

If you have activated **Force Legacy Installation**, remember to set the system to legacy/BIOS mode after installation.

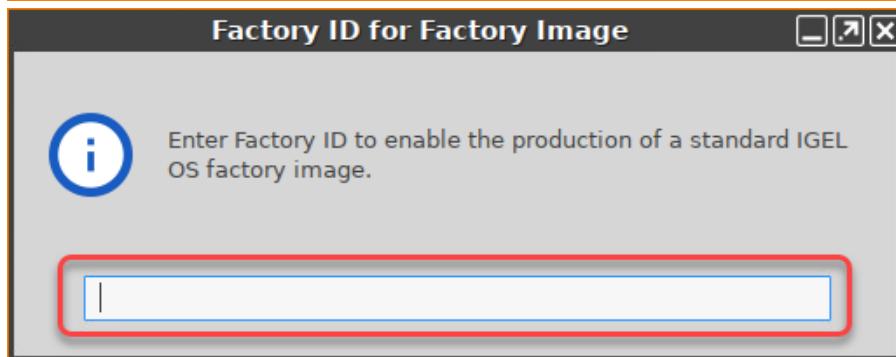
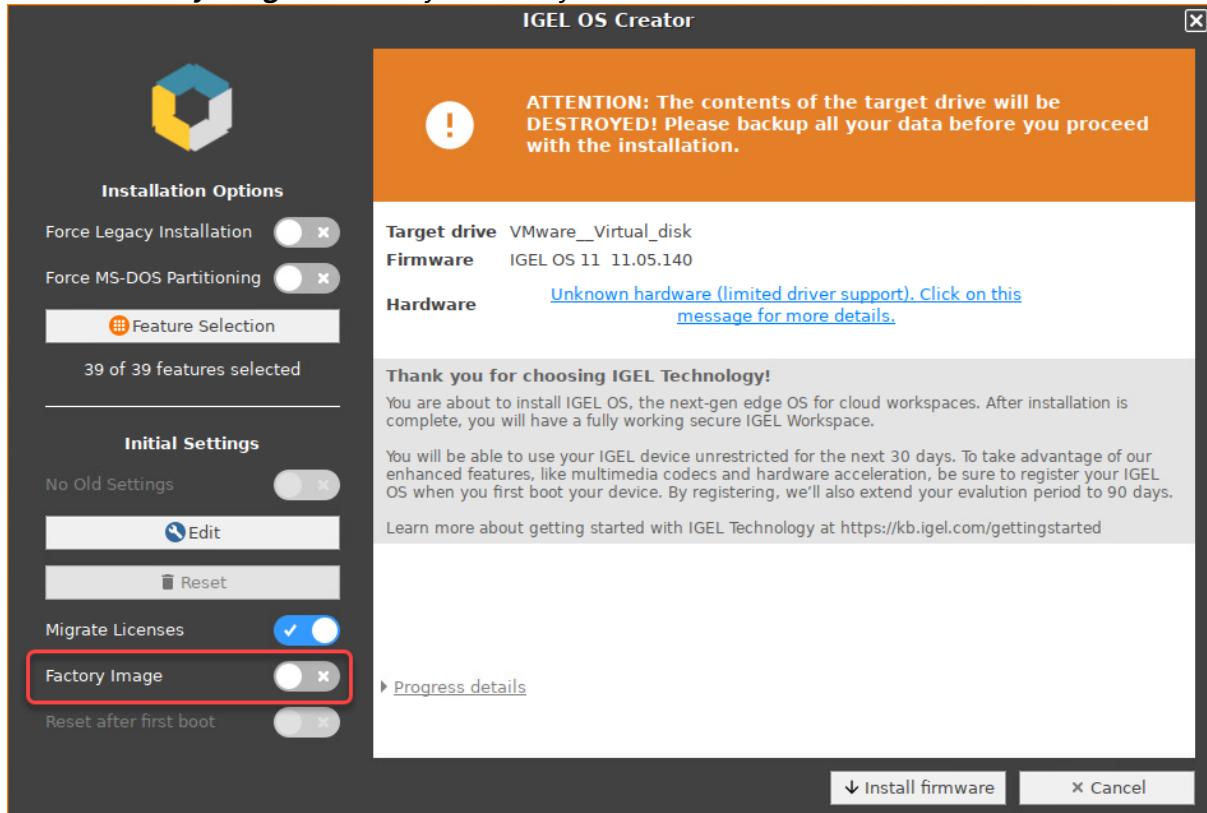


5. Optional; only available if your device has booted in UEFI mode: If you want to use an MS-DOS partition table instead of a GPT partition table, activate **Force MS-DOS Partitioning**.



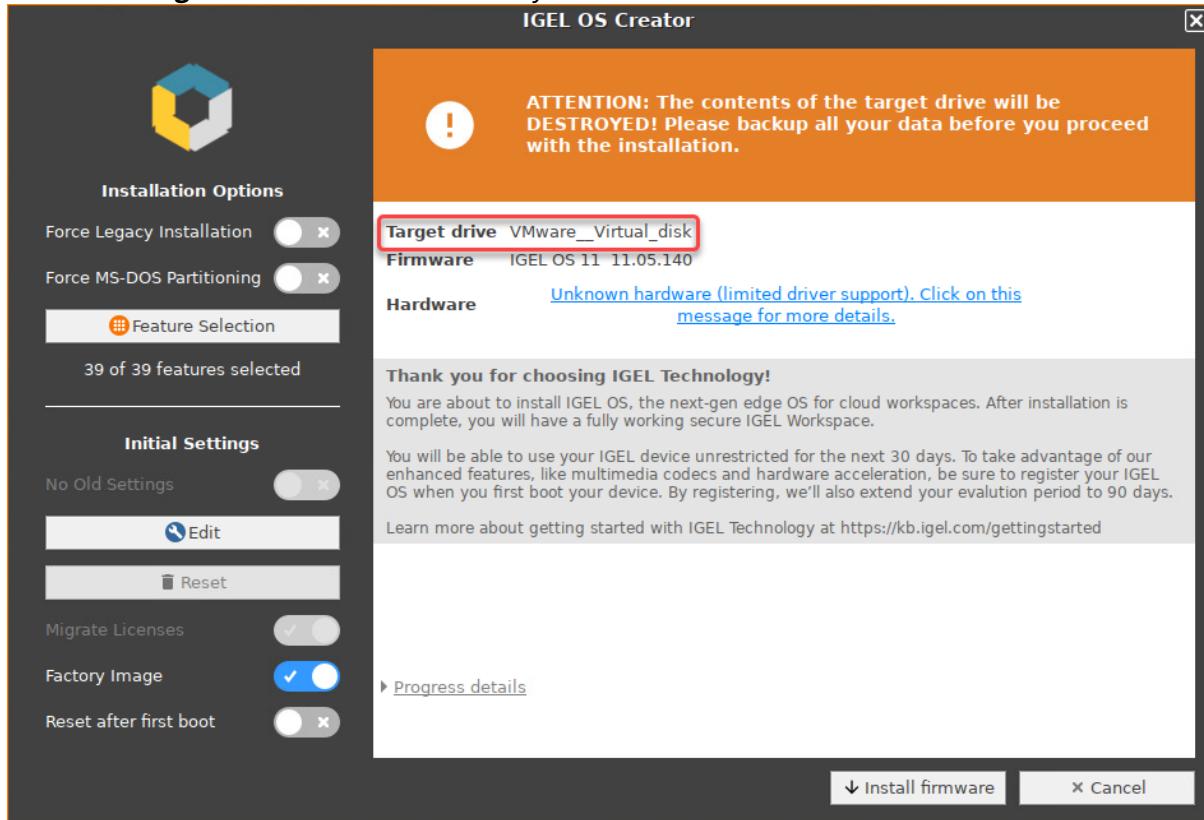


6. Activate **Factory Image** and enter your factory ID.

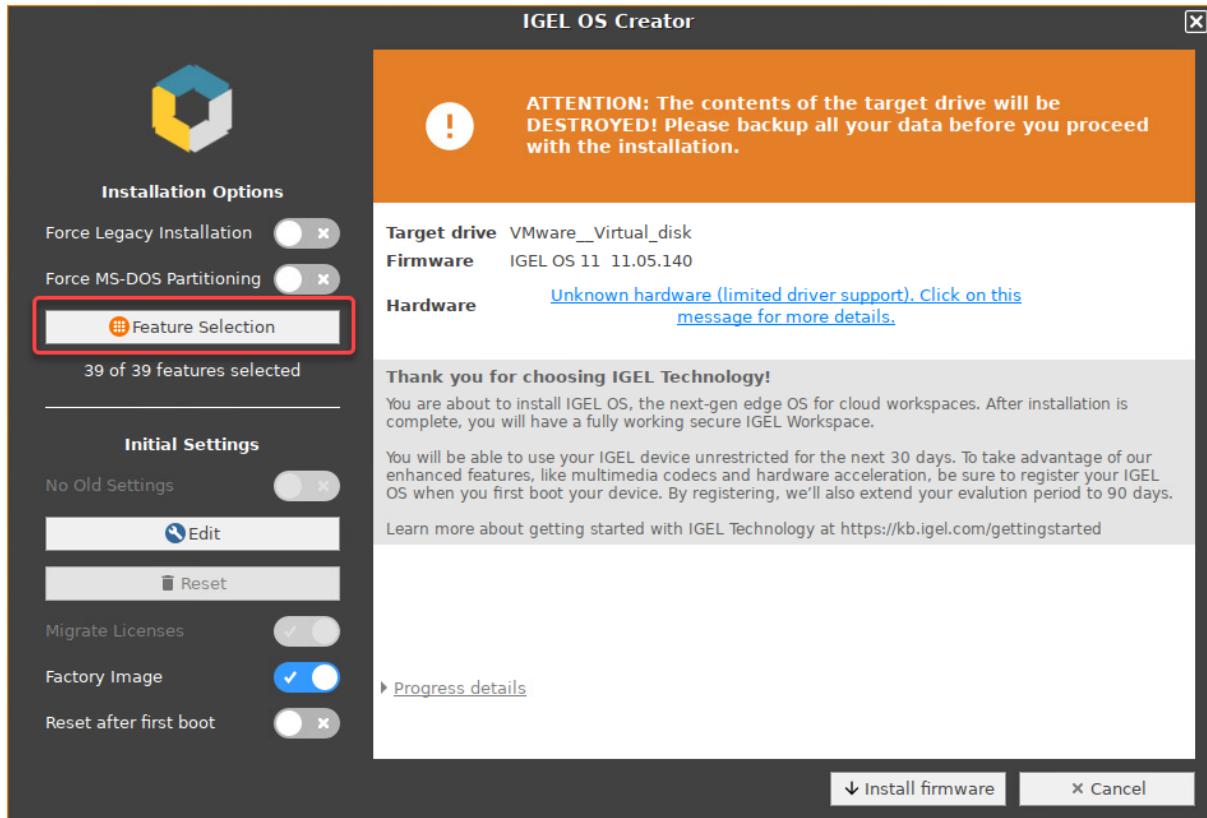




7. Check the **Target drive** to ensure that the system is installed on the desired drive.



8. If you want to exclude features of IGEL OS, e.g. to save storage space, click **Feature Selection** and edit the settings as required.





**Feature Selection**

Disk size 17.2 GB, firmware size 2.7 GB

Select the set of features to be installed on the target device.

All      None      Total size of all features: 1.9 GB

| Install                             | Feature                              | Size     |
|-------------------------------------|--------------------------------------|----------|
| <input checked="" type="checkbox"/> | Citrix ICA                           | 301.7 MB |
| <input checked="" type="checkbox"/> | Imprivata                            | 273.4 MB |
| <input checked="" type="checkbox"/> | Local browser (Chromium)             | 198.7 MB |
| <input checked="" type="checkbox"/> | VMware Horizon                       | 137.6 MB |
| <input checked="" type="checkbox"/> | Local Browser (Firefox)              | 133.7 MB |
| <input checked="" type="checkbox"/> | NVIDIA graphics driver               | 132.9 MB |
| <input checked="" type="checkbox"/> | Windows Virtual Desktop Client (WVD) | 93.6 MB  |
| <input checked="" type="checkbox"/> | IBM i Access Client Solutions        | 76.0 MB  |
| <input checked="" type="checkbox"/> | VirtualBox                           | 66.8 MB  |
| <input checked="" type="checkbox"/> | Cisco JVDI client                    | 64.7 MB  |
| <input checked="" type="checkbox"/> | Zoom VDI                             | 49.5 MB  |
| <input checked="" type="checkbox"/> | Cisco Webex Teams VDI                | 45.9 MB  |

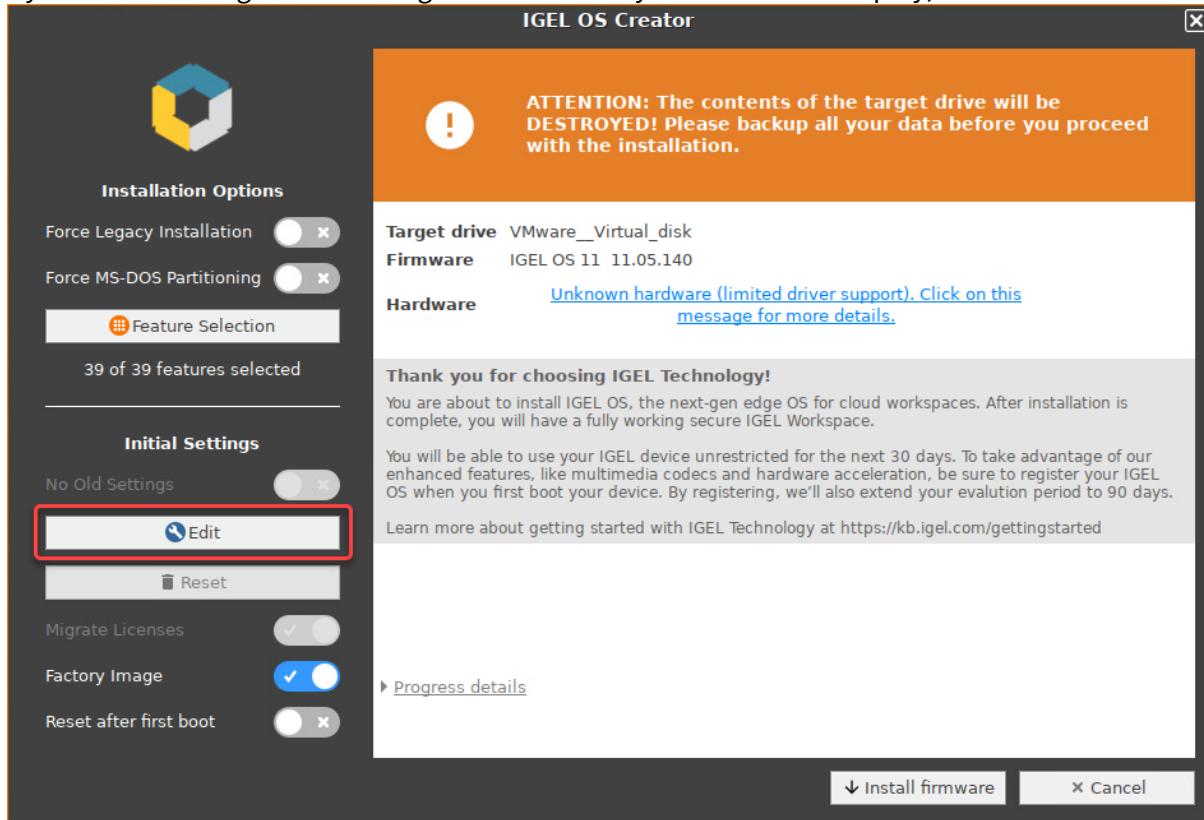
✓ OK

A screenshot of a software window titled "Feature Selection". It displays a message about disk and firmware sizes, a note to select features for installation, and two buttons ("All" and "None"). Below is a table listing installed features with their sizes. The table has columns for "Install" (checkboxes), "Feature" (list items), and "Size" (MB). A "Total size of all features: 1.9 GB" summary is shown at the top right of the table area. At the bottom right is an "OK" button with a checkmark.

- **All:** Select all features
- **None:** Select no feature
- **Feature:** Sort the list alphabetically
- **Size:** Sort the list by the memory requirements of the features



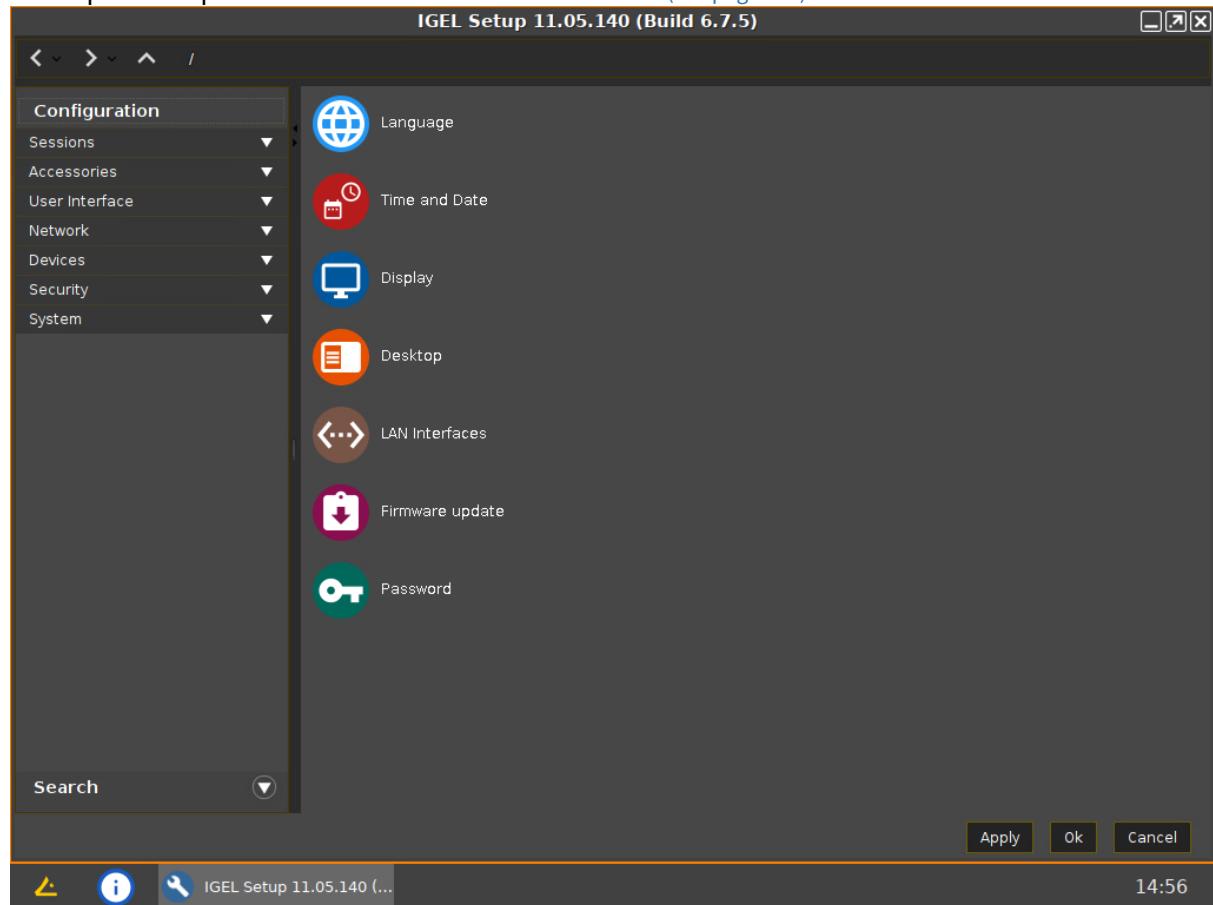
9. If you want to change initial settings for the devices you are about to deploy, click **Edit**.



The IGEL Setup opens, enabling you to change the settings in the same way as with a regular IGEL OS installation. The changes are stored on the USB memory stick from which the IGEL OS Creator (OSC) is executed. For details about the settings, see the chapters [Setup](#)(see page 772) and the

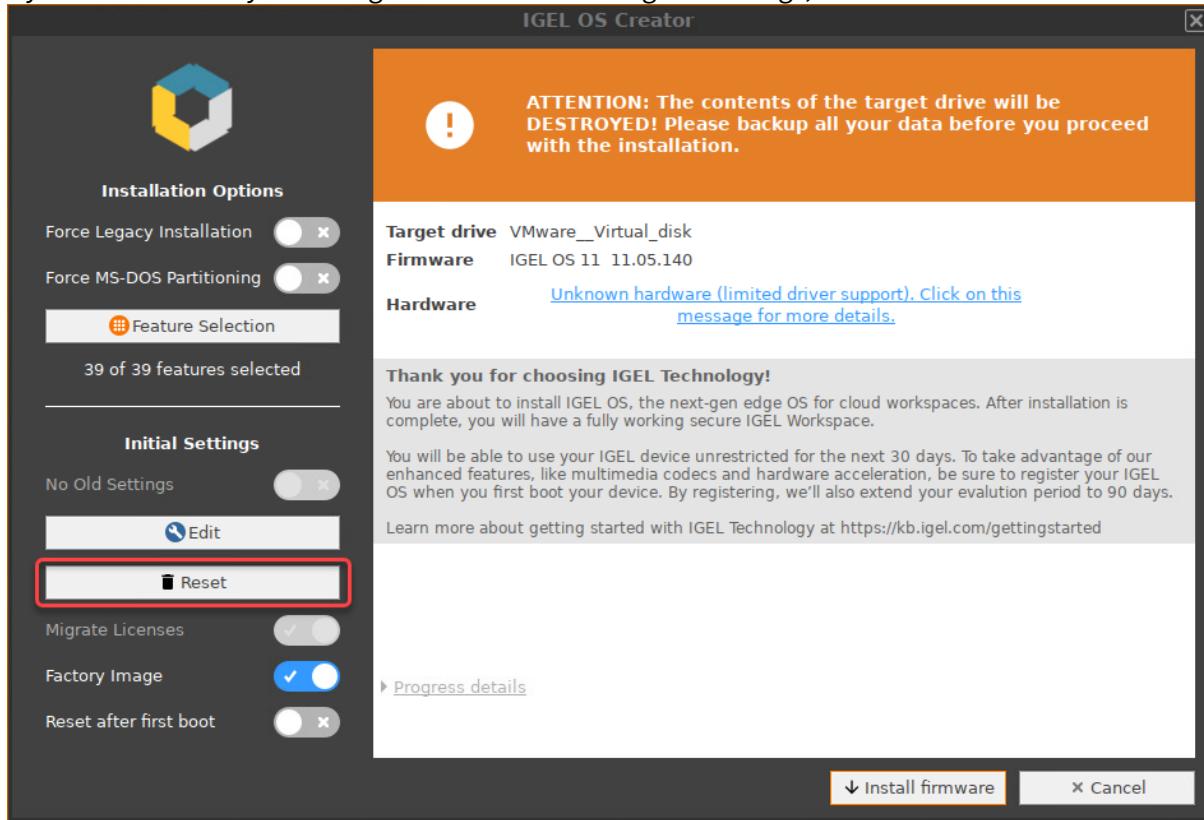


subsequent chapters in the **IGEL OS Reference Manual** (see page 750).





10. If you want to undo your changes and restore the original settings, click **Reset**.



11. If you want to change some device settings after the first boot for functional testing, enable **Reset after first boot**. These changes will not be persistent; after the second boot, the image will be restored to its initial state.

#### Important Note

If **Reset after first boot** is activated in your factory preload image, the first boot of your devices MUST take place BEFORE shipment to end customers!



**IGEL OS Creator**

**ATTENTION: The contents of the target drive will be DESTROYED! Please backup all your data before you proceed with the installation.**

**Target drive** VMware\_Virtual\_disk  
**Firmware** IGEL OS 11 11.05.140  
**Hardware** [Unknown hardware \(limited driver support\). Click on this message for more details.](#)

**Thank you for choosing IGEL Technology!**  
You are about to install IGEL OS, the next-gen edge OS for cloud workspaces. After installation is complete, you will have a fully working secure IGEL Workspace.  
You will be able to use your IGEL device unrestricted for the next 30 days. To take advantage of our enhanced features, like multimedia codecs and hardware acceleration, be sure to register your IGEL OS when you first boot your device. By registering, we'll also extend your evaluation period to 90 days.  
Learn more about getting started with IGEL Technology at <https://kb.igel.com/gettingstarted>

**Initial Settings**

No Old Settings

[Edit](#) [Reset](#)

Migrate Licenses

Factory Image

Reset after first boot

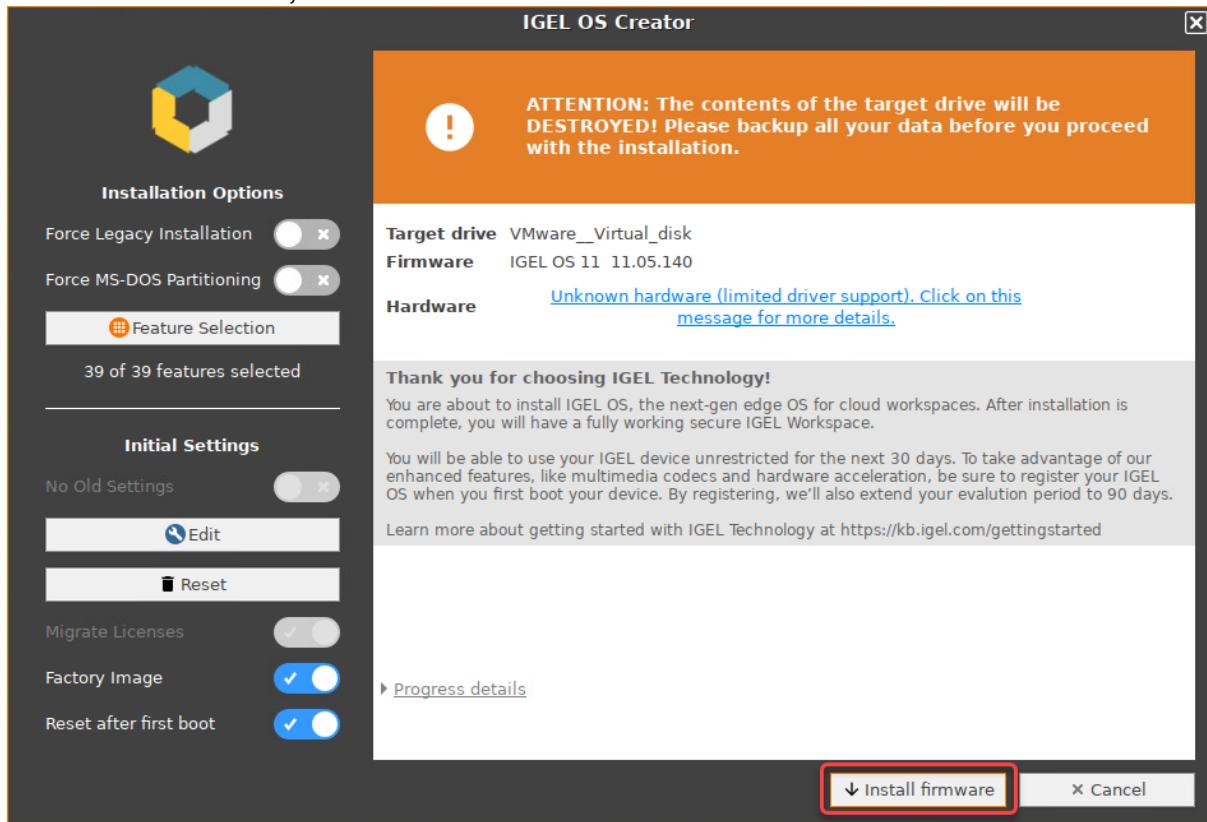
[Progress details](#)

**Install firmware** **Cancel**

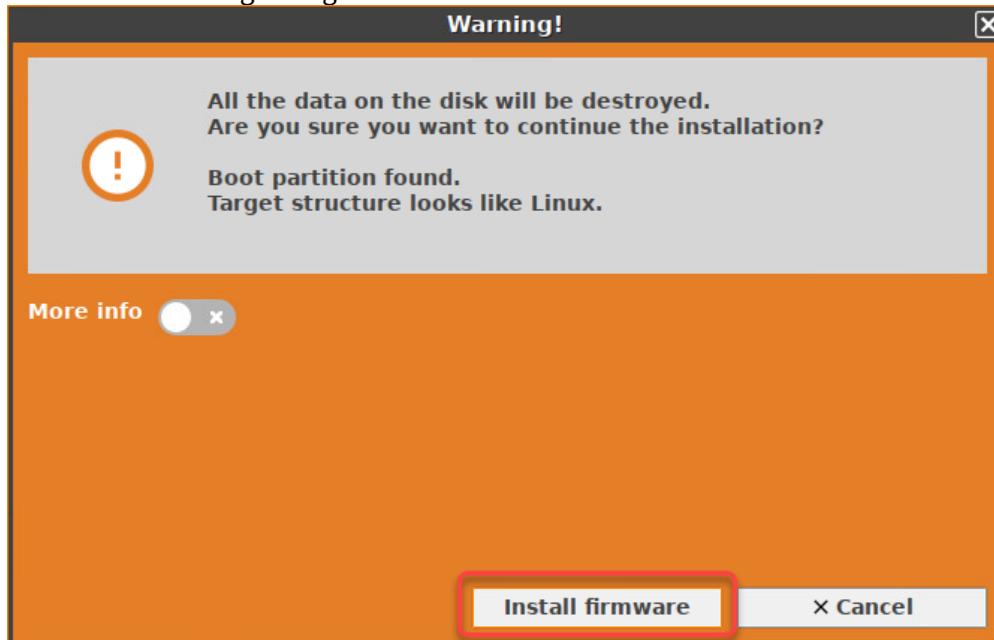
A screenshot of the IGEL OS Creator software window. On the left, there's a sidebar with a hexagonal logo and sections for 'Installation Options' (Force Legacy Installation, Force MS-DOS Partitioning), 'Feature Selection' (39 of 39 features selected), and 'Initial Settings' (No Old Settings, Migrate Licenses, Factory Image, Reset after first boot). The main area has an orange header warning about data destruction. It shows the target drive (VMware\_Virtual\_disk), firmware version (IGEL OS 11 11.05.140), and hardware information (Unknown hardware). Below that is a 'Thank you for choosing IGEL Technology!' message with instructions for registration and links for getting started. At the bottom are 'Install firmware' and 'Cancel' buttons.

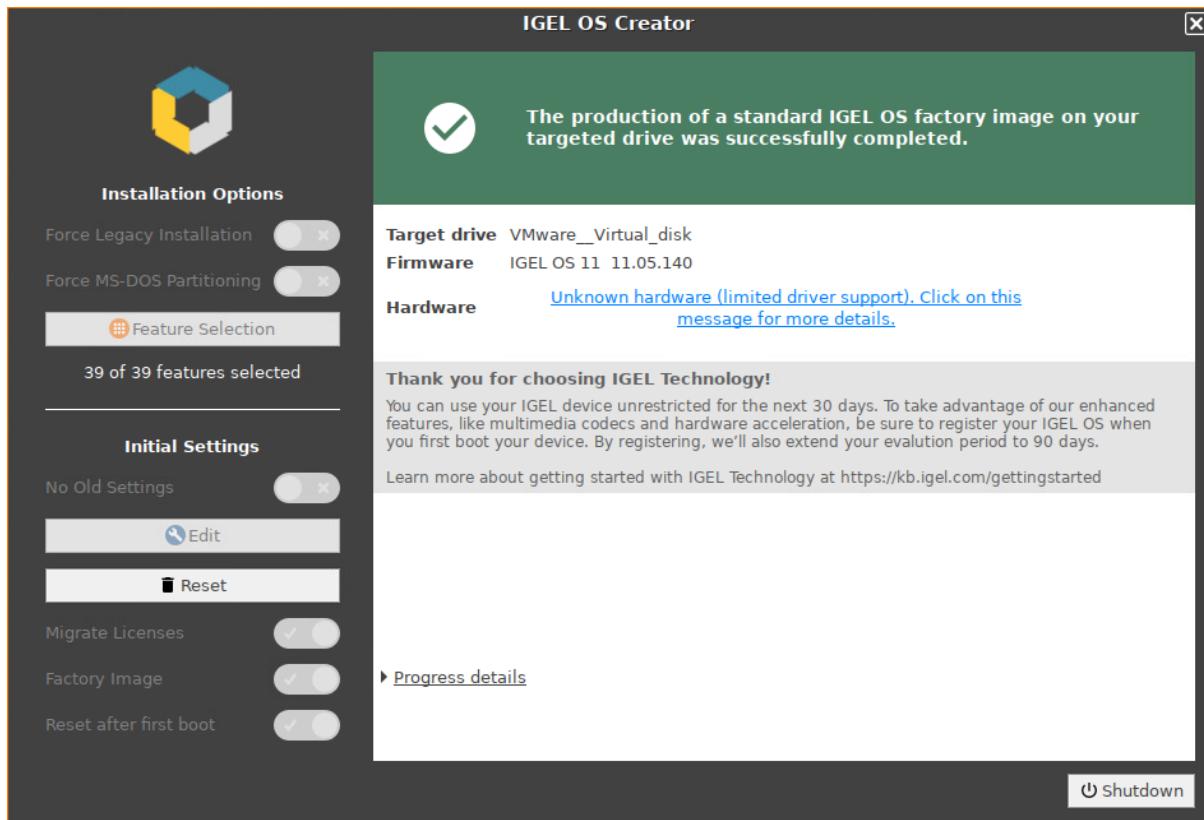


12. To start the installation, click **Install firmware**.



13. Confirm the warning dialog.

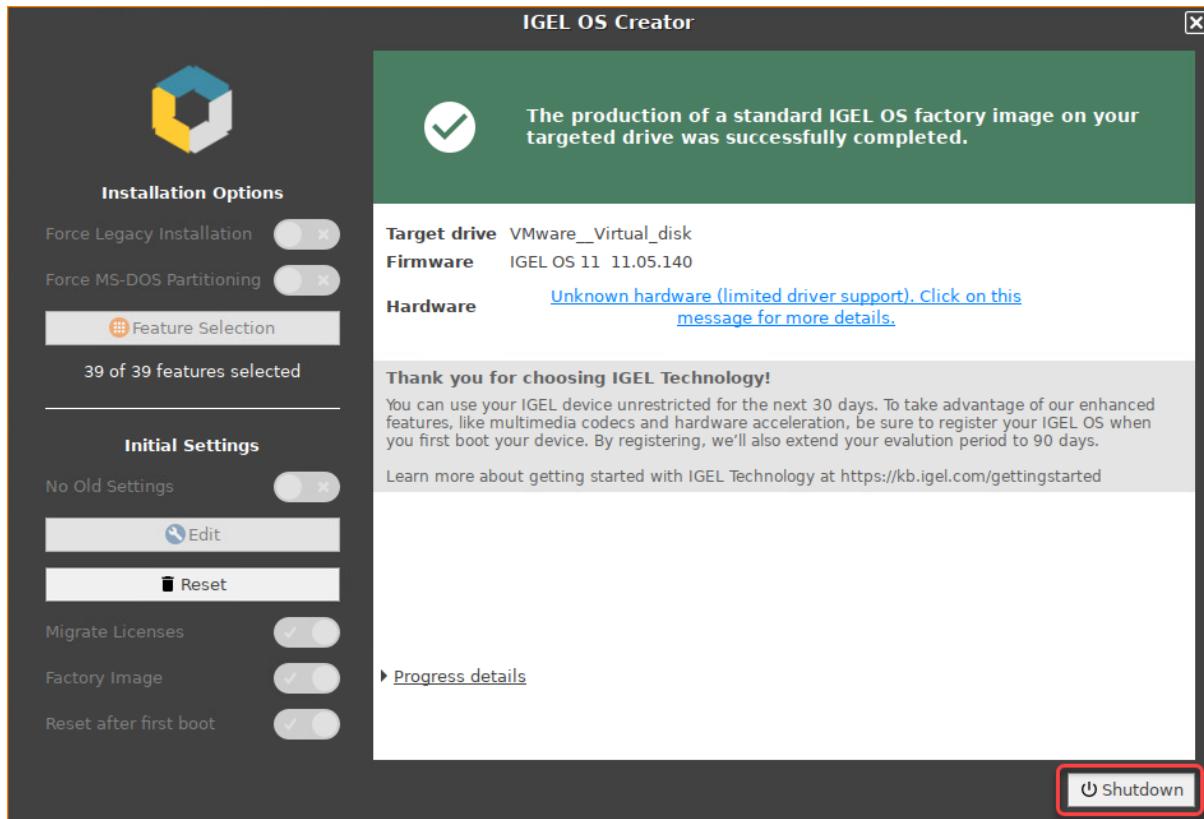




The installation program will set up IGEL OS 11 on the target drive. If you see the success message, the installation is complete.



**14. Click on Shutdown.**



15. Read out the image from your device to deploy it on the units.
16. To ensure the integrity of the image, you should create checksums of the original image and of the images that are deployed, and then compare them. For details, see [IGEL Third-party Endpoint Partners: Ensuring Image Integrity with Checksums](#)(see page 749).
17. Proceed as appropriate:
  - If **Reset after first boot** is inactive, you can deploy the images on the units and roll them out straight away. The deployment should include comparing the checksums.
  - If **Reset after first boot** has been activated, deploy the images on the units and continue with [Unit Testing](#)(see page 1327).(see page 0)

### Unit Testing

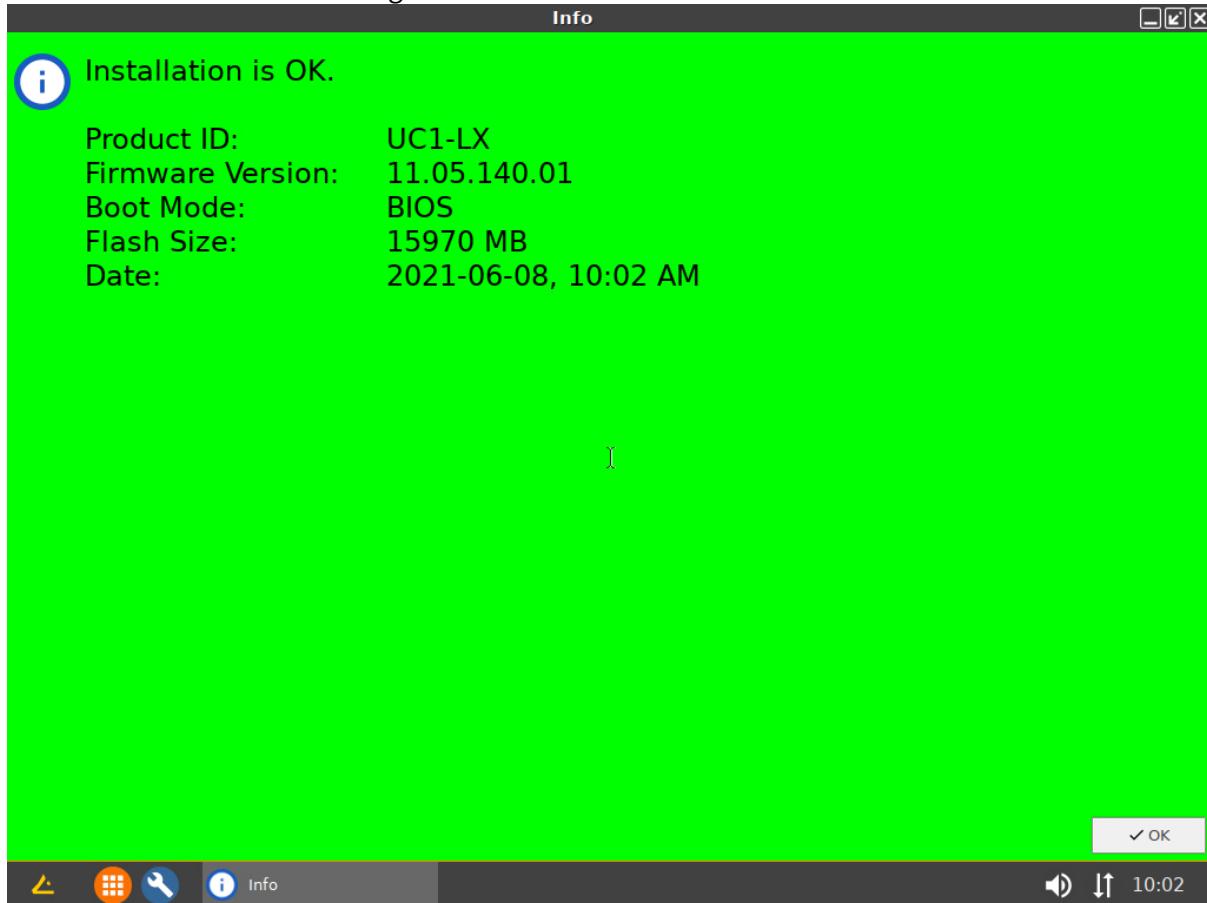
Perform the following procedure on the original device and on every unit on which the image has been deployed.

#### Important Note

The first boot test MUST take place with each unit BEFORE it is rolled out. (Otherwise, the device would present the green test screen instead of the IGEL Setup Assistant.)



1. Start the device and review the green test screen.



2. Click **OK**.

You can access IGEL OS in a regular way and perform your tests.

3. Shut the device down.

The device is ready for roll-out.

## 5.2 IGEL OS Creator Articles

- [Café Wireless \(Wi-Fi\)](#)(see page 1328)
- [Reduce CPU Power Consumption](#)(see page 1332)
- [Installing UDC3 on Secunet SINA Workstation](#)(see page 1333)
- [Setting up UDC3 on Mobile Devices](#)(see page 1335)

### 5.2.1 Café Wireless (Wi-Fi)

When you use your mobile device frequently at different Wi-Fi hotspots, automatic Wi-Fi roaming may be useful. This is what IGEL Café Wireless does. The IGEL Café Wireless feature can be used, for instance, with IGEL UDC3. After you have configured your wireless networks, your mobile device is ready to roam.

For optimizing the network switchover, please see [Configuring Wi-Fi Network Roaming](#)(see page 393).



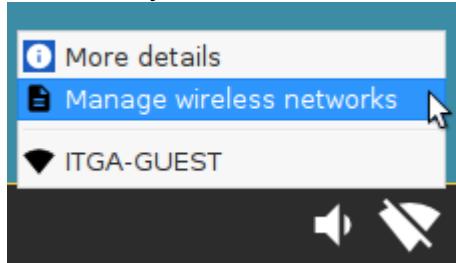
If the network's SSID is hidden, see [Connecting to a Wi-Fi Network with Hidden SSID](#)(see page 395).

See also the manual chapter "[Wireless](#)(see page 1178)".

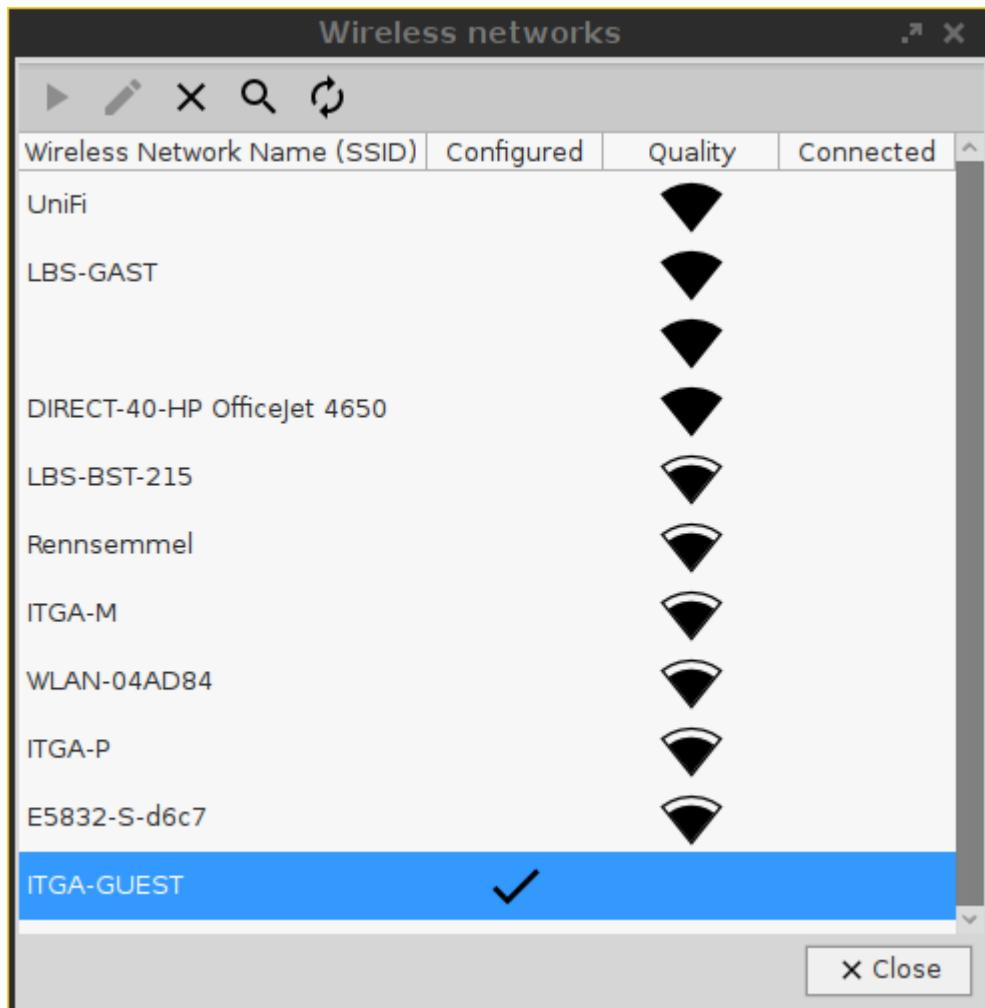
To configure a wireless network with the Wireless Manager:

1. Open **Network > LAN interfaces > Wireless** in the Setup.
2. Enable **Activate wireless interface**.
3. Activate **Enable Wireless Manager**.

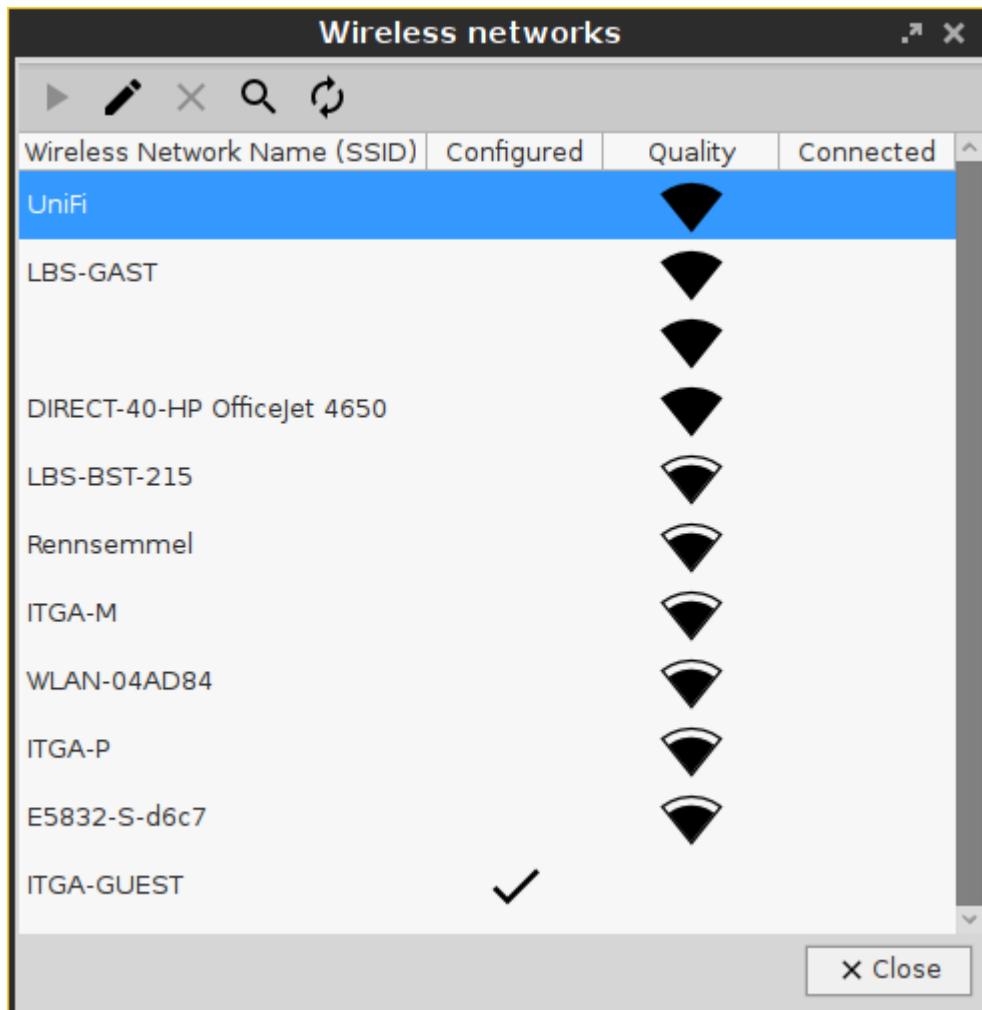
4. Click the tray icon  and select **Manage wireless networks**.



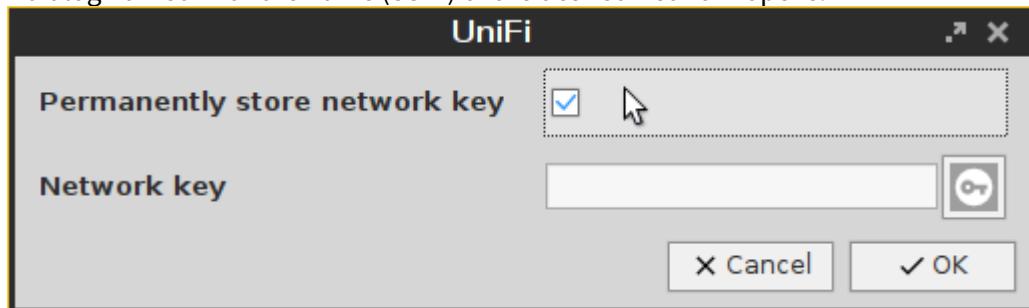
The **Wireless networks** dialog opens. After a few seconds, all wireless networks within reach are shown, sorted by signal strength. Previously configured connections are flagged with a tick in the **Configured** column. The connection currently active is flagged with a symbol under **Connected**.



5. Double-click the network to be configured.



A dialog named with the name (SSID) of the desired network opens.

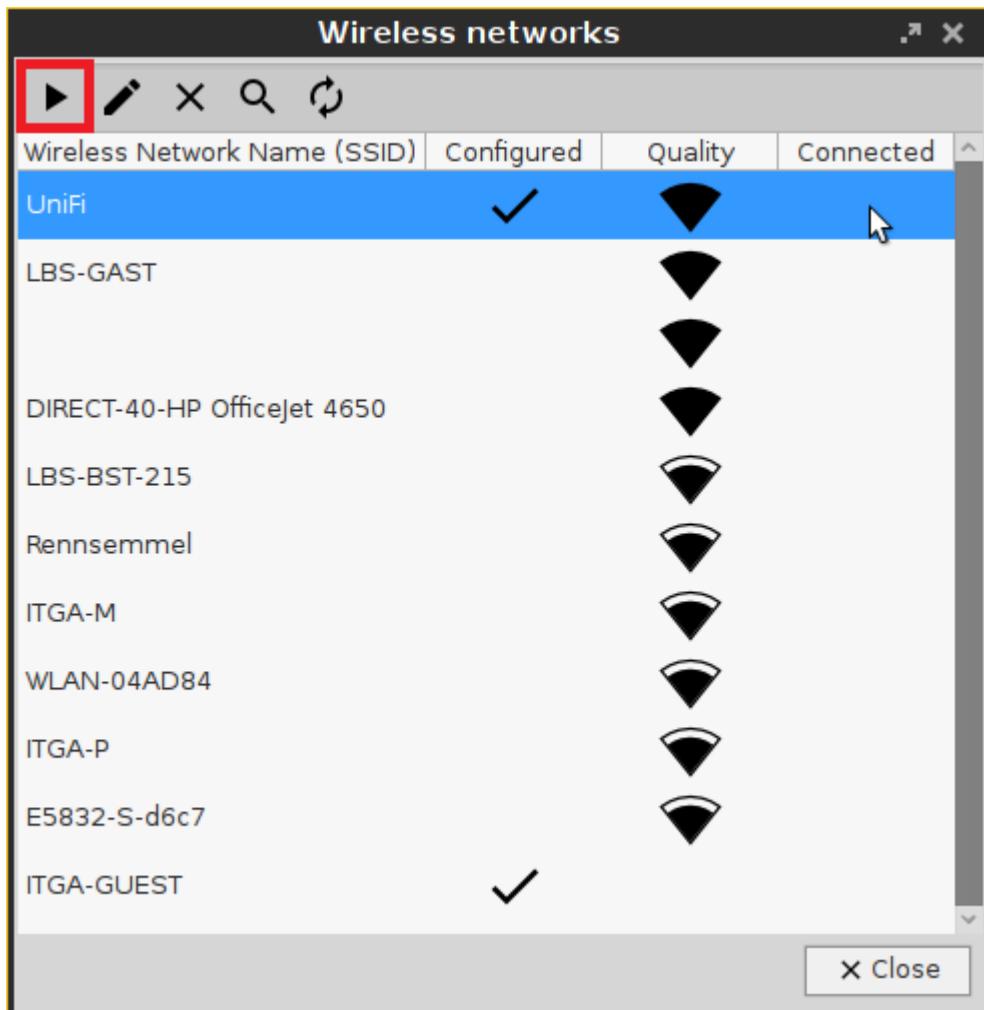


6. Activate **Permanently store network key** so that your mobile device remembers the network key.
7. Enter the **Network key**. To have the network key displayed while typing, click .
8. Click **OK**.
9. Repeat the steps described above for the remaining networks.



To connect to a configured network manually:

- ▶ Highlight the network and click on in the **Wireless networks** dialog.



Your mobile device is connected to the wireless network. The icon



shows the network's current signal strength.

## 5.2.2 Reduce CPU Power Consumption

### Reduce CPU Power Consumption

When you are using the *IGEL Universal Desktop Converter (UDC2)* on a mobile device in battery mode, you might want to reduce power consumption. One major power consumer is your CPU.

You can easily gain some control over the power consumption of your CPU using the tray icon (**CPU Power Plan**) on your taskbar.



- ▶ If the tray icon is not displayed, open the IGEL Setup, go to **System > Power Options > System** and activate **Tray Icon**.

To change the CPU power settings:

1. Click on .
2. Select the appropriate option. **High Performance** gives you the highest performance, but also the highest CPU power consumption, **Power Saver** results in lowest performance and lowest CPU power consumption. The other options are in between.
- For further information about the power plan settings, see the [system\(see page 1332\)](#) chapter in the manual.

### 5.2.3 Installing UDC3 on Secunet SINA Workstation

To install IGEL Universal Desktop Converter 3 on a SINA workstation, proceed as follows:

1. Download the UDC3 zip file under [IGEL Software Download](#)<sup>364</sup> and unzip the file.
2. Copy the ISO image to an USB stick.
3. Start the SINA workstation
4. Click **Administration > Volumes** in the navigation bar.
5. Click **+ Add item** at the bottom of the screen to add a new item.
6. Enter a distinct name for the volume in the **Name** field top right.  
The target drive is already specified.
7. Click **New CFS** under **Select volume type**.  
The form expands.
8. Choose the preconfigured **Security domain**, **Cipher algorithm** and **Hash algorithm**.
9. Click **Define Guest system** under **CFS content**.  
The form expands.
10. Enter a distinct name for the system under **Guest system name**.
11. Choose **2 GiB** as minimum for the **Guest system size**.
12. Select **Disabled** under **Quarantine**.
13. Click **Create**.

The system will now create the volume. This may take a while - depending on the size of the guest system.

1. Go to **Administration > Volumes** and click the new volume.  
Next to it a little form opens.
2. Open **Guest systems**.  
You will see the volume you've created.
3. Click **Local** under **Add guest system from...** to add the ISO image to this volume.  
The form expands.
4. Plug the USB Stick with the ISO image into the workstation.
5. Choose the stick as **Device** and the ISO image as **Guest system image**.
6. Click **Add** at the bottom of the form.

The system now adds the ISO image to your new volume. This will take a while.

---

<sup>364</sup> <https://www.igel.com/software-downloads/>



1. Switch to the **Workplaces** menu.
2. Click **+ Add item** at the bottom of the screen.
3. Enter a distinct name for the workplace in the **Name** field top right.
4. Choose the **Guest system** you've created. It has a small hard disk icon.
5. Choose the ISO image under **Secondary guest system**. It should have a small CD icon.
6. Select **Secured networking** under **Network mode**.
7. Choose your preferred settings under **Display layout**, **Workplace hotkey** and **Audio mode**.
8. Select **CD/DVD** under **Boot order**.
9. Select **Automatic reservation** under **IP to claim** and **MAC to claim**.
10. Select **Ubuntu** as **OS type**.
11. It is not necessary to activate the **Detailed settings**.
12. Click **Create**.

The system now creates the workplace.

1. Klick on the new workplace.  
Next to it a little form opens.
2. Click **Launch** to start the workplace.  
The IGEL Universal Desktop Converter starts.
3. After a few second you will see this screen:



4. Keep the first selected item **Boot IGEL UD Converter**.  
The conversion process starts.  
Next you will see the blue IGEL Linux background.  
A little popup appears.
5. Choose your desired **language**.
6. Agree the **license agreement**.
7. Install the IGEL Linux OS to the workspace.

Be aware, that all data of the volume will be deleted. That's why you should always create a new volume for the IGEL Linux OS.



## 5.2.4 Setting up UDC3 on Mobile Devices

- [Multi Monitor Environment](#)(see page 1335)
- [Presentation Mode](#)(see page 1335)
- [Display Brightness](#)(see page 1336)
- [Power Management](#)(see page 1337)
- [Wireless Manager \(Café Wireless\)](#)(see page 1338)
- [Shortening Network Timeouts in Mobile Scenarios](#)(see page 1339)
- [Battery Level Control](#)(see page 1340)

### Multi Monitor Environment

If you use your notebook in an office workstation, you can use a multi monitor environment.

To configure the display for multiple screens, use the **Display Switch**.

Respective Tray Icon:

| Tray Icon Name | Icon | Where to configure                                           |
|----------------|------|--------------------------------------------------------------|
| Display Switch |      | Menu path: <b>Setup &gt; Accessories &gt; Display Switch</b> |

Activating the Display Switch:

1. Enable the **Display Switch** in the **IGEL Setup** under **Accessories > Display Switch**.
2. Select **Quick Start Panel** as a starting method.  
The **Display Switch** icon is shown in the quick start panel.
3. Click the icon to open the display configuration dialogue.
4. Switch between simple and advanced settings.

For a detailed description, see the manual, chapter [Display Switch](#)(see page 1055).

Here you can find additional instructions concerning monitor settings:

- [How-To Dual Screen](#)(see page 517)
- [Manual topic RDP Global > Window](#)(see page 813)

### Presentation Mode

You are using your mobile device for a presentation. You neither want the monitor to enter power saving mode nor to start the screensaver during the presentation.

For this situation, use the **Presentation Mode** which disables the DPMS and the screen saver.

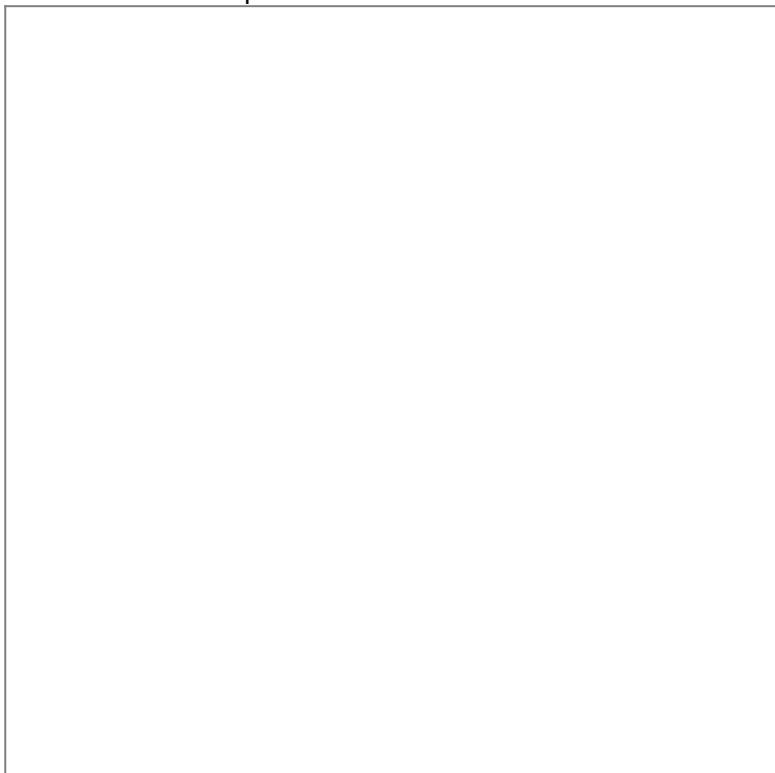
Respective Tray Icon:



| Tray Icon Name | Icon | Where to configure                                                  |
|----------------|------|---------------------------------------------------------------------|
| Notebook BAT   |      | Menu path: <b>Setup &gt; System &gt; Power Options &gt; Battery</b> |

**Activating the Presentation Mode:**

1. Right-click the battery symbol in the system tray.  
The context menu opens:



2. Click **Presentation Mode** to enable/disable it.

**Display Brightness**

In order to preserve the battery you want to reduce the display brightness.

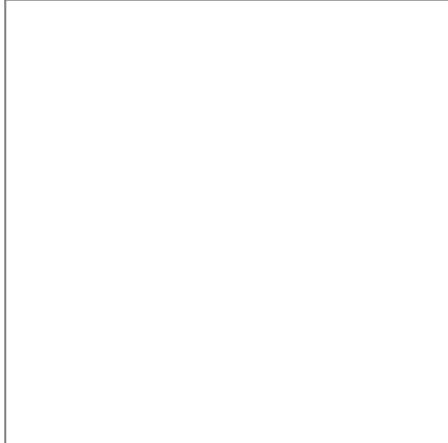
Respective Tray Icon:

| Tray Icon Name | Icon | Where to configure |
|----------------|------|--------------------|
|                |      |                    |



|              |                          |                                                                     |
|--------------|--------------------------|---------------------------------------------------------------------|
| Notebook BAT | <input type="checkbox"/> | Menu path: <b>Setup &gt; System &gt; Power Options &gt; Battery</b> |
|--------------|--------------------------|---------------------------------------------------------------------|

1. Right-click the battery symbol in the system tray.  
The context menu opens.
2. Click the slider of the brightness display to reduce the **Display Brightness**.



## Power Management

You are using your mobile device in battery mode and need to reduce power consumption to preserve the battery.

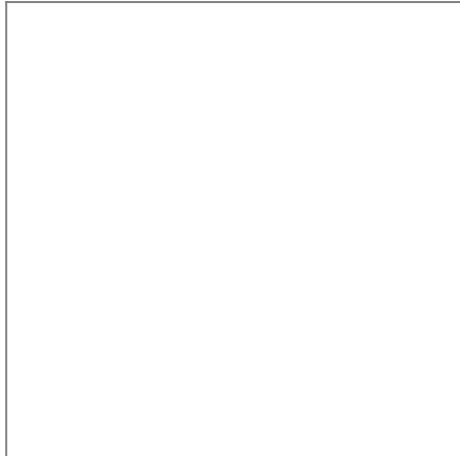
To save power, set CPU power options to scale the CPU frequency down.

Respective Tray Icon:

| Tray Icon Name | Icon                     | Where to configure                                                 |
|----------------|--------------------------|--------------------------------------------------------------------|
| CPU Power Plan | <input type="checkbox"/> | Menu path: <b>Setup &gt; System &gt; Power Options &gt; System</b> |

Setting CPU power options:

1. Click the CPU Power Plan icon in the system tray.  
The context menu opens.



2. Select the appropriate mode.

Here you can find additional instructions concerning the power management:

- Define the **CPU Power Plan, Critical Battery Level, Standby Time or Suspend Time, Brightness reduction, and Shut-down Options**. See the manual, chapter [System > Power Option > System](#)(see page 1261).

## Wireless Manager (Café Wireless)

If you are traveling with your notebook, you need to handle different WiFi connections.

You can use **Café wireless** to configure different wireless network connections.

Respective Tray Icon:

| Tray Icon Name              | Icon | Where to configure                                                     |
|-----------------------------|------|------------------------------------------------------------------------|
| Wireless Network Connection |      | Menu path: <b>Setup &gt; Network &gt; LAN Interfaces &gt; Wireless</b> |

Defining **Café wireless**:

1. Enable the **Wireless Manager** under **Network > LAN Interface > Wireless**.  
Set all options:



2. Click the WiFi tray icon in the right corner of the panel.
3. Open the **Wireless Manager** dialog.

You can find the complete instruction in the manual, chapter [Wireless Manager](#)(see page 1180).

## Shortening Network Timeouts in Mobile Scenarios

When on the road with their UDC2 mobile device, users often experience slow system startup. This is due to the system waiting for network connections or the UMS which are not available in the mobile scenario. This document describes how to minimize waiting by shortening various timeouts.

### Don't Wait for Wired Network

When an Ethernet interface is configured but not physically connected, startup is delayed by default. The goal is to give the user an opportunity to plug in the network cable. If this is not desired, as of IGEL Linux version 5.10.100 waiting can be turned off.

1. In Setup, go to **System > Registry**.
2. Go to the `network.interfaces.ethernet.device[number].nolink_nowait` registry key.  
Replace [number] with:
  - 0 for eth0, the first Ethernet interface
  - 1 for eth1, the second Ethernet interface
3. Enable **No waiting without physical link**. By default, this option is disabled.

### Don't Contact UMS Unless Specific Network Devices Are Up

Startup is also delayed because the system tries to contact UMS by default, which may not be available in a mobile scenario. You can configure IGEL Linux version 5.10.100 to contact UMS only if one of the network devices in a whitelist is up.

1. In Setup, go to **System > Registry**.
2. Go to the `system.remotemanager.device_whitelist` registry key.
3. Put a space-separated device list into the **Network device whitelist** field. Only if at least one of these devices is up, the system will try to contact UMS. Device names:
  - First Ethernet adapter: eth0



- Second Ethernet adapter: eth1
- Wireless: wlan0
- Mobile broadband: ppp10
- OpenVPN: tun0

#### Don't Contact UMS Unless Specific Networks Are Available

You can configure IGEL Linux version 5.10.100 to contact UMS only if one of the networks in a whitelist is reachable.

1. In Setup, go to **System > Registry**.
2. Go to the `system.remotemanager.network_whitelist` registry key.
3. Enter a space-separated list of networks in CIDR notation into the **Network whitelist** input field, e.g. `172.30.0.0/16 192.168.100.0/24`. If there are entries in this field, the system will only try to contact UMS if one of the device's current IP addresses happens to be in one of these ranges.

#### Shorten the UMS Timeout

When different environments cannot be distinguished by the previous two mechanisms, as of IGEL Linux version 5.10.100 the startup delay can be reduced by setting a shorter timeout for connections to the UMS.

1. In Setup, go to **System > Registry**.
2. Go to the `system.remotemanager.rmagent_timeout` registry key.
3. Enter an integer number of seconds into **IGEL Remote Management Timeout**. The default is 90.

#### Don't Wait for All Network Interfaces

You can configure IGEL Linux to wait only for one of the network interfaces to be up instead of all. This also means that error messages concerning Ethernet devices will only be displayed shortly.

1. In Setup, go to **System > Registry**.
2. Go to the `network.global.waitfor_interfaces` registry key.
3. Disable **Wait for interfaces to come up**. By default, this option is enabled.

#### Battery Level Control

Since Linux version 10.03.100 it is possible to display the battery level of a mobile device via UMS. The frequency of the battery level reports sent by the device to the UMS can be adjusted: A report is triggered when the battery status has changed at a specified percentage compared to the previously reported status. The percentage is specified by the **Battery status update frequency** parameter.

Example use case: The IT administrator in a hospital has to take care of battery-powered medical devices. Using the new feature, he can easily keep track of all these devices via the UMS, without any need of physical access or mirroring VNC.

To adjust the report frequency:

1. In Setup, go to **System > Registry**.
2. Go to the `system.remotemanager.battery_report_frequency` registry key.
3. Select the **Battery status update frequency**:
  - Often
  - Normal
  - Rarely
  - Very Rarely



- Never
4. Click **Apply** or **Ok**.



## 6 IGEL OS Creator for Windows (OSCW)

The IGEL OS Creator for Windows (OSCW) is able to convert Windows machines to IGEL OS 11, provided that they fulfill the [hardware requirements](#)(see page 1343).

Choose the instructions according to your needs:

- [IGEL OS Creator for Windows \(OSCW\) on Windows 7/10 Workstations](#)(see page 1342)
- [IGEL OS Creator for Windows \(OSCW\) on IGEL Windows Embedded 7/7+](#) (see page 1382)
- [IGEL OS Creator for Windows \(OSCW\) on IGEL Windows 10 IoT](#)(see page 1401)
- [IGEL OS SCCM Add-On](#)(see page 1408)

### 6.1 IGEL OS Creator for Windows (OSCW) on Windows 7/10 Workstations

#### 6.1.1 Introduction

The IGEL OS Creator (OSC) for Windows is able to convert any Windows 10 or Windows 7 machine to IGEL OS 11, provided that it fulfills the [hardware requirements](#)(see page 1343).

Read all the following chapters and follow the instructions in the order given.

- [Prerequisites](#)(see page 1343)
- [Getting the Required Software](#)(see page 1343)
- [Transferring the IGEL OSC File to the UMS](#)(see page 1344)
- [Deploying the OSCW Installer on the Target Machines](#)(see page 1345)
- [Installing the OSCW Installer](#)(see page 1345)
- [Registering the Target Machines to the UMS](#)(see page 1348)
- [Configuring the OSCW Installer](#)(see page 1351)
- [Starting the Conversion](#)(see page 1381)

#### 6.1.2 Video

A video is available to illustrate the procedure.

#### Part I



Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:

<https://www.youtube.com/watch?v=NGA0FNLBd0&feature=youtu.be>



## Part II



Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:

<https://www.youtube.com/watch?v=uXDdQ6aGrZs&feature=youtu.be>

### 6.1.3 Prerequisites

#### Hardware

- Memory: ≥ 4 GB RAM
- Storage: ≥ 3 GB free storage to store the ISO file containing IGEL OS Creator
- For supported hardware, see [Third-Party Devices Supported by IGEL OS 11<sup>365</sup>](#).

#### Software

The following software must be present on the target machines:

- Windows 10 or Windows 7
- Microsoft Hotfix KB3140245 (Windows 7 x86/x64)

#### Network

- All machines are in a network that can be reached by the UMS.
- For buddy mode: All machines must be joined to a Microsoft Active Directory (AD) and be accessible by the same AD user with reading permissions.

#### Next Step

>> When all requirements are met, continue with [Getting the Required Software](#)(see page 1343).

### 6.1.4 Getting the Required Software

The following software must be downloaded resp. installed:

---

<sup>365</sup> <https://kb.igel.com/display/hardware/Third-Party+Devices+Supported+by+IGEL+OS+11>



## IGEL Universal Management Suite (UMS) 6.04.120 or Higher

1. Download UMS 6.04.120 or higher from <https://www.igel.com/software-downloads/workspace-edition/> > **Universal Management Suite**.
2. Update your UMS to version 6.04.120 or later resp. install UMS 6.04.120. For update instructions, see [Updating UMS<sup>366</sup>](#); for installation instructions, see [Installation<sup>367</sup>](#).

## OSCW Files

1. Download OSC for Windows 1.01.100 or higher (EXE or MSI installer)
  - EXE file: <https://www.igel.com/software-downloads/workspace-edition/> > **OSC for Windows** > setup-igel-osc-for-windows\_1.01.100.exe
  - MSI file: <https://www.igel.com/software-downloads/workspace-edition/> > **OSC for Windows** > setup-igel-osc-for-windows\_1.01.100.msi
2. Download IGEL OS 11.03.560 or higher (ISO): <https://www.igel.com/software-downloads/workspace-edition/> > **OSC for Windows** > OSC\_11.03.560.zip

## Check List

- The UMS is updated to version 6.04.120 or higher.
- OSC for Windows 1.01.100 or higher is available.
- IGEL OS 11.03.560 or higher (ISO file) is available.

## Next Step

>> [Transferring the IGEL OS Creator File to the UMS\(see page 1344\)](#)

### 6.1.5 Transferring the IGEL OSC File to the UMS

In this step, we will transfer the IGEL OS firmware file (ISO) to the UMS so that the UMS can deploy it to the target machines.

Do not register the file as a file object. This might lead to various issues, particularly in ICG and HA environments.

1. Get access to the file system of the machine on which your UMS Server is running.
2. Copy osc.iso to <UMS Installation directory>\rmuiserver\webapps\ums\_filetransfer

<sup>366</sup> <https://kb.igel.com/display/endpointmgmt604/Updating+UMS>

<sup>367</sup> <https://kb.igel.com/display/endpointmgmt604/UMS+Installation+and+Update>



## Next Step

>> [Deploying the OSCW Installer on the Target Machines\(see page 1345\)](#)

### 6.1.6 Deploying the OSCW Installer on the Target Machines

In this step, we will deploy the OSCW installer on the target machines.

► Deploy the installer on all devices that are to be converted. The following methods are available for deployment:

- SCCM (System Center Configuration Manager): Use the MSI installer (`setup-igel-osc-for-windows_1.01.100.msi`) and deploy it just like any software. The OSCW installer is installed silently.
- Group policy: Use the MSI installer (`setup-igel-osc-for-windows_1.01.100.msi`) and deploy it just like any software. The OSCW installer is installed silently.
- File-based methods: Use the EXE file (`setup-igel-osc-for-windows_1.01.100.exe`). You can use file sources such as:
  - USB memory stick
  - Network drive
  - DVD

## Check List

The OSCW installer is deployed on all target machines. When SCCM or group policy was used, the installation has been executed silently.

## Next Step

If the OSCW installer has been deployed via SCCM or group policy and has been installed silently:

>> Continue with [Registering the Target Machines to the UMS\(see page 1348\)](#).

If the OSCW installer has been deployed via a file-based method:

>> Continue with [Installing the OSCW Installer\(see page 1345\)](#).

### 6.1.7 Installing the OSCW Installer

In this step, we will install the OSCW installer on the target machines. The method depends on how the OSCW installer has been deployed on the target machines.

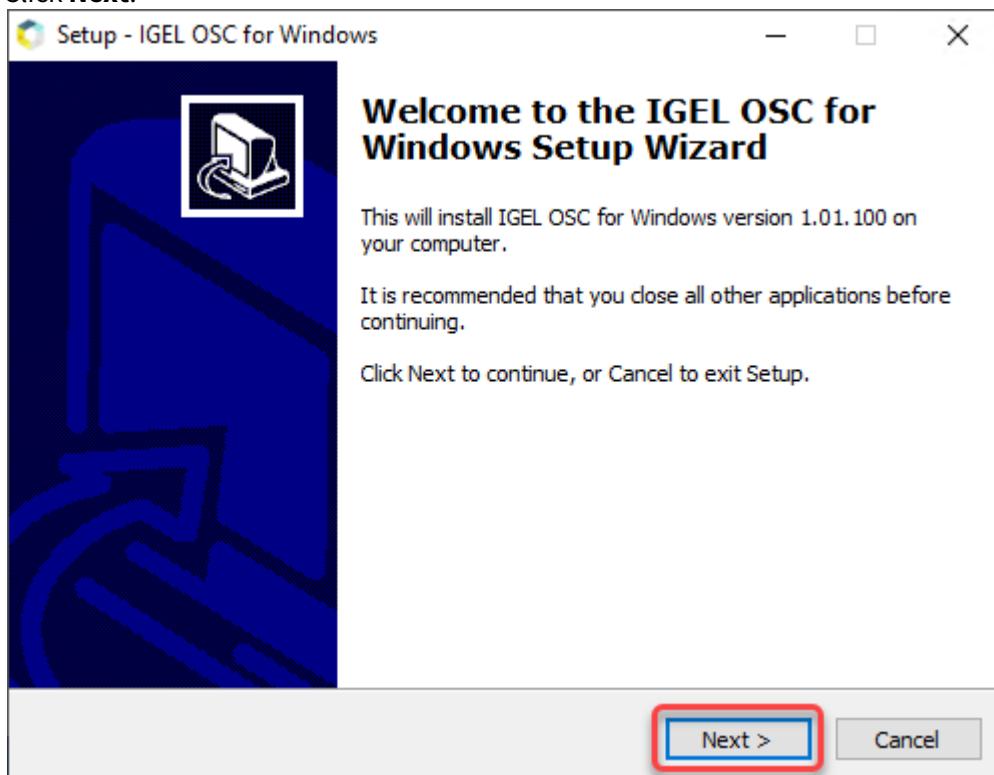
#### OSCW Installer Has Been Deployed via SCCM or Group Policy

If you have used SCCM or group policy to deploy the OSCW installer, the installation has been executed silently; continue with [Registering the Target Machines to the UMS\(see page 1348\)](#).



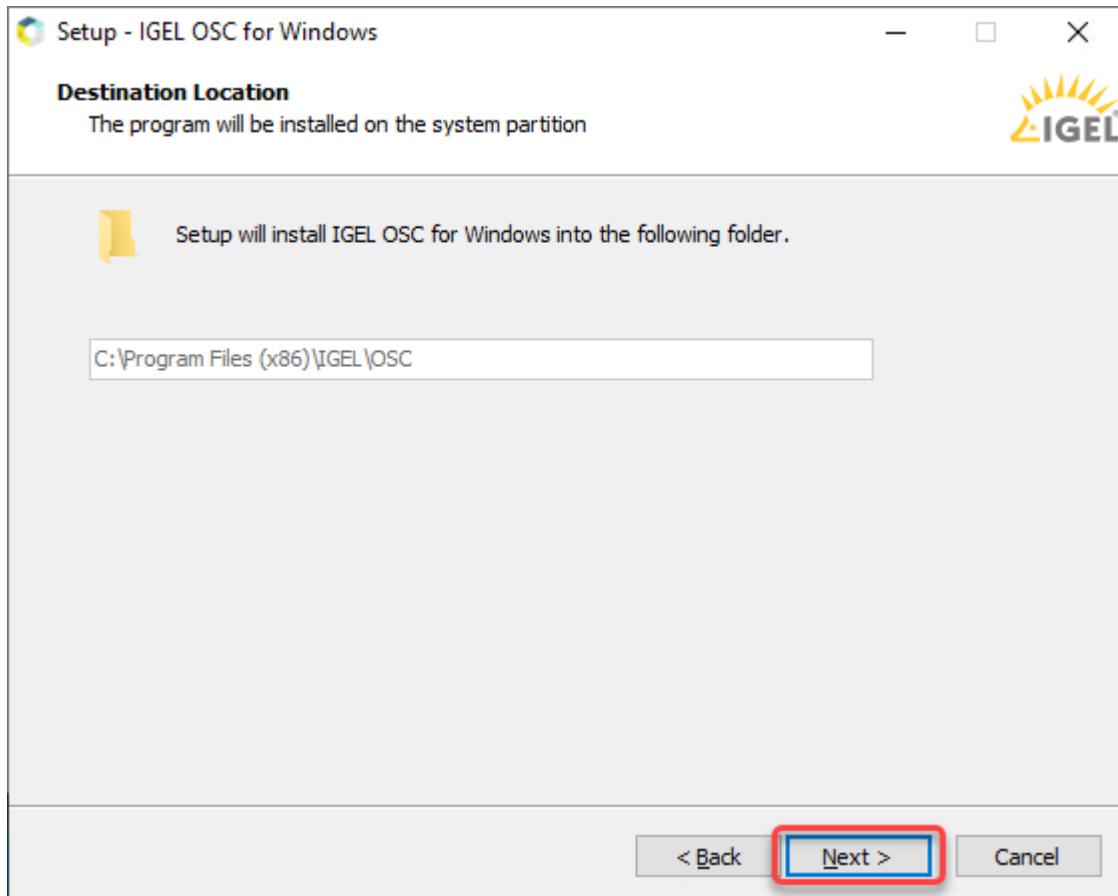
## OSCW Installer Has Been Deployed from a File

1. On the target machine, double-click setup-igel-osc-for-windows\_1.01.100.exe and confirm the Windows UAC (user account control). The OSCW installer is digitally signed by "IGEL Technology GmbH".  
The setup wizard opens.
2. Click **Next**.



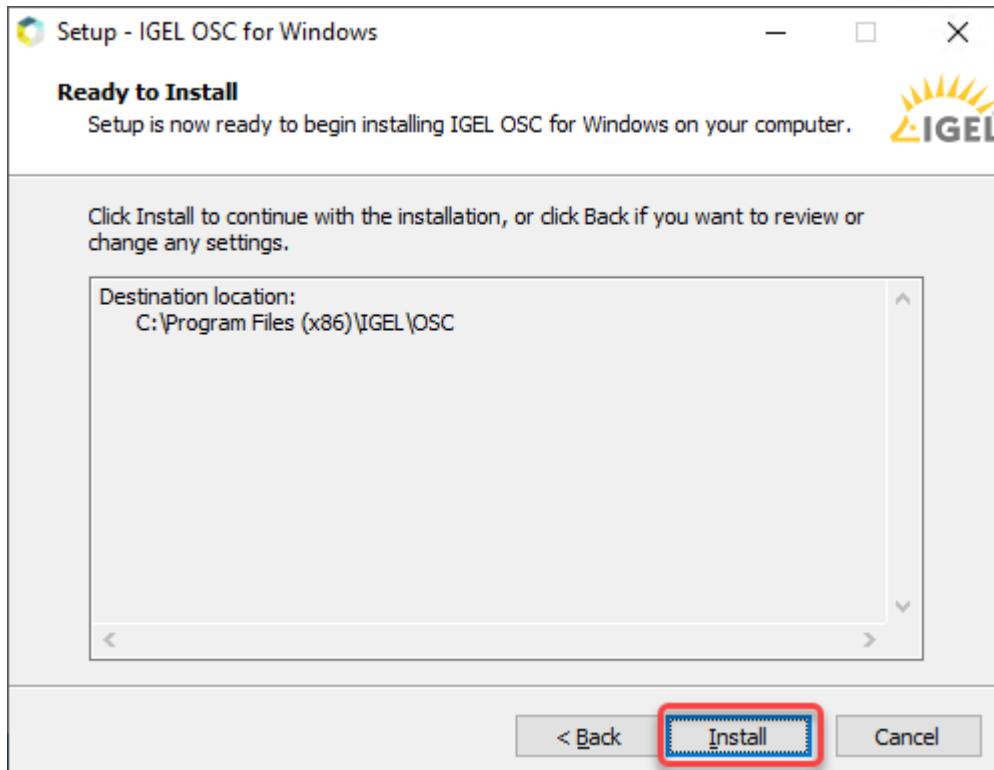


3. Review the installation folder and click **Next**.





4. Review the confirmed installation folder and click **Install**.



IGEL OSC for Windows is installed on the target machine.

5. The installer window is closed.

#### Check List

- The OSCW installer is installed on each target machine.

#### Next Step

>> [Registering the Target Machines to the UMS\(see page 1348\)](#)

### 6.1.8 Registering the Target Machines to the UMS

In this step, we will register all target machines to the UMS. This is necessary because the conversion to IGEL OS will be triggered by the UMS.

Two registration methods are available: a scan by the UMS and automatic registration.

- [Registering by a UMS Scan\(see page 1349\)](#)
- [Registering by Automatic Registration\(see page 1350\)](#)



## Registering by a UMS Scan

1. Open the UMS Console and click to scan for devices.
2. Select the scope in which the devices are located; for details, see [Searching for Devices](#)<sup>368</sup>.
3. Click **Scan**.  
The dialog **Found devices** opens.
4. In the **Filter** field, enter "IGEL Unified Management Agent OSCW".

**Found devices**

82 Devices were found. Filter **IGEL Unified Management Agent OSCW**

| Certificate stor... | Unit ID      | MAC Address       | Name            | IP address    | Product                            | Incl...                  |
|---------------------|--------------|-------------------|-----------------|---------------|------------------------------------|--------------------------|
| No                  | 0050569353A8 | 00:50:56:93:53:A8 | DESKTOP-L5NR64G | 172.30.91.63  | IGEL Unified Management Agent OSCW | <input type="checkbox"/> |
| No                  | 00505693842A | 00:50:56:93:84:2A | IGEL-CXQY1D374I | 172.30.91.56  | IGEL Unified Management Agent OSCW | <input type="checkbox"/> |
| No                  | 00505693A2F0 | 00:50:56:93:A2:F0 | Doku-HS-OSCW    | 172.30.91.118 | IGEL Unified Management Agent OSCW | <input type="checkbox"/> |

5. Select all target machines and click **Ok**.

**Found devices**

82 Devices were found. Filter **IGEL Unified Management Agent OSCW**

| Certificate stor... | Unit ID      | MAC Address       | Name            | IP address    | Product                            | Incl...                             |
|---------------------|--------------|-------------------|-----------------|---------------|------------------------------------|-------------------------------------|
| No                  | 0050569353A8 | 00:50:56:93:53:A8 | DESKTOP-L5NR64G | 172.30.91.63  | IGEL Unified Management Agent OSCW | <input checked="" type="checkbox"/> |
| No                  | 00505693842A | 00:50:56:93:84:2A | IGEL-CXQY1D374I | 172.30.91.56  | IGEL Unified Management Agent OSCW | <input checked="" type="checkbox"/> |
| No                  | 00505693A2F0 | 00:50:56:93:A2:F0 | Doku-HS-OSCW    | 172.30.91.118 | IGEL Unified Management Agent OSCW | <input checked="" type="checkbox"/> |

Put in directory:

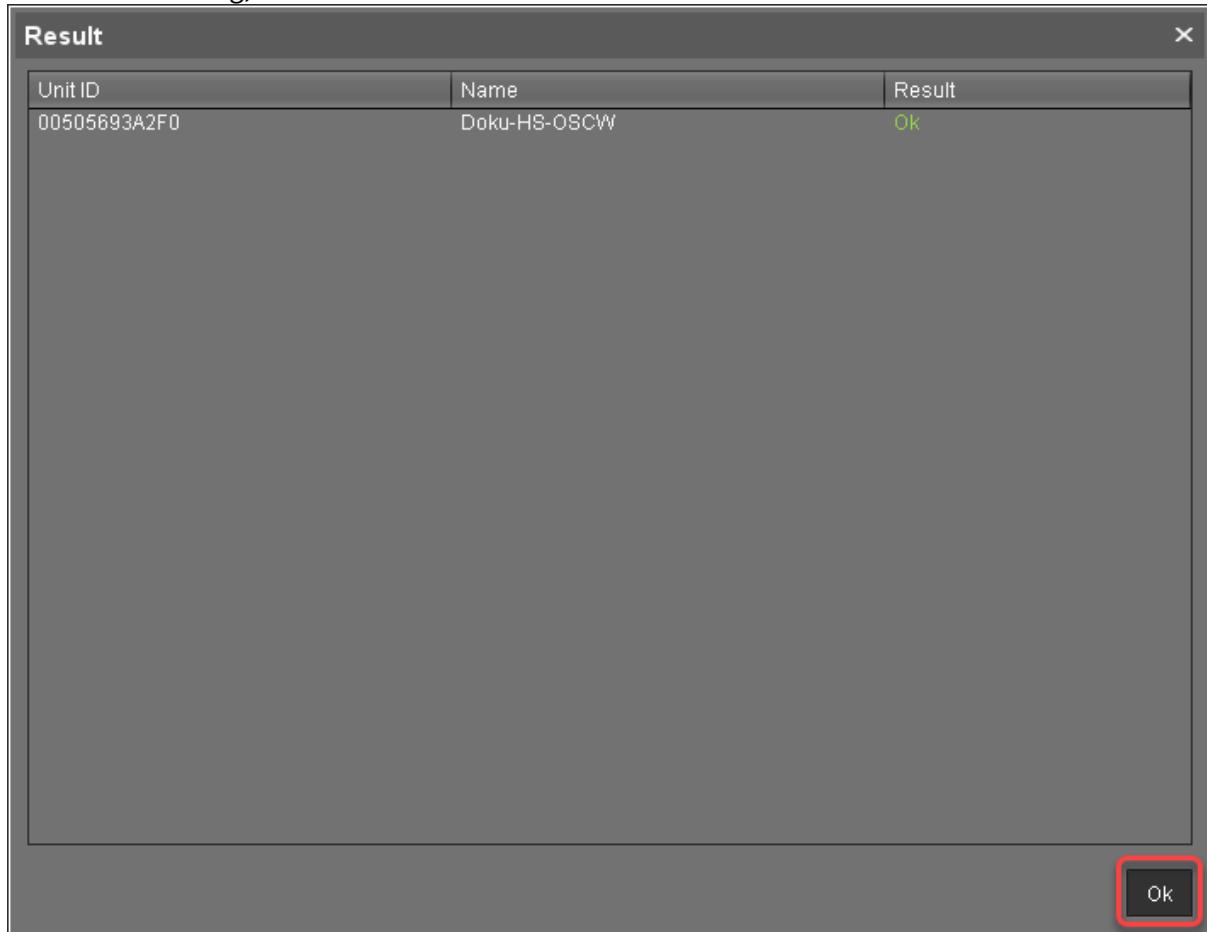
**Ok** **Cancel**

The target machines are registered with the UMS.

<sup>368</sup> <https://kb.igel.com/display/endpointmgmt604/Searching+for+Devices>



6. In the **Result** dialog, click **Ok**.



## Registering by Automatic Registration

For this method, a DNS entry or DHCP option must be set.

- ▶ Follow the instructions in [Registering Devices Automatically](#)<sup>369</sup>.

## Check List

- All target machines are registered with the UMS.

## Next Step

>> [Configuring the Installer](#)(see page 1351)

---

<sup>369</sup> <https://kb.igel.com/display/endpointmgmt604/Registering+devices+automatically>



### 6.1.9 Configuring the OSCW Installer

In this step, we will provide the OSCW installer with the download source for the ISO file that contains the IGEL OS Creator.

Two methods are available:

- [Configuring the OSCW Installer in Normal Mode](#)(see page 1351): Each target machine downloads the ISO file from the server (UMS) individually. This increases the amount of outgoing traffic from the UMS.
- [Configuring the OSCW Installer in Buddy Mode](#)(see page 1364): This method is recommended if the connection bandwidth of the download source is limited; it ensures a more balanced use of network bandwidth during the distribution of the ISO file to the target machines. First, a group of target machines downloads the ISO file. Then, these machines serve as the download source ("update buddies") for the remaining target machines. As a requirement, all devices must be joined to a Microsoft Active Directory (AD) and be accessible by the same AD user with reading permissions.

#### Configuring the OSCW Installer in Normal Mode

To provide the OSCW installer with the download source for the IGEL OS Creator file (ISO), we will create a profile that provides the path to that file. To assign the profile to the target machines, we will use a view that recognizes the target machines by their product ID.

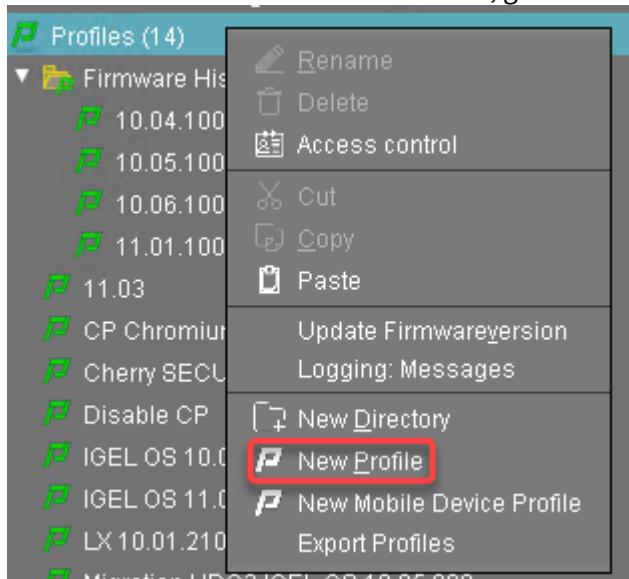
The configuration comprises the following steps:

- [Creating a Profile](#)(see page 1352)
- [Creating a View to Select All Target Machines](#)(see page 1354)
- [Assigning the Profile to the Target Machines](#)(see page 1359)
- [Monitoring the Process](#)(see page 1361)



## Creating a Profile

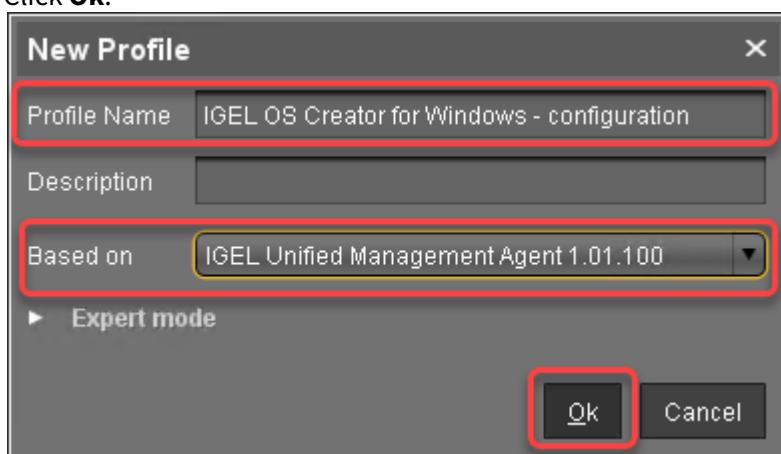
1. In the structure tree of the UMS Console, go to **Profiles** and open **New Profile** in the context menu.



2. In the **New Profile** dialog, change the settings as follows:

- **Profile Name:** A name for the profile, e. g. "IGEL OS Creator for Windows - configuration"
- **Based on:** Select "IGEL Unified Management Agent 1.01.100".

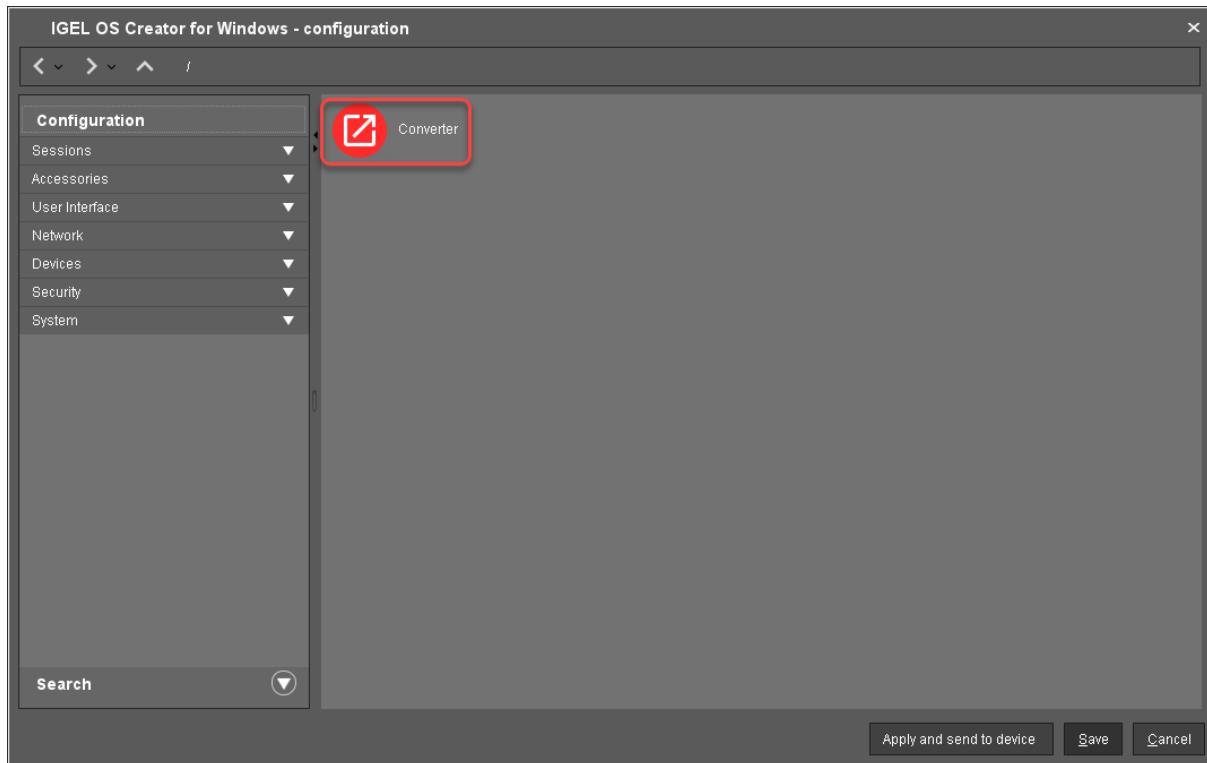
3. Click **Ok**.



The configuration dialog opens.



4. Click **Converter**.

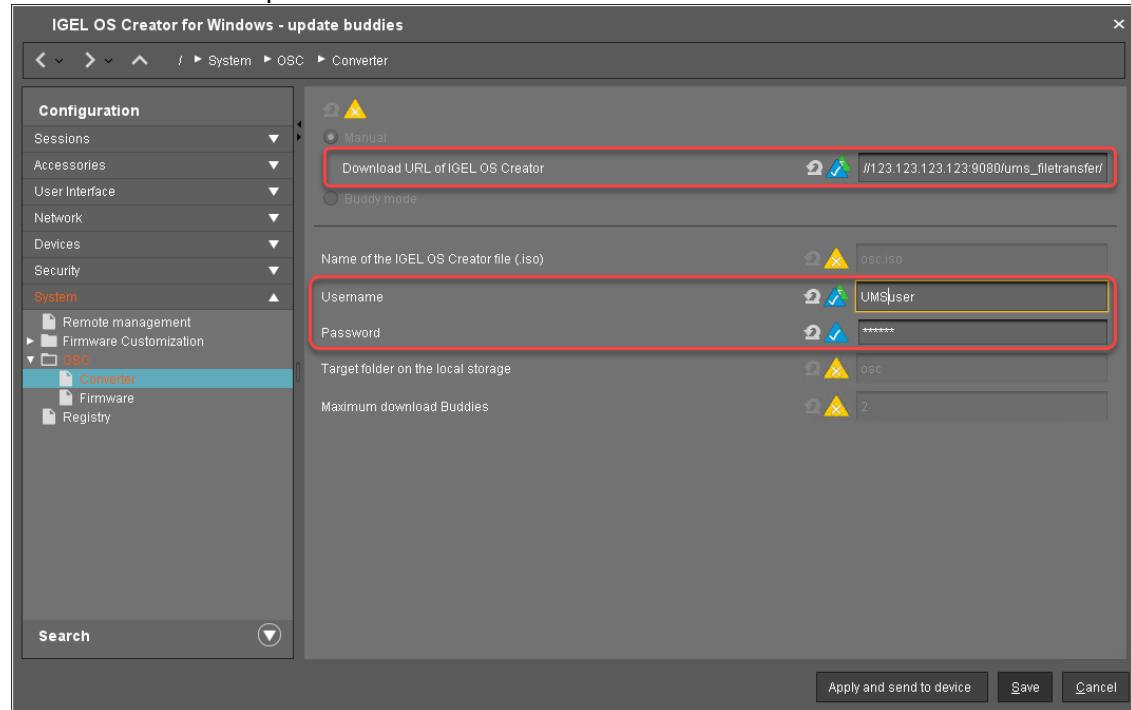


You are taken to **System > OSC > Converter** where you can set all relevant parameters.

5. Change the settings as follows (click the icon to enable the configuration; the icon will change to ):
- **Download URL of IGEL OS Creator:** Enter `https://[IP address of your UMS Server]:8443/ums_filetransfer/` or `http://[IP address of your UMS Server]:9080/ums_filetransfer/`  
Example: `https://192.168.178.100:8443/ums_filetransfer/` or `http://192.168.178.100:9080/ums_filetransfer/`
  - **Username:** Enter the username for the UMS.



- **Password:** Enter the password for the UMS user.

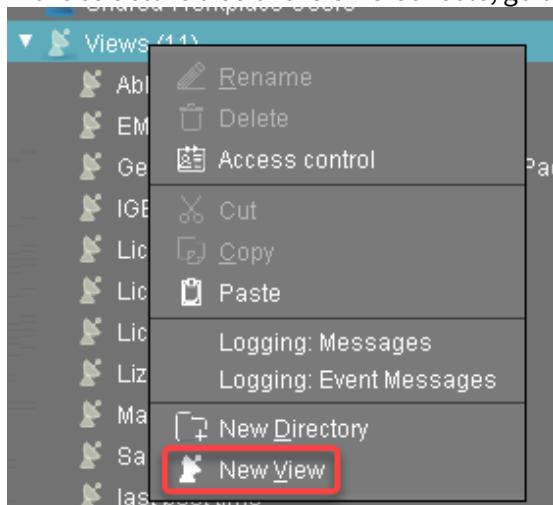


6. Click **Save**.

#### Creating a View to Select All Target Machines

The target machines must be selected in order to assign the profile to them. For the selection, a view will be used.

1. In the structure tree of the UMS Console, go to **Views** and select **New View** in the context menu.





2. Enter a name for the view, e. g. "IGEL OS Creator for Windows - target machines" and click **Next**.

**Create new view**

**View name**

Name   

Description

Expert mode

< Back > Next Finish Cancel



3. On the **Select criterion** page, select **Product ID** and click **Next**.

**Create new view**

**Select criterion**

CPU Speed       CPU Type       Device Type  
 Duplex Mode       Firmware Description       Firmware Update (Relative)  
 Firmware Version       Flash Player       Flash Player Version  
 Flash Size       Graphics Chipset 1       Graphics Chipset 2  
 Graphics Memory Size 1       Graphics Memory Size 2       Last Boot Time (Absolute)  
 Last Boot Time (Relative)       Memory Size       Network Name  
 Network Speed       OS Type       Partial Update (Name)  
 Partial Update (Relative)       Partial Update (Version)       Product  
 Product ID       Total Operating Time

**▼ Monitor Information**

Monitor Date of Production       Monitor Model       Monitor Native Resolution

**Back** **Next** **Finish** **Cancel**

A screenshot of a software window titled 'Create new view' with a sub-section 'Select criterion'. A list of various system parameters is shown as radio buttons. The 'Product ID' option is selected and has a red rectangular highlight around it. At the bottom of the window, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel', with the 'Next' button also having a red highlight around it.



4. On the **Text search** page, enter "OSCW" and click **Next**.

**Create new view**

**Text search**

OSCW

Consider case  
 Compare whole text  
 Use regular expression  
 Not like

< Back **Next** > Finish Cancel



5. On the **Create new view** page, click **Finish**.

**Create new view**

**Finish view creation**

Name: IGEL OS Creator for Windows - target machines

Description:

View criteria:  
Product ID is like (?i).\*OSCW.\*

Create view  
 Narrow search criterion (AND)  
 Create additional search criterion (OR)

**Back** **Next** **Finish** **Cancel**

The number of matches is shown.

6. Click **Load devices** to view the target machines.

Name: IGEL OS Creator for Windows - target machines

Description:

Rule: Product ID is like (?i).\*OSCW.\*

Result list was last updated at 1:02 PM. **Load devices** Refresh Settings

One matching device found.

7. The target machines are shown.

Name: IGEL OS Creator for Windows - target machines

Description:

Rule: Product ID is like (?i).\*OSCW.\*

Result list was last updated at 1:03 PM. Refresh Settings

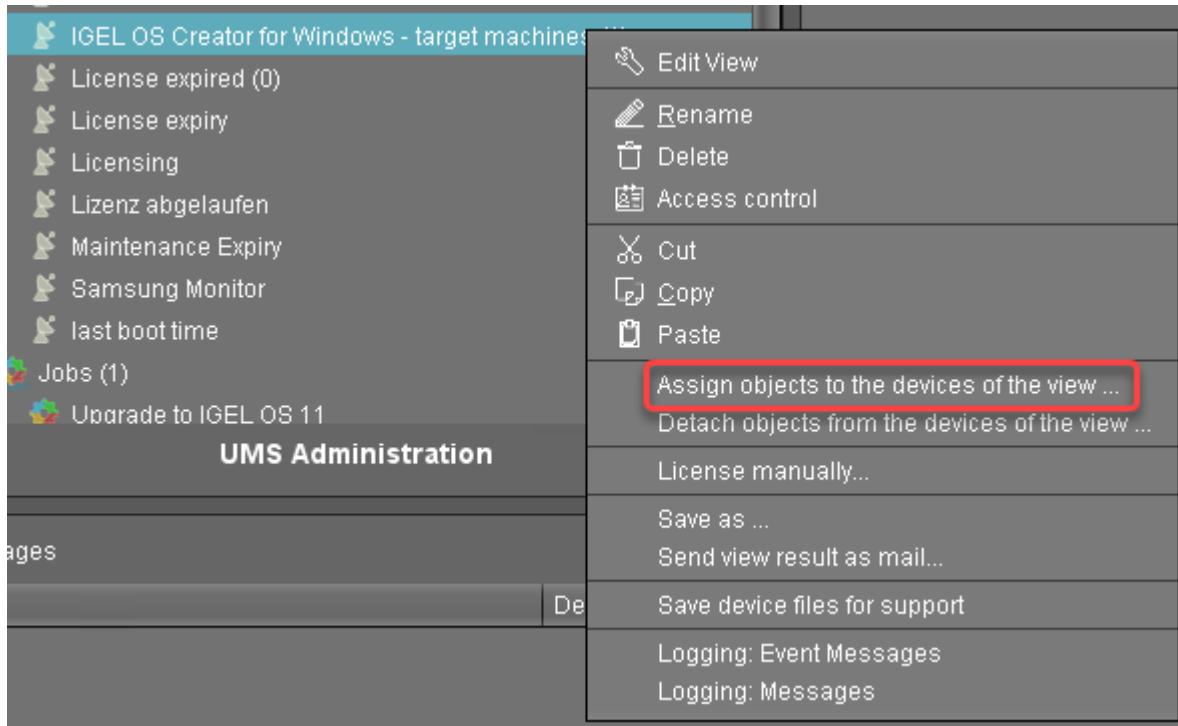
Matching devices (1 device)

| Name         | Last known IP address | MAC Address  | Product                       | Version  |
|--------------|-----------------------|--------------|-------------------------------|----------|
| Doku-HS-OSCW | 172.30.91.118         | 00505693A2F0 | IGEL Unified Management Agent | 1.01.100 |



## Assigning the Profile to the Target Machines

1. Select the view you have created beforehand and select **Assign objects to the devices of the view ....**

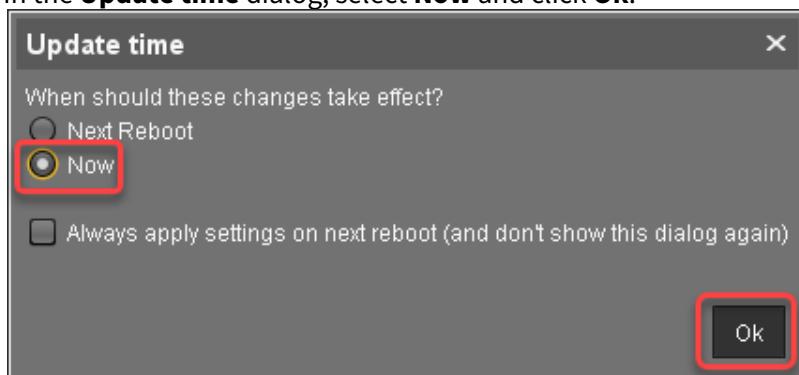




2. In the **Assign objects** dialog, select the profile you have created beforehand, click to assign it and then click **Ok**.

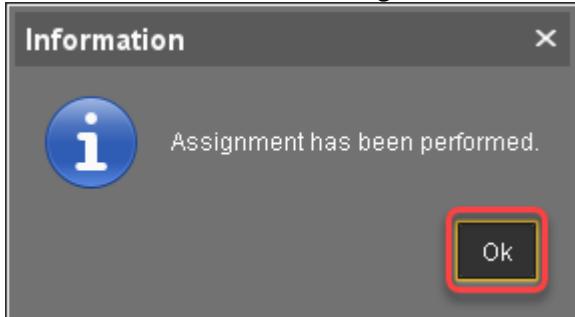


3. In the **Update time** dialog, select **Now** and click **Ok**.





4. Confirm the **Information** dialog.



The target machines download the ISO file. This may take a few minutes.

#### Monitoring the Process

1. In the structure tree of the UMS, open the context menu of one of the target machines and select **Other commands > Refresh system information**.
2. In the dialog, click **Refresh system information** and then from time to time. In the **Attribute** area, under **Firmware Description**, the current status of the OSC installation is shown.



/Devices/Doku-HS-OSCW

### Doku-HS-OSCW

| Attribute       | Value        |
|-----------------|--------------|
| Name            | Doku-HS-OSCW |
| Site            |              |
| Comment         |              |
| Department      |              |
| Cost Center     |              |
| Asset ID        |              |
| In-Service Date |              |
| Serial Number   |              |

▼ Advanced System Information

| Attribute                                        | Value                         |
|--------------------------------------------------|-------------------------------|
| Unit ID                                          | 00505693A2F0                  |
| MAC Address                                      | 00:50:56:93:A2:F0             |
| Last IP                                          | 172.30.91.118                 |
| Product                                          | IGEL Unified Management Agent |
| Product ID                                       | OSCW                          |
| Version                                          | 1.01.100                      |
| Firmware Description                             | IGEL OSC Downloading 55%      |
| IGEL Cloud Gateway                               |                               |
| Expiration Date of OS10-Maintenance Subscription |                               |
| Last Boot Time                                   |                               |
| Network Name (at Boot Time)                      | Doku-HS-OSCW                  |
| Runtime since last Boot                          |                               |
| Total Operating Time                             |                               |
| Battery Level                                    |                               |
| CPU Speed (MHz)                                  |                               |
| CPU Type                                         |                               |
| Flash Size (MB)                                  |                               |
| Memory Size (MB)                                 |                               |
| Network Speed                                    |                               |
| Duplex Mode                                      |                               |
| Graphics Chipset 1                               |                               |

When a device is ready, the value of **Firmware Description** changes to "IGEL OSC Ready for"



Conversion".

| /Devices/Doku-HS-OSCW                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|-----------|-------|---------|--------------|-------------|-------------------|---------|---------------|------------|-------------------------------|-------------|------|---------|----------|-----------------------------|-------------------------------|--------------------|--|--------------------------------------------------|--|----------------|--|-----------------------------|--------------|-------------------------|--|----------------------|--|---------------|--|-----------------|--|----------|--|-----------------|--|------------------|--|---------------|--|-------------|--|--------------------|--|
| <b>Doku-HS-OSCW</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| <table border="1"> <thead> <tr> <th>Attribute</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td>Doku-HS-OSCW</td> </tr> <tr> <td>Site</td> <td></td> </tr> <tr> <td>Comment</td> <td></td> </tr> <tr> <td>Department</td> <td></td> </tr> <tr> <td>Cost Center</td> <td></td> </tr> <tr> <td>AssetID</td> <td></td> </tr> <tr> <td>In-Service Date</td> <td></td> </tr> <tr> <td>Serial Number</td> <td></td> </tr> </tbody> </table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                               | Attribute | Value | Name    | Doku-HS-OSCW | Site        |                   | Comment |               | Department |                               | Cost Center |      | AssetID |          | In-Service Date             |                               | Serial Number      |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Attribute                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Value                         |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Doku-HS-OSCW                  |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Site                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Comment                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Department                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Cost Center                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| AssetID                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| In-Service Date                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Serial Number                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| <b>▼ Advanced System Information</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| <table border="1"> <thead> <tr> <th>Attribute</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Unit ID</td> <td>00505693A2F0</td> </tr> <tr> <td>MAC Address</td> <td>00:50:56:93:A2:F0</td> </tr> <tr> <td>Last IP</td> <td>172.30.91.118</td> </tr> <tr> <td>Product</td> <td>IGEL Unified Management Agent</td> </tr> <tr> <td>Product ID</td> <td>OSCW</td> </tr> <tr> <td>Version</td> <td>1.01.100</td> </tr> <tr> <td><b>Firmware Description</b></td> <td>IGEL OSC Ready for Conversion</td> </tr> <tr> <td>IGEL Cloud Gateway</td> <td></td> </tr> <tr> <td>Expiration Date of OS10-Maintenance Subscription</td> <td></td> </tr> <tr> <td>Last Boot Time</td> <td></td> </tr> <tr> <td>Network Name (at Boot Time)</td> <td>Doku-HS-OSCW</td> </tr> <tr> <td>Runtime since last Boot</td> <td></td> </tr> <tr> <td>Total Operating Time</td> <td></td> </tr> <tr> <td>Battery Level</td> <td></td> </tr> <tr> <td>CPU Speed (MHz)</td> <td></td> </tr> <tr> <td>CPU Type</td> <td></td> </tr> <tr> <td>Flash Size (MB)</td> <td></td> </tr> <tr> <td>Memory Size (MB)</td> <td></td> </tr> <tr> <td>Network Speed</td> <td></td> </tr> <tr> <td>Duplex Mode</td> <td></td> </tr> <tr> <td>Graphics Chipset 1</td> <td></td> </tr> </tbody> </table> |                               | Attribute | Value | Unit ID | 00505693A2F0 | MAC Address | 00:50:56:93:A2:F0 | Last IP | 172.30.91.118 | Product    | IGEL Unified Management Agent | Product ID  | OSCW | Version | 1.01.100 | <b>Firmware Description</b> | IGEL OSC Ready for Conversion | IGEL Cloud Gateway |  | Expiration Date of OS10-Maintenance Subscription |  | Last Boot Time |  | Network Name (at Boot Time) | Doku-HS-OSCW | Runtime since last Boot |  | Total Operating Time |  | Battery Level |  | CPU Speed (MHz) |  | CPU Type |  | Flash Size (MB) |  | Memory Size (MB) |  | Network Speed |  | Duplex Mode |  | Graphics Chipset 1 |  |
| Attribute                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Value                         |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Unit ID                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 00505693A2F0                  |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| MAC Address                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 00:50:56:93:A2:F0             |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Last IP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 172.30.91.118                 |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Product                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | IGEL Unified Management Agent |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Product ID                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | OSCW                          |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Version                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 1.01.100                      |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| <b>Firmware Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | IGEL OSC Ready for Conversion |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| IGEL Cloud Gateway                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Expiration Date of OS10-Maintenance Subscription                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Last Boot Time                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Network Name (at Boot Time)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Doku-HS-OSCW                  |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Runtime since last Boot                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Total Operating Time                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Battery Level                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| CPU Speed (MHz)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| CPU Type                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Flash Size (MB)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Memory Size (MB)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Network Speed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Duplex Mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |
| Graphics Chipset 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                               |           |       |         |              |             |                   |         |               |            |                               |             |      |         |          |                             |                               |                    |  |                                                  |  |                |  |                             |              |                         |  |                      |  |               |  |                 |  |          |  |                 |  |                  |  |               |  |             |  |                    |  |

- When **Firmware Description** reads "IGEL OSC Ready for Conversion", continue with [Starting the Conversion](#)(see page 1381).

#### Check List

- The conversion profile is assigned to all target machines.
- All target machines have downloaded the IGEL OS 11 Creator (ISO), which is indicated by the **Firmware Description** "IGEL OS Ready for Conversion".

#### Next Step

>> [Starting the Conversion](#)(see page 1381)



## Configuring the OSCW Installer in Buddy Mode

The target machines that are designated as update buddies download the ISO file containing the IGEL OS firmware from the UMS. When they have downloaded the file, the remaining target machines download it from the update buddies.

Make sure that all devices are joined to a Microsoft Active Directory and are accessible by the same AD user with reading permissions.

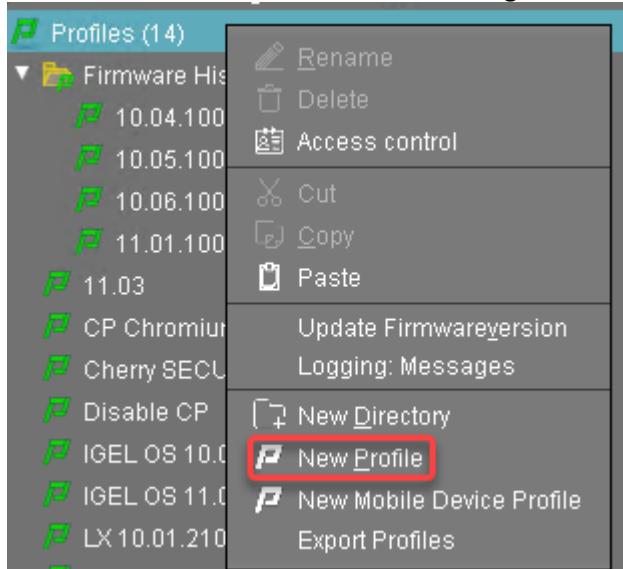
First, we create a profile for the update buddies that provides the OSCW installer with the download source for the ISO file. Then, we will assign this profile to the update buddies; the assignment of the profile triggers the update buddies to download the file. After that, we create a profile for the remaining target machines which configures them to use the update buddies. When the update buddies have downloaded the file, we can assign the profile to the remaining target machines. On assignment, each target machine selects an update buddy automatically and starts downloading the file from it.

The configuration comprises the following steps:

- [Creating a Profile for the Update Buddies](#)(see page 1364)
- [Assigning the Profile to the Update Buddies](#)(see page 1366)
- [Checking if the Update Buddies are ready](#)(see page 1367)
- [Creating a Profile for the Remaining Target Machines](#)(see page 1369)
- [Creating a View to Select the Target Machines](#)(see page 1371)
- [Assigning the Profile to the Target Machines](#)(see page 1376)
- [Monitoring the Process](#)(see page 1378)

### Creating a Profile for the Update Buddies

1. In the structure tree of the UMS Console, go to **Profiles** and open **New Profile** in the context menu.



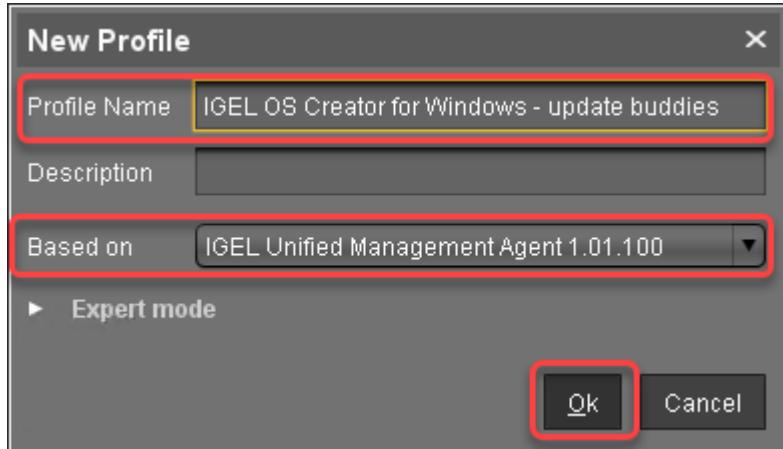
2. In the **New Profile** dialog, change the settings as follows:

- **Profile Name:** A name for the profile, e. g. "IGEL OS Creator for Windows - update buddies"



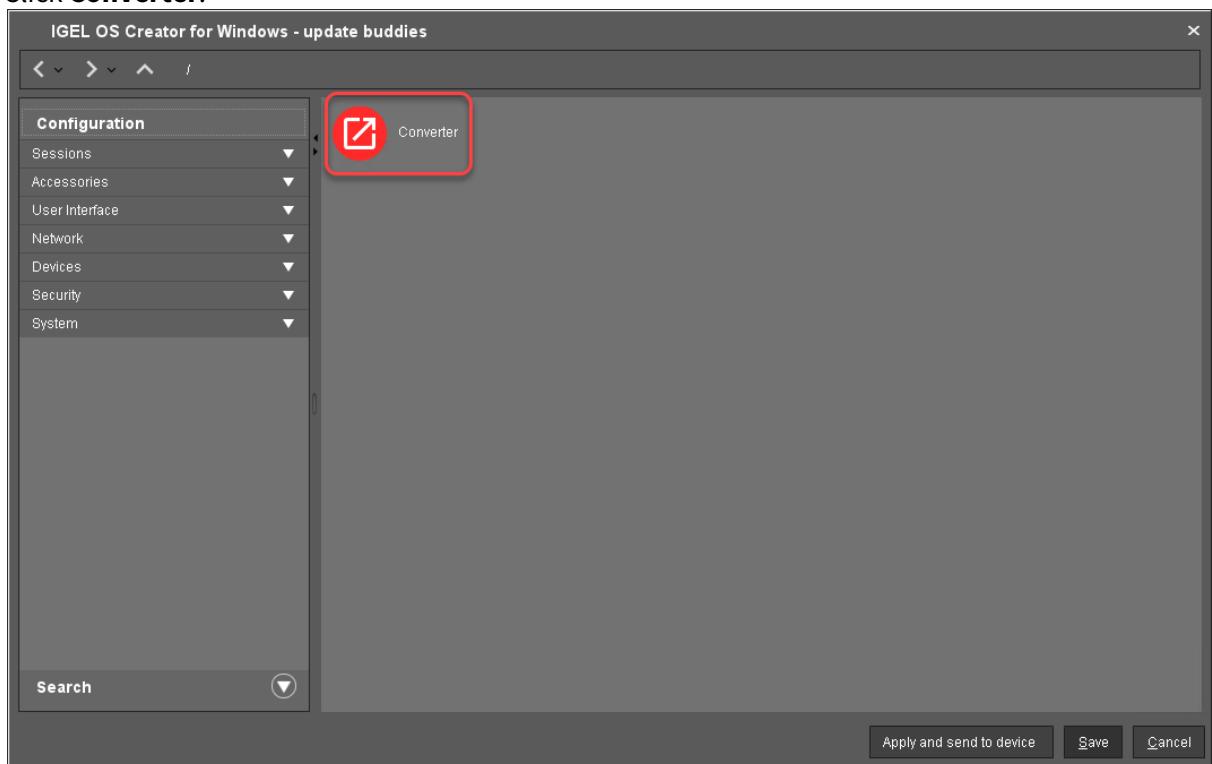
- **Based on:** Select "IGEL Unified Management Agent 1.01.100".

3. Click **Ok**.



The configuration dialog opens.

4. Click **Converter**.



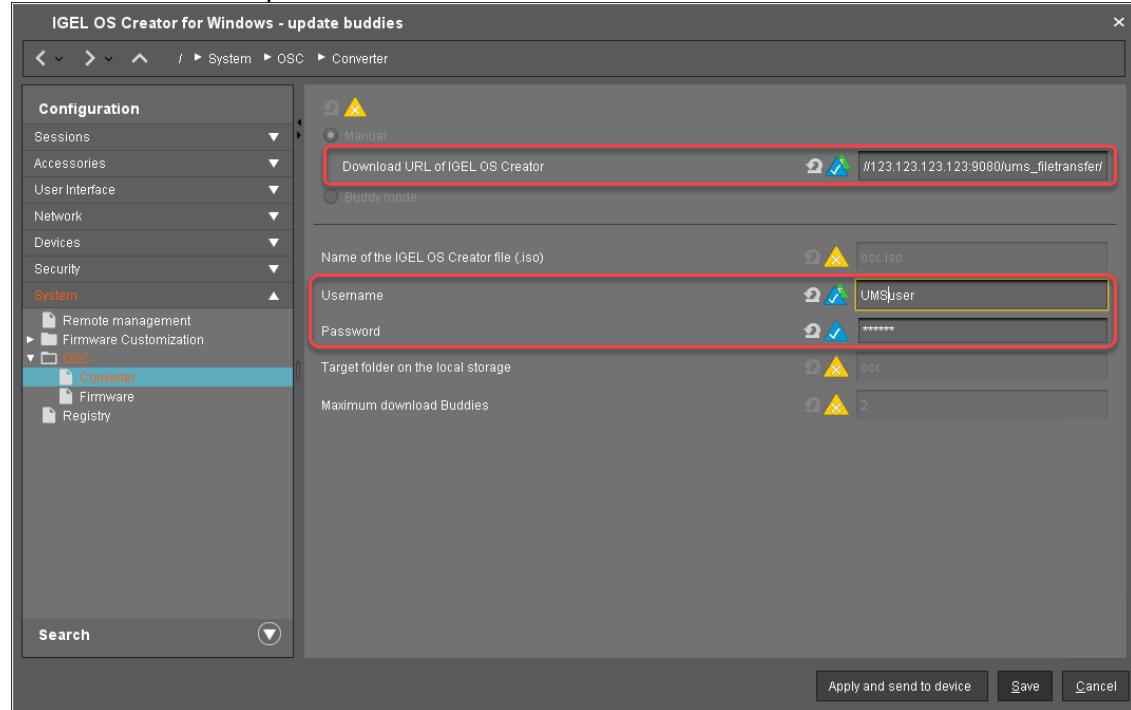
You are taken to **System > OSC > Converter** where you can set all relevant parameters.

5. Change the settings as follows (click the icon to enable the configuration; the icon will change to ):
- **Download URL of IGEL OS Creator:** Enter `https://[IP address of your UMS Server]:8443/ums_filetransfer/` or `http://[IP address of your UMS Server]:9080/ums_filetransfer/`  
Example: `https://192.168.178.100:8443/ums_filetransfer/` or `http://`



192.168.178.100:9080/ums\_filetransfer/

- **Username:** Enter the username for the UMS.
- **Password:** Enter the password for the UMS user.



## 6. Click **Save**.

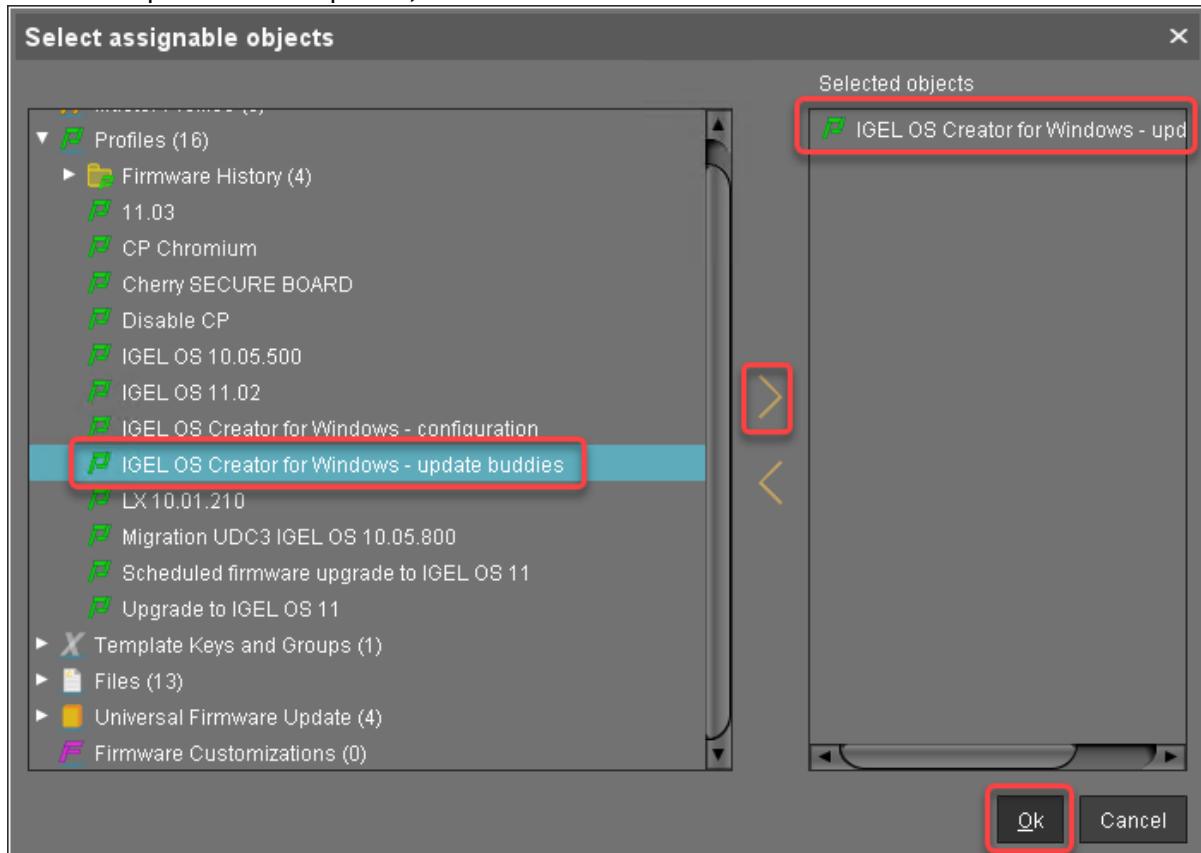
### Assigning the Profile to the Update Buddies

1. In the structure tree of the UMS console, select the machines that will serve as update buddies and click in the **Assigned objects** area.

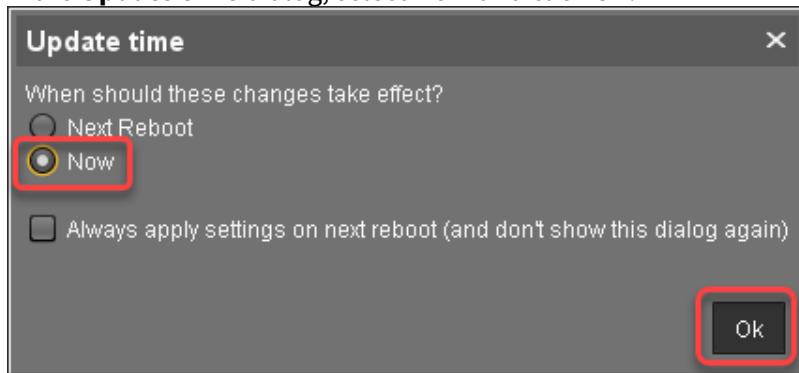




2. Select the update buddies profile, click and then **Ok**.



3. In the **Update time** dialog, select **Now** and click **Ok**.



#### Checking If the Update Buddies Are Ready

Perform the following check for each update buddy:

1. In the structure tree of the UMS, open the context menu of the update buddy and select **Other commands > Refresh system information**.



2. In the dialog, click **Refresh system information** and then every few seconds. In the **Attribute** area, under **Firmware Description**, the current status of the download is shown. When it reads "IGEL OSC Ready for Conversion", the update buddy is ready for use.

/Devices/Doku-HS-OSCW

### Doku-HS-OSCW

| Attribute       | Value        |
|-----------------|--------------|
| Name            | Doku-HS-OSCW |
| Site            |              |
| Comment         |              |
| Department      |              |
| Cost Center     |              |
| AssetID         |              |
| In-Service Date |              |
| Serial Number   |              |

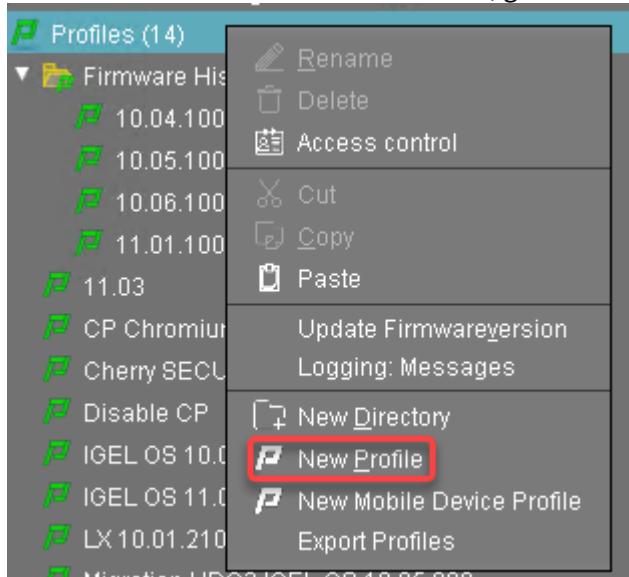
▼ Advanced System Information

| Attribute                                        | Value                         |
|--------------------------------------------------|-------------------------------|
| Unit ID                                          | 00505693A2F0                  |
| MAC Address                                      | 00:50:56:93:A2:F0             |
| Last IP                                          | 172.30.91.118                 |
| Product                                          | IGEL Unified Management Agent |
| Product ID                                       | OSCW                          |
| Version                                          | 1.01.100                      |
| <b>Firmware Description</b>                      | IGEL OSC Ready for Conversion |
| IGEL Cloud Gateway                               |                               |
| Expiration Date of OS10-Maintenance Subscription |                               |
| Last Boot Time                                   |                               |
| Network Name (at Boot Time)                      | Doku-HS-OSCW                  |
| Runtime since last Boot                          |                               |
| Total Operating Time                             |                               |
| Battery Level                                    |                               |
| CPU Speed (MHz)                                  |                               |
| CPU Type                                         |                               |
| Flash Size (MB)                                  |                               |
| Memory Size (MB)                                 |                               |
| Network Speed                                    |                               |
| Duplex Mode                                      |                               |
| Graphics Chipset                                 |                               |



## Creating a Profile for the Remaining Target Machines

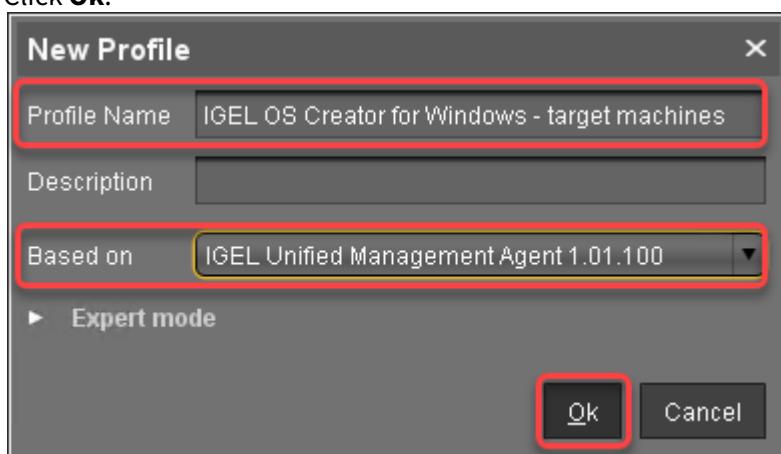
1. In the structure tree of the UMS Console, go to **Profiles** and open **New Profile** in the context menu.



2. In the **New Profile** dialog, change the settings as follows:

- **Profile Name:** A name for the profile, e. g. "IGEL OS Creator for Windows - target machines"
- **Based on:** Select "IGEL Unified Management Agent 1.01.100".

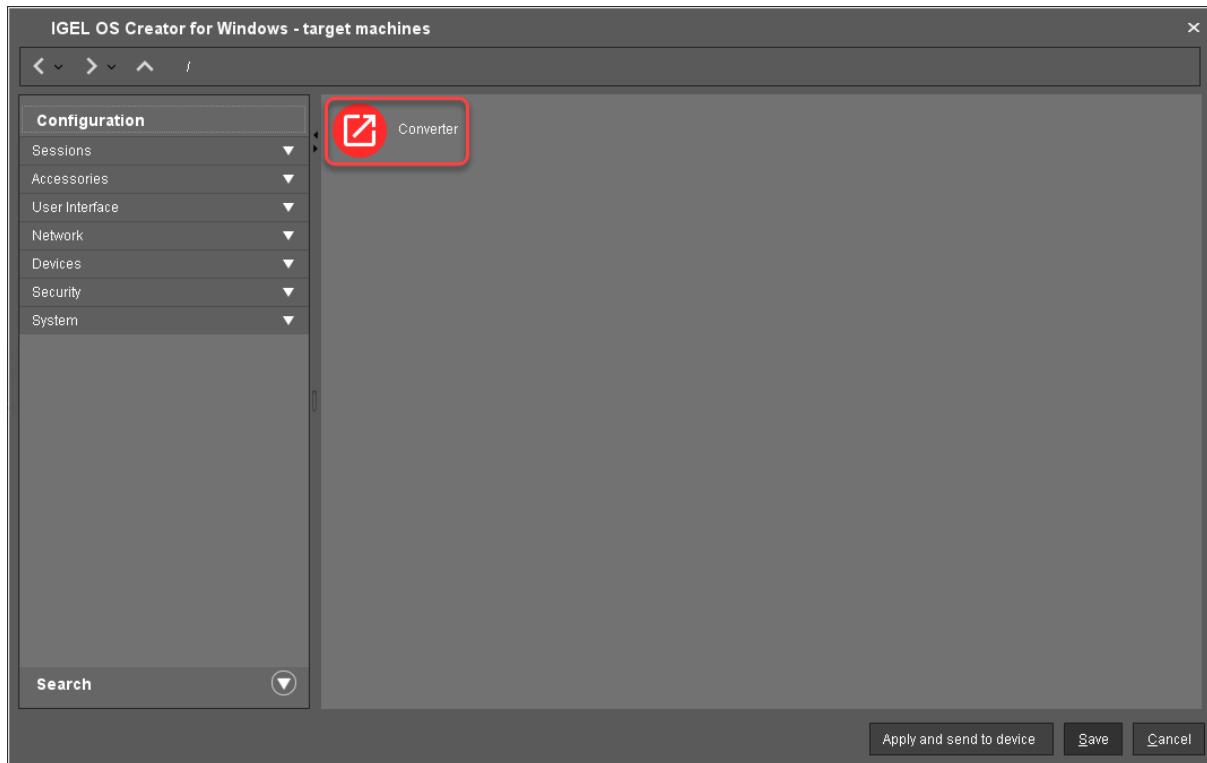
3. Click **Ok**.



The configuration dialog opens.



4. Click **Converter**.

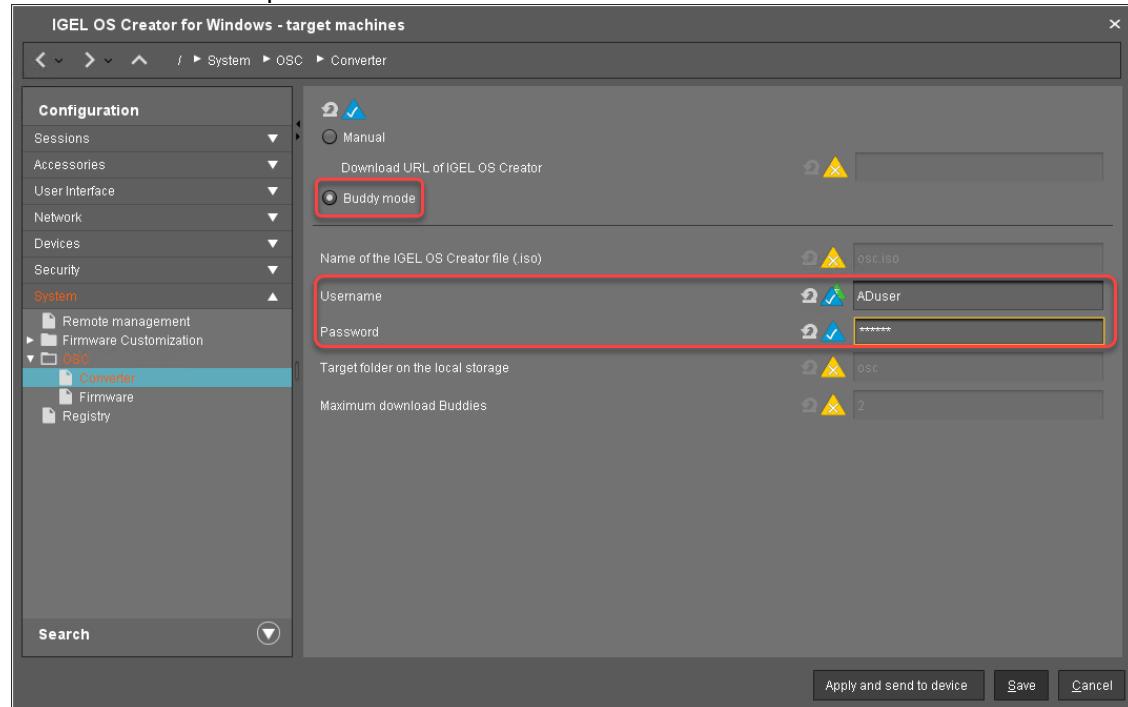


You are taken to **System > OSC > Converter** where you can set all relevant parameters.

5. Change the settings as follows (click the icon to enable the configuration; the icon will change to ):
- Select **Buddy Mode**.
  - **Username:** Common username in Microsoft Active Directory for all target machines, including the update buddies.



- **Password:** Common password associated with the **Username**.

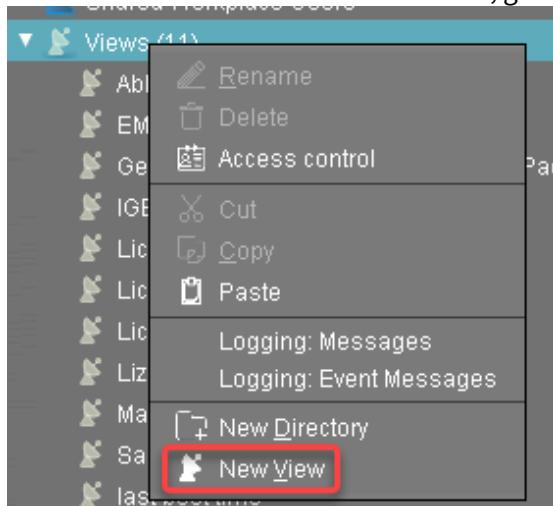


6. Click **Save**.

#### Creating a View to Select the Target Machines

The target machines must be selected in order to assign the profile to them. For the selection, a view will be used.

1. In the structure tree of the UMS Console, go to **Views** and select **New View** in the context menu.





2. Enter a name for the view, e. g. "IGEL OS Creator for Windows - target machines" and click **Next**.

**Create new view**

**View name**

Name

Description

Expert mode

The "Next" button is highlighted with a red rectangular border.



3. On the **Select criterion** page, select **Product ID** and click **Next**.

**Create new view**

**Select criterion**

CPU Speed       CPU Type       Device Type  
 Duplex Mode       Firmware Description       Firmware Update (Relative)  
 Firmware Version       Flash Player       Flash Player Version  
 Flash Size       Graphics Chipset 1       Graphics Chipset 2  
 Graphics Memory Size 1       Graphics Memory Size 2       Last Boot Time (Absolute)  
 Last Boot Time (Relative)       Memory Size       Network Name  
 Network Speed       OS Type       Partial Update (Name)  
 Partial Update (Relative)       Partial Update (Version)       Product  
 Product ID       Total Operating Time

**▼ Monitor Information**

Monitor Date of Production       Monitor Model       Monitor Native Resolution

**Back** **Next** **Finish** **Cancel**

A screenshot of a software window titled 'Create new view' with a sub-section 'Select criterion'. A list of various system parameters is shown as radio buttons. The 'Product ID' option is selected and has a red rectangular highlight around it. At the bottom of the window, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel', with the 'Next' button also having a red highlight around it.



4. On the **Text search** page, enter "OSCW" and click **Next**.

The screenshot shows the 'Create new view' dialog with the 'Text search' tab selected. In the search input field, the text 'OSCW' is entered and highlighted with a red box. Below the input field are four optional checkboxes: 'Consider case', 'Compare whole text', 'Use regular expression', and 'Not like'. At the bottom of the dialog are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'. The 'Next >' button is also highlighted with a red box.



5. On the **Create new view** page, click **Finish**.

**Create new view**

**Finish view creation**

Name: IGEL OS Creator for Windows - target machines

Description:

View criteria:  
Product ID is like (?i).\*OSCW.\*

Create view  
 Narrow search criterion (AND)  
 Create additional search criterion (OR)

**Back** **Next** **Finish** **Cancel**

The number of matches is shown.

6. Click **Load devices** to view the target machines.

Name: IGEL OS Creator for Windows - target machines

Description:

Rule: Product ID is like (?i).\*OSCW.\*

Result list was last updated at 1:02 PM. **Load devices** Refresh Settings

One matching device found.

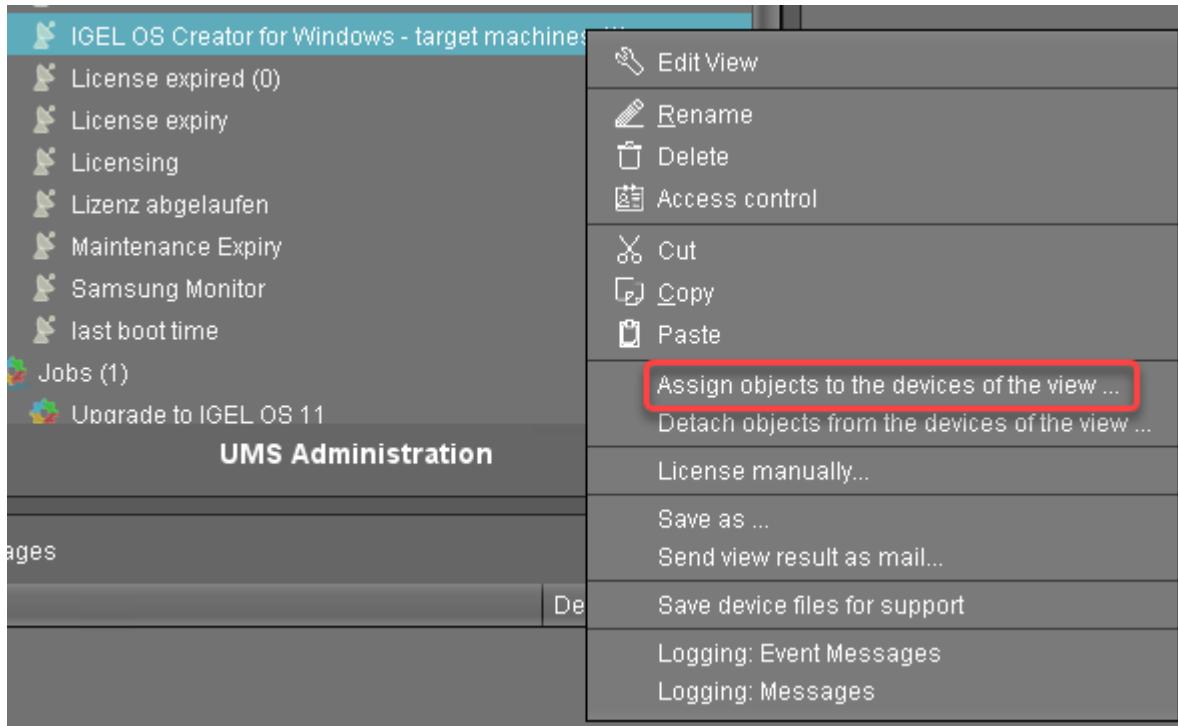
7. The target machines are shown.

| Name                                                             | IGEL OS Creator for Windows - target machines |              |                               |          |
|------------------------------------------------------------------|-----------------------------------------------|--------------|-------------------------------|----------|
| Description                                                      |                                               |              |                               |          |
| Rule                                                             | Product ID is like (?i).*OSCW.*               |              |                               |          |
| Result list was last updated at 1:03 PM. <b>Refresh</b> Settings |                                               |              |                               |          |
| Matching devices (1 device)                                      |                                               |              |                               |          |
| Name                                                             | Last known IP address                         | MAC Address  | Product                       | Version  |
| Doku-HS-OSCW                                                     | 172.30.91.118                                 | 00505693A2F0 | IGEL Unified Management Agent | 1.01.100 |



## Assigning the Profile to the Target Machines

1. Select the view you have created beforehand and select **Assign objects to the devices of the view ....**

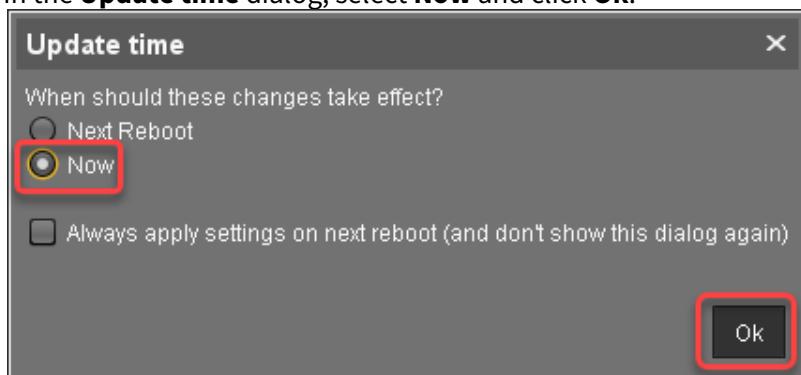




2. In the **Assign objects** dialog, select the profile for the target machines, click to assign it and then click **Ok**.

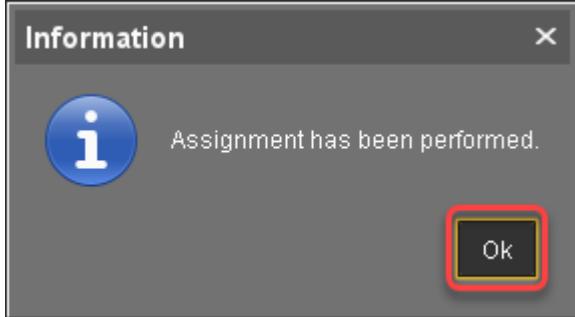


3. In the **Update time** dialog, select **Now** and click **Ok**.





4. Confirm the **Information** dialog.



The target machines download the ISO file.

#### Monitoring the Process

1. In the structure tree of the UMS, open the context menu of one of the target machines and select **Other commands > Refresh system information**.
2. In the dialog, click **Refresh system information** and then every few seconds. In the **Attribute** area, under **Firmware Description**, the current status of the download is shown.



/Devices/Doku-HS-OSCW

### Doku-HS-OSCW

| Attribute       | Value        |
|-----------------|--------------|
| Name            | Doku-HS-OSCW |
| Site            |              |
| Comment         |              |
| Department      |              |
| Cost Center     |              |
| Asset ID        |              |
| In-Service Date |              |
| Serial Number   |              |

▼ Advanced System Information

| Attribute                                        | Value                         |
|--------------------------------------------------|-------------------------------|
| Unit ID                                          | 00505693A2F0                  |
| MAC Address                                      | 00:50:56:93:A2:F0             |
| Last IP                                          | 172.30.91.118                 |
| Product                                          | IGEL Unified Management Agent |
| Product ID                                       | OSCW                          |
| Version                                          | 1.01.100                      |
| Firmware Description                             | IGEL OSC Downloading 55%      |
| IGEL Cloud Gateway                               |                               |
| Expiration Date of OS10-Maintenance Subscription |                               |
| Last Boot Time                                   |                               |
| Network Name (at Boot Time)                      | Doku-HS-OSCW                  |
| Runtime since last Boot                          |                               |
| Total Operating Time                             |                               |
| Battery Level                                    |                               |
| CPU Speed (MHz)                                  |                               |
| CPU Type                                         |                               |
| Flash Size (MB)                                  |                               |
| Memory Size (MB)                                 |                               |
| Network Speed                                    |                               |
| Duplex Mode                                      |                               |
| Graphics Chipset 1                               |                               |

When a device is ready, the value of **Firmware Description** changes to "IGEL OSC Ready for"



Conversion".

| /Devices/Doku-HS-OSCW                            |                               |
|--------------------------------------------------|-------------------------------|
| Doku-HS-OSCW                                     |                               |
| Attribute                                        | Value                         |
| Name                                             | Doku-HS-OSCW                  |
| Site                                             |                               |
| Comment                                          |                               |
| Department                                       |                               |
| Cost Center                                      |                               |
| AssetID                                          |                               |
| In-Service Date                                  |                               |
| Serial Number                                    |                               |
| <b>▼ Advanced System Information</b>             |                               |
| Attribute                                        | Value                         |
| Unit ID                                          | 00505693A2F0                  |
| MAC Address                                      | 00:50:56:93:A2:F0             |
| Last IP                                          | 172.30.91.118                 |
| Product                                          | IGEL Unified Management Agent |
| Product ID                                       | OSCW                          |
| Version                                          | 1.01.100                      |
| Firmware Description                             | IGEL OSC Ready for Conversion |
| IGEL Cloud Gateway                               |                               |
| Expiration Date of OS10-Maintenance Subscription |                               |
| Last Boot Time                                   |                               |
| Network Name (at Boot Time)                      | Doku-HS-OSCW                  |
| Runtime since last Boot                          |                               |
| Total Operating Time                             |                               |
| Battery Level                                    |                               |
| CPU Speed (MHz)                                  |                               |
| CPU Type                                         |                               |
| Flash Size (MB)                                  |                               |
| Memory Size (MB)                                 |                               |
| Network Speed                                    |                               |
| Duplex Mode                                      |                               |
| Graphics Chipset 1                               |                               |

- When **Firmware Description** reads "IGEL OSC Ready for Conversion", continue with [Starting the Conversion](#)(see page 1381).

#### Check List

- The conversion profile is assigned to all target machines.
- All target machines have downloaded the OSCW ISO file, which is indicated by the **Firmware Description** "IGEL OS Ready for Conversion".

#### Next Step

>> [Starting the Conversion](#)(see page 1381)



### 6.1.10 Starting the Conversion

1. In the UMS structure tree, select the view you have created for selecting the target machines, and click **Load devices**.

The screenshot shows a configuration dialog box. At the top, there are fields for 'Name' (set to 'IGEL OS Creator for Windows - target machines'), 'Description', and 'Rule' (set to 'Product ID is like (?i).\*OSCW.\*'). Below these are buttons for 'Result list was last updated at 2:18 PM.', 'Load devices' (which is highlighted with a red box), 'Refresh', and 'Settings'. A message at the bottom states 'One matching device found.'

2. Select all machines and in the context menu, select **Specific Device Command**.

The screenshot shows a list of devices in a table format. The first row, 'Doku-HS-OSCW', is selected and highlighted with a cyan background. A context menu is open over this row, listing various options: Edit Configuration, Rename, Delete, Clear 'Configuration Change Status' flag, Access control, Cut, Copy, Paste, Shadow, Secure Terminal, Suspend, Shutdown, Wake up, Reboot, Update & snapshot commands, Other commands, Specific Device Command (which is highlighted with a red box), Take over settings from ..., Export Device Settings, Save device files for support, Release IGEL Cloud Gateway license, Logging, License manually..., and Scan for devices.



3. In the **Specific Device Command** dialog, select **Convert to IGEL OS** and click **Execute**.



On the devices, a dialog is displayed. When the dialog is confirmed, the conversion starts immediately. If the dialog is not confirmed, the conversion starts after 20 seconds.

When the conversion is complete, the **Product** information in the UMS is changed to "IGEL OS 11".

## 6.2 IGEL OS Creator for Windows (OSCW) on IGEL Windows Embedded 7/7+

The IGEL OS Creator (OSC) for Windows is able to convert any device that is running IGEL Windows Embedded 7/7+ to IGEL OS 11. The IGEL OS Creator (OSC) for Windows is integrated into version 3.13.150 of IGEL Windows Embedded 7 and into version 3.14.110 of IGEL Windows Embedded 7+.

Read all the following chapters and follow the instructions in the order given.

1. [Prerequisites](#)(see page 1383)
2. [Getting the Required Software](#)(see page 1383)
3. [Updating the IGEL WES7/7+ Devices](#)(see page 1384)
4. [Transferring the IGEL OS 11 Firmware to the UMS](#)(see page 1389)
5. [Configuring the OSCW Installer](#)(see page 1389)
6. [Starting the Conversion](#)(see page 1400)



## 6.2.1 Prerequisites

### Network

- All machines are registered with the UMS.

### Next Step

>> When all requirements are met, continue with [Getting the Required Software](#)(see page 1383).

## 6.2.2 Getting the Required Software

The following software must be downloaded resp. installed:

### IGEL Universal Management Suite (UMS) 6.04.120 or Higher

1. Download UMS 6.04.120 or higher from <https://www.igel.com/software-downloads/workspace-edition/> > **Universal Management Suite**.
2. Update your UMS to version 6.04.120 or later. For update instructions, see [Updating UMS](#)<sup>370</sup>.

### IGEL OS 11

- Download IGEL OS 11.03.500 or higher from <https://www.igel.com/software-downloads/workspace-edition/> > **OS 11** > **FIRMWARE UPDATES**.

### IGEL WES 7/7+

- For IGEL WES 7 devices, download version 3.13.150.
- For IGEL WES 7+ devices, download version 3.14.110\_W7+.

### Check List

- ✓ The UMS is updated to version 6.04.120 or higher.
- ✓ The required firmware versions for IGEL WES7/7+ devices are available.
- ✓ The firmware files for IGEL OS 11.03.500 or higher are available.

### Next Step

>> [Updating the IGEL WES7/7+ Devices](#)(see page 1384)

---

<sup>370</sup> <https://kb.igel.com/display/endpointmgmt604/Updating+UMS>



### 6.2.3 Updating the IGEL WES7/7+ Devices

In this step, we will update the devices to the IGEL WES 7/7+ version that is capable of converting the device to IGEL OS 11.

For IGEL WES 7 devices, you use `UniversalDesktopWES-3.13.150.snp`; for IGEL WES 7+ devices, you use `UniversalDesktopWES7+-3.14.110.snp` as the snapshot file. If you have both device types, perform the steps described below for each device type separately.

After the update, you can update to another firmware only via IGEL rescue shell!

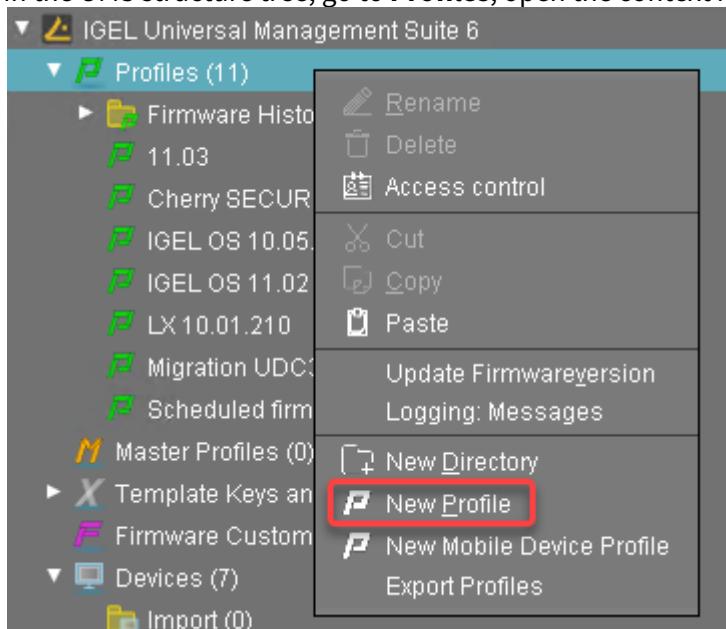
#### Transferring the Snapshot File to the UMS

The snapshot file must be placed in the file system of the UMS Server.

1. Get access to the file system of the machine on which your UMS Server is running.
2. Unzip the snapshot file to <UMS Installation directory>\rmguiserver\webapps\ums\_filetransfer

#### Creating an Update Profile

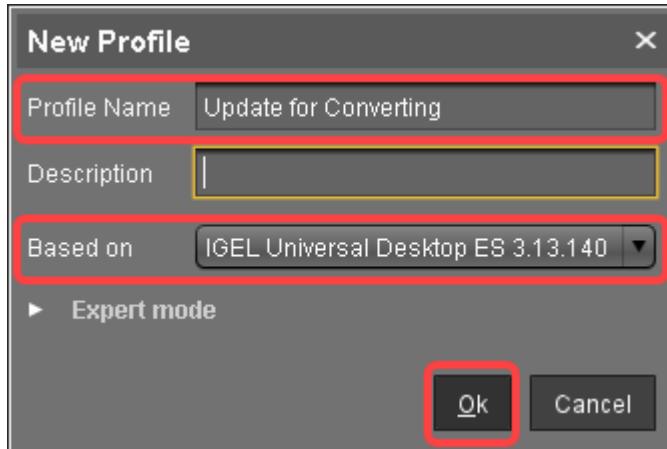
1. In the UMS structure tree, go to **Profiles**, open the context menu, and select **New Profile**.



2. Enter the following data:
  - Profile Name:** Name for the profile, e. g. "Update for Converting".
  - Description:** Optional description for the profile.
  - Based on:** Firmware version for the profile; select the current firmware of your devices.

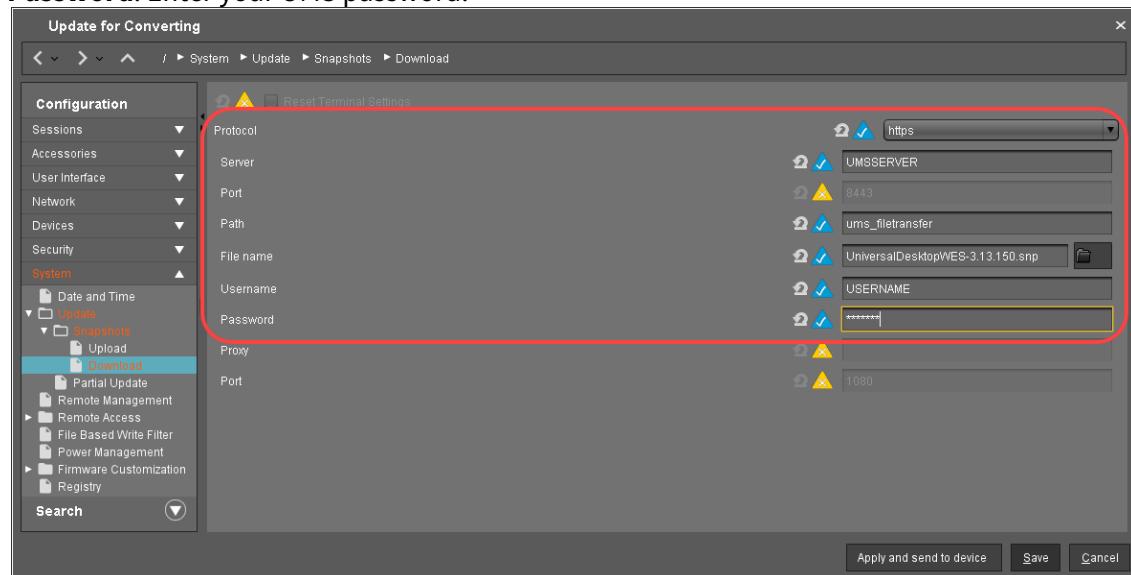


3. Click **Ok**.



4. Go to **System > Update > Snapshots > Download** and change the settings as follows:

- **Protocol:** Select "https".
- **Server:** Enter the IP address or hostname of the UMS.
- **Path:** Enter "ums\_filetransfer".
- **File name:** Enter the file name of the snapshot file.
- **Username:** Enter your UMS user name.
- **Password:** Enter your UMS password.

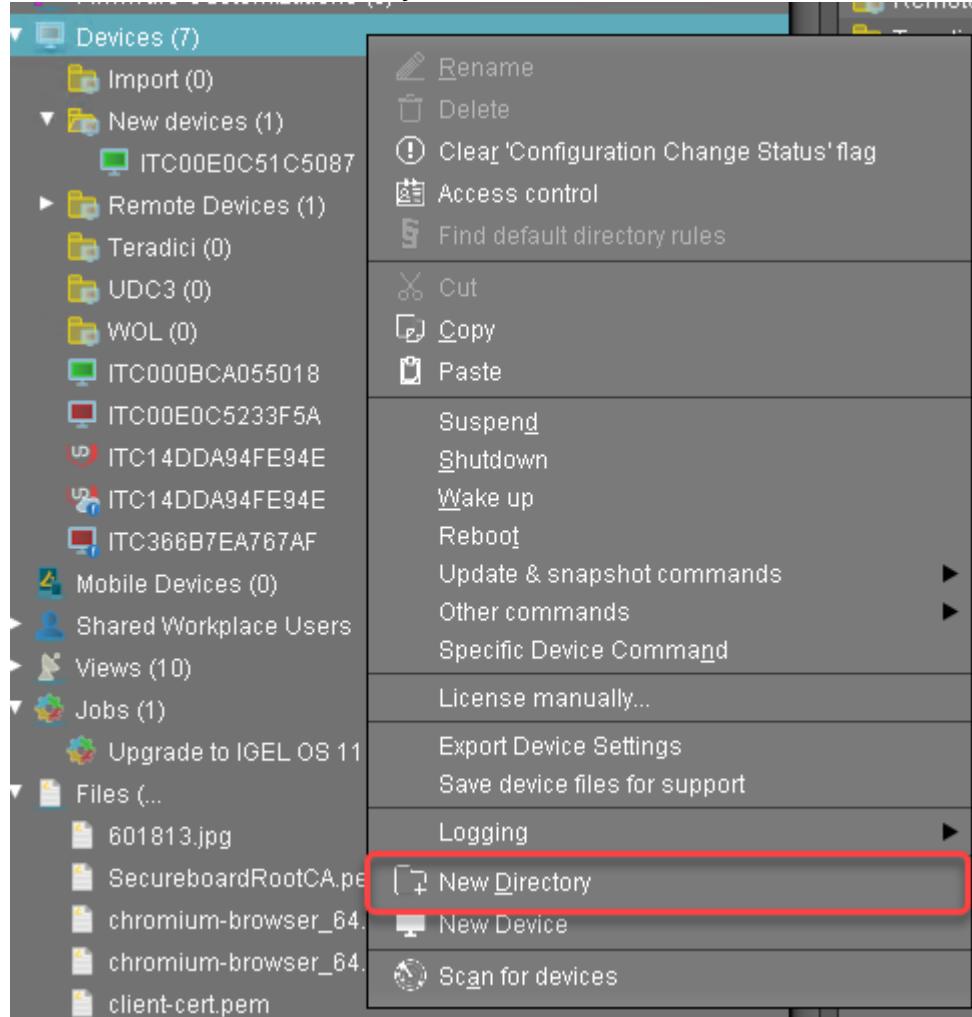


5. Click **Save** to save the profile.



## Starting the Update

1. Under **Devices**, create a directory and name it "Convert to IGEL OS 11", for instance.

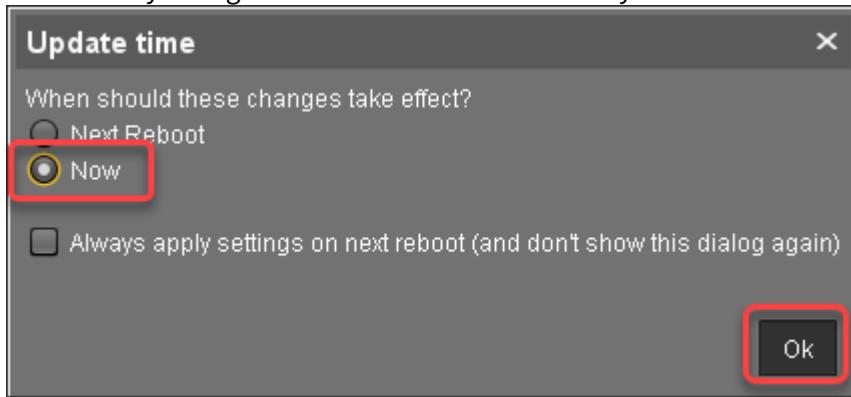


2. Put the devices that are to be updated into the new directory. You can use drag & drop.

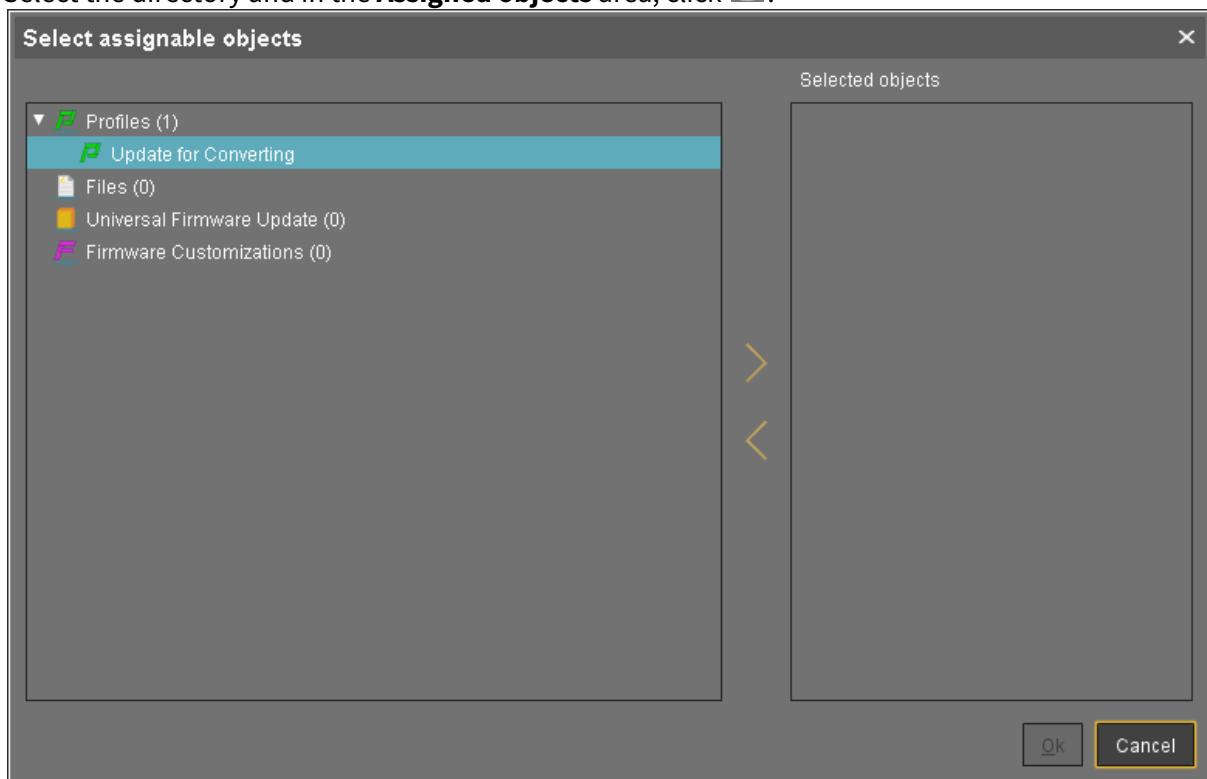


3. In the **Update time** dialog, select **Now** and click **Ok**.

The directory change is communicated immediately to the device.

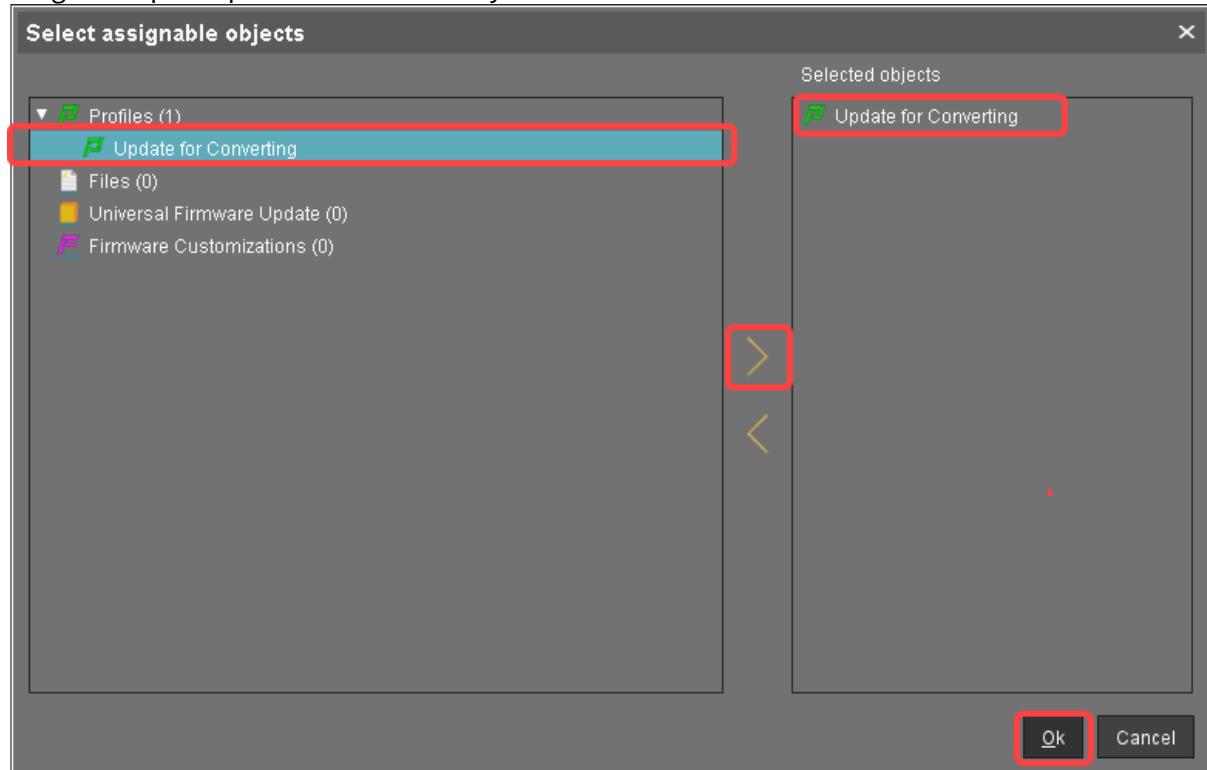


4. Select the directory and in the **Assigned objects** area, click **+**.

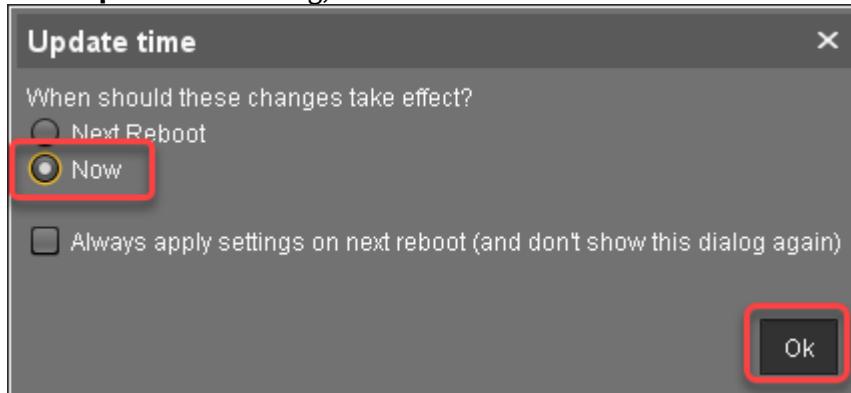




5. Assign the update profile to the directory and click **Ok**.



6. In the **Update time** dialog, select **Now** and click **Ok**.



The changes are sent to the devices immediately.

7. Go to the directory that contains the devices that are to be updated, open the context menu, and select **Update & snapshot commands > Update**.  
The update process is started.

8. When the update process is finished, go to one of the devices and click to refresh the screen.  
In the **Advanced System Information** area, **Product** is set to "IGEL Unified Management Agent",



and **Product ID** is set to "OSCW".

| Attribute       | Value           |
|-----------------|-----------------|
| Name            | IGEL-CXQY1D374I |
| Site            |                 |
| Comment         |                 |
| Department      |                 |
| Cost Center     |                 |
| Asset ID        |                 |
| In-Service Date |                 |
| Serial Number   |                 |

| Attribute                                        | Value                         |
|--------------------------------------------------|-------------------------------|
| Unit ID                                          | 00505693842A                  |
| MAC Address                                      | 00:50:56:93:84:2A             |
| Last IP                                          | 172.30.0.121                  |
| <b>Product</b>                                   | IGEL Unified Management Agent |
| <b>Product ID</b>                                | OSCW                          |
| Version                                          | 1.0.1.120                     |
| Firmware Description                             | IGEL Cloud Gateway            |
| Expiration Date of OS10-Maintenance Subscription | Jun 2, 2020 6:54 AM           |
| Last Boot Time                                   |                               |
| Network Name (at Boot Time)                      | (IGEL-CXQY1D374I)             |
| Runtime since last Boot                          |                               |

## Check List

- ✓ The devices are updated to version 3.13.150 (WES 7) or 3.14.110 (WES 7+).

## Next Step

>> [Transferring the IGEL OS 11 Firmware to the UMS](#)(see page 1389)

### 6.2.4 Transferring the IGEL OS 11 Firmware to the UMS

In this step, we will transfer the IGEL OS 11 firmware files to the UMS so that the target machines can fetch it from there.

1. Get access to the file system of the machine on which your UMS Server is running.
2. Unzip the firmware files to <UMS Installation directory>\rmguiserver\webapps\ums\_filetransfer

## Check List

- ✓ The IGEL OS firmware files are located in the /ums\_filetransfer/ directory of the UMS.

## Next Step

>> [Configuring the OSCW Installer](#)(see page 1389)

### 6.2.5 Configuring the OSCW Installer

In this step, we will provide the OSCW installer with the download source for the IGEL OS firmware.

Two methods are available:



- **Configuring the OSCW Installer in Normal Mode**([see page 1390](#)): Each target machine downloads the firmware files from the UMS individually. This increases the amount of outgoing traffic from the UMS.
- **Configuring the OSCW Installer in Buddy Mode**([see page 1394](#)): This method is recommended if the connection bandwidth of the download source is limited; it ensures a more balanced use of network bandwidth during the distribution of the firmware files to the target machines. First, a group of target machines is converted to IGEL OS 11. Then, these machines are configured to serve as buddy update servers for the remaining target machines.

## Configuring the OSCW Installer in Normal Mode

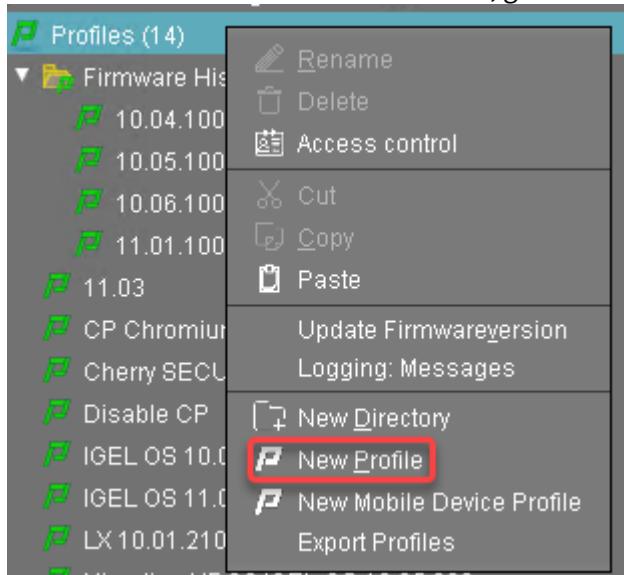
To provide the OSCW installer with the download source for the IGEL OS firmware files, we will create a profile that provides the path to those files.

The configuration comprises the following steps:

- [Creating a Profile](#)([see page 1390](#))
- [Assigning the Profile to the Target Machines](#)([see page 1392](#))

### Creating a Profile

1. In the structure tree of the UMS Console, go to **Profiles** and open **New Profile** in the context menu.

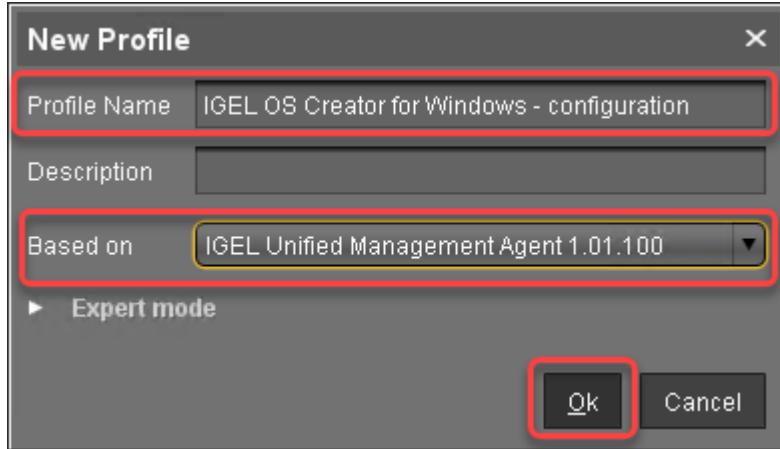


2. In the **New Profile** dialog, change the settings as follows:

- **Profile Name:** A name for the profile, e. g. "IGEL OS Creator for Windows - configuration"
- **Based on:** Select "IGEL Unified Management Agent 1.xx.xxx", e. g. "IGEL Unified Management Agent 1.01.100".



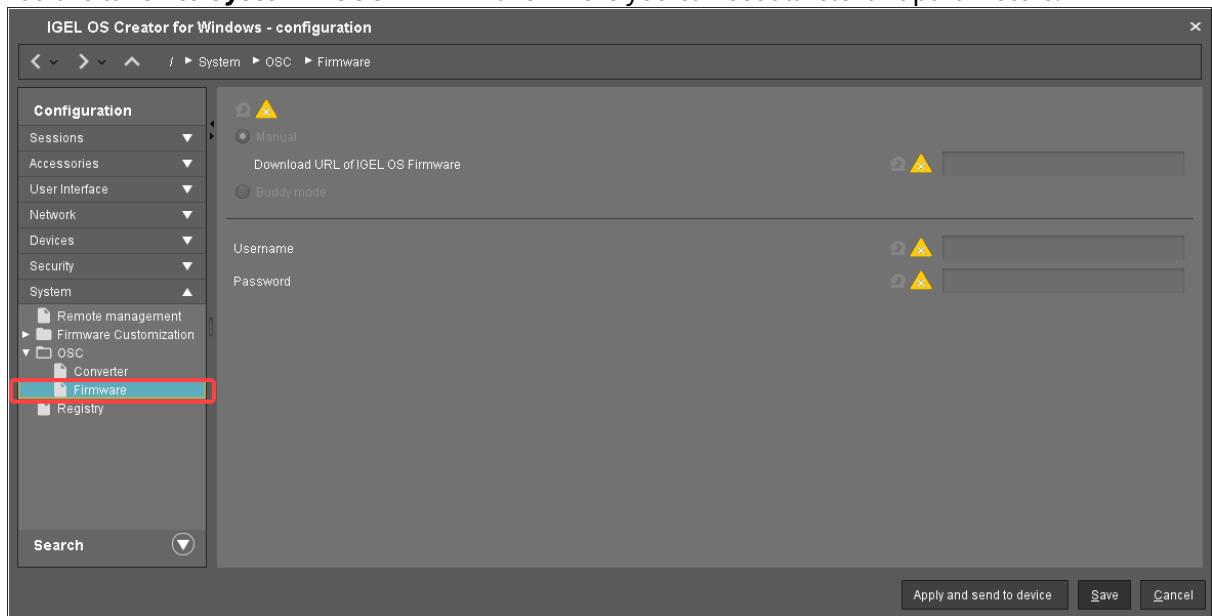
3. Click **Ok**.



The configuration dialog opens.

4. Click **Firmware**.

You are taken to **System > OSC > Firmware** where you can set all relevant parameters.

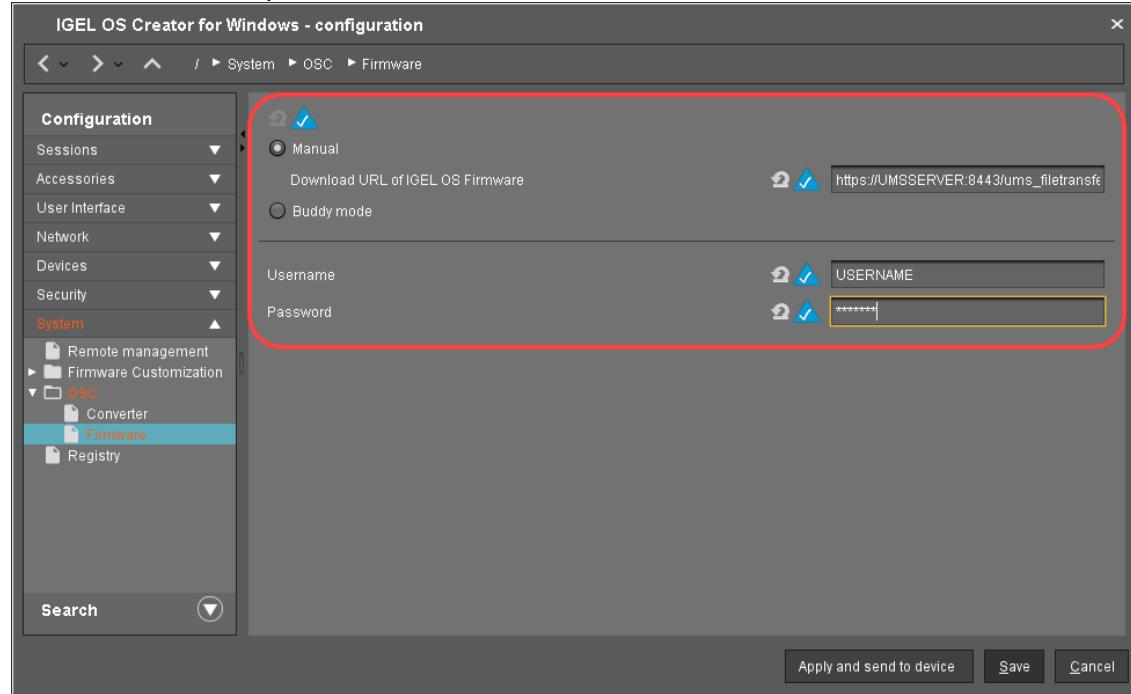


5. Change the settings as follows (click the icon to enable the configuration; the icon will change to ):

- **Download URL of IGEL OS Firmware:** Enter `https://[IP address of your UMS Server]:8443/ums_filetransfer/` or `http://[IP address of your UMS Server]:9080/ums_filetransfer/`  
Example: `https://192.168.178.100:8443/ums_filetransfer/` or `http://192.168.178.100:9080/ums_filetransfer/`
- **Username:** Enter the username for the UMS.



- **Password:** Enter the password for the UMS user.



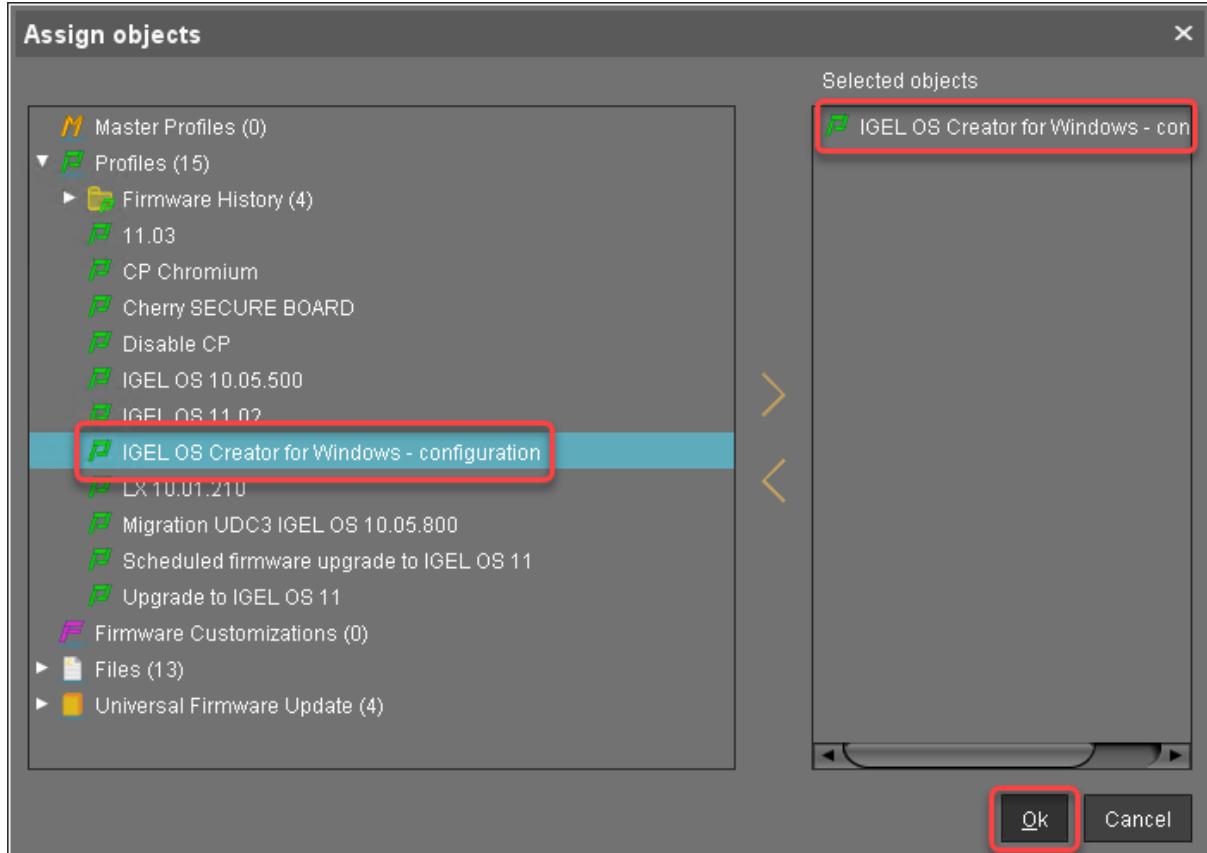
## 6. Click **Save**.

### Assigning the Profile to the Target Machines

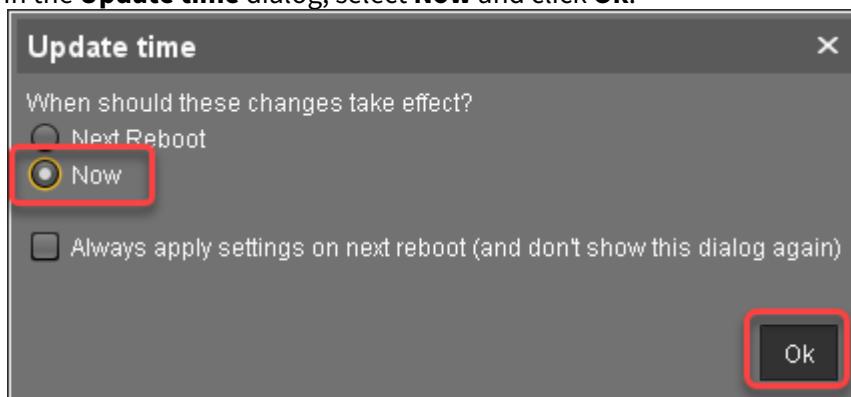
1. Select the directory that contains your target machines and in the **Assigned objects** area, click



2. In the **Assign objects** dialog, select the profile you have created beforehand, click to assign it and then click **Ok**.

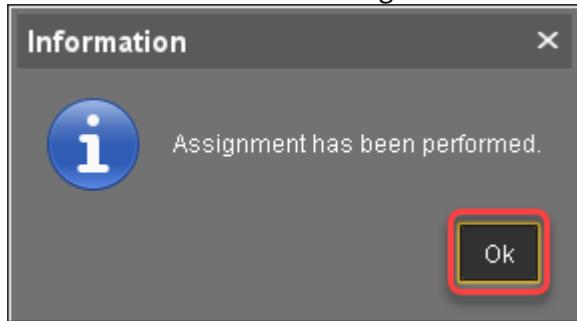


3. In the **Update time** dialog, select **Now** and click **Ok**.





4. Confirm the **Information** dialog.



Check List

- The conversion profile is assigned to all target machines.

Next Step

>> [Starting the Conversion\(see page 1400\)](#)

### Configuring the OSCW Installer in Buddy Mode

When buddy update is used, one or more machines convert to IGEL OS first and then serve as buddy update servers.

The configuration comprises the following steps:

- [Setting up the Buddy Update Servers\(see page 1394\)](#)
- [Creating a Profile for the Buddy Update Clients\(see page 1395\)](#)
- [Assigning the Profile to the Target Machines\(see page 1397\)](#)

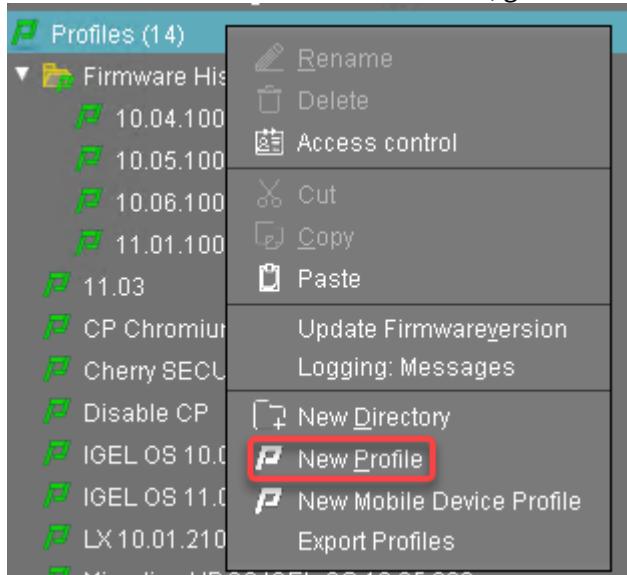
#### Setting Up the Buddy Update Servers

1. Convert the machines that are to be used as buddy update servers as described under [Configuring the OSCW Installer in Normal Mode\(see page 1390\)](#) and [Starting the Conversion\(see page 1400\)](#).
2. Configure the converted machines as buddy update servers as described under [Configuring the Buddy Update Server\(see page 223\)](#), "Basic Configuration".



## Creating a Profile for the Buddy Update Clients

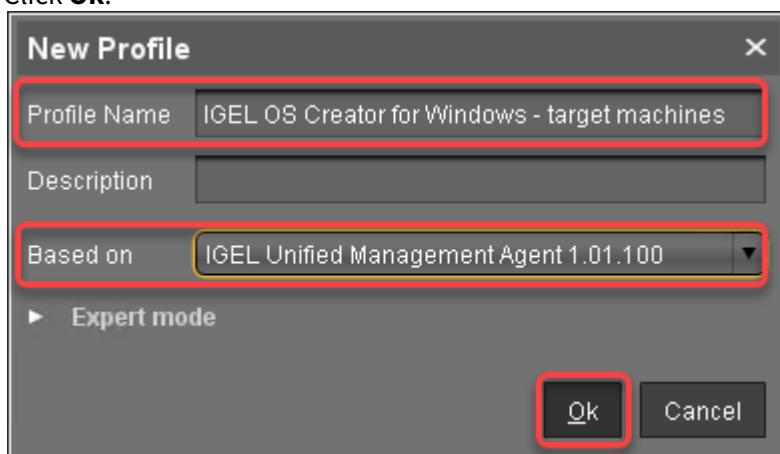
1. In the structure tree of the UMS Console, go to **Profiles** and open **New Profile** in the context menu.



2. In the **New Profile** dialog, change the settings as follows:

- **Profile Name:** A name for the profile, e. g. "IGEL OS Creator for Windows - target machines"
- **Based on:** Select "IGEL Unified Management Agent 1.xx.xxx", e. g. "IGEL Unified Management Agent 1.01.100".

3. Click **Ok**.



The configuration dialog opens.



#### 4. Click **Firmware**.

You are taken to **System > OSC > Firmware** where you can set all relevant parameters.

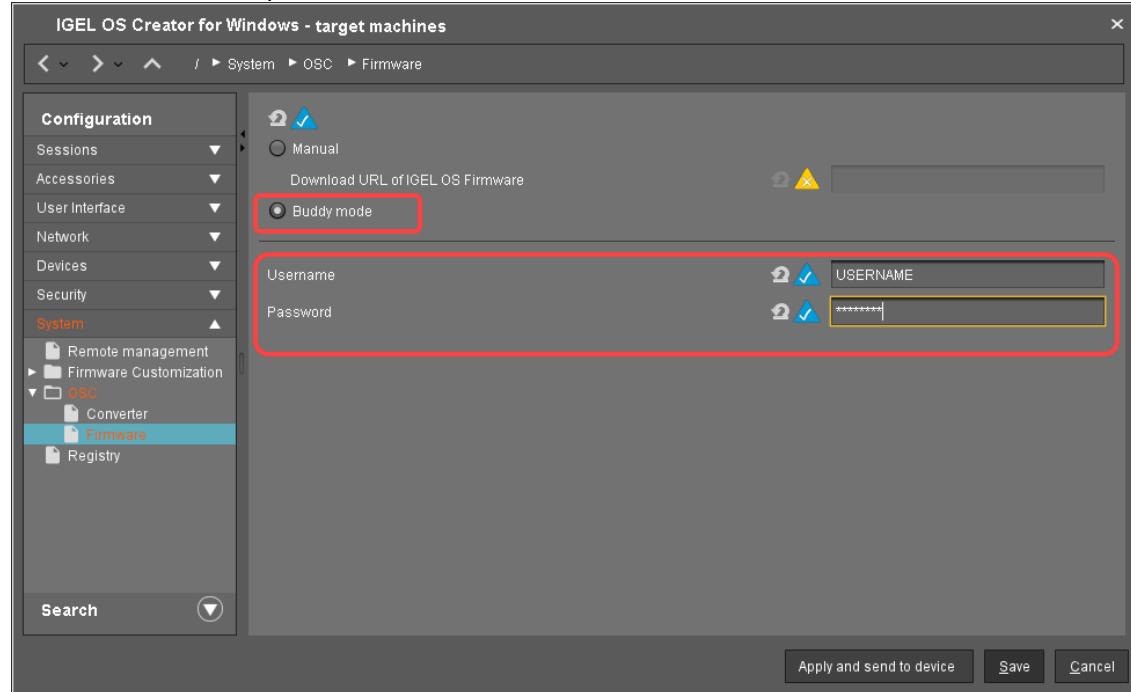
A screenshot of the "IGEL OS Creator for Windows - target machines" software window. The left sidebar shows a navigation tree with sections like Configuration, Sessions, Accessories, User Interface, Network, Devices, Security, System, OSC, Converter, Registry, and a search bar. The "Firmware" item under the OSC section is highlighted with a red border. The main right panel displays configuration settings for Firmware. It includes a "Manual" tab selected, a "Download URL of IGEL OS Firmware" input field, a "Buddy mode" tab, and fields for "Username" and "Password". Each setting has a yellow triangle icon with an 'X' to its left, indicating it's not yet configured. At the bottom right are "Apply and send to device", "Save", and "Cancel" buttons.

#### 5. Change the settings as follows (click the icon to enable the configuration; the icon will change to ):

- Select **Buddy mode**.
- **Username:** Username that is configured on the buddy update servers.



- **Password:** Common password associated with the **Username**.



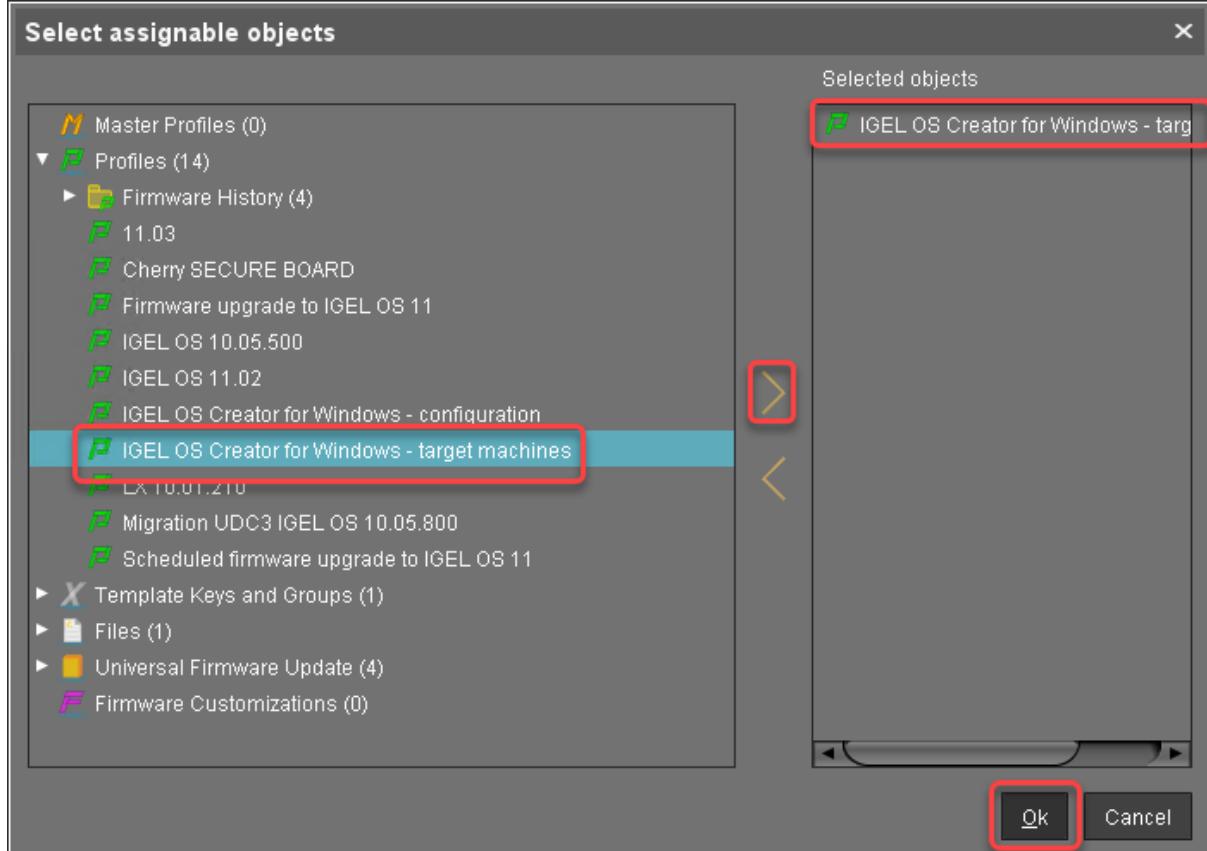
## 6. Click **Save**.

Assigning the Profile to the Buddy Update Clients

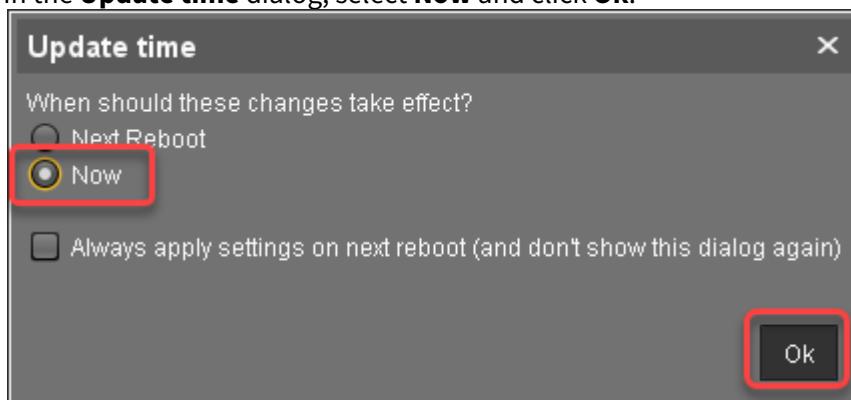
1. Select the directory that contains your target machines and in the **Assigned objects** area, click **(+)**



2. In the **Assign objects** dialog, select the profile you have created beforehand, click to assign it and then click **Ok**.

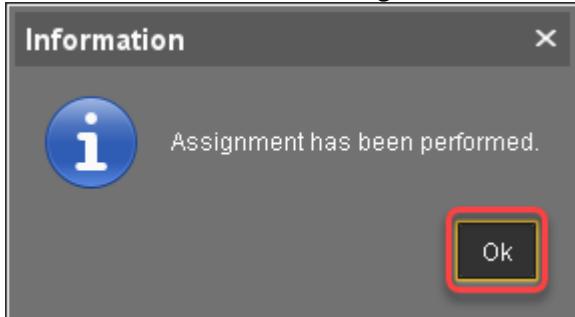


3. In the **Update time** dialog, select **Now** and click **Ok**.





4. Confirm the **Information** dialog.



The target machines download the firmware files. This may take a few minutes.

Check List

- The conversion profile is assigned to all target machines.
- All target machines have found a buddy update server, which is indicated by the **Firmware Description** "IGEL OSC Ready for Conversion".

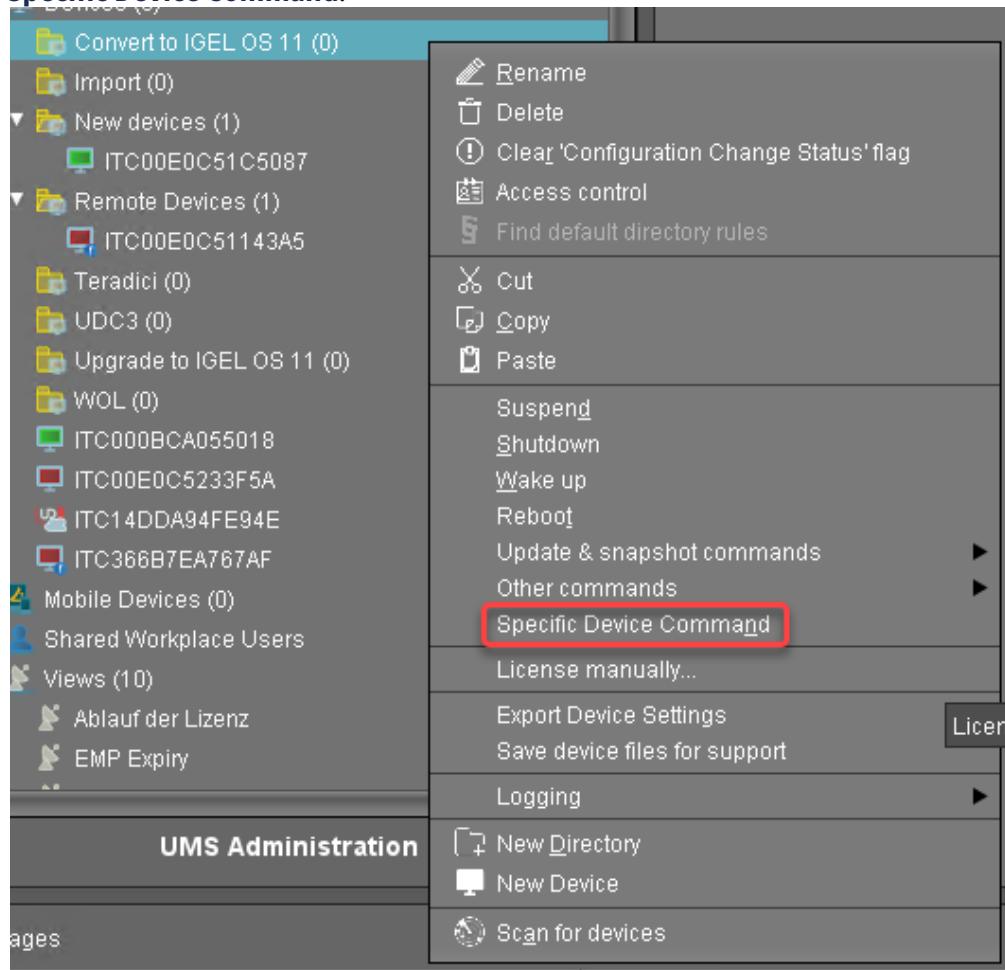
Next Step

>> [Starting the Conversion](#)(see page 1400)



## 6.2.6 Starting the Conversion

1. Select the directory that contains your target machines, open the context menu, and select **Specific Device Command**.





2. In the **Specific Device Command** dialog, select **Convert to IGEL OS** and click **Execute**.



On the devices, a dialog is displayed. When the dialog is confirmed, the conversion starts immediately. If the dialog is not confirmed, the conversion starts after 20 seconds.

When the conversion is complete, the **Product** information in the UMS is changed to "IGEL OS 11".

## 6.3 IGEL OS Creator for Windows (OSCW) on IGEL Windows 10 IoT

The IGEL OS Creator (OSC) for Windows is able to convert any device that is running IGEL Windows 10 IoT to IGEL OS 11. The IGEL OS Creator (OSC) for Windows is integrated into version 4.04.150 of IGEL Windows 10 IoT.

The devices will be converted to IGEL OS 11 automatically when the update is executed. The devices cannot be converted back to IGEL Windows 10 IoT.

Read all the following chapters and follow the instructions in the order given.

1. [Prerequisites](#)(see page 1402)
2. [Getting the Required Software](#)(see page 1402)
3. [Starting the Conversion by Updating the Devices](#)(see page 1402)



### 6.3.1 Prerequisites

#### Network

- All machines are registered with the UMS.

#### Next Step

>> When all requirements are met, continue with [Getting the Required Software](#)(see page 1402).

### 6.3.2 Getting the Required Software

The following software must be downloaded resp. installed:

#### IGEL Universal Management Suite (UMS)

- ▶ Ensure that you have UMS version 6.04 or higher. For update instructions, see [Updating UMS<sup>371</sup>](#).

#### IGEL Windows 10 IoT

- ▶ Download version 10-4.04.150 from <https://www.igel.com/software-downloads/workspace-edition/> > **OSC for Windows > UniversalDesktopW10-4.04.150.zip**.

#### Check List

- ✓ The UMS is available in the correct version.
- ✓ The required firmware version for IGEL Windows IoT devices is available.

#### Next Step

>> [Starting the Conversion by Updating the Devices](#)(see page 1402)

### 6.3.3 Starting the Conversion by Updating the Devices

In this step, we will update the devices, which includes the conversion to IGEL OS 11.

The devices will be converted to IGEL OS 11 automatically when the update is executed. The devices cannot be converted back to IGEL Windows 10 IoT.

<sup>371</sup> <https://kb.igel.com/display/endpointmgmt604/Updating+UMS>

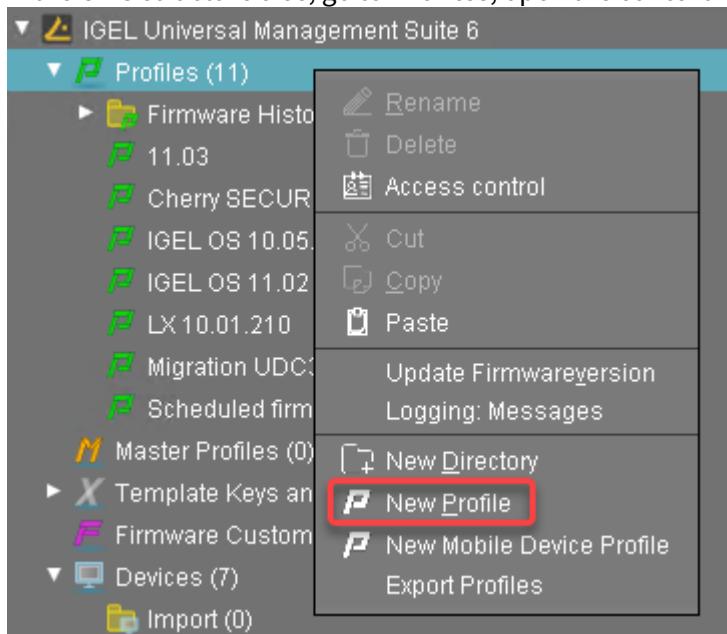
## Transferring the Snapshot File to the UMS

The snapshot file must be placed in the file system of the UMS Server.

1. Get access to the file system of the machine on which your UMS Server is running.
2. Unzip the snapshot file to <UMS Installation directory>\rmguiserver\webapps\ums\_filetransfer

## Creating an Update Profile

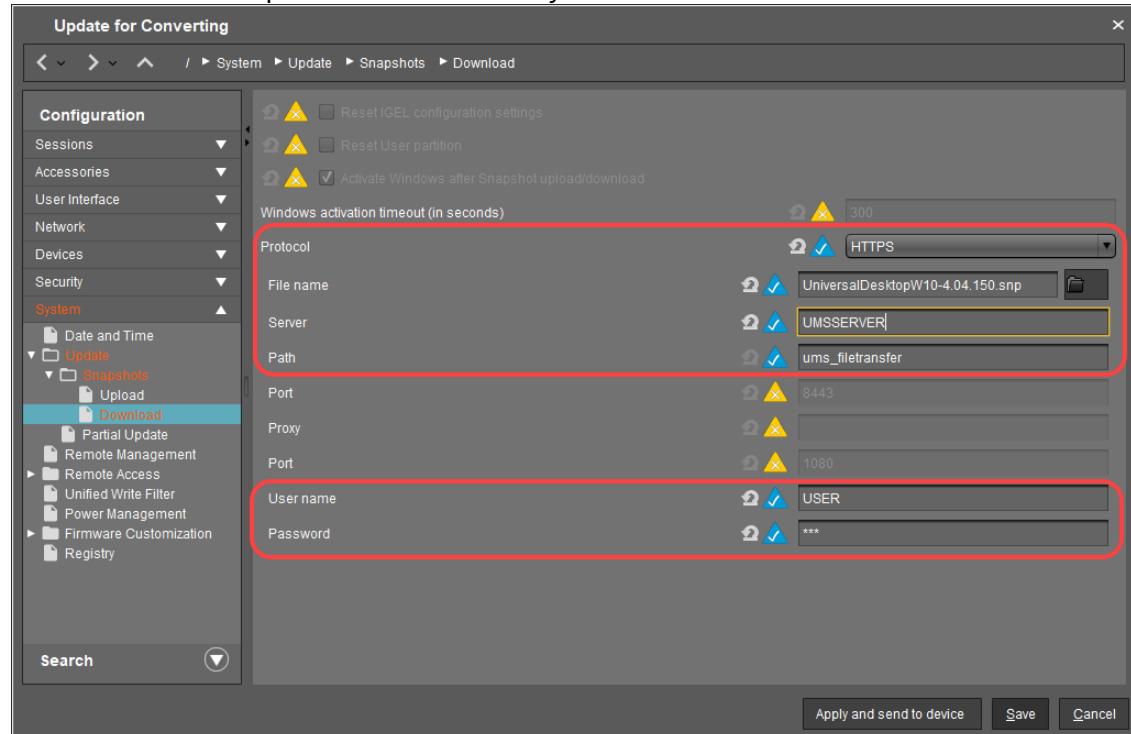
1. In the UMS structure tree, go to **Profiles**, open the context menu, and select **New Profile**.



2. Enter the following data:
  - **Profile Name:** Name for the profile, e. g. "Update for Converting".
  - **Description:** Optional description for the profile.
  - **Based on:** Firmware version for the profile; select the current firmware of your devices.
3. Click **Ok**.
4. Go to **System > Update > Snapshots > Download** and change the settings as follows:
  - Select "https" as the **Protocol**.
  - **File name:** Enter the file name of the snapshot file.
  - **Server:** Enter the IP address or hostname of the UMS.
  - **Path:** Enter "ums\_filetransfer".
  - **Username:** Enter the user name under which you have access to the UMS.



- **Password:** Enter the password under which you have access to the UMS.

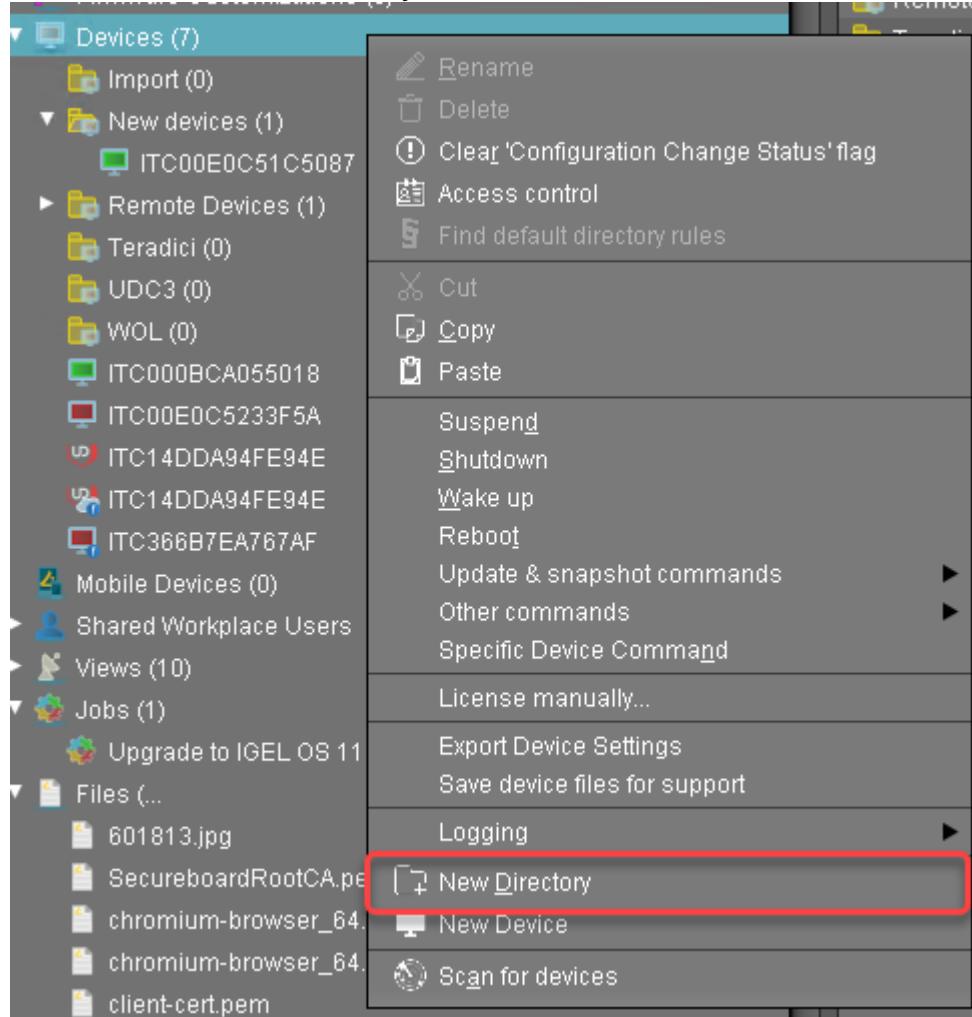


5. Click **Save** to save the profile.



## Starting the Update

1. Under **Devices**, create a directory and name it "Convert to IGEL OS 11", for instance.

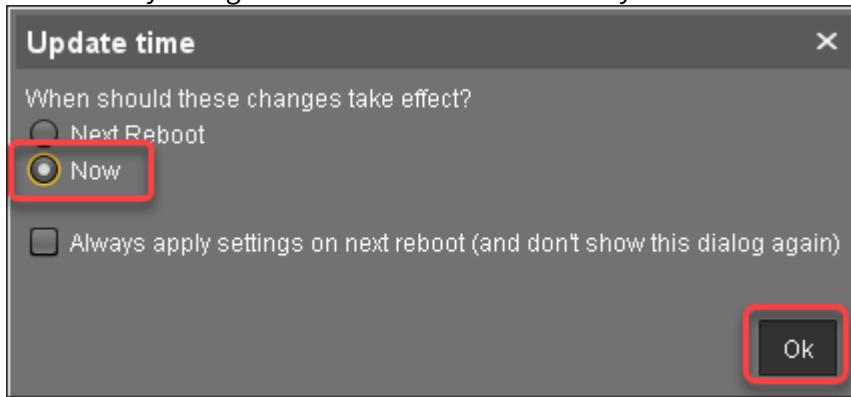


2. Put the devices that are to be updated into the new directory. You can use drag & drop.

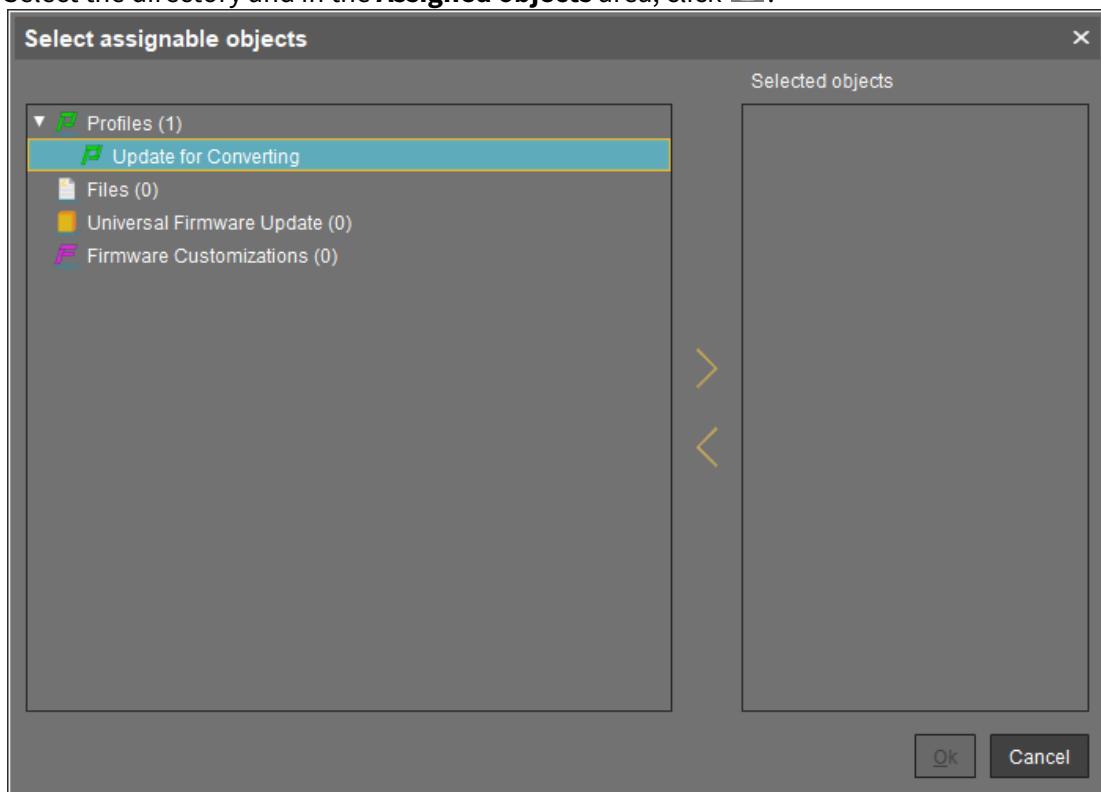


3. In the **Update time** dialog, select **Now** and click **Ok**.

The directory change is communicated immediately to the device.

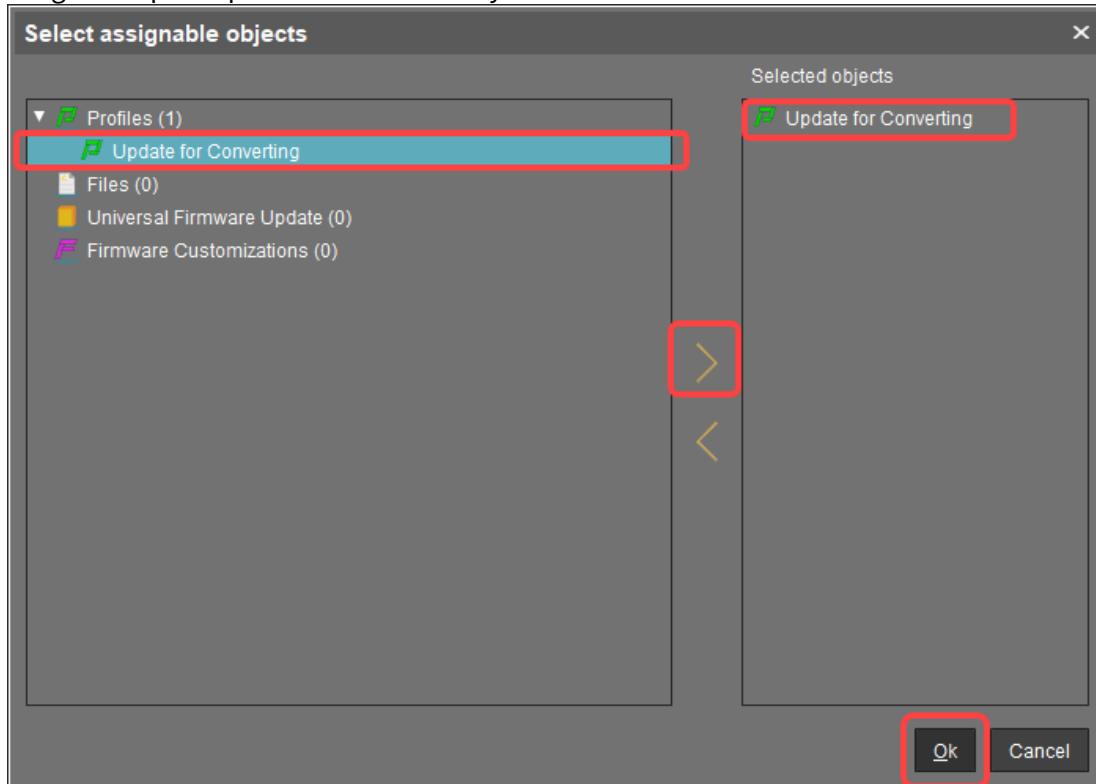


4. Select the directory and in the **Assigned objects** area, click **+**.

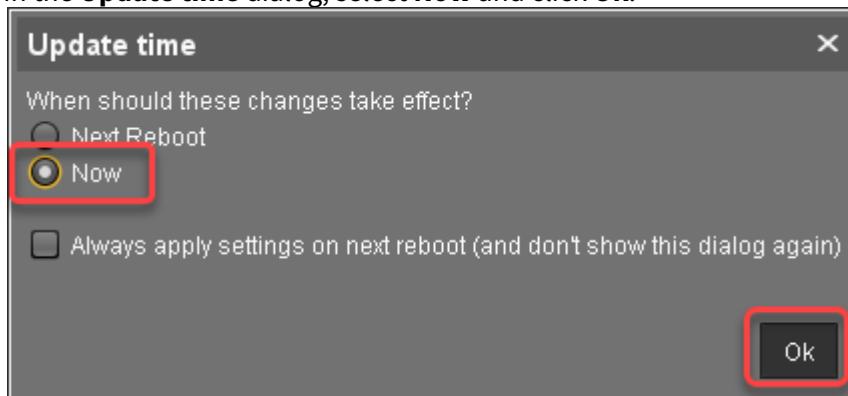




5. Assign the update profile to the directory and click **Ok**.



6. In the **Update time** dialog, select **Now** and click **Ok**.



The changes are sent to the devices immediately.

7. Go to the directory that contains the devices that are to be updated and select **Update & snapshot commands** > **Download Firmware Snapshot**.

The update and conversion process is started.

8. When the update process is finished, go to one of the devices and click to refresh the screen. In the **Advanced System Information** area, **Product** is set to "IGEL OS 11", and **Product ID** is set



according to the device.

| Attribute                                  | Value                          |
|--------------------------------------------|--------------------------------|
| Unit ID                                    | 0050569300FC                   |
| MAC Address                                | 00:50:56:93:00:FC              |
| Last IP                                    | 100.100.12.100                 |
| <b>Product</b>                             | <b>IGEL OS 11</b>              |
| <b>Product ID</b>                          | <b>UC1-LX No valid license</b> |
| Version                                    | 11.03.560.01                   |
| Firmware Description                       | IGEL Cloud Gateway             |
| Expiration Date of OS10-Maintenance Sub... |                                |
| Last Boot Time                             |                                |
| Network Name (at Boot Time)                | ITC0050569300FC                |
| Runtime since last Boot                    | 00:01:23                       |

## 6.4 IGEL OS SCCM Add-On

### 6.4.1 Overview

The IGEL OS SCCM add-on facilitates deploying IGEL OS via Microsoft SCCM. The package contains a minimized IGEL OS image that will be booted initially. If the target devices have enough RAM, a full-featured IGEL OS can be used as an alternative; see [Deploying an Alternative IGEL OS Image](#)(see page 1419).

With the installation of the package, a customized Windows PE image and a task sequence for deploying IGEL OS are created, and the IGEL OS Image Manager is installed.

### 6.4.2 Short Video Summary



Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:

<https://www.youtube.com/watch?v=6nrTmW0ECyk&feature=youtu.be>

### 6.4.3 Prerequisites

- Microsoft Endpoint Configuration Manager (see <https://docs.microsoft.com/en-us/mem/configmgr/>)

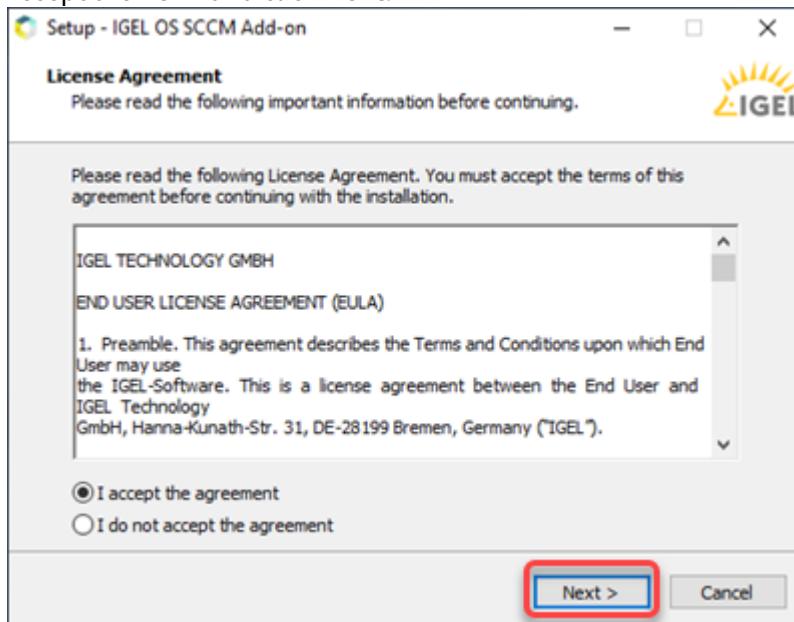


The solution presented here has been developed and tested with version 1902 of Microsoft Endpoint Configuration Manager. For details on the versioning of Microsoft Endpoint Configuration Manager, see <https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/changes/whats-new-incremental-versions>.

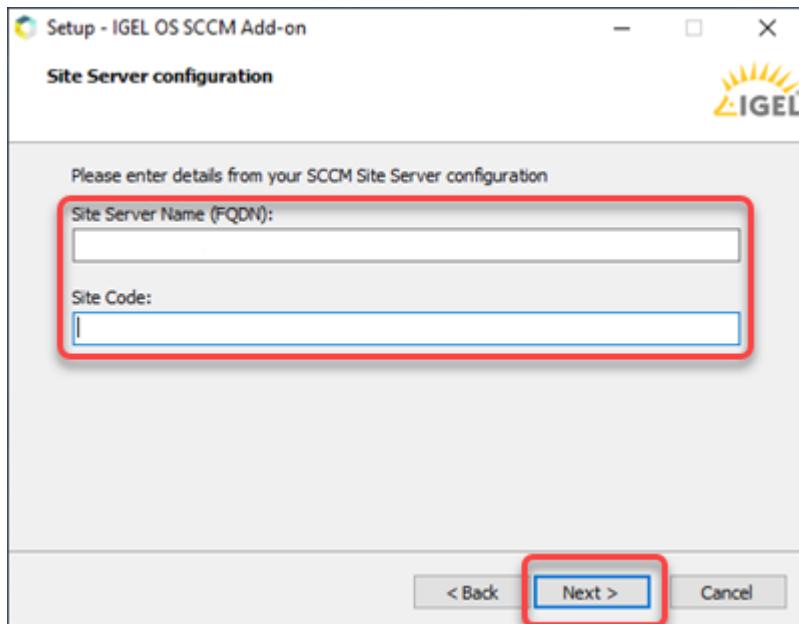
- Configured PXE environment for OS deployment; all target devices must be in a network where they are available either from the main site server or a distribution point. (For further information, see <https://docs.microsoft.com/en-us/mem/configmgr/osd/plan-design/infrastructure-requirements-for-operating-system-deployment>)
- All target devices have a minimum of 2 GB RAM.
- On the host on which Microsoft Endpoint Configuration Manager is running, Microsoft Power Shell Script execution must be allowed, at least for signed scripts (the Powershell scripts that come with the IGEL OS SCCM add-on are signed by IGEL).

#### 6.4.4 Installing the IGEL OS SCCM Add-On

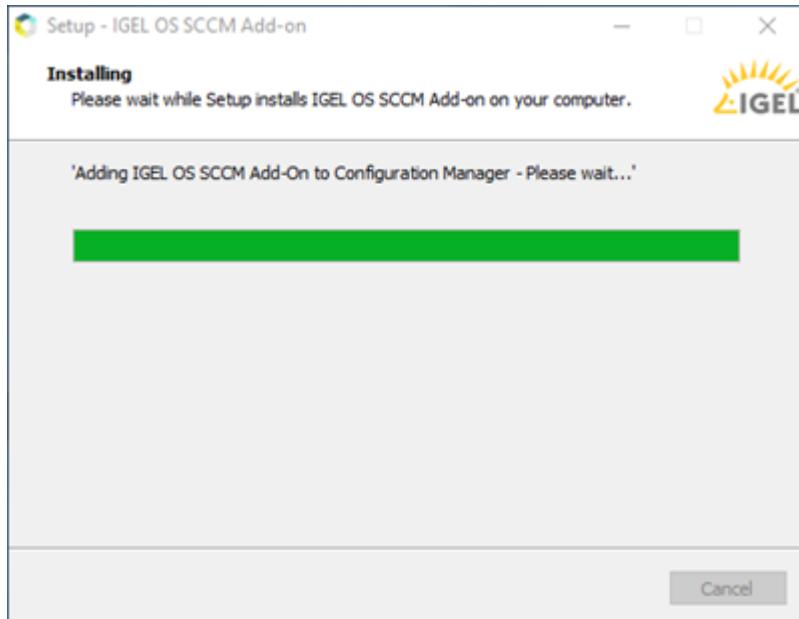
- Go to <https://www.igel.com/software-downloads/workspace-edition/> > **OS DEPLOYMENT TOOL FOR SCCM** and download the executable file (setup-igel\_os-sccm\_add\_on\_[version].exe) to the host on which Microsoft Endpoint Configuration Manager is running.
- Start the executable file.
- Accept the EULA and click **Next**.



- On the **Site Server configuration** page, review the field **Site Server Name (FQDN)**, which should be prefilled, and enter the **Site Code** of this Endpoint Configuration Manager site. Then, click **Next**.

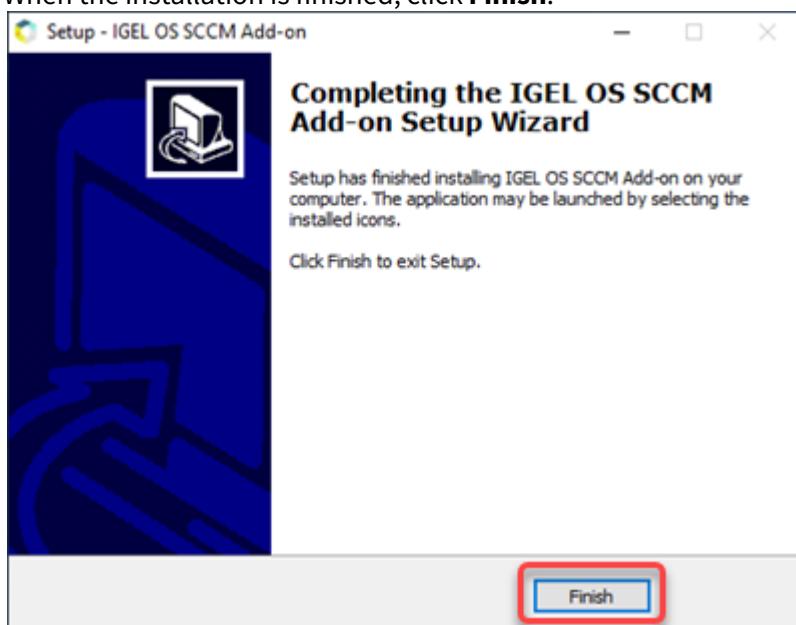


The installation of the IGEL OS SCCM add-on starts.





- When the installation is finished, click **Finish**.





## 6.4.5 Verifying the Installation

1. In the **Home** tab of the Endpoint Configuration Manager, go to **Boot Images** and check if the **IGEL Boot Image (WIM)** is available.

A screenshot of the System Center Configuration Manager interface. The title bar reads "System Center Configuration Manager (Connected to POU - windows site)". The ribbon tabs are "Home" and "Folder Tools". The main navigation pane on the left shows "Software Library" expanded, with "Operating Systems" selected. Under "Operating Systems", "Boot Images" is highlighted with a red box. The central pane displays a table titled "Boot Images 3 items".

| Icon   | Name             | V. | Comment                                  | Image ID | OS Version   | Client... | Date Modified    |
|--------|------------------|----|------------------------------------------|----------|--------------|-----------|------------------|
| [x64]  | Boot image (x64) |    | This boot image is created during setup. | P0100005 | 10.0.18362.1 | 5.00.8... | 12.05.2020 14:26 |
| [x86]  | Boot image (x86) |    | This boot image is created during setup. | P0100002 | 10.0.18362.1 | 5.00.8... | 12.05.2020 14:25 |
| [IGEL] | IGEL Boot Image  | 1  | WinPE Boot Image for deploying IGEL OS   | P010005A | 10.0.18362.1 | 5.00.8... | 22.06.2020 11:36 |



2. Go to **Task Sequences** and check if **IGEL Create** and **IGEL Inplace Upgrade** are available. These task sequences will drive and control the deployment process.

The screenshot shows the System Center Configuration Manager interface. The left navigation pane is expanded to show 'Operating Systems' and its sub-options: Drivers, Driver Packages, Operating System Images, Operating System Upgrade Packages, Boot Images, and Task Sequences. The 'Task Sequences' option is highlighted with a red box. The main content area displays a table titled 'Task Sequences 2 items' with two entries:

| Icon | Name                 | Description | Package ID | Date Created     |
|------|----------------------|-------------|------------|------------------|
|      | IGEL Create          |             | P010005B   | 22.06.2020 11:35 |
|      | IGEL Inplace Upgrade |             | P010005C   | 22.06.2020 11:35 |

Below the table, a detailed view for 'IGEL Create' is shown under the 'IGEL Create' section. The 'Summary' tab is selected, displaying the following information:

- Name: IGEL Create
- Description:
- Package ID: P010005B
- Package Type: 4
- Boot Image ID: P010005A

At the bottom of the summary view, there are tabs for 'Summary', 'References', 'Deployments', and 'Phased Deployments'. The 'Summary' tab is currently active.

#### 6.4.6 Provisioning IGEL OS via a PXE Boot Environment

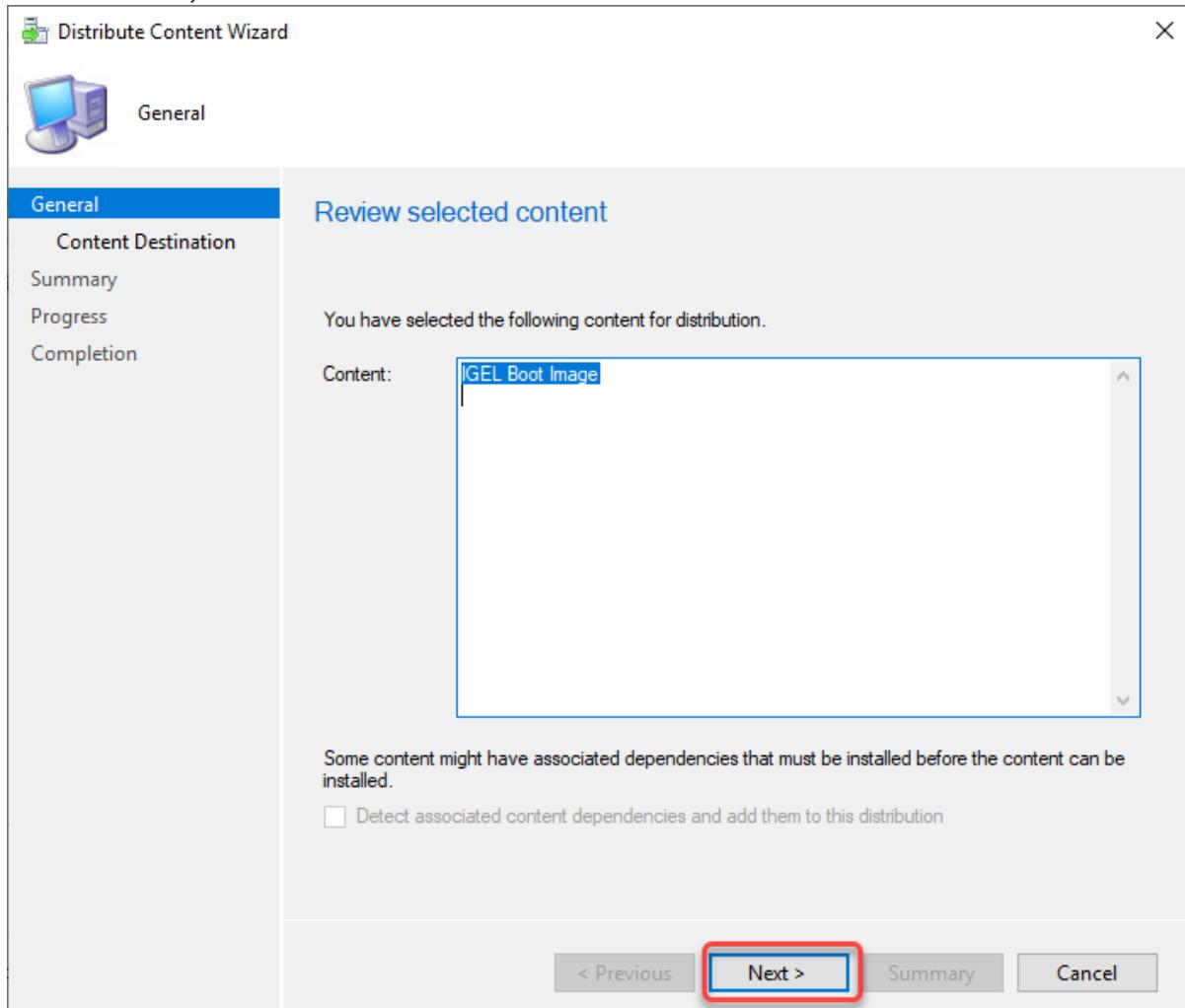
The task sequence "IGEL Create" will deploy IGEL OS to a device collection via a PXE boot environment. The task sequence will be executed after the device has booted into the IGEL OS Boot Image (WIM).

To deploy the PXE boot environment:

1. Check if you need to define your own custom device collection to allocate your target devices or if you can use one of the preconfigured collections.
2. In the **Home** tab of the Endpoint Configuration Manager, select **Boot Images**, open the context menu for **IGEL Boot Image**, and select **Distribute content**.



3. Open the **Distribute Content Wizard** and check if "IGEL Boot Image" is shown in the **Content** area. Afterward, continue with the wizard.



4. If your device requires a specific network driver: In the **Home** tab of the Endpoint Configuration Manager, select **Boot Images**, open the context menu for **IGEL Boot Image**, and select **Properties**. Then,



select the **Drivers** tab and add the driver.

A screenshot of the "IGEL Boot Image Properties" dialog box. The title bar shows the window name. Below it is a tab bar with "Content Locations", "Optional Components", and "Security" on the left, and "General", "Images", "Drivers", "Customization", "Data Source", "Data Access", and "Distribution Settings" on the right. The "Drivers" tab is selected and highlighted with a blue border. In the main area, there is a section titled "Drivers:" with a "Filter..." input field and a search icon. Below this is a table with columns: "Driver name", "Version", "Class", "Signed", "Architecture", and "INF File". A message "There are no items to show in this view." is displayed. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

IGEL Boot Image Properties

Content Locations Optional Components Security

General Images Drivers Customization Data Source Data Access Distribution Settings

Drivers:

Filter...

| Driver name                              | Version | Class | Signed | Architecture | INF File |
|------------------------------------------|---------|-------|--------|--------------|----------|
| There are no items to show in this view. |         |       |        |              |          |

OK Cancel Apply



5. In the **Home** tab of the Endpoint Configuration Manager, select **Task Sequences**, open the context menu for **IGEL Create**, and select **Update distribution points**. Then, continue with the wizard.

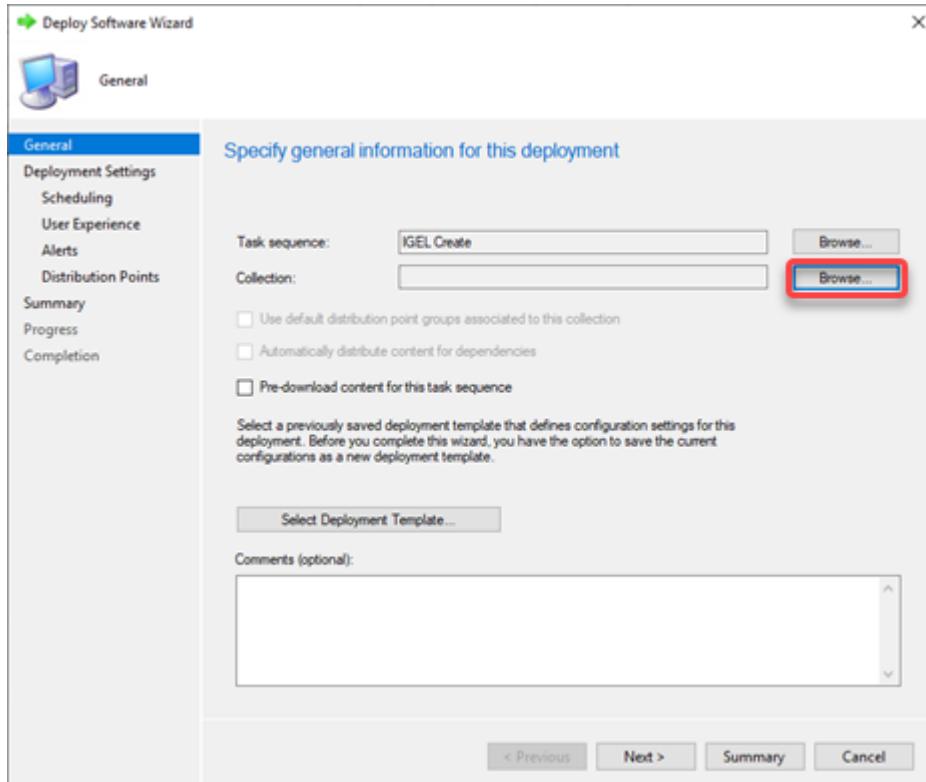
A screenshot of the "Update Distribution Points Wizard" window. The title bar says "Update Distribution Points Wizard". The left sidebar has tabs: General (selected), Summary, Progress, and Completion. The main area has a heading "Update distribution points with this boot image". It contains descriptive text about the wizard's function, a note about the boot image being updated, and current version information (Windows ADK 10.0.18362.0, Client Version 5.00.8790.1007). There is a checkbox for "Reload this boot image with the current Windows PE version from the Windows ADK". Below it is a table showing one boot image entry. At the bottom are buttons for "Previous", "Next >" (highlighted in blue), "Summary", and "Cancel".

| Version | Comment                   | OS Version   | Client Version | Package ID |
|---------|---------------------------|--------------|----------------|------------|
| 1       | WinPE Boot Image for d... | 10.0.18362.1 | 5.00.8790.1007 | P010005A   |

6. In the **Home** tab of the Endpoint Configuration Manager, select **Task Sequences**, open the context menu for **IGEL Create**, and select **Deploy**.  
The **Deploy Software Wizard** opens.



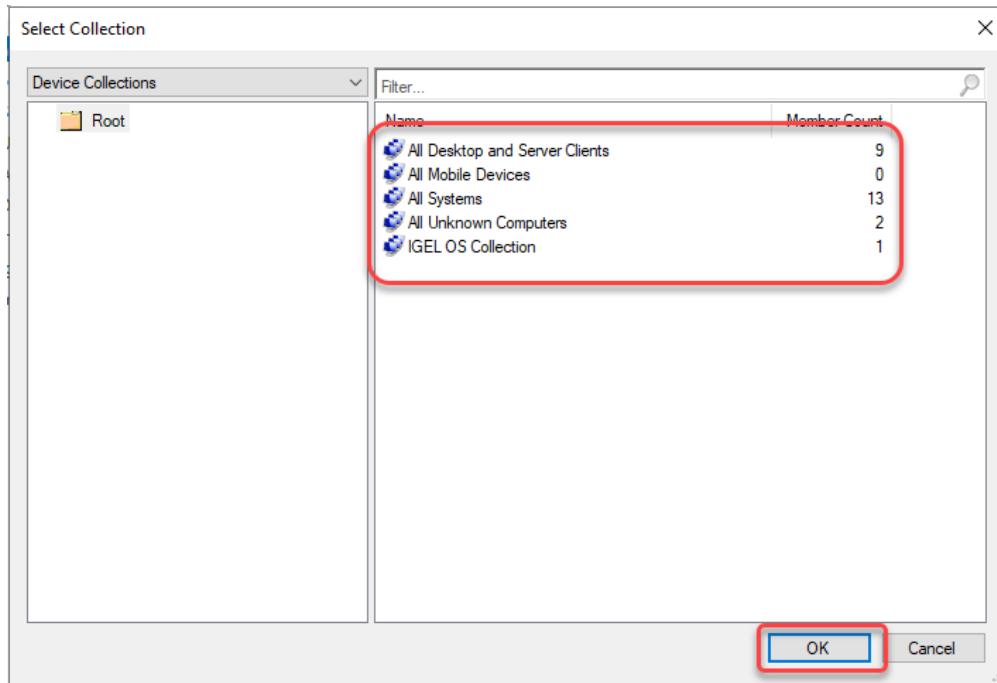
7. Click the **Browse** button next to **Collection**:



The **Select Collection** dialog opens.

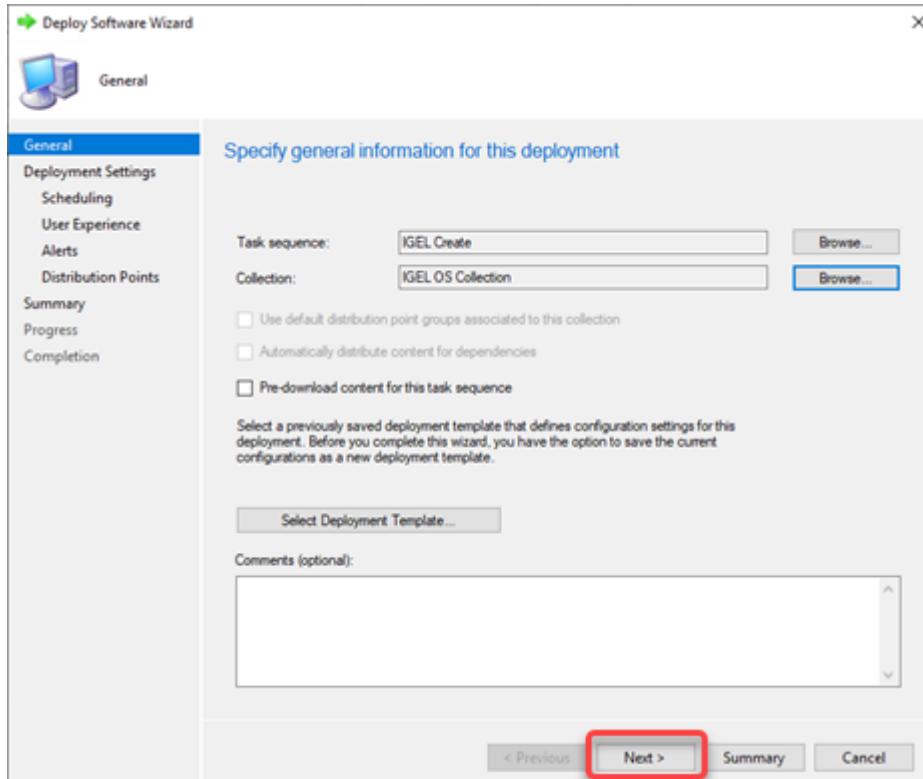
8. From the list of collections, select the collection that contains your target devices and click **OK**.

If you want to deploy IGEL OS to all new devices on the network and any existing third-party devices running IoT, use the pre-existing collection "All Unknown Computers".



In the following example, a user-created collection named "IGEL OS Collection" has been selected:

9. Click **Next** to continue with the wizard.



All target devices receive the PXE boot request that triggers them to boot the IGEL OS Boot Image (WIM).

A screenshot of a terminal window titled "Player". The window displays various system logs and configuration details. It includes information about the client's MAC address, GUID, IP addresses, and network settings. It also shows a message from an administrator regarding a pending request and instructions to press F12 for network service boot.

```
Copyright (C) 2003-2018 VMware, Inc.
Copyright (C) 1997-2008 Intel Corporation

CLIENT MAC ADDR: 00 50 56 93 7C GE  GUID: 4213A24A-BB74-1ABC-8C12-8EAF9642C1B1
CLIENT IP: 192.168.12.108  MASK: 255.255.255.0  DHCP IP: 192.168.12.2
GATEWAY IP: 192.168.12.1

Downloaded WDSNBP from 192.168.12.12
Architecture: x64

The details below show the information relating to the PXE boot request for
this computer. Please provide these details to your Windows Deployment Services
Administrator so that this request can be approved.

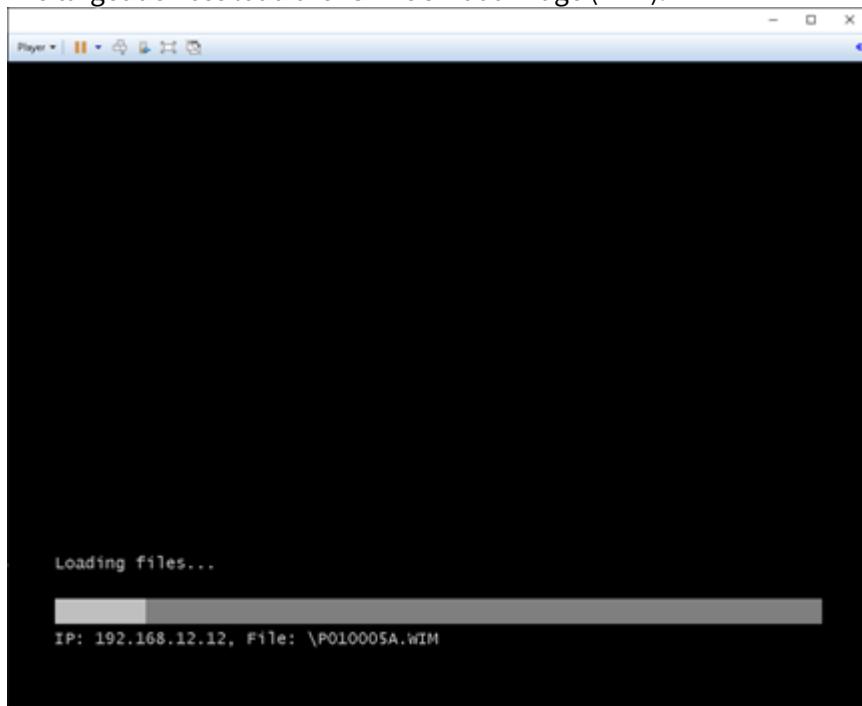
Pending Request ID: 8

Message from Administrator:
SCCM PXE

Contacting Server: 192.168.12.12.
TFTP Download: smsboot\PB100005A\x64\pxeboot.com

Press F12 for network service boot
```

The target devices load the IGEL OS Boot Image (WIM).



#### 6.4.7 Deploying an Alternative IGEL OS Image

As an alternative to the minimized IGEL OS image that comes with the IGEL OS SCCM add-on, you can deploy a full-featured IGEL OS image. The current main version is available from [igel.com](http://igel.com). Optionally, you can add pre-configured settings and certificates to the image.



The RAM size of the target device must be equal to or greater than the storage size required by the IGEL OS image plus the initial size of the IGEL OS Boot Image (WIM), which is between 300 and 400 MB. For deploying an alternative IGEL OS Image, at least 4 GB RAM is needed.

1. Open a web browser, go to <https://www.igel.com/software-downloads/workspace-edition/> > **OS DEPLOYMENT TOOL FOR SCCM**, download the current IGEL OS file, and unzip it.

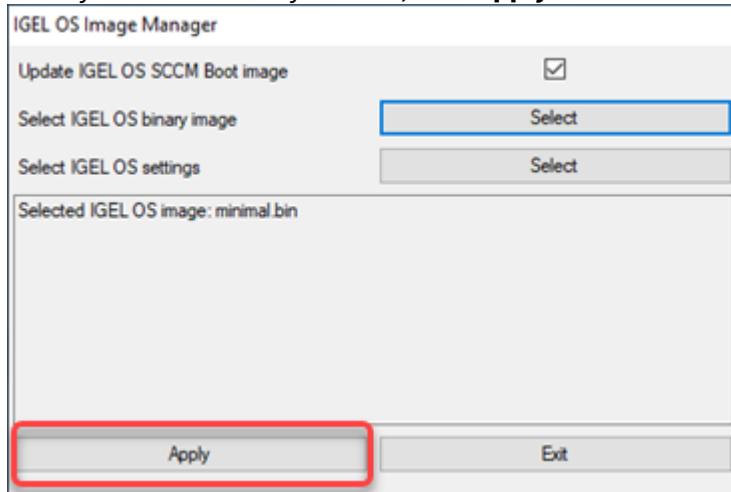
|                                                                                                                                                                    |                                    |                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/>                                                                                                                                           | <b>OS 11</b>                       | <b>+</b>                                                                                                              |
| <input type="checkbox"/>                                                                                                                                           | <b>UNIVERSAL MANAGEMENT SUITE</b>  | <b>+</b>                                                                                                              |
| <input type="checkbox"/>                                                                                                                                           | <b>OS DEPLOYMENT APPLIANCE</b>     | <b>+</b>                                                                                                              |
| <input type="checkbox"/>                                                                                                                                           | <b>OS 10 MIGRATION FIRMWARE</b>    | <b>+</b>                                                                                                              |
| <input type="checkbox"/>                                                                                                                                           | <b>OSC FOR WINDOWS</b>             | <b>+</b>                                                                                                              |
| <input type="checkbox"/>                                                                                                                                           | <b>OS DEPLOYMENT TOOL FOR SCCM</b> | <b>X</b>                                                                                                              |
| <b>11.05.100.zip</b><br><small>MD5: 18c8372e2fb8962cc043e880ff6ae95</small><br><small>Updated BIN file for deploying 11.05.100 via OSCW</small>                    |                                    | <small>2021/03/01</small><br><small>SHA-256: e7e9c14e73884c2cb7a571b0bd6a769600a2cc09a16c504f899172fafc2b9b61</small> |
| <b>setup-igel_os-sccm_add_on_1.01.100.exe</b><br><small>MD5: 958060e5d71605a3738e46c33225daca</small><br><small>Tool for initial OS 11 Deployment via SCCM</small> |                                    | <small>2020/10/08</small><br><small>SHA-256: ca9598f36a5a37156303f8c2ffa1a927e0c631e03a0c5ec9ad531952c23585b5</small> |
| <a href="#">Detailed Description</a>                                                                                                                               |                                    |                                                                                                                       |

The IGEL OS image is ready for deployment (example: **11.05.100.bin**).

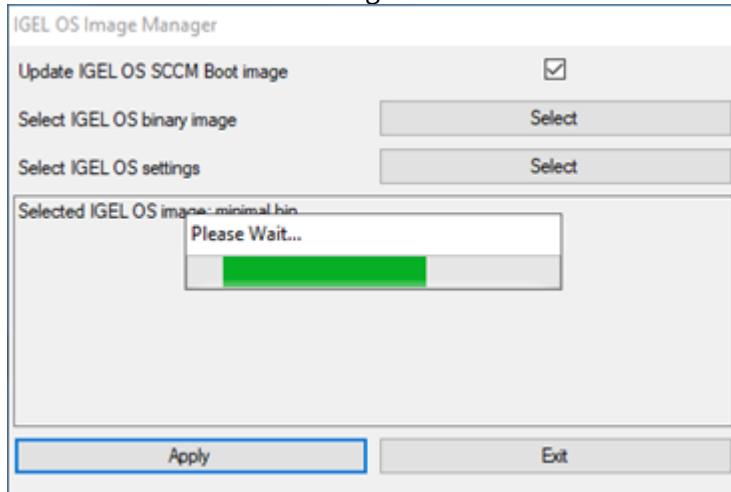
2. Start the IGEL OS Image Manager by clicking on the desktop icon.
3. Click **Select** next to **Select IGEL OS binary image** and choose your image file.
4. If you want to add settings or certificates, click **Select** next to **Select IGEL OS settings** and choose the relevant files. You can add the following files:
  - **setup.ini**: The settings for IGEL OS; these are the settings that can be configured via IGEL Setup, the UMS configuration dialog, or a UMS profile.
  - **Certificate files**



- When you have chosen your files, click **Apply**.



The files are added to the image.





## 7 IGEL OS Release Notes

- [Notes for Release 11.06.100 \(see page 1422\)](#)
- [Notes for Release 11.05.133 \(see page 1480\)](#)
- [Notes for Release 11.05.120 \(see page 1494\)](#)
- [Notes for Release 11.05.100 \(see page 1512\)](#)
- [Notes for Release 11.04.270 \(see page 1557\)](#)
- [Notes for Release 11.04.240 \(see page 1572\)](#)
- [Notes for Release 11.04.200 \(see page 1588\)](#)
- [Notes for Release 11.04.100 \(see page 1603\)](#)
- [Notes for Release 11.03.500 \(see page 1680\)](#)
- [Notes for Release 11.03.110 \(see page 1699\)](#)
- [Notes for Release 11.03.100 \(see page 1712\)](#)
- [Notes for Release 11.02.150 \(see page 1743\)](#)
- [Notes for Release 11.02.130 \(see page 1755\)](#)
- [Notes for Release 11.02.100 \(see page 1766\)](#)
- [Notes for Release 11.01.130 \(see page 1817\)](#)
- [Notes for Release 11.01.120 \(see page 1825\)](#)
- [Notes for Release 11.01.110 \(see page 1832\)](#)
- [Notes for Release 11.01.100 \(see page 1853\)](#)
- [Notes for Release 10.06.190 \(see page 1871\)](#)
- [Notes for Release 10.06.170 \(see page 1871\)](#)
- [Notes for Release 10.06.130 \(see page 1893\)](#)
- [Notes for Release 10.06.120 \(see page 1912\)](#)
- [Notes for Release 10.06.110 \(see page 1938\)](#)
- [Notes for Release 10.06.100 \(see page 1955\)](#)
- [Notes for Release 10.05.830 \(see page 2036\)](#)
- [Notes for Release 10.05.800 \(see page 2078\)](#)
- [Notes for Release 10.05.700 \(see page 2110\)](#)
- [Notes for Release 10.05.500 \(see page 2128\)](#)
- [Notes for Release 10.05.100 \(see page 2164\)](#)
- [Notes for Release 10.04.100 \(see page 2260\)](#)
- [Notes for Release 10.03.570 \(see page 2324\)](#)
- [Notes for Release 10.03.550 \(see page 2338\)](#)
- [Notes for Release 10.03.500 \(see page 2353\)](#)

### 7.1 Notes for Release 11.06.100

|                       |            |              |
|-----------------------|------------|--------------|
| <b>Software:</b>      | Version    | 11.06.100    |
| <b>Release Date:</b>  | 2021-09-22 |              |
| <b>Release Notes:</b> | Version    | RN-1106100-1 |



|                     |            |  |
|---------------------|------------|--|
| <b>Last update:</b> | 2021-09-22 |  |
|---------------------|------------|--|

- [IGEL OS 11](#)(see page 1423)
- [IGEL OS Creator \(OSC\)](#)(see page 1477)

### 7.1.1 IGEL OS 11

- [Supported Devices 11.06.100](#)(see page 1423)
- [Component Versions 11.06.100](#)(see page 1425)
- [General Information 11.06.100](#)(see page 1432)
- [Known Issues 11.06.100](#)(see page 1432)
- [Security Fixes 11.06.100](#)(see page 1436)
- [New Features 11.06.100](#)(see page 1440)
- [Resolved Issues 11.06.100](#)(see page 1461)
- [CA Certificates Contained in IGEL OS 11.06](#)(see page 1467)

#### Supported Devices 11.06.100

|         |                                     |
|---------|-------------------------------------|
| UD2-LX: | UD2-LX 51<br>UD2-LX 50<br>UD2-LX 40 |
| UD3-LX: | UD3-LX 60<br>UD3-LX 51              |
| UD5-LX: | UD5-LX 50                           |
| UD6-LX: | UD6-LX 51                           |
| UD7-LX: | UD7-LX 20<br>UD7-LX 11<br>UD7-LX 10 |
| UD9-LX: | UD9-LX Touch 41<br>UD9-LX 40        |



See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>372</sup>,

---

<sup>372</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



## Component Versions 11.06.100

## Clients

| <b>Product</b>                        | <b>Version</b>                  |
|---------------------------------------|---------------------------------|
| Amazon WorkSpaces Client              | 3.1.9                           |
| Chromium                              | 91.0.4472.164-igel1626429779    |
| Cisco JVDI Client                     | 14.0.1                          |
| Cisco Webex VDI plugin                | 41.8.0.19732                    |
| Cisco Webex Meetings VDI plugin       | 41.6.7.16                       |
| Cisco Webex Meetings VDI plugin       | 41.7.8.5                        |
| Cisco Webex Meetings VDI plugin       | 41.8.4.11                       |
| ControlUp Agent                       | 8.1.5.500                       |
| Zoom Media Plugin                     | 5.4.59458                       |
| Zoom Media Plugin                     | 5.5.12716                       |
| Zoom Media Plugin                     | 5.5.8.20606                     |
| Citrix HDX Realtime Media Engine      | 2.9.400                         |
| Citrix Workspace App                  | 20.10.0.6                       |
| Citrix Workspace App                  | 21.04.0.11                      |
| Citrix Workspace App                  | 21.06.0.28                      |
| deviceTRUST Citrix Channel            | 20.2.310.0                      |
| Crossmatch DP Citrix Channel          | 0125                            |
| deskMate Client                       | 2.1.3                           |
| DriveLock Agent                       | 20.1.4.30482                    |
| Ericom PowerTerm                      | 12.0.1.0.20170219.2-_dev_-34574 |
| Ericom PowerTerm                      | 14.0.0.45623                    |
| Evidian AuthMgr                       | 1.5.7789                        |
| Evince PDF Viewer                     | 3.28.4-0ubuntu1.2               |
| FabulaTech USB for Remote Desktop     | 6.0.28                          |
| FabulaTech Scanner for Remote Desktop | 2.7.0.1                         |
| FabulaTech Webcam for Remote Desktop  | 2.8.10                          |



|                                           |                                           |
|-------------------------------------------|-------------------------------------------|
| Firefox                                   | 78.12.0                                   |
| IBM iAccess Client Solutions              | 1.1.8.6                                   |
| IGEL RDP Client                           | 2.2igel1628056781                         |
| IGEL AVD Client                           | 1.0.30igel1630670236                      |
| deviceTRUST RDP Channel                   | 20.2.310.0                                |
| Imprivata OneSign ProvID Embedded         | onesign-bootstrap-loader_1.0.523630_amd64 |
| Lakeside SysTrack Channel                 | 9.0                                       |
| NCP Secure Enterprise Client              | 5.10_rev40552                             |
| NX Client                                 | 7.1.3-1igel9                              |
| Open VPN                                  | 2.5.1-3igel1621236751                     |
| Zulu JRE                                  | 8.0.302-1                                 |
| Parallels Client                          | 18.1.0                                    |
| Spice GTK (Red Hat Virtualization)        | 0.39-1igel106                             |
| Remote Viewer (Red Hat Virtualization)    | 8.0-2git20191213.e4bacb8igel83            |
| Usbredir (Red Hat Virtualization)         | 0.8.0-1+b1igel71                          |
| SpeechWrite                               | 1.0                                       |
| Stratusphere UX Connector ID Key software | 6.5.0-2                                   |
| Systancia AppliDis                        | 6.0.0-4                                   |
| Teradici PCoIP Software Client            | 21.03.0-18.04                             |
| ThinLinc Client                           | 4.12.1-6733                               |
| ThinPrint Client                          | 7-7.6.126                                 |
| Totem Media Player                        | 2.30.2-0ubuntu1igel55                     |
| Parole Media Player                       | 4.16.0-1igel1611217037                    |
| VNC Viewer                                | 1.11.0+dfsg-2igel19                       |
| VMware Horizon Client                     | 2106-8.3.0-18251983                       |
| Voip Client Ekiga                         | 4.0.1-9build1igel6                        |

## Dictation

|                               |            |
|-------------------------------|------------|
| Diktamen driver for dictation | 2017/09/29 |
|-------------------------------|------------|



|                                           |          |
|-------------------------------------------|----------|
| Grundig Business Systems dictation driver | 20-09-16 |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 4.0.0    |
| Philips Speech driver                     | 12.9.1   |

## Signature

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.9    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.4.2    |

## Smartcard

|                                           |                 |
|-------------------------------------------|-----------------|
| PKCS#11 Library A.E.T SafeSign            | 3.6.0.0-AET.000 |
| PKCS#11 Library Athena IDProtect          | 7               |
| PKCS#11 Library cryptovision sc/interface | 7.3.1           |
| PKCS#11 Library Gemalto SafeNet           | 10.7.77         |
| PKCS#11 Library OpenSC                    | 0.21.0-1igel39  |
| PKCS#11 Library SecMaker NetID            | 6.8.3.21        |
| PKCS#11 Library 90meter                   | 20190522        |
| Reader Driver ACS CCID                    | 1.1.6-1igel2    |
| Reader Driver Gemalto eToken              | 10.7.77         |
| Reader Driver HID Global Omnikey          | 4.3.3           |
| Reader Driver Identive CCID               | 5.0.35          |
| Reader Driver Identive eHealth200         | 1.0.5           |
| Reader Driver Identive SCRKBC             | 5.0.24          |



|                                    |                        |
|------------------------------------|------------------------|
| Reader Driver MUSCLE CCID          | 1.4.31-1igel12         |
| Reader Driver REINER SCT cyberJack | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite        | 1.9.1-1igel18          |
| Cherry USB2LAN Proxy               | 3.2.0.3                |

## System Components

|                                         |                               |
|-----------------------------------------|-------------------------------|
| OpenSSL                                 | 1.0.2n-1ubuntu5.7             |
| OpenSSL                                 | 1.1.1-1ubuntu2.1~18.04.13     |
| OpenSSH Client                          | 8.4p1-5igel6                  |
| OpenSSH Server                          | 8.4p1-5igel6                  |
| Bluetooth stack (bluez)                 | 5.56-0ubuntu2igel12           |
| MESA OpenGL stack                       | 21.1.5-1igel145               |
| VAAPI ABI Version                       | 0.40                          |
| VDPAU Library version                   | 1.4-3igel1099                 |
| Graphics Driver INTEL                   | 2.99.917+git20200515-igel1013 |
| Graphics Driver ATI/RADEON              | 19.1.0-2igel1066              |
| Graphics Driver ATI/AMDGPU              | 19.1.0-2+git20210202igel1122  |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867               |
| Graphics Driver Nvidia                  | 460.91.03-0ubuntu0.20.04.1    |
| Graphics Driver VMware                  | 13.3.0-2igel857               |
| Graphics Driver QXL (Spice)             | 0.1.5-2build2-igel925         |
| Graphics Driver FBDEV                   | 0.5.0-1igel1012               |
| Graphics Driver VESA                    | 2.4.0-1igel1010               |
| Input Driver Evdev                      | 2.10.6-2igel1037              |
| Input Driver Elographics                | 1.4.2-1igel1113               |
| Input Driver eGalax                     | 2.5.8825                      |
| Input Driver Synaptics                  | 1.9.1-1ubuntu1igel1009        |



|                                      |                                    |
|--------------------------------------|------------------------------------|
| Input Driver VMMouse                 | 13.1.0-1ubuntu2igel957             |
| Input Driver Wacom                   | 0.39.0-0ubuntu1igel1036            |
| Input Driver ELO Multitouch          | 3.0.0                              |
| Input Driver ELO Singletouch         | 5.1.0                              |
| Kernel                               | 5.12.19 #mainline-lxos-g1631108722 |
| Xorg X11 Server                      | 1.20.11-1igel1120                  |
| Xorg Xephyr                          | 1.20.11-1igel1120                  |
| CUPS printing daemon                 | 2.2.7-1ubuntu2.8igel32             |
| PrinterLogic                         | 25.1.0.500                         |
| Lightdm Graphical Login Manager      | 1.26.0-0ubuntu1igel13              |
| XFCE4 Window Manager                 | 4.14.5-1~18.04igel1600422786       |
| ISC DHCP Client                      | 4.3.5-3ubuntu7.3                   |
| NetworkManager                       | 1.30.0-2igel111                    |
| ModemManager                         | 1.10.0-1~ubuntu18.04.2             |
| GStreamer 0.10                       | 0.10.36-2ubuntu0.1igel201          |
| GStreamer 0.10 Fluendo aacdec        | 0.10.42                            |
| GStreamer 0.10 Fluendo asfdemux      | 0.10.92                            |
| GStreamer 0.10 Fluendo h264dec       | 0.10.59                            |
| GStreamer 0.10 Fluendo mp3dec        | 0.10.41                            |
| GStreamer 0.10 Fluendo mpegdemux     | 0.10.85                            |
| GStreamer 0.10 Fluendo mpeg4videodec | 0.10.44                            |
| GStreamer 0.10 Fluendo vadec         | 0.10.229                           |
| GStreamer 0.10 Fluendo wmadec        | 0.10.70                            |
| GStreamer 0.10 Fluendo wmvdec        | 0.10.66                            |
| GStreamer 1.x                        | 1.18.3-1igel283                    |
| GStreamer 1.0 Fluendo aacdec         | 0.10.42                            |
| GStreamer 1.0 Fluendo asfdemux       | 0.10.92                            |
| GStreamer 1.0 Fluendo h264dec        | 0.10.59                            |
| GStreamer 1.0 Fluendo mp3dec         | 0.10.41                            |
| GStreamer 1.0 Fluendo mpeg4videodec  | 0.10.44                            |
| GStreamer 1.0 Fluendo vadec          | 0.10.229                           |



|                              |                        |
|------------------------------|------------------------|
| GStreamer 1.0 Fluendo wmadec | 0.10.70                |
| GStreamer 1.0 Fluendo wmvdec | 0.10.66                |
| WebKit2Gtk                   | 2.32.3-1igel1628055206 |
| Python2                      | 2.7.17                 |
| Python3                      | 3.6.9                  |

## VM Guest Support Components

|                            |                         |
|----------------------------|-------------------------|
| Virtualbox Guest Utils     | 6.1.22-dfsg-1igel55     |
| Virtualbox X11 Guest Utils | 6.1.22-dfsg-1igel55     |
| Open VM Tools              | 11.0.5-4ubuntu0.18.04.1 |
| Open VM Desktop Tools      | 11.0.5-4ubuntu0.18.04.1 |
| Xen Guest Utilities        | 7.10.0-0ubuntu1         |
| Spice Vdagent              | 0.20.0-2igel104         |
| Qemu Guest Agent           | 5.2+dfsg-3igel17        |

## Features with Limited IGEL Support

|                                    |                     |
|------------------------------------|---------------------|
| Mobile Device Access USB (MTP)     | 1.1.17-3igel5       |
| Mobile Device Access USB (imobile) | 1.3.0-6igel12       |
| Mobile Device Access USB (gphoto)  | 2.5.27-1igel8       |
| VPN OpenConnect                    | 8.10-2igel6         |
| Scanner support                    | 1.0.27-1            |
| VirtualBox VM within IGEL OS       | 6.1.22-dfsg-1igel55 |

## Services

| Service                       | Size    | Reduced Firmware |
|-------------------------------|---------|------------------|
| Asian Language Support        | 22.5 M  | Included         |
| Java SE Runtime Environment   | 36.2 M  | Included         |
| Citrix Appliance              | 365.8 M | Included         |
| Citrix Workspace app          |         |                  |
| Citrix StoreFront             |         |                  |
| Ericom PowerTerm InterConnect | 15.5 M  | Included         |
| Media Player                  | 512.0 K | Included         |
| Local Browser (Firefox)       | 76.8 M  | Included         |
| Citrix Appliance              |         |                  |
| VMware Horizon                | 4.5 M   | Included         |
| RDP                           |         |                  |



|                                            |         |              |
|--------------------------------------------|---------|--------------|
| Cendio ThinLinc                            | 10.0 M  | Included     |
| Printing (Internet printing protocol CUPS) | 22.2 M  | Included     |
| NoMachine NX                               | 28.0 M  | Included     |
| VMware Horizon                             | 143.0 M | Included     |
| Voice over IP (Ekiga)                      | 6.5 M   | Included     |
| Citrix Appliance                           | 768.0 K | Included     |
| NCP Enterprise VPN Client                  | 27.0 M  | Not included |
| Fluendo GStreamer Codec Plugins            | 6.5 M   | Included     |
| IBM i Access Client Solutions              | 128.2 M | Not included |
| Red Hat Enterprise Virtualization          | 3.0 M   | Included     |
| Parallels Client                           | 6.0 M   | Included     |
| NVIDIA graphics driver                     | 165.5 M | Not included |
| Imprivata Appliance                        | 10.8 M  | Included     |
| AppliDis                                   | 256.0 K | Included     |
| Evidian AuthMgr                            | 2.8 M   | Included     |
| Hardware Video Acceleration                | 13.8 M  | Included     |
| Extra Font Package                         | 1.0 M   | Included     |
| Fluendo GStreamer AAC Decoder              | 1.2 M   | Included     |
| x32 Compatibility Support                  | 3.5 M   | Included     |
| Cisco JVDI client                          | 61.8 M  | Included     |
| PrinterLogic                               | 42.5M   | Not included |
| Biosec BS Login                            | 10.0 M  | Not included |
| Login VSI Login Enterprise                 | 28.8 M  | Not included |
| Stratusphere UX CID Key software           | 2.8 M   | Not included |
| Elastic Filebeat                           | 15.8 M  | Not included |
| AVD                                        | 89.8 M  | Included     |
| Local Browser (Chromium)                   | 99.2 M  | Not included |
| Amazon WorkSpaces Client                   | 32.2 M  | Included     |
| deskMate client                            | 5.8 M   | Included     |
| Cisco WebEx VDI                            | 45.0 M  | Not included |
| Cisco Webex Meetings VDI                   | 75.0 M  | Not included |
| Zoom VDI Media Plugin                      | 107.5 M | Not included |
| DriveLock                                  | 13.2 M  | Included     |
| SpeechWrite Client                         | 256.0 K | Included     |
| Fluendo Browser Codec Plugins              | 1.5 M   | Included     |
| Teradici PCoIP Client                      | 16.0 M  | Included     |
| 90meter Smart Card Support                 | 256.0 K | Included     |



|                                            |         |              |
|--------------------------------------------|---------|--------------|
| Limited Support Features                   | 256.0 K | Not included |
| Virtualbox (Limited support)               |         |              |
| VPN OpenConnect (Limited support)          |         |              |
| Mobile Device Access USB (Limited support) |         |              |
| Scanner support / SANE (Limited support)   |         |              |
| Mobile Device Access USB (Limited support) | 256.0 K | Not included |
| VPN OpenConnect (Limited support)          | 1.0 M   | Not included |
| Scanner support / SANE (Limited support)   | 2.5 M   | Not included |
| VirtualBox (Limited support)               | 64.0 M  | Not included |

## General Information 11.06.100

To be beneficial to all new features and implementations, it is recommended to use UMS 6.08.110 or higher and update the corresponding profiles.

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- VIA graphics driver

## Known Issues 11.06.100

### Citrix

- To launch **multiple desktop sessions** with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key must be enabled.



### More...

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Value     | <u>enabled</u> / <u>disabled</u>                                 |

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** while the session is ongoing does not work. The reader is visible, but **cannot be used due to permanently unknown reader status**.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1, and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with activated DRI3 and hardware-accelerated H.264 deep compression codec.
- With activated DRI3 and an AMD GPU, **Citrix H.264 acceleration plugin could freeze**. Selective H.264 mode (API v2) is not affected by this issue.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- With **Citrix Workspace** app versions **21.04.0 and 21.06.0**, **smartcard authentication fails to forward the PIN** correctly into the session for login. Instead, the user has to input the PIN a second time within the session. The problem does not occur with Citrix Workspace App 20.10.0.

### VMware Horizon

- **Client drive mapping** and **USB redirection** for storage devices **should not be enabled both at the same time**.
  - On the one hand, when using USB redirection for storage devices:  
The USB on-insertion feature is only working when the client drive mapping is switched off.  
In the IGEL Setup client drive mapping can be found in:  
**Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**.  
It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules.  
Furthermore, Horizon Client relies on the OS to mount the storage devices themselves.  
Enable local `Storage Hotplug` on setup page **Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection do not appear in the remote desktop.  
**Workaround: map the directory /media as a drive**. Then the external devices will show up inside the media drive.
- After disconnect of an RDP-based session, the **Horizon main window** which contains the server or sessions overview, **cannot be resized anymore**.
- **Copying Text from Horizon Blast sessions** isn't possible.



- The **on-screen keyboard in Horizon appliance mode** does not work correctly with the local logon.  
It is necessary to switch off the local logon and enable these two keys in the IGEL registry:  
`userinterface.softkeyboard.autoshow`  
`userinterface.softkeyboard.autohide`
- Zoom VDI Media Plugin makes Horizon Client crash** upon connection to the remote desktop in cases when TCSetup is running at the same time.
- When using the PCoIP protocol the virtual channel provided by VMware used for serial port and scanner redirection can make Horizon client hang** on logout from the remote session.  
This **happens when enabling scanner or serial port redirection**. The freeze does not occur if both redirection methods are enabled or none of them. The Blast Protocol isn't affected by this bug.  
The respective settings can be found here in the IGEL Registry:  
`vmware.view.enable-serial-port-redir`  
`vmware.view.enable-scanner-redir`
- Keyboard Input Source Language Synchronization** works only when using a local layout which has **deadkeys** enabled.  
If a keyboard layout is used which has deadkeys disabled (which is the default on IGEL OS), Horizon client falls back to en-US layout.

#### Parallels Client

- Native USB redirection** does not work with Parallels Client.

#### Firefox

- Certain modern **web portals used for cloud login** may fail to display because of **incompatibility with the current Firefox 78 ESR browser**.

#### Network

- Wakeup** from system suspend **fails on DELL Latitude 5510**.

#### Wi-Fi

- TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.  
**Workaround:** Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

#### Cisco JVDI Client

- There may be a **segfault** shown in the logs (during log out of Citrix Desktop session). Occurs only when using **Citrix Workspace app 20.10** and **Cisco JVDI**.

#### Base system

- Hyper-V (Generation 2) needs a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.
- Update from memory stick requires network online state** (at least when multiple update stages are involved)
- Unreliable messages** in user dialog for applying settings during boot. Could occur when new settings were fetched from the UMS.

#### deskMate



- Some **stability issues** may remain.

#### Conky

- The **right screen when using multiscreen environment** may not be shown correctly.  
**Workaround:** The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920)

#### Firmware update

- On **devices with 2 GB of flash** storage, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit [Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher<sup>373</sup>](#) for a possible solution and additional information.

#### OSC Installer

- OSC **not deployable with IGEL Deployment Appliance**: **New version 11.3 is required** for 11.06.100 deployment.

#### Appliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice instead of once.
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow **Native** client (auto is also possible) and should be started in fullscreen to prevent any opening windows.
- **Browser Appliance mode** can fail when the **Web URL contains special control characters** like ampersands (& character).  
**Workaround:** Add quotes at the beginning and the end of an affected URL. E.g.: '<https://www.google.com/search?q=aSearchTerm&source=lnms&tbo=isch>'

#### Audio

- **IGEL UD2 (D220)** fails to restore the **volume level** of the speaker when the device used firmware version 11.01.110 before.
- **Audio jack detection** on **Advantec POC-W243L** does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- **UD3 M340C**: Sound preferences are **showing Headphone & Microphone, although not connected**.

#### Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU** driver.

#### Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work on INTEL-based devices.

#### Remote Management

- **AIT feature with IGEL Starter License** is only supported by UMS version 6.05.100 or newer.

---

<sup>373</sup><https://kb.igel.com/igelos-11.04/en/error-not-enough-%C2%A0space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.html>



- If a parameter value is stored in a **template parameter**, the "**Apply changes**" dialog is displayed on each boot while receiving remote settings.

A possible **workaround**: Deactivate the "Apply changes" dialog with parameter:

[More...](#)

|            |                                                  |
|------------|--------------------------------------------------|
| IGEL Setup | <b>System &gt; Remote management</b>             |
| Parameter  | Display 'Apply changes' dialog on boot           |
| Registry   | userinterface.rmagent.enable_usermessage_on_boot |
| Value      | <u>enabled</u> / disabled                        |

## Security Fixes 11.06.100

### Firefox

- Updated Mozilla Firefox to **78.12.0esr**
  - aka mfsa2021-29:
    - CVE-2021-29970: **Use-after-free** in accessibility features of a document
    - CVE-2021-30547: **Out of bounds write in ANGLE**
    - CVE-2021-29976: **Memory safety** bugs fixed in Firefox 90 and Firefox ESR 78.12  
For details, see <https://www.mozilla.org/en-US/security/advisories/mfsa2021-29/>
  - aka mfsa2021-24:
    - CVE-2021-29964: **Out of bounds-read** when parsing a 'WM\_COPYDATA' message
    - CVE-2021-29967: **Memory safety** bugs fixed in Firefox 89 and Firefox ESR 78.11  
For details, see <https://www.mozilla.org/en-US/security/advisories/mfsa2021-24/>
  - aka mfsa2021-15:
    - CVE-2021-29951: **Mozilla Maintenance Service** could have been **started or stopped by domain users**
      - CVE-2021-23994: **Out of bound write** due to lazy initialization
      - CVE-2021-23995: **Use-after-free** in Responsive Design Mode
      - CVE-2021-23998: **Secure Lock icon** could have been spoofed
      - CVE-2021-23961: More **internal network hosts** could have been **probed by a malicious webpage**
      - CVE-2021-23999: **Blob URLs** may have been granted additional privileges
      - CVE-2021-24002: **Arbitrary FTP command execution** on FTP servers using an encoded URL
      - CVE-2021-29945: **Incorrect size computation in WebAssembly JIT** could lead to **null-reads**
      - CVE-2021-29946: **Port blocking** could be bypassed
    - For details, see <https://www.mozilla.org/en-US/security/advisories/mfsa2021-15/>

### Network

- Sensitive **SCEP settings** cannot be accessed by the **non-root user** anymore.

### Base system

- Fixed **chromium browser** security issues:



**More...**

CVE-2021-21157, CVE-2021-21156,  
CVE-2021-21155, CVE-2021-21154, CVE-2021-21153, CVE-2021-21152,  
CVE-2021-21151, CVE-2021-21150, CVE-2021-21149, CVE-2021-21190,  
CVE-2021-21189, CVE-2021-21188, CVE-2021-21187, CVE-2021-21186,  
CVE-2021-21185, CVE-2021-21184, CVE-2021-21183, CVE-2021-21182,  
CVE-2021-21181, CVE-2021-21180, CVE-2021-21179, CVE-2021-21178,  
CVE-2021-21177, CVE-2021-21176, CVE-2021-21175, CVE-2021-21174,  
CVE-2021-21173, CVE-2021-21172, CVE-2021-21171, CVE-2021-21170,  
CVE-2021-21169, CVE-2021-21168, CVE-2021-21167, CVE-2021-21166,  
CVE-2021-21165, CVE-2021-21164, CVE-2021-21163, CVE-2021-21162,  
CVE-2021-21161, CVE-2021-21160, CVE-2021-21159, CVE-2020-27844,  
CVE-2021-21193, CVE-2021-21192, CVE-2021-21191, CVE-2021-21199,  
CVE-2021-21198, CVE-2021-21197, CVE-2021-21196, CVE-2021-21195,  
CVE-2021-21194, CVE-2021-21220, CVE-2021-21206, CVE-2021-21221,  
CVE-2021-21219, CVE-2021-21218, CVE-2021-21217, CVE-2021-21216,  
CVE-2021-21215, CVE-2021-21214, CVE-2021-21213, CVE-2021-21212,  
CVE-2021-21211, CVE-2021-21210, CVE-2021-21209, CVE-2021-21208,  
CVE-2021-21207, CVE-2021-21205, CVE-2021-21204, CVE-2021-21203,  
CVE-2021-21202, CVE-2021-21201, CVE-2021-21226, CVE-2021-21225,  
CVE-2021-21224, CVE-2021-21223, CVE-2021-21222, CVE-2021-21233,  
CVE-2021-21232, CVE-2021-21231, CVE-2021-21230, CVE-2021-21229,  
CVE-2021-21228, CVE-2021-21227, CVE-2021-30520, CVE-2021-30519,  
CVE-2021-30518, CVE-2021-30517, CVE-2021-30516, CVE-2021-30515,  
CVE-2021-30514, CVE-2021-30513, CVE-2021-30512, CVE-2021-30511,  
CVE-2021-30510, CVE-2021-30509, CVE-2021-30508, CVE-2021-30507,  
CVE-2021-30506, CVE-2021-30521, CVE-2021-30522, CVE-2021-30523,  
CVE-2021-30524, CVE-2021-30525, CVE-2021-30526, CVE-2021-30527,  
CVE-2021-30528, CVE-2021-30529, CVE-2021-30530, CVE-2021-30531,  
CVE-2021-30532, CVE-2021-30533, CVE-2021-30534, CVE-2021-30535,  
CVE-2021-21212, CVE-2021-30536, CVE-2021-30537, CVE-2021-30538,  
CVE-2021-30539, CVE-2021-30540, CVE-2021-30544, CVE-2021-30545,  
CVE-2021-30546, CVE-2021-30547, CVE-2021-30548, CVE-2021-30549,  
CVE-2021-30550, CVE-2021-30551, CVE-2021-30552, CVE-2021-30553,  
CVE-2021-30554, CVE-2021-30555, CVE-2021-30556, and CVE-2021-30557

- Fixed **mysql-5.7** security issues:

**More...**

CVE-2021-2060, CVE-2021-2032, CVE-2021-2022,  
CVE-2021-2014, CVE-2021-2011, CVE-2021-2010, CVE-2021-2307, CVE-2021-2226,  
CVE-2021-2194, CVE-2021-2180, CVE-2021-2179, CVE-2021-2171, CVE-2021-2169,  
CVE-2021-2166, CVE-2021-2162, CVE-2021-2154, CVE-2021-2146, CVE-2021-2390,  
CVE-2021-2389, CVE-2021-2385, CVE-2021-2372, and CVE-2021-2342

- Fixed **wpa** security issue CVE-2021-0326.

- Fixed **openldap** security issues:

**More...**



CVE-2021-27212,  
CVE-2020-36230, CVE-2020-36229, CVE-2020-36228, CVE-2020-36227, CVE-2020-36226,  
CVE-2020-36225, CVE-2020-36224, CVE-2020-36223, CVE-2020-36222, and CVE-2020-36221

- Fixed **qemu** security issues:

[More...](#)

CVE-2021-20221, CVE-2021-20181, CVE-2020-35517,  
CVE-2021-3416, CVE-2021-20263, CVE-2021-20257,  
CVE-2021-3409, CVE-2021-3392, CVE-2020-25085, and CVE-2020-17380

- Fixed **zulu8** security issues:

[More...](#)

CVE-2020-14779, CVE-2020-14781, CVE-2020-14782,  
CVE-2020-14792, CVE-2020-14796, CVE-2020-14797,  
CVE-2020-14798, CVE-2020-14803, CVE-2021-2161,  
CVE-2021-2163, CVE-2021-2388, CVE-2021-2369, and CVE-2021-2341

- Fixed **bind9** security issues CVE-2020-8625, CVE-2021-25216, CVE-2021-25215,  
and CVE-2021-25214.

- Fixed **openssl1.0** security issues CVE-2021-23841, and CVE-2021-23840.

- Fixed **openssl** security issues CVE-2021-23841, CVE-2021-23840, CVE-2021-3449, CVE-2021-3712,  
and CVE-2021-3711.

- Fixed **xterm** security issue CVE-2021-27135.

- Fixed **aspell** security issue CVE-2019-25051.

- Fixed **nvidia-graphics-drivers-460** security issues CVE-2021-1052, CVE-2021-1053, CVE-2021-1076,  
and CVE-2021-1077.

- Fixed **python3.6** security issues CVE-2021-3177 and CVE-2020-27619.

- Fixed **tiff** security issues CVE-2020-35524 and CVE-2020-35523.

- Fixed **grub2** security issues:

[More...](#)

CVE-2020-14372, CVE-2020-27779, CVE-2020-25632, CVE-2020-25647,  
CVE-2021-20225, CVE-2021-20233, and CVE-2020-27749

- Fixed **python2.7** security issue CVE-2021-3177.

- Fixed **glib2.0** security issues CVE-2021-27219, CVE-2021-27218, CVE-2021-2721, and  
CVE-2021-28153.

- Fixed **pillow** security issues:

[More...](#)

CVE-2021-27923, CVE-2021-27922, CVE-2021-27921,  
CVE-2021-2792, CVE-2021-25293, CVE-2021-25292, CVE-2021-25290, CVE-2021-28678,  
CVE-2021-28677, CVE-2021-28676, CVE-2021-28675, CVE-2021-25288, and CVE-2021-25287

- Fixed **libjpeg-turbo** security issue CVE-2021-0384.

- Fixed **spice** security issue CVE-2021-20201.



- Fixed **.openssh** security issue CVE-2021-28041.
- Fixed **ldb** security issues CVE-2021-20277 and CVE-2020-27840.
- Fixed **lxml** security issue CVE-2021-28957.
- Fixed **openjpeg2** security issues CVE-2018-5727, CVE-2018-21010, and CVE-2018-20847.
- Fixed **unzip** security issue CVE-2019-13232.
- Fixed **curl** security issues CVE-2021-22890 and CVE-2021-22876.
- Fixed **xorg-server** security issue CVE-2021-3472.
- Fixed **nettle** security issues CVE-2021-20305, CVE-2021-3580, and CVE-2018-16869.
- Fixed **underscore** security issue CVE-2021-23358.
- Fixed **network-manager** security issue CVE-2021-20297.
- Fixed **libcaca** security issue CVE-2021-3410.
- Fixed **gst-plugins-good1.0** security issues CVE-2021-3498 and CVE-2021-3497.
- Fixed **webkit2gtk** security issues:

[More...](#)

CVE-2021-1871, CVE-2021-1844, CVE-2021-1788,  
 CVE-2021-30799, CVE-2021-30797, CVE-2021-30795, CVE-2021-30762,  
 CVE-2021-30761, CVE-2021-30758, CVE-2021-30749, CVE-2021-30744,  
 CVE-2021-30734, CVE-2021-30720, CVE-2021-30689, CVE-2021-30682,  
 CVE-2021-30666, CVE-2021-30665, CVE-2021-30663, CVE-2021-30661,  
 CVE-2021-21806, CVE-2021-21779, CVE-2021-21775, CVE-2021-1826,  
 CVE-2021-1825, CVE-2021-1820, and CVE-2021-1817

- Fixed **samba** security issue CVE-2021-20254.
- Fixed **openvpn** security issue CVE-2020-15078.
- Fixed **libxml2** security issues CVE-2021-3537, CVE-2021-3518, CVE-2021-3517, and CVE-2021-3516.
- Fixed **djvu** security issues:

[More...](#)

CVE-2021-3500, CVE-2021-32493, CVE-2021-32492,  
 CVE-2021-32491, CVE-2021-32490, and CVE-2021-3630

- Fixed **libx11** security issue CVE-2021-31535.
- Fixed **avahi** security issue CVE-2021-3468.
- Fixed **qpdf** security issues CVE-2021-36978 and CVE-2018-18020.
- Fixed **ffmpeg** security issues:

[More...](#)

CVE-2020-22033, CVE-2020-22021, CVE-2020-22019,  
 CVE-2020-22015, and CVE-2020-21041

- Fixed **systemd** security issues CVE-2021-33910 and CVE-2020-13529.
- **Update of ntfs-3g** to solve some security issues.

## Audio

- Fixed **libsndfile** security issue CVE-2021-3246.

## Remote Management



- Added **timeout for Secure VNC** and **Secure Terminal** connections, by default the timeout is 180 seconds. The **timeout can be changed by** the environment variable **IGEL\_TLS\_TUNNEL\_TIMEOUT** (in seconds, 0 for infinite).
- Fixed a possible **privilege escalation while sending user logoff** event to the UMS.

## VNC

- Fixed a **Secure Terminal** and **Secure VNC Shadowing remote code execution** vulnerability.

## Java

- Updated Zulu-8 JRE** to version **8u292**.

## New Features 11.06.100

## Citrix

- Added **Citrix Workspace App 2106**  
Available Citrix Workspace Apps in this release: **2106** (default), **2104**, and **2010**
- New registry keys:
  - The **battery status** of the device (notebooks/mobile devices) is now shown within the notification area of the Citrix Windows Desktop session.  
[More...](#)

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Battery status indicator                      |
| Registry  | ica.module.virtualdriver.mobilerceiver.enable |
| Type      | bool                                          |
| Value     | <u>enabled</u> / disabled                     |

- Added registry key for enabling **screen pinning or multi-monitor support with native Workspace app**.  
[More...](#)

|           |                                                |
|-----------|------------------------------------------------|
| Parameter | Enhanced experience for Multi-monitor scenario |
| Registry  | ica.authman.screenpinenabled                   |
| Value     | on / off                                       |

- Added registry key to enable **DNS cache**.  
[More...](#)

|           |                             |
|-----------|-----------------------------|
| Parameter | Enable DNS Cache            |
| Registry  | ica.authman.dnscacheenabled |
| Value     | on / off                    |

- Implemented "**Synchronize Citrix password with screensaver**" for **SelfService**. Parameter for StoreFront was (re-) used for that purpose.
- Updated **Citrix HDX RTME 2.9.400**
- Updated **Grundig Dictation driver** to version **20-09-16**.
- Added **passthrough authentication** for Citrix **SelfService**. Activate via parameter:



[More...](#)

|           |                                                                      |
|-----------|----------------------------------------------------------------------|
| Setup     | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; StoreFront Login</b> |
| Parameter | Use passthrough authentication                                       |
| Registry  | sessions.pnlogin0.settings.passthrough                               |
| Value     | true / <u>false</u>                                                  |

- Added: All parameters of the **Citrix setlog program** are now available in IGEL Setup via `ica.logging.setlog`. **Logging** can be **set permanently** now.
- Optimized structure of parameters for showing the inheritance more clearly.

- Added **automatic configuration of the Citrix webcam redirection** in ICA sessions.

[More...](#)

|           |                                                                    |
|-----------|--------------------------------------------------------------------|
| Setup     | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; HDX Multimedia</b> |
| Parameter | Automatic HDX webcam configuration                                 |
| Registry  | <code>ica.igel_hdxwebcam.enabled</code>                            |
| Value     | <u>enabled</u> / disabled                                          |
| Parameter | Resolution grade                                                   |
| Registry  | <code>ica.igel_hdxwebcam.quality</code>                            |
| Range     | [Very low] [Low] [ <u>Normal</u> ] [High] [Very high] [Best]       |
| Parameter | Minimal frame rate                                                 |
| Registry  | <code>ica.igel_hdxwebcam.framerate</code>                          |
| Value     | 15                                                                 |

- Added configuration for **h.264 encoding** in the **Citrix webcam redirection**

[More...](#)

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | HDX Webcam H264 encoding                      |
| Registry  | <code>ica.wfclient.hdxh264inputenabled</code> |
| Value     | <u>enabled</u> / <u>disabled</u>              |

- Added configuration for **native h.264 encoding** provided by webcam, for usage via the Citrix webcam redirection. This parameter **requires** the `ica.wfclient.hdxh264inputenabled` **set to "true"**.

[More...](#)

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | HDX Webcam H264 native                        |
| Registry  | <code>ica.wfclient.hdxh264enablenative</code> |
| Value     | <u>enabled</u> / <u>disabled</u>              |

## OSC Installer

- Enhanced OSC Installer for **creation of 'Factory preload images (master images)'**
  - Added possibility to **add initial settings to OSC Installer ISO**.
  - Added **support for 'Reset after first boot' for OSC Factory Image function**.
- Further information at <https://kb.igel.com/igelos-11.05/en/installation-42011487.html>

## RDP/IGEL RDP Client 2

- Added **multitouch** support for RDP Sessions.



[More...](#)

|          |                                               |
|----------|-----------------------------------------------|
| Registry | sessions.winconnect%.option.enable-multitouch |
| Value    | <a href="#">enabled / disabled</a>            |

- Added parameter to enable **server-side audio** for RDP sessions

[More...](#)

|          |                                                     |
|----------|-----------------------------------------------------|
| Registry | sessions.winconnect%.option.enable-serverside-audio |
| Value    | <a href="#">enabled / disabled</a>                  |

- Added option to enable/disable **automatic reconnect** for RDP session.

[More...](#)

|          |                                              |
|----------|----------------------------------------------|
| Registry | sessions.winconnect%.option.enable-reconnect |
| Type     | bool                                         |
| Value    | <a href="#">enabled / disabled</a>           |

## RD Web Access

- Added option to **save username** and **domain** for RD WebAccess login. In **legacy** mode, RD Web Access login uses the settings from **Sessions > RDP > RDP Global > Local Logon**.

[More...](#)

|           |                                                                             |
|-----------|-----------------------------------------------------------------------------|
| Setup     | <b>Sessions &gt; RDP &gt; Remote Desktop Web Access &gt; Authentication</b> |
| Parameter | Save username and domain from last login                                    |
| Registry  | rdp.rd_web_access.options.save_user_and_domain                              |
| Type      | string                                                                      |
| Value     | <a href="#">[Legacy] [Yes] [No]</a>                                         |

- Added option to enable/disable **automatic reconnect** for RD Web Access Apps.

[More...](#)

|          |                                    |
|----------|------------------------------------|
| Registry | rdp.rd_web_access.enable-reconnect |
| Type     | bool                               |
| Value    | <a href="#">enabled / disabled</a> |

## AVD / WVD

- Renamed WVD** (Windows Virtual Desktop) **to AVD** (Azure Virtual Desktop)
- Added **timezone redirection** support.
- Added **AVD printer redirection** support.

[More...](#)

|           |                                                                                                         |
|-----------|---------------------------------------------------------------------------------------------------------|
| Setup     | <b>Sessions &gt; AVD &gt; AVD Sessions &gt; AVD Session &gt; Printing &gt; CUPS Printer Redirection</b> |
| Parameter | CUPS printer redirection                                                                                |
| Registry  | sessions.wvd%.printing.cups                                                                             |
| Value     | <a href="#">enabled / disabled</a>                                                                      |



|           |                                                                                                                                                                                                                                                                         |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Setup     | <b>Devices &gt; Printer &gt; CUPS &gt; Printers &gt; Add Printer &gt; Mapping in sessions</b>                                                                                                                                                                           |
| Parameter | Map printer in AVD sessions                                                                                                                                                                                                                                             |
| Registry  | print.cups.printer%.map_wvd                                                                                                                                                                                                                                             |
| Value     | <u>enabled</u> / disabled                                                                                                                                                                                                                                               |
| Setup     | <b>Devices &gt; Printer &gt; CUPS &gt; Printers &gt; Add Printer &gt; Mapping in sessions</b>                                                                                                                                                                           |
| Parameter | Printer driver                                                                                                                                                                                                                                                          |
| Registry  | print.cups.printer%.wvd_printer_driver                                                                                                                                                                                                                                  |
| Note      | The default Windows driver name is "Microsoft PS Class Driver", which is installed by default and should work in general. For usage of a custom printer driver, the exact printer name must be set and the corresponding driver must be installed on AVD (server-)side. |

## UD Pocket

- Added official support for '**Secured Kobra Stick**' from **Digittrade**.

## VMware Horizon

- Allow wildcard symbol in Horizon client USB redirection rules:
  - Product ID can contain asterisks (\*\*\*) - \* represents one hexadecimal digit.
  - Product ID can be left empty which is equivalent to \*\*\*\* - for any Product ID.
- Added param to enable **MS Teams** support.

**Changed default of html5 multimedia redirection** to "enabled".

**More...**

|           |                                                                                                               |
|-----------|---------------------------------------------------------------------------------------------------------------|
| Setup     | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Unified Communications &gt; VDI Solutions</b> |
| Parameter | HTML5 multimedia redirection                                                                                  |
| Registry  | vmware.view.html5mmr                                                                                          |
| Type      | bool                                                                                                          |
| Value     | <u>enabled</u> / disabled                                                                                     |
| Setup     | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Unified Communications &gt; VDI Solutions</b> |
| Parameter | Microsoft Teams optimization                                                                                  |
| Registry  | vmware.view.vdwebrtc.enable                                                                                   |
| Type      | bool                                                                                                          |
| Value     | <u>enabled</u> / disabled                                                                                     |

- Added entry in IGEL Setup regarding Unified Communication: In **Sessions > Horizon Client > Horizon Client Global > Unified Communications > Cisco** for enabling **VDI support for Cisco**



**Webex Meetings** and in **Sessions > Horizon Client > Horizon Client Global > Unified Communications > VDI Solutions** for enabling **Zoom VDI Media Plugin**.

#### Parallels Client

- Updated **Parallels client** to version **18.1.0**

#### IBM\_5250

- Updated **IBM iAccess Client Solutions** to version **1.1.8.6**

#### NX client

- Updated **NoMachine client** to version **7.1.3**

#### Amazon WorkSpaces Client

- Updated **AWSC** to **3.1.9**

#### Chromium

- Updated **Chromium** browser to version **91.0.4472.164**
- Added "Block third party cookies" as parameter in the registry.
- Added **h.264 and AAC A/V playback support**. A/V playback support is only possible either in Chromium or in Firefox browser depending on these conditions:
  1. If Chromium feature is disabled, codecs are used in Firefox.
  2. If Firefox feature is disabled, codecs are used in Chromium.
  3. Number of sessions of each browser type are compared, codecs are used for browser with more sessions.
  4. Usage of codecs as configured via set of "default" browser, by registry key `system.default_apps.browser`.
- Added "Default web browser" configuration:

**More...**

|                                                                  |                                                                    |
|------------------------------------------------------------------|--------------------------------------------------------------------|
| Setup                                                            | <b>Sessions &gt; Chromium Browser &gt; Chromium Browser Global</b> |
| <b>Sessions &gt; Firefox Browser &gt; Firefox Browser Global</b> |                                                                    |
| Parameter                                                        | Default web browser                                                |
| Registry                                                         | <code>system.default_apps.browser</code>                           |
| Type                                                             | string                                                             |
| Value                                                            | <u>Firefox Browser</u>                                             |

- Added new configuration:

**More...**

|           |                                                                                  |
|-----------|----------------------------------------------------------------------------------|
| Setup     | <b>Sessions &gt; Chromium Browser &gt; Chromium Browser Global &gt; Security</b> |
| Parameter | Download allowlist                                                               |
| Registry  | <code>chromiumglobal.app.mimetype_forced_download</code>                         |
| Type      | string                                                                           |



|           |                                                                                                                                                                                                         |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Value     | <code>application/x-ica; application/x-rdp; application/smil; application/nxs; application/x-java-jnlp-file; application/x-2xa; application/x-sapshortcut; application/x-virt-viewer; image/tiff</code> |
| Setup     | <b>Sessions &gt; Chromium Browser &gt; Chromium Browser Global &gt; Security</b>                                                                                                                        |
| Parameter | Open file types automatically after downloading                                                                                                                                                         |
| Registry  | <code>chromiumglobal.app.mimetype_forced_open</code>                                                                                                                                                    |
| Type      | string                                                                                                                                                                                                  |
| Value     | <code>ica; rpd; smi; smil; nxs; jnlp; vv; tif; tiff</code>                                                                                                                                              |
| Setup     | <b>Sessions &gt; Chromium Browser &gt; Chromium Browser Global &gt; Security</b>                                                                                                                        |
| Parameter | File access                                                                                                                                                                                             |
| Registry  | <code>chromiumglobal.app.file_access_enabled</code>                                                                                                                                                     |
| Type      | bool                                                                                                                                                                                                    |
| Value     | <code>false</code>                                                                                                                                                                                      |

- **Removed redundant "Incognito mode"** as it has been replaced by "Allow incognito mode".
- **Renamed "Enable phishing and malware protection"** to "Safe Browsing".

[More...](#)

|           |                                                                                  |
|-----------|----------------------------------------------------------------------------------|
| Setup     | <b>Sessions &gt; Chromium Browser &gt; Chromium Browser Global &gt; Security</b> |
| Parameter | Safe Browsing                                                                    |
| Registry  | <code>chromiumglobal.app.safebrowsing_enabled</code>                             |
| Type      | bool                                                                             |
| Value     | <code>false</code>                                                               |

- Added the possibility to **clean the profile partition when Chromium browser is not used**.

## Firefox

- **Added "Default web browser"** to "Firefox Browser Global".

[More...](#)

|           |                                                                    |
|-----------|--------------------------------------------------------------------|
| Setup     | <b>Sessions &gt; Firefox Browser &gt; Firefox Browser Global</b>   |
|           | <b>Sessions &gt; Chromium Browser &gt; Chromium Browser Global</b> |
| Parameter | Default web browser                                                |
| Registry  | <code>system.default_apps.browser</code>                           |



|       |                        |
|-------|------------------------|
| Type  | string                 |
| Value | <u>Firefox Browser</u> |

- **Moved "Hide local file system"** from "Window" to "Security".

[More...](#)

|           |                                                                                |
|-----------|--------------------------------------------------------------------------------|
| Setup     | <b>Sessions &gt; Firefox Browser &gt; Firefox Browser Global &gt; Security</b> |
| Parameter | Hide local file system                                                         |
| Registry  | browserglobal.app.filepicker_dialog_hidden                                     |
| Type      | bool                                                                           |
| Value     | <u>True</u>                                                                    |

## Network

- **Changed names of Ethernet and Wi-Fi interfaces.** Apart from some symbolic occurrences, "**eth0**", "**eth1**", and "**wlan0**" have been **replaced by** so-called **predictable network interface names**.

Improved reliability of associating configurations with interfaces.

More than two Ethernet interfaces can be configured by creating further instances of `network.interfaces.ethernet.device%`. The following registry key may be used to explicitly assign a configuration instance to an interface:

[More...](#)

|           |                                                         |
|-----------|---------------------------------------------------------|
| Parameter | Fixed interface                                         |
| Registry  | <code>network.interfaces.ethernet.device%.ifname</code> |
| Type      | string                                                  |
| Value     | <u>empty</u>                                            |

- Added **r8152 third-party network driver**

- Added new registry key to enable the use of **r8152 third-party driver**:

[More...](#)

|           |                                                      |
|-----------|------------------------------------------------------|
| Parameter | Use thirdparty r8152 kernel module                   |
| Registry  | <code>network.drivers.r8152.prefer_thirdparty</code> |
| Range     | [Auto] [Yes] [No]                                    |

- In the **tcpdump** configuration, `eth0`, `eth1`, and `wlan0` are treated as symbolic names. These remain functional even if the true interface names are different.
- "**urkill**" tool has been removed from the firmware.
- Following **scripts provided by "urkill"** tool are **not available** anymore:
  - `/usr/share/urkill/scripts/block`
  - `/usr/share/urkill/scripts/flight-mode`
- In the case of using above mentioned commands via custom scripts: For turning radio devices on/off, usage of '**rfkill**' tool **may be needed** to enable custom scripts.  
`rfkill \<block`  
`|unblock> \<wlan|bluetooth|uwb|wimax|wwan|`  
`gps>`  
`rfkill \<block|unblock> all`



- Added registry key for specifying the **anonymous identity in authentication methods**.

[More...](#)

|           |                                                                          |
|-----------|--------------------------------------------------------------------------|
| Parameter | Anonymous Identity                                                       |
| Registry  | network.interfaces.ethernet.device%.ieee8021x.anonymous_identity         |
| Type      | string                                                                   |
| Value     | <u>empty</u>                                                             |
| Parameter | Anonymous Identity                                                       |
| Registry  | network.interfaces.wirelesslan.device0.wpa.anonymous_identity            |
| Type      | string                                                                   |
| Value     | <u>empty</u>                                                             |
| Parameter | Anonymous Identity                                                       |
| Registry  | network.interfaces.wirelesslan.device0.alt_ss_id%.wpa.anonymous_identity |
| Type      | string                                                                   |
| Value     | <u>empty</u>                                                             |

- Added support for **EAP FAST with inner method MSCHAPV2**. PAC files are stored persistently in /wfs/eap\_fast\_pacs/. File names can be determined with the script /bin/gen\_pac\_filename.sh.

In internal tests with hostapd, it was **necessary to disable TLS1.2** (registry key **phase1\_direct:tls\_disable\_tls1v1\_2=1**). The following registry keys have been added and "FAST" has been added to the range of the corresponding eap\_type registry keys:

[More...](#)

|           |                                                                        |
|-----------|------------------------------------------------------------------------|
| Parameter | Automatic PAC Provisioning                                             |
| Registry  | network.interfaces.ethernet.device%.ieee8021x.pac_provisioning         |
| Range     | [disabled] [unauthenticated] [authenticated] <b>[unrestricted]</b>     |
| Parameter | Automatic PAC Provisioning                                             |
| Registry  | network.interfaces.wirelesslan.device0.wpa.pac_provisioning            |
| Range     | [disabled] [unauthenticated] [authenticated] <b>[unrestricted]</b>     |
| Parameter | Automatic PAC Provisioning                                             |
| Registry  | network.interfaces.wirelesslan.device0.alt_ss_id%.wpa.pac_provisioning |
| Range     | [disabled] [unauthenticated] [authenticated] <b>[unrestricted]</b>     |

- Added **Realtek RTL8125 2.5Gigabit Ethernet driver**.

Wi-Fi



- Added new feature **Wi-Fi automatic switch on/off**. The following registry key has been added:  
[More...](#)

|           |                                                 |
|-----------|-------------------------------------------------|
| Parameter | Enable Wi-Fi automatic switch                   |
| Registry  | network.applet.wireless.enable_wifi_auto_switch |
| Value     | <u>enabled</u> / <u>disabled</u>                |

- Enabling this feature in combination with the following registry key will add a menu to the Wi-Fi manager applet which enables the user to switch Wi-Fi on, off, or select the automatic mode.  
[More...](#)

|           |                                            |
|-----------|--------------------------------------------|
| Parameter | Enable Wi-Fi switch                        |
| Registry  | network.applet.wireless.enable_wifi_switch |
| Type      | bool                                       |
| Value     | <u>enabled</u> / <u>disabled</u>           |

- When **automatic mode** is selected, **Wi-Fi will automatically switch to "off" if a LAN connection is available or switch to "on" if a LAN connection gets disconnected.**
- If "**Enable Wi-Fi switch**" is disabled and "**Enable Wi-Fi automatic switch**" is enabled, Wi-Fi automatic switch functionality will work in background and the user cannot see the menu entry in the Wi-Fi manager applet for changing the Wi-Fi mode.

NOTE: Any workaround for switching Wi-Fi on/off automatically using custom scripts should be eliminated.

- Added support for **Realtek RTW8852AE** Wi-Fi device.

#### AppliDis

- Integrated **Systancia AppliDis 6.0.0-4**

#### Imprivata

- Added registry key to **overcome the window overlap** that complicates the use of the local Setup or hotkeyed applications like the display switch.

[More...](#)

|          |                                  |
|----------|----------------------------------|
| Setup    | Registry                         |
| Registry | imprivata.avoid_focus_ownership  |
| Type     | bool                             |
| Value    | <u>enabled</u> / <u>disabled</u> |

- Added parameter to **ignore the VMware protocol selection** done by the appliance, local selection.

[More...](#)

|           |                                     |
|-----------|-------------------------------------|
| Parameter | Ignore the demanded VMWare protocol |
| Registry  | imprivata.ignore_horizon_protocol   |



|       |               |
|-------|---------------|
| Value | <u>false</u>  |
| Note: | Registry only |

## Smartcard

- Added support for **certgate AirID Bluetooth smartcard reader**. Enable with the registry parameter `scard.pcscd.certgate.airid_enable`. In addition, Bluetooth must be enabled in the Setup under **Devices > Bluetooth**.

[More...](#)

|           |                                                        |
|-----------|--------------------------------------------------------|
| Parameter | certgate AirID driver for Bluetooth smart card readers |
| Registry  | <code>scard.pcscd.certgate.airid_enable</code>         |
| Value     | <u>enabled / disabled</u>                              |

- Added **smartcard reader driver** for '**Kobra stick**' from **Digittrade**.

## Cisco Webex

- Added **version selection for Cisco Webex Meetings VDI** plugins. Available Cisco Webex Meetings VDI plugins in this release: **41.8.4.11** (default), **41.7.8.5** and **41.6.7.16**
- Added a registry key for **enabling the "active version"** of Cisco Webex Meetings client.

[More...](#)

|           |                                                                                     |
|-----------|-------------------------------------------------------------------------------------|
| Setup     | <b>Sessions &gt; Unified Communications &gt; Cisco WebEx Meetings VDI Selection</b> |
| Parameter | Cisco webex Meetings client version                                                 |
| Registry  | <code>multimedia.ciscomeetings.activeversion</code>                                 |
| Value     | <u>41.8.4.11, 41.7.8.5, and 41.6.7.16</u>                                           |

NOTE: Webex meetings plugin and application versions must match. Otherwise, it may fail to launch Webex VDI optimized meeting.  
With the integration of this selection, the necessary partition size was increased.

- Updated **Cisco Webex VDI** to version **41.8.0.19732**

## Cisco JVDI Client

- Updated **Cisco JVDI** to version **14.0.1**

## Base system

- Updated **IGEL EULA** to version April 2021.
- Removed permission to start **mousepad editor for non-root users**.
- Added new registry key to **toggle the executable rights** via the parameter:

[More...](#)

|           |                                                   |
|-----------|---------------------------------------------------|
| Parameter | Permission to start text editor                   |
| Registry  | <code>system.security.texteditorpermission</code> |



|       |                           |
|-------|---------------------------|
| Type  | bool                      |
| Value | <u>enabled / disabled</u> |

- Updated **kernel** to version **5.12.x**
- Added **compressed filesystem for Firefox and Chromium profile partitions**.
- Added **IGEL Device Encryption Feature**. Following registry keys have been added:  
[\*\*More...\*\*](#)

|           |                                                |
|-----------|------------------------------------------------|
| Parameter | Minimum password length                        |
| Registry  | system.deviceencryption.pwpolicy.minlen        |
| Type      | int                                            |
| Value     | <u>8</u>                                       |
| Parameter | Minimum amount of upper case letters           |
| Registry  | system.deviceencryption.pwpolicy.minupper      |
| Type      | int                                            |
| Value     | <u>0</u>                                       |
| Parameter | Minimum amount of lower case letters           |
| Registry  | system.deviceencryption.pwpolicy.minlower      |
| Type      | int                                            |
| Value     | <u>1</u>                                       |
| Parameter | Minimum amount of special characters           |
| Registry  | system.deviceencryption.pwpolicy.minspecial    |
| Type      | int                                            |
| Value     | <u>0</u>                                       |
| Parameter | Minimum amount of numbers                      |
| Registry  | system.deviceencryption.pwpolicy.minnumbers    |
| Type      | int                                            |
| Value     | <u>0</u>                                       |
| Parameter | Special characters allowed                     |
| Registry  | system.deviceencryption.pwpolicy.specialset    |
| Type      | string                                         |
| Value     | <u>!"\$%&amp;/()[]{}?+~-**"</u>                |
| Parameter | Unwanted strings in password (comma separated) |
| Registry  | system.deviceencryption.pwpolicy.exclude       |
| Type      | string                                         |
| Value     | <u>empty</u>                                   |
| Parameter | The password must contain                      |
| Registry  | system.deviceencryption.pwpolicy.fulfill       |
| Range     | <u>[all] [2 of] [3 of]</u>                     |
| Parameter | Device encryption state                        |
| Registry  | system.deviceencryption.state                  |
| Range     | <u>[0] [1] [2]</u>                             |



|                                                                                                                                                              |                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                                                                                                                                                    | Password aggregation function                                                                                                                                         |
| Registry                                                                                                                                                     | system.deviceencryption.security_level                                                                                                                                |
| Range                                                                                                                                                        | [I: Argon2id, 8M/7 ops] [II: Argon2id, 128M/3 ops]<br>[III: Argon2id, 256M/3 ops] [IV: Argon2id, 512M/3 ops]<br>[V: Argon2id, 1024M/4 ops] [VI: Argon2id, 128M/4 ops] |
| Parameter                                                                                                                                                    | Security level                                                                                                                                                        |
| Registry                                                                                                                                                     | system.deviceencryption.security_mode                                                                                                                                 |
| Range                                                                                                                                                        | [Auto, constant-time] [Auto, at least level] [Manual]                                                                                                                 |
| Parameter                                                                                                                                                    | Target time delay (ms)                                                                                                                                                |
| Registry                                                                                                                                                     | system.deviceencryption.security_delay_ms                                                                                                                             |
| Type                                                                                                                                                         | int                                                                                                                                                                   |
| Value                                                                                                                                                        | <u>700</u>                                                                                                                                                            |
| Parameter                                                                                                                                                    | Device Encryption mode                                                                                                                                                |
| Registry                                                                                                                                                     | system.deviceencryption.                                                                                                                                              |
| Range                                                                                                                                                        | [keep] [activate] [deactivate]                                                                                                                                        |
| Parameter                                                                                                                                                    | Authentication type                                                                                                                                                   |
| Registry                                                                                                                                                     | system.deviceencryption.auth_type                                                                                                                                     |
| Range                                                                                                                                                        | [PW]                                                                                                                                                                  |
| Value                                                                                                                                                        | <u>PW</u>                                                                                                                                                             |
| Parameter                                                                                                                                                    | Wipe config and user data upon activation                                                                                                                             |
| Registry                                                                                                                                                     | system.deviceencryption.wipe_data                                                                                                                                     |
| Type                                                                                                                                                         | bool                                                                                                                                                                  |
| Value                                                                                                                                                        | enabled / <u>disabled</u>                                                                                                                                             |
| Parameter                                                                                                                                                    | Display password as plain text on logon screen is possible                                                                                                            |
| Registry                                                                                                                                                     | system.deviceencryption.option_display_ptpass                                                                                                                         |
| Type                                                                                                                                                         | bool                                                                                                                                                                  |
| Value                                                                                                                                                        | enabled / <u>disabled</u>                                                                                                                                             |
| Parameter                                                                                                                                                    | Downgrade without warning of data loss                                                                                                                                |
| Registry                                                                                                                                                     | system.deviceencryption.force_downgrade                                                                                                                               |
| Type                                                                                                                                                         | bool                                                                                                                                                                  |
| Value                                                                                                                                                        | enabled / <u>disabled</u>                                                                                                                                             |
| <ul style="list-style-type: none"> <li>Added a new registry to <b>show verbose boot messages and disable the splash</b> (for debugging purposes).</li> </ul> |                                                                                                                                                                       |
| <b>More...</b>                                                                                                                                               |                                                                                                                                                                       |
| Parameter                                                                                                                                                    | Disable splash and show verbose messages on bootup                                                                                                                    |
| Registry                                                                                                                                                     | system.kernel.bootparams.noquiet                                                                                                                                      |
| Type                                                                                                                                                         | bool                                                                                                                                                                  |
| Value                                                                                                                                                        | enabled / <u>disabled</u>                                                                                                                                             |



- Added **automatic proxy detection and PAC file support** for proxy authentication pass through with cntlm.
- Updated **French translation**
- Added support for **multiple batteries** in the taskbar. If enabled, the taskbar shows a battery indicator for each device battery.

[More...](#)

|           |                                                                         |
|-----------|-------------------------------------------------------------------------|
| Parameter | Display multi battery                                                   |
| Registry  | windowmanager.wm0.variables.battery_indicator<br>.display_multi_battery |
| Type      | bool                                                                    |
| Value     | enabled / <u>disabled</u>                                               |

- Hide "Other user" label on login screen** when not needed.
- Add **TLS** options for **rsyslog**

[More...](#)

|           |                                     |
|-----------|-------------------------------------|
| Parameter | TLS enabled                         |
| Registry  | system.syslog.output%.tls           |
| Type      | bool                                |
| Value     | enabled / <u>disabled</u>           |
| Parameter | CA Certificate                      |
| Registry  | system.syslog.output%.cacertificate |
| Type      | string                              |
| Value     | <u>empty</u>                        |

- Added support to **monitor multiple sessions** and **have a post-session command triggered** if all sessions exited successfully.

Configurable at Setup page: **System > Firmware Customization > Custom Commands > Post Session**

- Added configuration for **EMP license notification**:

[More...](#)

|           |                                                                              |
|-----------|------------------------------------------------------------------------------|
| Parameter | Enable Enterprise Management Pack license notification                       |
| Registry  | userinterface.license_notification.enable_enterprise_management_notification |
| Type      | bool                                                                         |
| Value     | <u>enabled</u> / disabled                                                    |

- Added further configuration of **logon with local user password**. In Setup on page **Security > Logon > Local User** and also within IGEL Setup Assistant. The used password parameter is the former screenlock password.

[More...](#)

|           |                                            |
|-----------|--------------------------------------------|
| Setup     | <b>Security &gt; Logon &gt; Local User</b> |
| Parameter | Login with local user password             |
| Registry  | auth.login.xlock                           |



|           |                                            |
|-----------|--------------------------------------------|
| Value     | true / false                               |
| Setup     | <b>Security &gt; Logon &gt; Local User</b> |
| Parameter | Password                                   |
| Registry  | sessions.xlock0.options.password           |
| Value     | empty                                      |

- Added **passthrough NTLM authentication** for Firefox. If enabled, the user name and password from the local logon mask will be used for automatic NTLM authentication to websites and proxies.

[More...](#)

|           |                                     |
|-----------|-------------------------------------|
| Parameter | Passthrough for NTLM authentication |
| Registry  | auth.login.ntlm.passthrough         |
| Value     | true / false                        |

- Added **Single Sign on NTLM authentication to Firefox after Kerberos smartcard authentication**. If enabled, NTLM credentials are retrieved at smartcard logon. These credentials are then used for automatic NTLM authentication to websites and proxies. For this functionality, an appropriate Kerberos keytab has to be specified in parameter auth.krb5.keytab.crypt\_password.

[More...](#)

|           |                                             |
|-----------|---------------------------------------------|
| Parameter | Store supplemental credentials              |
| Registry  | auth.krb5.appdefaults.pam.store_nt_owf_pass |
| Value     | true / false                                |

- Added **client-side NTLM authenticating proxy**. If it is enabled, applications which use the system proxy settings will connect via this local proxy. It will transparently do NTLM authentication.

[More...](#)

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Enable client side NTLM authenticating proxy |
| Registry  | network.proxy.cntlm.enable                   |
| Value     | true / false                                 |
| Parameter | Listening Port                               |
| Registry  | network.proxy.cntlm.port                     |
| Value     | 3128                                         |

- Added **Kerberos login verification**. If this is enabled, login will fail unless a service ticket sent from the KDC/domain controller can be verified. For this, the configuration of an appropriate Kerberos keytab is necessary. The keytab must be encoded in base64.

[More...](#)

|           |                                            |
|-----------|--------------------------------------------|
| Parameter | Verify credentials against a local key     |
| Registry  | auth.krb5.libdefaults.verify_ap_req_nofail |
| Value     | true / false                               |
| Parameter | Keytab (base64)                            |
| Registry  | auth.krb5.keytab.crypt_password            |
| Value     | empty                                      |

- Set **device hostname based on a remote asset service**.



[More...](#)

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Enable remote asset service                  |
| Registry  | network.remote_asset.enable                  |
| Type      | bool                                         |
| Value     | <u>enabled</u> / <u>disabled</u>             |
| Parameter | Url                                          |
| Registry  | network.remote_asset.url                     |
| Type      | string                                       |
| Value     | <u>empty</u>                                 |
| Parameter | Response type                                |
| Registry  | network.remote_asset.response_type           |
| Range     | [Xml][Json]                                  |
| Parameter | Validation path                              |
| Registry  | network.remote_asset.validation_path         |
| Type      | string                                       |
| Value     | <u>empty</u>                                 |
| Parameter | Pre fallback identifier                      |
| Registry  | network.remote_asset.pre_fallback_identifier |
| Type      | string                                       |
| Value     | <u>ITC</u>                                   |

#### Lakeside SysTrack

- Updated **Lakeside SysTrack client plugin** for Citrix, RDP, and VMware Horizon Client to **version 9.0**. New support for Microsoft AVD Client:

[More...](#)

|           |                                     |
|-----------|-------------------------------------|
| Parameter | Lakeside SysTrack                   |
| Registry  | sessions.wvd<inst>.plugins.lakeside |
| Value     | <u>true</u> / <u>false</u>          |

#### Conky

- Added **support for Conky system monitor**:

[More...](#)

| IGEL Setup | Accessories > Conky System Monitor > Options        |
|------------|-----------------------------------------------------|
| Parameter  | Use IGEL Setup for configuration                    |
| Registry   | userinterface.system_monitor.conky.igelsetup.config |
| Type       | bool                                                |
| Value      | <u>enabled</u> / <u>disabled</u>                    |
| IGEL Setup | Accessories > Conky System Monitor > Options        |



|                   |                                                                                                                       |
|-------------------|-----------------------------------------------------------------------------------------------------------------------|
| Parameter         | Monitor                                                                                                               |
| Registry          | userinterface.system_monitor.conky.display                                                                            |
| Range             | [Automatic][1st monitor][2nd monitor][3rd monitor][4th monitor][5th monitor][6th monitor][7th monitor][8th monitor]   |
| Value             | <u>1st monitor</u>                                                                                                    |
| <b>IGEL Setup</b> | <b>Accessories &gt; Conky System Monitor &gt; Options</b>                                                             |
| Parameter         | Window type                                                                                                           |
| Registry          | userinterface.system_monitor.conky.window_type                                                                        |
| Range             | [Normal][Desktop][Dock][Panel][Override]                                                                              |
| Value             | <u>Normal</u>                                                                                                         |
| <b>IGEL Setup</b> | <b>Accessories &gt; Conky System Monitor &gt; Options</b>                                                             |
| Parameter         | Alignment                                                                                                             |
| Registry          | userinterface.system_monitor.conky.alignment                                                                          |
| Range             | [Top Left][Top Right][Top Middle][Bottom Left][Bottom Right][Bottom Middle][Middle Left][Middle Middle][Middle Right] |
| Value             | <u>Top Right</u>                                                                                                      |
| <b>IGEL Setup</b> | <b>Accessories &gt; Conky System Monitor &gt; Options</b>                                                             |
| Parameter         | Layer                                                                                                                 |
| Registry          | userinterface.system_monitor.conky.hint_layer                                                                         |
| Range             | [Below][Above][None]                                                                                                  |
| Value             | <u>Below</u>                                                                                                          |
| <b>IGEL Setup</b> | <b>Accessories &gt; Conky System Monitor &gt; Options</b>                                                             |
| Parameter         | Decorations                                                                                                           |
| Registry          | userinterface.system_monitor.conky.hint_decorations                                                                   |
| Type              | bool                                                                                                                  |
| Value             | <u>enabled / disabled</u>                                                                                             |
| <b>IGEL Setup</b> | <b>Accessories &gt; Conky System Monitor &gt; Options</b>                                                             |
| Parameter         | Show in taskbar                                                                                                       |
| Registry          | userinterface.system_monitor.conky.hint_taskbar                                                                       |
| Type              | bool                                                                                                                  |
| Value             | <u>enabled / disabled</u>                                                                                             |
| <b>IGEL Setup</b> | <b>Accessories &gt; Conky System Monitor &gt; Options</b>                                                             |
| Parameter         | Default color                                                                                                         |
| Registry          | userinterface.system_monitor.conky.default_color                                                                      |



|                   |                                                                |
|-------------------|----------------------------------------------------------------|
| Type              | string                                                         |
| Value             | <u>#ff8000</u>                                                 |
| <b>IGEL Setup</b> | <b>Accessories &gt; Conky System Monitor &gt; Options</b>      |
| Parameter         | Font type                                                      |
| Registry          | userinterface.system_monitor.conky.font_type                   |
| Type              | editable                                                       |
| Value             | <u>Monospace / Sans / &lt;custom-string&gt;</u>                |
| <b>IGEL Setup</b> | <b>Accessories &gt; Conky System Monitor &gt; Options</b>      |
| Parameter         | Font size                                                      |
| Registry          | userinterface.system_monitor.conky.font_size                   |
| Type              | integer                                                        |
| Value             | <u>8</u>                                                       |
| <b>IGEL Setup</b> | <b>Accessories &gt; Conky System Monitor &gt; Options</b>      |
| Parameter         | Opacity                                                        |
| Registry          | userinterface.system_monitor.conky.opacity                     |
| Type              | integer                                                        |
| Value             | <u>255</u>                                                     |
| <b>IGEL Setup</b> | <b>Accessories &gt; Conky System Monitor &gt; Options</b>      |
| Parameter         | Borders                                                        |
| Registry          | userinterface.system_monitor.conky.draw_borders                |
| Type              | bool                                                           |
| Value             | <u>enabled / disabled</u>                                      |
| <b>IGEL Setup</b> | <b>Accessories &gt; Conky System Monitor &gt; Options</b>      |
| Parameter         | Offset horizontal                                              |
| Registry          | userinterface.system_monitor.conky.gap_x                       |
| Type              | integer                                                        |
| Value             | <u>5</u>                                                       |
| <b>IGEL Setup</b> | <b>Accessories &gt; Conky System Monitor &gt; Options</b>      |
| Parameter         | Offset vertical                                                |
| Registry          | userinterface.system_monitor.conky.gap_y                       |
| Type              | integer                                                        |
| Value             | <u>60</u>                                                      |
| <b>IGEL Setup</b> | <b>Accessories &gt; Conky System Monitor &gt; Custom Setup</b> |
| Parameter         | Config name                                                    |
| Registry          | userinterface.system_monitor.conky.custom_config%.config_name  |
| Type              | string                                                         |
| Value             | <u>empty</u>                                                   |
| <b>IGEL Setup</b> | <b>Accessories &gt; Conky System Monitor &gt; Custom Setup</b> |
| Parameter         | Config value                                                   |



|                   |                                                                             |
|-------------------|-----------------------------------------------------------------------------|
| Registry          | <code>userinterface.system_monitor.conky.custom_config%.config_value</code> |
| Type              | string                                                                      |
| Value             | <u>empty</u>                                                                |
| <b>IGEL Setup</b> | <b>Accessories &gt; Conky System Monitor &gt; Custom Setup</b>              |
| Parameter         | Text                                                                        |
| Registry          | <code>userinterface.system_monitor.conky.custom_text%.text_line</code>      |
| Type              | string                                                                      |
| Value             | <u>empty</u>                                                                |

## Driver

- Updated **Grundig Dictation driver** to version **20-09-16**. This **fixes termination of Citrix sessions** when USB devices are plugged or unplugged with Citrix Workspace App newer than 2009.
- Added **basic HyperV DRM driver** to support resolution changes during runtime in HyperV VM.

## Firmware update

- Added support for IGEL's **automatic update service**; supposed to be used **for devices during evaluation**.  
[More...](#)

|           |                                                      |
|-----------|------------------------------------------------------|
| Parameter | Enable automatic update service                      |
| Registry  | <code>update.auto-service.enable</code>              |
| Range     | [During evaluation only][Off]                        |
| Value     | <u>During evaluation only</u>                        |
| Parameter | Check interval                                       |
| Registry  | <code>update.auto-service.interval</code>            |
| Type      | integer                                              |
| Value     | <u>0</u>                                             |
| Parameter | Randomized delay                                     |
| Registry  | <code>update.auto-service.randomized_delay</code>    |
| Type      | integer                                              |
| Value     | <u>0</u>                                             |
| Parameter | Count of maximal delays                              |
| Registry  | <code>update.auto-service.max_delays</code>          |
| Type      | integer                                              |
| Value     | <u>0</u>                                             |
| Parameter | Timeout for user dialog                              |
| Registry  | <code>update.auto-service.user_dialog_timeout</code> |
| Type      | integer                                              |



|           |                             |
|-----------|-----------------------------|
| Value     | 0                           |
| Parameter | Target version              |
| Registry  | update.auto-service.version |
| Type      | string                      |
| Value     | <u>empty</u>                |
| Parameter | Server address              |
| Registry  | update.auto-service.server  |
| Type      | string                      |
| Value     | <u>empty</u>                |

- Added: **sftp protocol** supports now the following key exchange methods:  
ecdh-sha2-nistp256 (BSI)  
ecdh-sha2-nistp384 (BSI)  
ecdh-sha2-nistp521 (BSI)  
curve25519-sha256 (BSI)  
curve25519-sha256@libssh.org (BSI)  
diffie-hellman-group-exchange-sha256  
diffie-hellman-group-exchange-sha1  
diffie-hellman-group14-sha1  
diffie-hellman-group1-sha1
- Added: **Prevent firmware update if battery level has reached critical status** (on battery-powered devices). The following registry key has been introduced to configure this option:  
[More...](#)

|           |                                                           |
|-----------|-----------------------------------------------------------|
| Parameter | Allow firmware update even when battery state is critical |
| Registry  | update.update_on_critical_battery_status                  |
| Type      | bool                                                      |
| Value     | <u>enabled</u> / <u>disabled</u>                          |

## Driver

- Updated **deviceTRUST** client plugin for Citrix, RDP, and Amazon WorkSpaces Client to version **20.2.310**. New support for **Amazon WorkSpaces Client and Microsoft AVD Client**, enabling via:  
[More...](#)

|           |                                        |
|-----------|----------------------------------------|
| Parameter | deviceTRUST                            |
| Registry  | awsc.plugins.devicetrust               |
| Value     | <u>true</u> / <u>false</u>             |
| Parameter | deviceTRUST                            |
| Registry  | sessions.wvd<inst>.plugins.devicetrust |
| Value     | <u>true</u> / <u>false</u>             |

## X11 system



- Added: **Inhibit screensaver while a Zoom, Teams, or Skype for Business meeting is active.**  
Works for native clients and Citrix optimization plugins.
  - Added: **Inhibit screensaver while a Cisco Webex Meetings session is active in Citrix Workspace App.**
- More...**

|          |                                             |
|----------|---------------------------------------------|
| Registry | debug.tools.igel-screensaver-monitor.enable |
| Value    | <u>enabled / disabled</u>                   |

## Window manager

- Allow user to define rules which inhibit the screensaver. Audio and USB rules can be configured.** Audio rules are applied if a matched audio stream is played back and USB rules are applied if a matched USB device is connected.

|           |                                                      |
|-----------|------------------------------------------------------|
| Parameter | Regular expression to match audio stream name        |
| Registry  | userinterface.screenlock.inhibit.audio%.name         |
| Value     | .*                                                   |
| Parameter | Regular expression to match audio stream application |
| Registry  | userinterface.screenlock.inhibit.audio%.application  |
| Value     | .*                                                   |
| Parameter | Regular expression to match USB serial               |
| Registry  | userinterface.screenlock.inhibit.usb%.serial         |
| Value     | .*                                                   |
| Parameter | Regular expression to match USB product name         |
| Registry  | userinterface.screenlock.inhibit.usb%.product        |
| Value     | .*                                                   |
| Parameter | Regular expression to match USB vendor name          |
| Registry  | userinterface.screenlock.inhibit.usb%.vendor         |
| Value     | .*                                                   |
| Parameter | Regular expression to match USB product id           |
| Registry  | userinterface.screenlock.inhibit.usb%.pid            |
| Value     | .*                                                   |
| Parameter | Regular expression to match USB vendor id            |
| Registry  | userinterface.screenlock.inhibit.usb%.vid            |
| Value     | .*                                                   |

## VNC Viewer



- Added: **Exit VNC client silently** without prompting an error message.

[More...](#)

|           |                              |
|-----------|------------------------------|
| Parameter | Alert on fatal error         |
| Registry  | network.vncserver.promptuser |
| Value     | <u>enabled</u> / disabled    |

## Audio

- Added possibility to **disable webcam audio**.

[More...](#)

|          |                                 |
|----------|---------------------------------|
| Registry | multimedia.webcam.disable_audio |
| Value    | true / <u>false</u>             |

## Zoom Media Plugin

- Added **selection for Zoom VDI Clients**.

Available Zoom Media Plugins in this release: **5.5.12716**, **5.4.59458** and **5.5.8.20606** (default)

[More...](#)

|           |                                                                        |
|-----------|------------------------------------------------------------------------|
| Setup     | <b>Sessions &gt; Unified Communications &gt; Zoom Client Selection</b> |
| Parameter | Zoom client version                                                    |
| Registry  | multimedia.zoomvdi.activeversion                                       |
| Value     | 5.5.8.20606, 5.5.12716, 5.4.59458                                      |

With the integration of this selection, the necessary partition size was increased.

## Evidian

- Updated **Evidians rsUserAuth** to version **1.5.7789**, with that the "**Ignore Smartcard Removal**" feature was **fixed**.

[More...](#)

|           |                                                           |
|-----------|-----------------------------------------------------------|
| Setup     | <b>Sessions &gt; Evidian AuthMgr Session &gt; Options</b> |
| Parameter | Ignore Smartcard Removal on this Reader                   |
| Type      | string                                                    |

## HID

- Added **touchscreen support for Microsoft Surface Pro 4**.

## Hardware

- Added new registry keys for **configuring new i915 parameter**. New registry keys:

[More...](#)

|           |                                                          |
|-----------|----------------------------------------------------------|
| Parameter | Disable the use of limited color range for DisplayPort 1 |
| Registry  | x.drivers.intel.dp1_no_limited_color_range               |



|       |                                                                                     |
|-------|-------------------------------------------------------------------------------------|
| Range | [Default] [No] [Yes]                                                                |
| Value | <u>Default</u> (only for M250C, the use of limited color range for DP1 is disabled) |

- Added hardware **support for HP t540**.
- Updated **DisplayLink driver** to version **5.4**.
- Note: The IGEL device **UD3-LX50** reached **End of Maintenance**.

#### TC Setup (Java)

- Updated **TC Setup** to version **6.8.8**

#### Fabulatech

- Updated **FabulaTech USB for Remote Desktop** to version **6.0.28**
- Updated **FabulaTech Scanner for Remote Desktop** to version **2.7.0.1**
- Fixed **FabulaTech scanner redirection** not working for **Citrix**

#### Remote Management

- Changed the **default behavior of the user dialog about applying remote settings received during boot**. The dialog now has a **timeout of 20 seconds by default**. If the **timeout is exceeded**, the received **settings will be automatically applied**. The behavior is configurable at Setup page **System > Remote management**.

#### Resolved Issues 11.06.100

##### Citrix

- Improved **startup of Citrix USB daemon**.
  - Updated **Grundig Dictation** driver to version **20-09-16**. This **fixes termination of Citrix sessions when USB devices are plugged / unplugged** with Citrix Workspace App newer than 20.09.
  - Fixed: The **NSAP virtual channel** is loaded correctly and works as expected.
  - Improved dialog for **Citrix farm selection**.
  - Changed the default value of** the parameter '**HDX Adaptive Transport over EDT**' to '**TCP only**'.
- With the previous default value 'UDP with fallback to TCP' performance problems occurred.
- [More...](#)

|            |                                                                                          |
|------------|------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix XenDesktop/XenApp &gt; HDX/ICA Global &gt; Options</b>           |
| Parameter  | HDX Adaptive Transport over EDT                                                          |
| Registry   | ica.wfclient.hdxoverudp                                                                  |
| Range      | [UDP without fallback to TCP]<br>[TCP Only - UDP disabled]<br>[UDP with fallback to TCP] |

- Fixed problems with **Citrix multimedia redirection**
- Fixed Browser Appliance mode a **white screen is shown when the browser was not closed correctly** but the process got terminated.
- Fixed **Citrix login with certain passwords and PINs**.



- Improved start of Citrix **logging** daemon **ctxlogd with CWA 2104**
- Fixed **Citrix SelfService passthrough login** in case the user interface is set to German.
- Fixed **post-session commands for Citrix sessions**, an exception for return code 2 and process **wfica** was added to the registry under **pcom**.
- Updated **HDX Realtime Optimization Pack** to version **2.9.300**

#### OSC Installer

- OSC **not deployable with IGEL Deployment Appliance: New version 11.3 is required for 11.06.100 deployment.**
- Enhanced the **boot cmdline** options for OSC

#### AVD / WVD

- Fixed access **bearer token re-authentication** (see also "sign-in frequency" setting in Azure).
- Fixed issue with **AVD workspace names that contain slashes**.
- Fixed **timezone redirection** for MS-Teams chat/calendar and for Edge browser.  
Note: **Page reload or MS-Teams application restart might be needed** when the timezone actually changes.
- Fixed **sporadic appearance of claims token dialog** while in a running session.
- Fixed **claims token dialog** being shown **when session reconnects happen too fast** (within 60s).
- Added: Set the **HttpAcceptLanguage property in browser instance** to the currently selected language for showing the Azure login page in the correct language.

#### VMware Horizon

- Fixed the broken session handling when using **Webex Teams where the Horizon session could only be started once**.
- Fixed '**Remember last user**' functionality in **Appliance Mode**.
- Fixed Horizon session **bouncing back to login**
- Fixed setting regarding **Blast HEVC decoding**: `vmware.view.blast-hevc`
- Fixed setting regarding **synchronization of lock modifiers** (num lock, shift lock, and scroll lock): `vmware.view.enable-sync-numlock`

#### Parallels Client

- Fixed an issue where the **post-session command got triggered too early**

#### IBM\_5250

- Fixed error in **iAccess configuration**.

#### Chromium

- Fixed **browser certificates were lost after reboot** if UMS was not reachable
- Fixed **too small chromium profile partition**.
- Removed parameter "**On startup->Continue where you left off**" for Chromium sessions
- Added "**Autostart requires network**" to Chromium Browser Session settings
- Modified: '**Automatic browser restart on exit**' no longer needs a reboot to be deactivated
- Removed option "**On Startup->Continue where you left off**" for Chromium sessions, this feature only works globally
- Fixed **reboot was required to toggle the splash screen**
- Modified: '**Automatic browser restart on exit**' does now restart every time the browser is closed



- Fixed '**Language**' and '**Chromium translation**' was not working as expected
- Changed: Replaced **download location prompt** by download confirmation popup
- Added warning **popup if downloads are blocked**
- Fixed: **Auto-opened files will not be blocked** (e.g. ica connection files)
- Added: **RDP now works with Chromium** Browser

#### Network

- The currently used parameter **tls-remote is deprecated** and was **removed in openVPN 2.4**. It was **changed to verify-x509-name**.
- **Certificate keys without passwords** can be used.
- Improved network device order for **LG Electronics CL60**.
- Improved **WWAN device connection activation**.
- Fixed **handling 802.1X** registry keys phase1\_direct, phase2\_direct
- Improved network interface order for **LG Electronics 27CN650W** (dmi product\_name CN65)

#### Wi-Fi

- Added registry key for **tweaking the WPA supplicant**. In general, the value is a comma-separated list of names. If it contains LATESUCCESS, a late EAP-Success message will be ignored. When such a message arrives, it had been dropped. This might cause WPA Enterprise authentication to restart.

**More...**

|           |                                                        |
|-----------|--------------------------------------------------------|
| Parameter | IGEL Tweaks                                            |
| Registry  | network.interfaces.wirelesslan.device0.wpa.igel_tweaks |
| Type      | string                                                 |
| Value     | empty                                                  |

- Added registry key to **activate usage of broadcom sta driver** (needed for older broadcom Wi-Fi devices)

**More...**

|           |                                                 |
|-----------|-------------------------------------------------|
| Parameter | Use broadcom sta driver instead of b43 for WLAN |
| Registry  | network.drivers.broadcom.use_broadcom_sta       |
| Type      | bool                                            |
| Value     | enabled / disabled                              |

- Updated **wireless regulatory database** to version from **July 2021**.

#### Open VPN

- Added: **Certificate keys without passwords** can be used.
- Added new **config parameter in dropdown menu to use tls-crypt**

#### Imprivata

- Fixed **Horizon session bouncing back to login**
- Fixed **missing vendor logo**
- Fixed: **Horizon failed to launch**
- **Removed** outdated parameter: imprivata.xen\_new\_session



## Smartcard

- Fixed problem with **Nexus Personal smartcard in Gemalto IDBridge CT30 reader** via Citrix and RDP
- Fixed **smartcard resource manager**: if an eject of a card fails, perform a reset of card.

## Base system

- Fixed: Options **dialog keeps the settings** that were previously set
- Fixed **boot problems** due to 2 partitions are marked active (legacy boot with GPT partition table).
- Fixed support for **Datalogic barcode scanner**.
- Fixed **keyboard layout switcher**: show popup menu for selecting layouts also in screen lock and logon screen; show correct keyboard layout after switching from or to lock screen.
- Fixed an issue where the **post-session command was not triggering Media Player and Chromium** Browser sessions.
- Added: **Windows-key can be used as modifier for all hotkeys. AltGR does not work as a modifier.**
- Fixed a **graphics distortion in IGEL Setup Assistant**
- Fixed an issue with **VMware Horizon not triggering the post-session command**.
- Fixed an issue with **RDP not triggering the post-session command** on session disconnect.
- Fixed **ntlm\_auth helper** to terminate gracefully if no password is given.
- Minimized **periodic write access to flash drive**.
- Fixed: **Bootcode update** is done on each reboot on some EFI devices.
- Added: **Setup** parameter are also **checked after suspend**.
- Fixed an issue with **powerplan switching via the systray icon** on systems with specific Intel CPUs.
- Fixed an issue where the **post-session command was not triggered at sessions with long binary names**, for example, VMware Horizon.
- Fixed system **proxy** handling for **Chromium and Firefox**
- Added: An **improved implementation of the post-session command** mechanism has been integrated.
- Fixed **system messages where lines were cut off**
- Fixed **usable space issues with self-extracting factory preload images**

## X11 system

- Fixed **screen sorting order** to be **independent from screen startup time** (GTK-3)
- Fixed **panel on wrong screen** when original one takes longer to start
- Fixed **start menu** (whiskermenu) **restart** due to crash
- Fixed **taskbar hide/show delay** has no effect
- Fixed **Turkish (Q) and Turkish (F) keyboard layout** configuration.
- Fixed **panel keyboard layout indicator** for **French (Switzerland), Turkish (Q) and Turkish (F)** keyboard layouts.
- Fixed **screen configuration** done with **monitor defaults on the 2nd graphic card**.
- Fixed **touchscreen** screen configuration when **screen is connected on the 2nd graphic card**.

## X server

- Fixed issue with **the screen staying black** if master monitor in a **DisplayPort Daisy Chaining** environment is turned off and on again.

## Window manager



- Fixed an issue where **disabling the local window manager caused a significant boot delay.**
- **Desktop Icon Font Color** will now be previewed correctly in the setup.

#### VirtualBox

- Fixed **screen** remains **black after start in VirtualBox multi-monitor configurations.**
- Fixed **second screen in VirtualBox environment only is configured with 1024x768.**
- Fixed issue with getting **screen resolution from special VirtualBox version.**

#### Audio

- Fixed non-working audio on **Intel Tiger Lake-based devices.**
- Added handling for **microphone mute multimedia key.**
- Added possibility to **disable pci audio**, this **includes internal speaker and HDMI/DP audio.**  
[More...](#)

|          |                              |
|----------|------------------------------|
| Registry | multimedia.disable_audio.pci |
| Value    | true / false                 |

- To be more consistent, **moved** parameter `multimedia.webcam.disable_audio` to `multimedia.disable_audio.webcam`:

[More...](#)

|          |                                 |
|----------|---------------------------------|
| Registry | multimedia.disable_audio.webcam |
| Value    | true / false                    |

- Improved **playback function in the ALSA Pulse PCM** involved by applications using ALSA API (Citrix ICA Receiver).
- Fixed **automatic start of output audio stream in ALSA Pulse PCM**. The bug **caused a complete freeze of a Parallels session** while playback audio.
- Fixed **autostart of ALSA Pulse PCM**.

#### Multimedia

- Fixed **playback of Zoom recordings if hardware-accelerated decoder** is used.
- Fixed **hardware-accelerated decoding of Zoom** recordings **on VA-API platforms.**

#### Hardware

- Fixed issue with **limited colors on the DisplayPort 1 of UD2 LX50.**
- Fixed **touchpad** issues for some **Dynabook laptops** (for devices with and without fingerprint reader within touchpad).
- Added possibility to use **Touchpad toggle FN key.**
- Added new registry keys to possible solve some **touchpad** issues:  
[More...](#)

|           |                                                        |
|-----------|--------------------------------------------------------|
| Parameter | Blacklist i2c-i801 driver                              |
| Registry  | system.module_params.i2c_i801.blacklist                |
| Range     | [Default] [Yes] [No]                                   |
| Value     | Default (blacklist as there are some known problems)   |
| Parameter | Set this if touchpad is a synaptics intertouch device. |
| Registry  | system.module_params.psmouse.synaptics_inter_touch     |



|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Type      | bool                                                             |
| Value     | <u>enabled / disabled</u>                                        |
| Parameter | Set this if touchpad needs the a4tech workaround                 |
| Registry  | system.module_params.psmouse.a4tech_workaround                   |
| Type      | bool                                                             |
| Value     | <u>enabled / disabled</u>                                        |
| Parameter | Compat protocol to use can help with non working touchpads       |
| Registry  | system.module_params.psmouse.protocol                            |
| Range     | [Default] [PS/2] [ImPS/2] [ImExPS/2]                             |
| Parameter | Resolution in dpi (0 means use default)                          |
| Registry  | system.module_params.psmouse.resolution                          |
| Type      | integer                                                          |
| Value     | <u>0</u>                                                         |
| Parameter | Report rate in reports per second (0 means use default)          |
| Registry  | system.module_params.psmouse.rate                                |
| Type      | integer                                                          |
| Value     | <u>0</u>                                                         |
| Parameter | Reset device after so many packages (0 means never)              |
| Registry  | system.module_params.psmouse.resetafter                          |
| Type      | integer                                                          |
| Value     | <u>0</u>                                                         |
| Parameter | Mouse idle time before forcing resync in seconds (0 means never) |
| Registry  | system.module_params.psmouse.resync_time                         |
| Type      | integer                                                          |
| Value     | <u>0</u>                                                         |

## Remote Management

- Modified AssetInfo:  
Recurring **ADD/REMOVE commands for the same device are suppressed within 30 seconds.**
- Fixed the **indefinite time point of applying remote settings during boot**. The received remote settings are now merged and applied at the same time (at end of the boot process).
- Fixed handling of **UMS scheduled jobs during boot process**.
- Fixed **WOL proxy** command.
- Fixed execution of **generic commands** (Deploy Jabra Xpress package) **when invoked as UMS scheduled job**.
- Fixed **online check mechanism** if the client has more than one active network interface.
- Fixed broken **UMS Registering dialog**.

## IGEL Cloud Gateway



- Fixed **unreliable ICG status shown by ICG tray icon.**
- Fixed **security issue in remote management** - validate the UMS server certificate for incoming UMS requests if the endpoint has an established connection to ICG.

## CA Certificates Contained in IGEL OS 11.06

IGEL OS 11.06 contains the following CA certificates:

| Certificate name                                             | Expiry date                 | File in /etc/ssl/certs                                                |
|--------------------------------------------------------------|-----------------------------|-----------------------------------------------------------------------|
| ACCVRAIZ1                                                    | Dec 31 09:37:37 2030<br>GMT | ACCVRAIZ1.crt                                                         |
| AC RAIZ FNMT-RCM                                             | Jan 1 00:00:00 2030 GMT     | AC_RAIZ_FNMT-RCM.crt                                                  |
| Actalis Authentication Root CA                               | Sep 22 11:22:02 2030<br>GMT | Actalis_Authentication_Ro<br>ot_CA.crt                                |
| AffirmTrust Commercial                                       | Dec 31 14:06:06 2030<br>GMT | AffirmTrust_Commercial.c<br>rt                                        |
| AffirmTrust Networking                                       | Dec 31 14:08:24 2030<br>GMT | AffirmTrust_Networking.c<br>rt                                        |
| AffirmTrust Premium                                          | Dec 31 14:10:36 2040<br>GMT | AffirmTrust_Premium.crt                                               |
| AffirmTrust Premium ECC                                      | Dec 31 14:20:24 2040<br>GMT | AffirmTrust_Premium_ECC.c<br>rt                                       |
| Amazon Root CA 1                                             | Jan 17 00:00:00 2038<br>GMT | AmazonRootCA1.pem)                                                    |
| Amazon Root CA 1                                             | Jan 17 00:00:00 2038<br>GMT | Amazon_Root_CA_1.crt                                                  |
| Amazon Root CA 2                                             | May 26 00:00:00 2040<br>GMT | Amazon_Root_CA_2.crt                                                  |
| Amazon Root CA 3                                             | May 26 00:00:00 2040<br>GMT | Amazon_Root_CA_3.crt                                                  |
| Amazon Root CA 4                                             | May 26 00:00:00 2040<br>GMT | Amazon_Root_CA_4.crt                                                  |
| Atos TrustedRoot 2011                                        | Dec 31 23:59:59 2030<br>GMT | Atos_TrustedRoot_2011.crt                                             |
| Autoridad de Certificacion<br>Firmaprofesional CIF A62634068 | Dec 31 08:38:15 2030<br>GMT | Autoridad_de_Certificacio<br>n_Firmaprofesional_CIF_A6<br>2634068.crt |



| Certificate name                                                                                                             | Expiry date                 | File in /etc/ssl/certs                 |
|------------------------------------------------------------------------------------------------------------------------------|-----------------------------|----------------------------------------|
| Baltimore CyberTrust Root                                                                                                    | May 12 23:59:00 2025<br>GMT | BTCTRoot.pem)                          |
| Baltimore CyberTrust Root                                                                                                    | May 12 23:59:00 2025<br>GMT | Baltimore_CyberTrust_Root.crt          |
| Buypass Class 2 Root CA                                                                                                      | Oct 26 08:38:03 2040<br>GMT | Buypass_Class_2_Root_CA.crt            |
| Buypass Class 3 Root CA                                                                                                      | Oct 26 08:28:58 2040<br>GMT | Buypass_Class_3_Root_CA.crt            |
| CA Disig Root R2                                                                                                             | Jul 19 09:15:30 2042 GMT    | CA_Disig_Root_R2.crt                   |
| CFCA EV ROOT                                                                                                                 | Dec 31 03:07:01 2029<br>GMT | CFCA_EV_ROOT.crt                       |
| COMODO Certification Authority                                                                                               | Dec 31 23:59:59 2029<br>GMT | COMODO_Certification_Authority.crt     |
| COMODO ECC Certification Authority                                                                                           | Jan 18 23:59:59 2038<br>GMT | COMODO_ECC_Certification_Authority.crt |
| COMODO RSA Certification Authority                                                                                           | Jan 18 23:59:59 2038<br>GMT | COMODO_RSA_Certification_Authority.crt |
| Certigna                                                                                                                     | Jun 29 15:13:05 2027<br>GMT | Certigna.crt                           |
| Certigna Root CA                                                                                                             | Oct 1 08:32:27 2033 GMT     | Certigna_Root_CA.crt                   |
| Certum Trusted Network CA                                                                                                    | Dec 31 12:07:37 2029<br>GMT | Certum_Trusted_Network_CA.crt          |
| Certum Trusted Network CA 2                                                                                                  | Oct 6 08:39:56 2046 GMT     | Certum_Trusted_Network_CA_2.crt        |
| Chambers of Commerce Root - 2008                                                                                             | Jul 31 12:29:50 2038 GMT    | Chambers_of_Commerce_Root_-_2008.crt   |
| Class 3 Public Primary Certification Authority - G2 (c) 1998 VeriSign, Inc. - For authorized use only VeriSign Trust Network | Aug 1 23:59:59 2028 GMT     | Class3PCA_G2_v2.pem)                   |



| Certificate name                                                                                                             | Expiry date              | File in /etc/ssl/certs                    |
|------------------------------------------------------------------------------------------------------------------------------|--------------------------|-------------------------------------------|
| Class 4 Public Primary Certification Authority - G2 (c) 1998 VeriSign, Inc. - For authorized use only VeriSign Trust Network | Aug 1 23:59:59 2028 GMT  | Class4PCA_G2_v2.pem)                      |
| AAA Certificate Services                                                                                                     | Dec 31 23:59:59 2028 GMT | Comodo_AAA_Services_root.crt              |
| Cybertrust Global Root                                                                                                       | Dec 15 08:00:00 2021 GMT | Cybertrust_Global_Root.crt                |
| D-TRUST Root Class 3 CA 2 2009                                                                                               | Nov 5 08:35:58 2029 GMT  | D-<br>TRUST_Root_Class_3_CA_2_2009.crt    |
| D-TRUST Root Class 3 CA 2 EV 2009                                                                                            | Nov 5 08:50:46 2029 GMT  | D-<br>TRUST_Root_Class_3_CA_2_EV_2009.crt |
| DST Root CA X3                                                                                                               | Sep 30 14:01:15 2021 GMT | DST_Root_CA_X3.crt                        |
| DigiCert Global Root CA                                                                                                      | Nov 10 00:00:00 2031 GMT | DigiCertGlobalRootCA.pem)                 |
| DigiCert Global Root CA                                                                                                      | Mar 8 12:00:00 2023 GMT  | DigiCertSHA2SecureServerCA.pem)           |
| DigiCert Assured ID Root CA                                                                                                  | Nov 10 00:00:00 2031 GMT | DigiCert_Assured_ID_Root_CA.crt           |
| DigiCert Assured ID Root G2                                                                                                  | Jan 15 12:00:00 2038 GMT | DigiCert_Assured_ID_Root_G2.crt           |
| DigiCert Assured ID Root G3                                                                                                  | Jan 15 12:00:00 2038 GMT | DigiCert_Assured_ID_Root_G3.crt           |
| DigiCert Global Root CA                                                                                                      | Nov 10 00:00:00 2031 GMT | DigiCert_Global_Root_CA.crt               |
| DigiCert Global Root G2                                                                                                      | Jan 15 12:00:00 2038 GMT | DigiCert_Global_Root_G2.crt               |



| Certificate name                                          | Expiry date                 | File in /etc/ssl/certs                         |
|-----------------------------------------------------------|-----------------------------|------------------------------------------------|
| DigiCert Global Root G3                                   | Jan 15 12:00:00 2038<br>GMT | DigiCert_Global_Root_G3.crt                    |
| DigiCert High Assurance EV Root CA                        | Nov 10 00:00:00 2031<br>GMT | DigiCert_High_Assurance_EV_Root_CA.crt         |
| DigiCert Trusted Root G4                                  | Jan 15 12:00:00 2038<br>GMT | DigiCert_Trusted_Root_G4.crt                   |
| E-Tugra Certification Authority                           | Mar 3 12:09:48 2023 GMT     | E-Tugra_Certification_Authority.crt            |
| EC-ACC                                                    | Jan 7 22:59:59 2031 GMT     | EC-ACC.crt                                     |
| Entrust.net <sup>374</sup> Certification Authority (2048) | Jul 24 14:15:12 2029 GMT    | Entrust.net_Premium_2048_Secure_Server_CA.crt  |
| Entrust Root Certification Authority                      | Nov 27 20:53:42 2026<br>GMT | Entrust_Root_Certification_Authority.crt       |
| Entrust Root Certification Authority - EC1                | Dec 18 15:55:36 2037<br>GMT | Entrust_Root_Certification_Authority_-_EC1.crt |
| Entrust Root Certification Authority - G2                 | Dec 7 17:55:54 2030 GMT     | Entrust_Root_Certification_Authority_-_G2.crt  |
| Entrust Root Certification Authority - G4                 | Dec 27 11:41:16 2037<br>GMT | Entrust_Root_Certification_Authority_-_G4.crt  |
| GDCA TrustAUTH R5 ROOT                                    | Dec 31 15:59:59 2040<br>GMT | GDCA_TrustAUTH_R5_ROOT.crt                     |
| GlobalSign                                                | Dec 15 08:00:00 2021<br>GMT | GSR2.pem)                                      |
| GTE CyberTrust Global Root                                | Aug 13 23:59:00 2018<br>GMT | GTECTGlobalRoot.pem)                           |
| GTS Root R1                                               | Jun 22 00:00:00 2036<br>GMT | GTS_Root_R1.crt                                |

<sup>374</sup> <http://Entrust.net>



| <b>Certificate name</b>                                     | <b>Expiry date</b>          | <b>File in /etc/ssl/certs</b>                                   |
|-------------------------------------------------------------|-----------------------------|-----------------------------------------------------------------|
| GTS Root R2                                                 | Jun 22 00:00:00 2036<br>GMT | GTS_Root_R2.crt                                                 |
| GTS Root R3                                                 | Jun 22 00:00:00 2036<br>GMT | GTS_Root_R3.crt                                                 |
| GTS Root R4                                                 | Jun 22 00:00:00 2036<br>GMT | GTS_Root_R4.crt                                                 |
| GeoTrust Global CA                                          | May 21 04:00:00 2022<br>GMT | GeoTrust_Global_CA.pem)                                         |
| GeoTrust Primary Certification Authority - G2               | Jan 18 23:59:59 2038<br>GMT | GeoTrust_Primary_Certification_Authority_-_G2.crt               |
| GlobalSign                                                  | Jan 19 03:14:07 2038<br>GMT | GlobalSign_ECC_Root_CA_-_R4.crt                                 |
| GlobalSign                                                  | Jan 19 03:14:07 2038<br>GMT | GlobalSign_ECC_Root_CA_-_R5.crt                                 |
| GlobalSign Root CA                                          | Jan 28 12:00:00 2028<br>GMT | GlobalSign_Root_CA.crt                                          |
| GlobalSign                                                  | Dec 15 08:00:00 2021<br>GMT | GlobalSign_Root_CA_-_R2.crt                                     |
| GlobalSign                                                  | Mar 18 10:00:00 2029<br>GMT | GlobalSign_Root_CA_-_R3.crt                                     |
| GlobalSign                                                  | Dec 10 00:00:00 2034<br>GMT | GlobalSign_Root_CA_-_R6.crt                                     |
| Global Chambersign Root - 2008                              | Jul 31 12:31:40 2038 GMT    | Global_Chambersign_Root_-_2008.crt                              |
| Go Daddy Class 2 Certification Authority                    | Jun 29 17:06:20 2034<br>GMT | Go_Daddy_Class_2_CA.crt                                         |
| Go Daddy Root Certificate Authority - G2                    | Dec 31 23:59:59 2037<br>GMT | Go_Daddy_Root_Certificate_Authority_-_G2.crt                    |
| Hellenic Academic and Research Institutions ECC RootCA 2015 | Jun 30 10:37:12 2040<br>GMT | Hellenic_Academic_and_Research_Institutions_ECC_RootCA_2015.crt |



| Certificate name                                        | Expiry date              | File in /etc/ssl/certs                                      |
|---------------------------------------------------------|--------------------------|-------------------------------------------------------------|
| Hellenic Academic and Research Institutions RootCA 2011 | Dec 1 13:49:52 2031 GMT  | Hellenic_Academic_and_Research_Institutions_RootCA_2011.crt |
| Hellenic Academic and Research Institutions RootCA 2015 | Jun 30 10:11:21 2040 GMT | Hellenic_Academic_and_Research_Institutions_RootCA_2015.crt |
| Hongkong Post Root CA 1                                 | May 15 04:52:29 2023 GMT | Hongkong_Post_Root_CA_1.crt                                 |
| Hongkong Post Root CA 3                                 | Jun 3 02:29:46 2042 GMT  | Hongkong_Post_Root_CA_3.crt                                 |
| ISRG Root X1                                            | Jun 4 11:04:38 2035 GMT  | ISRG_Root_X1.crt                                            |
| IdenTrust Commercial Root CA 1                          | Jan 16 18:12:23 2034 GMT | IdenTrust_Commercial_Root_CA_1.crt                          |
| IdenTrust Public Sector Root CA 1                       | Jan 16 17:53:32 2034 GMT | IdenTrust_Public_Sector_Root_CA_1.crt                       |
| Imprivata Embedded Code Signing CA                      | Sep 7 16:20:00 2033 GMT  | Imprivata.crt                                               |
| Izenpe.com <sup>375</sup>                               | Dec 13 08:27:25 2037 GMT | Izenpe.com <sup>376</sup> .crt                              |
| Microsec e-Szigno Root CA 2009                          | Dec 30 11:30:18 2029 GMT | Microsec_e-Szigno_Root_CA_2009.crt                          |
| Microsoft ECC Root Certificate Authority 2017           | Jul 18 23:16:04 2042 GMT | Microsoft_ECC_Root_Certificate_Authority_2017.crt           |
| Microsoft RSA Root Certificate Authority 2017           | Jul 18 23:00:23 2042 GMT | Microsoft_RSA_Root_Certificate_Authority_2017.crt           |
| NAVER Global Root Certification Authority               | Aug 18 23:59:59 2037 GMT | NAVER_Global_Root_Certification_Authority.crt               |

<sup>375</sup> <http://Izenpe.com><sup>376</sup> <http://Izenpe.com>



| Certificate name                                              | Expiry date              | File in /etc/ssl/certs                             |
|---------------------------------------------------------------|--------------------------|----------------------------------------------------|
| NetLock Arany (Class Gold)<br>FÅ'tanÃºsÃtvÃ¡ny               | Dec 6 15:08:21 2028 GMT  | NetLock_Arany_=Class_Gold=_FÅ'tanÃºsÃtvÃ¡ny.crt   |
| Network Solutions Certificate Authority                       | Dec 31 23:59:59 2029 GMT | Network_Solutions_Certificate_Authority.crt        |
| OISTE WISEKey Global Root GB CA                               | Dec 1 15:10:31 2039 GMT  | OISTE_WISEKey_Global_Root_GB_CA.crt                |
| OISTE WISEKey Global Root GC CA                               | May 9 09:58:33 2042 GMT  | OISTE_WISEKey_Global_Root_GC_CA.crt                |
| Class 3 Public Primary Certification Authority                | Aug 1 23:59:59 2028 GMT  | Pcs3ss_v4.pem)                                     |
| QuoVadis Root Certification Authority                         | Mar 17 18:33:33 2021 GMT | QuoVadis_Root_CA.crt                               |
| QuoVadis Root CA 1 G3                                         | Jan 12 17:27:44 2042 GMT | QuoVadis_Root_CA_1_G3.crt                          |
| QuoVadis Root CA 2                                            | Nov 24 18:23:33 2031 GMT | QuoVadis_Root_CA_2.crt                             |
| QuoVadis Root CA 2 G3                                         | Jan 12 18:59:32 2042 GMT | QuoVadis_Root_CA_2_G3.crt                          |
| QuoVadis Root CA 3                                            | Nov 24 19:06:44 2031 GMT | QuoVadis_Root_CA_3.crt                             |
| QuoVadis Root CA 3 G3                                         | Jan 12 20:26:32 2042 GMT | QuoVadis_Root_CA_3_G3.crt                          |
| SSL.com <sup>377</sup> EV Root Certification Authority ECC    | Feb 12 18:15:23 2041 GMT | SSL.com_EV_Root_Certification_Authority_ECC.crt    |
| SSL.com <sup>378</sup> EV Root Certification Authority RSA R2 | May 30 18:14:37 2042 GMT | SSL.com_EV_Root_Certification_Authority_RSA_R2.crt |
| SSL.com <sup>379</sup> Root Certification Authority ECC       | Feb 12 18:14:03 2041 GMT | SSL.com_Root_Certification_Authority_ECC.crt       |

<sup>377</sup> <http://SSL.com><sup>378</sup> <http://SSL.com><sup>379</sup> <http://SSL.com>



| Certificate name                                        | Expiry date                 | File in /etc/ssl/certs                                 |
|---------------------------------------------------------|-----------------------------|--------------------------------------------------------|
| SSL.com <sup>380</sup> Root Certification Authority RSA | Feb 12 17:39:39 2041<br>GMT | SSL.com_Root_Certification_Authority_RSA.crt           |
| SZAFIR ROOT CA2                                         | Oct 19 07:43:30 2035<br>GMT | SZAFIR_ROOT_CA2.crt                                    |
| SecureSign RootCA11                                     | Apr 8 04:56:47 2029 GMT     | SecureSign_RootCA11.crt                                |
| SecureTrust CA                                          | Dec 31 19:40:55 2029<br>GMT | SecureTrust_CA.crt                                     |
| Secure Global CA                                        | Dec 31 19:52:06 2029<br>GMT | Secure_Global_CA.crt                                   |
| Security Communication RootCA2                          | May 29 05:00:39 2029<br>GMT | Security_Communication_RootCA2.crt                     |
| Security Communication RootCA1                          | Sep 30 04:20:49 2023<br>GMT | Security_Communication_Root_CA.crt                     |
| Sonera Class2 CA                                        | Apr 6 07:29:40 2021 GMT     | Sonera_Class_2_Root_CA.crt                             |
| Staat der Nederlanden EV Root CA                        | Dec 8 11:10:28 2022 GMT     | Staat_der_Nederlanden_EV_Root_CA.crt                   |
| Staat der Nederlanden Root CA - G3                      | Nov 13 23:00:00 2028<br>GMT | Staat_der_Nederlanden_Root_CA_-_G3.crt                 |
| Starfield Class 2 Certification Authority               | Jun 29 17:39:16 2034<br>GMT | Starfield_Class_2_CA.crt                               |
| Starfield Root Certificate Authority - G2               | Dec 31 23:59:59 2037<br>GMT | Starfield_Root_Certificate_Authority_-_G2.crt          |
| Starfield Services Root Certificate Authority - G2      | Dec 31 23:59:59 2037<br>GMT | Starfield_Services_Root_Certificate_Authority_-_G2.crt |
| SwissSign Gold CA - G2                                  | Oct 25 08:30:35 2036<br>GMT | SwissSign_Gold_CA_-_G2.crt                             |

<sup>380</sup> <http://SSL.com>



| Certificate name                                  | Expiry date                 | File in /etc/ssl/certs                                        |
|---------------------------------------------------|-----------------------------|---------------------------------------------------------------|
| SwissSign Silver CA - G2                          | Oct 25 08:32:46 2036<br>GMT | SwissSign_Silver_CA_-<br>_G2.crt                              |
| T-TeleSec GlobalRoot Class 2                      | Oct 1 23:59:59 2033 GMT     | T-<br>TeleSec_GlobalRoot_Class_<br>2.crt                      |
| T-TeleSec GlobalRoot Class 3                      | Oct 1 23:59:59 2033 GMT     | T-<br>TeleSec_GlobalRoot_Class_<br>3.crt                      |
| TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1     | Oct 25 08:25:55 2043<br>GMT | TUBITAK_Kamu_SM_SSL_Kok_S<br>ertifikasi_-_Surum_1.crt         |
| TWCA Global Root CA                               | Dec 31 15:59:59 2030<br>GMT | TWCA_Global_Root_CA.crt                                       |
| TWCA Root Certification Authority                 | Dec 31 15:59:59 2030<br>GMT | TWCA_Root_Certification_A<br>uthority.crt                     |
| TeliaSonera Root CA v1                            | Oct 18 12:00:50 2032<br>GMT | TeliaSonera_Root_CA_v1.cr<br>t                                |
| TrustCor ECA-1                                    | Dec 31 17:28:07 2029<br>GMT | TrustCor_ECA-1.crt                                            |
| TrustCor RootCert CA-1                            | Dec 31 17:23:16 2029<br>GMT | TrustCor_RootCert_CA-1.cr<br>t                                |
| TrustCor RootCert CA-2                            | Dec 31 17:26:39 2034<br>GMT | TrustCor_RootCert_CA-2.cr<br>t                                |
| Trustis FPS Root CA                               | Jan 21 11:36:54 2024<br>GMT | Trustis_FPS_Root_CA.crt                                       |
| Trustwave Global Certification Authority          | Aug 23 19:34:12 2042<br>GMT | Trustwave_Global_Certific<br>ation_Authority.crt              |
| Trustwave Global ECC P256 Certification Authority | Aug 23 19:35:10 2042<br>GMT | Trustwave_Global_ECC_P256<br>_Certification_Authority.<br>crt |



| Certificate name                                  | Expiry date              | File in /etc/ssl/certs                                |
|---------------------------------------------------|--------------------------|-------------------------------------------------------|
| Trustwave Global ECC P384 Certification Authority | Aug 23 19:36:43 2042 GMT | Trustwave_Global_ECC_P384_Certification_Authority.crt |
| UCA Extended Validation Root                      | Dec 31 00:00:00 2038 GMT | UCA_Extended_Validation_Root.crt                      |
| UCA Global G2 Root                                | Dec 31 00:00:00 2040 GMT | UCA_Global_G2_Root.crt                                |
| USERTrust ECC Certification Authority             | Jan 18 23:59:59 2038 GMT | USERTrust_ECC_Certification_Authority.crt             |
| USERTrust RSA Certification Authority             | Jan 18 23:59:59 2038 GMT | USERTrust_RSA_Certification_Authority.crt             |
| VeriSign Universal Root Certification Authority   | Dec 1 23:59:59 2037 GMT  | VeriSign_Universal_Root_Certification_Authority.crt   |
| XRamp Global Certification Authority              | Jan 1 05:37:19 2035 GMT  | XRamp_Global_CA_Root.crt                              |
| certSIGN ROOT CA                                  | Jul 4 17:20:04 2031 GMT  | certSIGN_ROOT_CA.crt                                  |
| certSIGN ROOT CA G2                               | Feb 6 09:27:35 2042 GMT  | certSIGN_Root_CA_G2.crt                               |
| e-Szigno Root CA 2017                             | Aug 22 12:07:06 2042 GMT | e-Szigno_Root_CA_2017.crt                             |
| ePKI Root Certification Authority                 | Dec 20 02:31:27 2034 GMT | ePKI_Root_Certification_Authority.crt                 |
| emSign ECC Root CA - C3                           | Feb 18 18:30:00 2043 GMT | emSign_ECC_Root_CA_-_C3.crt                           |
| emSign ECC Root CA - G3                           | Feb 18 18:30:00 2043 GMT | emSign_ECC_Root_CA_-_G3.crt                           |
| emSign Root CA - C1                               | Feb 18 18:30:00 2043 GMT | emSign_Root_CA_-_C1.crt                               |
| emSign Root CA - G1                               | Feb 18 18:30:00 2043 GMT | emSign_Root_CA_-_G1.crt                               |



### 7.1.2 IGEL OS Creator (OSC)

#### Supported Devices

|         |                                     |
|---------|-------------------------------------|
| UD2-LX: | UD2-LX 51<br>UD2-LX 50<br>UD2-LX 40 |
| UD3-LX: | UD3-LX 60<br>UD3-LX 51              |
| UD5-LX: | UD5-LX 50                           |
| UD6-LX: | UD6-LX 51                           |
| UD7-LX: | UD7-LX 20<br>UD7-LX 11<br>UD7-LX 10 |
| UD9-LX: | UD9-LX Touch 41<br>UD9-LX 40        |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>381</sup>.

- [Component Versions 11.06.100](#)(see page 1477)
- [New Features 11.06.100](#)(see page 1479)
- [Resolved Issues 11.06.100](#)(see page 1479)

#### Component Versions 11.06.100

##### Clients

| Product | Version |
|---------|---------|
|         |         |

<sup>381</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



|                                         |                                    |
|-----------------------------------------|------------------------------------|
| Zulu JRE                                | 8.0.302-1                          |
| System Components                       |                                    |
| OpenSSL                                 | 1.0.2n-1ubuntu5.7                  |
| OpenSSL                                 | 1.1.1-1ubuntu2.1~18.04.13          |
| Bluetooth stack (bluez)                 | 5.56-0ubuntu2igel12                |
| MESA OpenGL stack                       | 21.1.5-1igel145                    |
| VDPAU Library version                   | 1.4-3igel1099                      |
| Graphics Driver INTEL                   | 2.99.917+git20200515-igel1013      |
| Graphics Driver ATI/Radeon              | 19.1.0-2igel1066                   |
| Graphics Driver ATI/AMDGPU              | 19.1.0-2+git20210202igel1122       |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867                    |
| Graphics Driver Nvidia                  | 460.91.03-0ubuntu0.20.04.1         |
| Graphics Driver VMware                  | 13.3.0-2igel857                    |
| Graphics Driver QXL (Spice)             | 0.1.5-2build2-igel925              |
| Graphics Driver FBDEV                   | 0.5.0-1igel1012                    |
| Graphics Driver VESA                    | 2.4.0-1igel1010                    |
| Input Driver Evdev                      | 2.10.6-2igel1037                   |
| Input Driver Elographics                | 1.4.2-1igel1113                    |
| Input Driver Synaptics                  | 1.9.1-1ubuntu1igel1009             |
| Input Driver VMMouse                    | 13.1.0-1ubuntu2igel957             |
| Input Driver Wacom                      | 0.39.0-0ubuntu1igel1036            |
| Kernel                                  | 5.12.19 #mainline-lxos-g1631108722 |
| Xorg X11 Server                         | 1.20.11-1igel1120                  |
| Lightdm Graphical Login Manager         | 1.26.0-0ubuntu1igel13              |
| XFCE4 Window Manager                    | 4.14.5-1~18.04igel1600422786       |



|                 |                  |
|-----------------|------------------|
| ISC DHCP Client | 4.3.5-3ubuntu7.3 |
| Python3         | 3.6.9            |

#### VM Guest Support Components

|                            |                         |
|----------------------------|-------------------------|
| Virtualbox Guest Utils     | 6.1.22-dfsg-1igel55     |
| Virtualbox X11 Guest Utils | 6.1.22-dfsg-1igel55     |
| Open VM Tools              | 11.0.5-4ubuntu0.18.04.1 |
| Open VM Desktop Tools      | 11.0.5-4ubuntu0.18.04.1 |
| Xen Guest Utilities        | 7.10.0-0ubuntu1         |
| Spice Vdagent              | 0.20.0-2igel104         |
| Qemu Guest Agent           | 5.2+dfsg-3igel17        |

#### Services

| Service                     | Size    | Reduced Firmware |
|-----------------------------|---------|------------------|
| Java SE Runtime Environment | 36.2 M  | Included         |
| NVIDIA graphics driver      | 161.2 M | Included         |

#### New Features 11.06.100

##### OSC Installer

- **Enhanced** OSC Installer for **creation of 'Factory preload images (master images)'**
- Added possibility to **add initial settings to OSC Installer ISO**.
- Added **support for 'Reset after first boot'** for OSC Factory Image function.  
Further information / details at <https://kb.igel.com/igelos-11.05/en/installation-42011487.html>

##### Base system

- Updated IGEL **EULA** to version April 2021.
- Updated **kernel** to version **5.12.x**

##### Hardware

- Added hardware **support for HP t540**.
- Note: The IGEL device **UD3-LX50** reached **End of Maintenance**.

#### Resolved Issues 11.06.100

##### OSC Installer

- OSC **not deployable with IGEL Deployment Appliance: New version 11.3 is required** for 11.06.100 deployment.
- Enhanced the boot **cmdline** options for OSC



## 7.2 Notes for Release 11.05.133

|                       |            |              |
|-----------------------|------------|--------------|
| <b>Software:</b>      | Version    | 11.05.133    |
| <b>Release Date:</b>  | 2021-04-29 |              |
| <b>Release Notes:</b> | Version    | RN-1105133-1 |
| <b>Last update:</b>   | 2021-04-26 |              |

- [Supported Devices 11.05.133](#)(see page 1480)
- [Component Versions 11.05.133](#)(see page 1481)
- [General Information 11.05.133](#)(see page 1488)
- [Known Issues 11.05.133](#)(see page 1488)
- [Security Fixes 11.05.133](#)(see page 1491)
- [New Features 11.05.133](#)(see page 1491)
- [Resolved Issues 11.05.133](#)(see page 1493)

### 7.2.1 Supported Devices 11.05.133

|         |                                             |
|---------|---------------------------------------------|
| UD2-LX: | UD2-LX 51<br><br>UD2-LX 50<br><br>UD2-LX 40 |
| UD3-LX: | UD3-LX 60<br><br>UD3-LX 51<br><br>UD3-LX 50 |
| UD5-LX: | UD5-LX 50                                   |
| UD6-LX: | UD6-LX 51                                   |
| UD7-LX: | UD7-LX 20<br><br>UD7-LX 11<br><br>UD7-LX 10 |



|         |                 |
|---------|-----------------|
| UD9-LX: | UD9-LX Touch 41 |
|         | UD9-LX 40       |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>382</sup>.

## 7.2.2 Component Versions 11.05.133

### Clients

| Product                               | Version                         |
|---------------------------------------|---------------------------------|
| Chromium (experimental)               | 88.0.4324.150-igel1612763117    |
| CID Key                               | 6.5.0-2                         |
| Cisco JVDI Client                     | 14.0.0                          |
| Cisco Webex Teams VDI Client          | 41.4.0.18516                    |
| Cisco Webex Meetings VDI Client       | 41.4.0.162                      |
| Zoom Media Plugin                     | 5.5.12716                       |
| Citrix HDX Realtime Media Engine      | 2.9.300                         |
| Citrix Workspace App                  | 19.12.0.19                      |
| Citrix Workspace App                  | 20.12.0.12                      |
| Citrix Workspace App                  | 21.03.0.38                      |
| deskMate Client                       | 2.1.3                           |
| deviceTRUST Citrix Channel            | 20.1.200.0                      |
| Crossmatch DP Citrix Channel          | 0125                            |
| Ericom PowerTerm                      | 12.0.1.0.20170219.2-_dev_-34574 |
| Ericom PowerTerm                      | 14.0.0.45623                    |
| Evidian AuthMgr                       | 1.5.7617                        |
| Evince PDF Viewer                     | 3.28.4-0ubuntu1.2               |
| FabulaTech USB for Remote Desktop     | 6.0.28                          |
| FabulaTech Scanner for Remote Desktop | 2.7.0.1                         |
| FabulaTech Webcam for Remote Desktop  | 2.8.10                          |

<sup>382</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



|                                        |                                           |
|----------------------------------------|-------------------------------------------|
| Firefox                                | 78.6.1                                    |
| IBM iAccess Client Solutions           | 1.1.8.1                                   |
| IGEL RDP Client                        | 2.2igel1605251065                         |
| IGEL WVD Client                        | 1.0.24igel1619015530                      |
| Imprivata OneSign ProveID Embedded     | onesign-bootstrap-loader_1.0.523630_amd64 |
| deviceTRUST RDP Channel                | 20.1.200.0                                |
| NCP Secure Enterprise Client           | 5.10_rev40552                             |
| NX Client                              | 6.11.2-1igel8                             |
| Open VPN                               | 2.5.0-1igel1606475118                     |
| Zulu JRE                               | 8.48.0.51-2                               |
| Parallels Client                       | 17.1.3                                    |
| Spice GTK (Red Hat Virtualization)     | 0.39-1igel106                             |
| Remote Viewer (Red Hat Virtualization) | 8.0-2git20191213.e4bacb8igel83            |
| Usbredir (Red Hat Virtualization)      | 0.8.0-1+b1igel71                          |
| SpeechWrite                            | 1.0                                       |
| Teradici PCoIP Software Client         | 21.03.0-18.04                             |
| ThinLinc Client                        | 4.12.0-6517                               |
| ThinPrint Client                       | 7-7.6.126                                 |
| Totem Media Player                     | 2.30.2-0ubuntu1igel55                     |
| Parole Media Player                    | 1.0.5-1igel1583919770                     |
| VNC Viewer                             | 1.10.1+dfsg-9igel17                       |
| VMware Horizon Client                  | 2012-8.1.0-17349998                       |
| Voip Client Ekiga                      | 4.0.1-9build1igel6                        |

## Dictation

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20201118 |



|                       |        |
|-----------------------|--------|
| Philips Speech driver | 12.9.1 |
|-----------------------|--------|

### Signature

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.9    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.4.2    |

### Smartcard

|                                           |                        |
|-------------------------------------------|------------------------|
| PKCS#11 Library A.E.T SafeSign            | 3.6.0.0-AET.000        |
| PKCS#11 Library Athena IDProtect          | 7                      |
| PKCS#11 Library cryptovision sc/interface | 7.3.1                  |
| PKCS#11 Library Gemalto SafeNet           | 10.7.77                |
| PKCS#11 Library OpenSC                    | 0.21.0-1igel39         |
| PKCS#11 Library SecMaker NetID            | 6.8.3.21               |
| PKCS#11 Library 90meter                   | 20190522               |
| Reader Driver ACS CCID                    | 1.1.6-1igel2           |
| Reader Driver Gemalto eToken              | 10.7.77                |
| Reader Driver HID Global Omnikey          | 4.3.3                  |
| Reader Driver Identive CCID               | 5.0.35                 |
| Reader Driver Identive eHealth200         | 1.0.5                  |
| Reader Driver Identive SCRKBC             | 5.0.24                 |
| Reader Driver MUSCLE CCID                 | 1.4.31-1igel12         |
| Reader Driver REINER SCT cyberJack        | 3.99.5final.sp13igel15 |



|                             |               |
|-----------------------------|---------------|
| Resource Manager PC/SC Lite | 1.9.0-1igel18 |
| Cherry USB2LAN Proxy        | 3.2.0.3       |

## System Components

|                                         |                               |
|-----------------------------------------|-------------------------------|
| OpenSSL                                 | 1.0.2n-1ubuntu5.5             |
| OpenSSL                                 | 1.1.1-1ubuntu2.1~18.04.7      |
| OpenSSH Client                          | 8.4p1-3igel4                  |
| OpenSSH Server                          | 8.4p1-3igel4                  |
| Bluetooth stack (bluez)                 | 5.55-0ubuntu1.1igel10         |
| MESA OpenGL stack                       | 20.2.6-1igel131               |
| VAAPI ABI Version                       | 0.40                          |
| VDPAU Library version                   | 1.4-3igel1099                 |
| Graphics Driver INTEL                   | 2.99.917+git20200515-igel1013 |
| Graphics Driver ATI/RADEON              | 19.1.0-2igel1066              |
| Graphics Driver ATI/AMDGPU              | 19.1.0-2+git20200828igel1064  |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867               |
| Graphics Driver Nvidia                  | 450.102.04-0ubuntu0.20.04.1   |
| Graphics Driver VMware                  | 13.3.0-2igel857               |
| Graphics Driver QXL (Spice)             | 0.1.5-2build2-igel925         |
| Graphics Driver FBDEV                   | 0.5.0-1igel1012               |
| Graphics Driver VESA                    | 2.4.0-1igel1010               |
| Input Driver Evdev                      | 2.10.6-2igel1037              |
| Input Driver Elographics                | 1.4.1-1+b6igel952             |
| Input Driver eGalax                     | 2.5.8825                      |
| Input Driver Synaptics                  | 1.9.1-1ubuntu1igel1009        |
| Input Driver VMMouse                    | 13.1.0-1ubuntu2igel957        |
| Input Driver Wacom                      | 0.39.0-0ubuntu1igel1036       |



|                                      |                                   |
|--------------------------------------|-----------------------------------|
| Input Driver ELO Multitouch          | 3.0.0                             |
| Input Driver ELO Singletouch         | 5.1.0                             |
| Kernel                               | 5.9.16 #mainline-lxos-g1615563496 |
| Xorg X11 Server                      | 1.20.10-2igel1100                 |
| Xorg Xephyr                          | 1.20.10-2igel1100                 |
| CUPS printing daemon                 | 2.2.7-1ubuntu2.8igel32            |
| PrinterLogic                         | 25.1.0.425                        |
| Lightdm Graphical Login Manager      | 1.26.0-0ubuntu1igel13             |
| XFCE4 Window Manager                 | 4.14.2-1~18.04igel1600339249      |
| ISC DHCP Client                      | 4.3.5-3ubuntu7.1                  |
| NetworkManager                       | 1.20.4-2ubuntu2.2igel109          |
| ModemManager                         | 1.10.0-1~ubuntu18.04.2            |
| GStreamer 0.10                       | 0.10.36-2ubuntu0.1igel201         |
| GStreamer 0.10 Fluendo aacdec        | 0.10.42                           |
| GStreamer 0.10 Fluendo asfdemux      | 0.10.90                           |
| GStreamer 0.10 Fluendo h264dec       | 0.10.58                           |
| GStreamer 0.10 Fluendo mp3dec        | 0.10.40                           |
| GStreamer 0.10 Fluendo mpegdemux     | 0.10.85                           |
| GStreamer 0.10 Fluendo mpeg4videodec | 0.10.44                           |
| GStreamer 0.10 Fluendo vadec         | 0.10.224                          |
| GStreamer 0.10 Fluendo wmadec        | 0.10.70                           |
| GStreamer 0.10 Fluendo wmvdec        | 0.10.66                           |
| GStreamer 1.x                        | 1.18.3-1igel283                   |
| GStreamer 1.0 Fluendo aacdec         | 0.10.42.2-8d6d                    |
| GStreamer 1.0 Fluendo asfdemux       | 0.10.90                           |
| GStreamer 1.0 Fluendo h264dec        | 0.10.58                           |
| GStreamer 1.0 Fluendo mp3dec         | 0.10.40                           |
| GStreamer 1.0 Fluendo mpeg4videodec  | 0.10.44                           |
| GStreamer 1.0 Fluendo vadec          | 0.10.224                          |
| GStreamer 1.0 Fluendo wmadec         | 0.10.70                           |
| GStreamer 1.0 Fluendo wmvdec         | 0.10.66                           |
| WebKit2Gtk                           | 2.30.4-1igel40                    |
| Python2                              | 2.7.17                            |



Python3

3.6.9

### VM Guest Support Components

|                            |                         |
|----------------------------|-------------------------|
| Virtualbox Guest Utils     | 6.1.18-dfsg-3igel52     |
| Virtualbox X11 Guest Utils | 6.1.18-dfsg-3igel52     |
| Open VM Tools              | 11.0.5-4ubuntu0.18.04.1 |
| Open VM Desktop Tools      | 11.0.5-4ubuntu0.18.04.1 |
| Xen Guest Utilities        | 7.10.0-0ubuntu1         |
| Spice Vdagent              | 0.20.0-2igel104         |
| Qemu Guest Agent           | 5.2+dfsg-3igel17        |

### Features with Limited IGEL Support

|                                    |                     |
|------------------------------------|---------------------|
| Mobile Device Access USB (MTP)     | 1.1.17-3igel5       |
| Mobile Device Access USB (imobile) | 1.3.0-5igel11       |
| Mobile Device Access USB (gphoto)  | 2.5.26-2igel7       |
| VPN OpenConnect                    | 8.10-2igel6         |
| Scanner support                    | 1.0.27-1            |
| VirtualBox                         | 6.1.18-dfsg-3igel52 |

### Services

| Service                                    | Size    | Reduced Firmware |
|--------------------------------------------|---------|------------------|
| Asian Language Support                     | 22.5 M  | Included         |
| Java SE Runtime Environment                | 36.0 M  | Included         |
| Citrix Appliance                           | 329.0M  | Included         |
| Citrix Workspace app                       |         |                  |
| Citrix StoreFront                          |         |                  |
| Ericom PowerTerm InterConnect              | 15.5 M  | Included         |
| Media Player                               | 512.0 K | Included         |
| Local Browser (Firefox)                    | 76.5 M  | Included         |
| Citrix Appliance                           |         |                  |
| VMware Horizon                             | 4.5 M   | Included         |
| RDP                                        |         |                  |
| Cendio ThinLinc                            | 10.0 M  | Included         |
| Printing (Internet printing protocol CUPS) | 22.2 M  | Included         |
| NoMachine NX                               | 26.8 M  | Included         |



|                                   |         |              |
|-----------------------------------|---------|--------------|
| VMware Horizon                    | 131.2 M | Included     |
| Voice over IP (Ekiga)             | 6.5 M   | Included     |
| Citrix Appliance                  | 768.0 K | Included     |
| NCP Enterprise VPN Client         | 27.0 M  | Not included |
| Fluendo GStreamer Codec Plugins   | 6.5 M   | Included     |
| IBM i Access Client Solutions     | 72.5 M  | Not included |
| Red Hat Enterprise Virtualization | 3.0 M   | Included     |
| Parallels Client                  | 5.5 M   | Included     |
| NVIDIA graphics driver            | 126.8 M | Not included |
| Imprivata Appliance               | 10.8 M  | Included     |
| Evidian AuthMgr                   | 2.5 M   | Included     |
| Hardware Video Acceleration       | 13.5 M  | Included     |
| Extra Font Package                | 1.0 M   | Included     |
| Fluendo GStreamer AAC Decoder     | 1.2 M   | Included     |
| x32 Compatibility Support         | 3.5 M   | Included     |
| Cisco JVDI client                 | 61.8 M  | Included     |
| PrinterLogic                      | 40.8 M  | Not included |
| Biosec BS Login                   | 10.0 M  | Not included |
| Login VSI Login Enterprise        | 28.8 M  | Not included |
| Stratusphere UX CID Key software  | 2.8 M   | Not included |
| Elastic Filebeat                  | 15.8 M  | Not included |
| WVD                               | 89.2 M  | Included     |
| Local Browser (Chromium)          | 87.8 M  | Not included |
| deskMate client                   | 5.8 M   | Included     |
| Cisco Webex Teams VDI             | 43.8 M  | Not included |
| Cisco Webex Meetings VDI          | 32.8 M  | Not included |
| Zoom VDI Media Plugin             | 47.2 M  | Not included |
| DriveLock                         | 13.2 M  | Included     |
| SpeechWrite Client                | 256.0 K | Included     |
| Teradici PCoIP Client             | 16.0 M  | Included     |
| 90meter Smart Card Support        | 256.0 K | Included     |



|                                            |         |              |
|--------------------------------------------|---------|--------------|
| Virtualbox (Limited support)               | 256.0K  | Not included |
| Mobile Device Access USB (Limited support) |         |              |
| VPN OpenConnect (Limited support)          |         |              |
| Scanner support / SANE (Limited support)   |         |              |
| Limited Support Features                   |         |              |
| Mobile Device Access USB (Limited support) | 256.0 K | Not included |
| VPN OpenConnect (Limited support)          | 1.0 M   | Not included |
| Scanner support / SANE (Limited support)   | 2.5 M   | Not included |
| VirtualBox (Limited support)               | 63.8 M  | Not included |

### 7.2.3 General Information 11.05.133

To be beneficial to all new features and implementations, it is recommended to use UMS 6.07.100 or higher and update the corresponding profiles.

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

### 7.2.4 Known Issues 11.05.133

Citrix



- To launch **multiple desktop sessions** with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key must be enabled.

[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Value     | enabled / <u>disabled</u>                                        |

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** while the session is ongoing does not work. The reader is visible, but **cannot be used due to permanently unknown reader status**.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1, and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- Browser content redirection** does not work with activated DRI3 and hardware-accelerated H.264 deep compression codec.
- With activated DRI3 and an AMD GPU, **Citrix H.264 acceleration plugin could freeze**. Selective H.264 mode (API v2) is not affected by this issue.
- Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.

#### VMware Horizon

- Client drive mapping** and **USB redirection** for storage devices **should not be enabled both at the same time**.
  - On the one hand, when using USB redirection for storage devices:  
The USB on-insertion feature is only working when the client drive mapping is switched off.  
In the IGEL Setup client drive mapping can be found in:  
**Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**.  
It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules.  
Furthermore, Horizon Client relies on the OS to mount the storage devices themselves.  
Enable local `Storage Hotplug` on setup page **Devices > Storage Devices > Storage Hotplug**.
- External drives** mounted already before connection do not appear in the remote desktop.  
Workaround: **map the directory /media as a drive**. Then the external devices will show up inside the media drive.
- After disconnect of an RDP-based session, the **Horizon main window** which contains the server or sessions overview, **cannot be resized anymore**.
- Copying Text from Horizon Blast sessions** isn't possible.



- The **on-screen keyboard in Horizon appliance mode** does not work correctly with the local logon.  
You have to switch off the local logon and switch on these two keys in the IGEL registry:  
`userinterface.softkeyboard.autoshow`  
`userinterface.softkeyboard.autohide`
- **Zoom VDI Media Plugin makes Horizon Client crash** upon connection to the remote desktop in cases when TCSetup is running at the same time.
- **When using the PCoIP protocol the virtual channel provided by VMware used for serial port and scanner redirection can make Horizon client hang** on logout from the remote session.  
This happens if you enable only one of scanner or serial port redirection. The freeze does not occur if both redirection methods are enabled or none of them. The Blast Protocol isn't affected by this bug.  
The respective settings can be found here in the IGEL Registry:  
`vmware.view.enable-serial-port-redir`  
`vmware.view.enable-scanner-redir`

#### Parallels Client

- **Native USB redirection** does not work with Parallels Client.

#### Chromium

- **H.264 decoding is not supported** anymore.

#### WiFi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.  
Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

#### Cisco JVDI Client

- There may be a **segfault** shown in the logs (during log out of Citrix Desktop session). Occurs only when using **Citrix Workspace app 20.10** and **Cisco JVDI**.

#### Base system

- **Hyper-V (Generation 2) needs a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.
- **Update from memory stick requires network online state** (at least when multiple update stages are involved)
- **Unreliable messages** in user dialog for applying settings during boot. Could occur when new settings were fetched from the UMS.

#### deskMate

- Some **stability issues** may remain.

#### Firmware update

- On **devices with 2 GB of flash** storage, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit [Error: "Not](#)



"enough space on local drive" when Updating to **IGEL OS 11.04 or Higher**<sup>383</sup> for a possible solution and additional information.

#### Appliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice instead of once.
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported.  
The **Console Invocation** has to allow **Native** client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

#### VirtualBox

- The current **VirtualBox Guest Tools/Drivers will not work with VirtualBox 5.2.x or older hosts**.  
This results in a black screen and non-working graphic.  
Possible workaround: Installation with **Failsafe Installation + Recovery** and set of `x.drivers.force_vesa` registry key to "true".

#### Audio

- **IGEL UDD (D220)** fails to restore the **volume level** of the speaker when the device used firmware version 11.01.110 before.
- **Audio jack detection** on **Advantec POC-W243L** does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.

#### Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU** driver.

#### Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work on INTEL-based devices.

#### Remote Management

- **AIT feature** with **IGEL Starter License** is only supported by UMS version 6.05.100 or newer.

### 7.2.5 Security Fixes 11.05.133

#### Remote Management

- Fixed a **possible privilege escalation** while sending **user logoff event to the UMS**.

### 7.2.6 New Features 11.05.133

#### Citrix

- Integrated **Zoom Media Plugin 5.5.12716.0227**
- Added: In **StoreFront** sessions, **HTTP can now be selected for the URL** in addition to HTTPS.

---

<sup>383</sup><https://kb.igel.com/igelos-11.04/en/error-not-enough-%C2%A0space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.html>



- Implement "**Synchronize Citrix password with screensaver**" for **SelfService**. The parameter for StoreFront was reused.

## UD Pocket

- Added official support for **Secured Kobra Stick from DIGITTRADE**.

## VMware Horizon

- Added **switch for enabling Cisco Webex Meetings** within VMware Horizon.  
**More...**

|           |                                    |
|-----------|------------------------------------|
| Parameter | Cisco Webex Meetings VDI           |
| Registry  | vmware.view.vdciscomeetings.enable |
| Type      | bool                               |
| Value     | <u>enabled</u> / <u>disabled</u>   |

- **Removed** deprecated **ThinPrint virtual channel (tprpdः.so)** from Horizon sessions used for virtual printing. It is **replaced by Horizon's integrated printing mechanism**.

## Imprivata

- Added registry key to overcome the **window overlap**. That occurred when using local setup or hotkeyed applications like the 'Display switch'.

**More...**

|            |                                  |
|------------|----------------------------------|
| IGEL Setup | <b>Registry</b>                  |
| Registry   | imprivata.avoid_focus_ownership  |
| Type       | bool                             |
| Value      | <u>enabled</u> / <u>disabled</u> |

## Smartcard

- Added smartcard reader driver for **DIGITTRADE "Secured Kobra Stick"**.

## WVD

- Added **WVD printer redirection**.

**More...**

|          |                                        |
|----------|----------------------------------------|
| Registry | sessions.wvd%.printing.cups            |
| Value    | <u>enabled</u> / <u>disabled</u>       |
| Registry | print.cups.printer%.map_wvd            |
| Value    | <u>enabled</u> / <u>disabled</u>       |
| Registry | print.cups.printer%.wvd_printer_driver |
| Value    | ""                                     |

- The **default Windows driver name is "Microsoft PS Class Driver"**, which should be installed by default and work generically.  
To install a **custom printer driver**, the exact name must be set and the driver must be installed on the WVD side.

## Base system



- **Post-session commands:** Added support to monitor multiple sessions and have a post-session command triggered if all sessions exited successfully.

## 7.2.7 Resolved Issues 11.05.133

Citrix

- Integrated **HDX Realtime Optimization Pack 2.9.300**
- Updated **Grundig Dictation driver** to version **20-09-16**. This **fixes termination of Citrix sessions when USB devices are plugged or unplugged** - happens with Citrix Workspace App versions newer than 20.09.
- **Citrix Hardware Decoder doesn't crash** anymore **when using 12 CPU cores** (or even more) at the server.

WVD

- Fixed **forced Azure re-authentication** (every 30 minutes)

Parallels Client

- Updated **Parallels client** to version **17.1.3**

Teradici PCoIP Client

- **Teradici client update 21.03**

Imprivata

- Fixed **missing vendor logo**

Firefox

- Fixed **apparmor** rule for allowing Firefox to use **widevine DRM plugin**.

Smartcard

- Fixed **smartcard resource manager**: Reset is triggered when eject of smartcard fails.

Cisco Webex

- Updated **Cisco Webex Teams VDI** to **41.4.0.18516**
- Updated **Cisco Webex Meetings VDI** to **41.4.0.162**
- Please **make sure your Webex meetings client version is WBS 41.4.0 or later**, otherwise it will fail to launch Webex VDI optimized meeting.

Cisco JVDI Client

- Updated **Cisco JVDI** to **14.0.0**

IBM\_5250

- Fixed **error in iAccess configuration**.

Base system

- Fixed **bootcode update is done on each reboot** on some **EFI** devices.
- Changed: Minimized **periodic write access to permanent storage**.

Firmware update



- Added: **sftp** protocol supports now the following **key exchange methods**:
  - ecdh-sha2-nistp256 (BSI)
  - ecdh-sha2-nistp384 (BSI)
  - ecdh-sha2-nistp521 (BSI)
  - curve25519-sha256 (BSI)
  - curve25519-sha256@libssh.org (BSI)
  - diffie-hellman-group-exchange-sha256
  - diffie-hellman-group-exchange-sha1
  - diffie-hellman-group14-sha1
  - diffie-hellman-group1-sha1

#### X11 system

- Fixed **monitor sorting order** to be independent from monitor startup time (GTK-3)
- Fixed **panel on wrong monitor**, when original monitor takes longer to come online
- Fixed **Turkish (Q) and Turkish (F) keyboard layout** configuration.
- Fixed **panel keyboard layout** indicator for **French (Switzerland), Turkish (Q) and Turkish (F)** keyboard layouts.
- Added **inhibit screensaver** while a **Cisco Webex Meetings** session is active in Citrix Workspace App.

#### Audio

- Fixed **not working** audio on **Intel Tiger Lake-based** devices.
- Fixed **automatic start of output audio** stream in **ALSA Pulse PCM**. The bug caused a complete **freeze of a Parallels session** while playback audio data.
- Bugfix for USB audio **default device switch** and update of **igel-sound-control**

#### Hardware

- Fixed **touchpad** issues for some **Dynabook laptops**.

#### Remote Management

- Fixed **execution of generic commands (Deploy Jabra Xpress package)** if they invoked as a UMS scheduled job.
- Fixed **handling of UMS scheduled jobs during boot** process.

#### Network

- Improved **network device order** for **LG CL600N, LG CN650N**
- The currently used parameter **tls-remote** is **deprecated** and was **removed in openVPN 2.4**. It was be **changed to** **verify-x509-name**.

#### H264

- Citrix Hardware Decoder doesn't crash** anymore **when using 12 CPU cores** (or even more) at the server.

## 7.3 Notes for Release 11.05.120

| Software: | Version | 11.05.120 |
|-----------|---------|-----------|
|           |         |           |



|                       |            |              |
|-----------------------|------------|--------------|
| <b>Release Date:</b>  | 2021-03-25 |              |
| <b>Release Notes:</b> | Version    | RN-1105120-1 |
| <b>Last update:</b>   | 2021-03-23 |              |

- [IGEL OS 11](#)(see page 1495)
- [IGEL OS Creator \(OSC\)](#)(see page 1510)

### 7.3.1 IGEL OS 11

- [Supported Devices 11.05.120](#)(see page 1495)
- [Component Versions 11.05.120](#)(see page 1496)
- [General Information 11.05.120](#)(see page 1503)
- [Known Issues 11.05.120](#)(see page 1503)
- [New Features 11.05.120](#)(see page 1506)
- [Resolved Issues 11.05.120](#)(see page 1508)

#### Supported Devices 11.05.120

|         |                                     |
|---------|-------------------------------------|
| UD2-LX: | UD2-LX 51<br>UD2-LX 50<br>UD2-LX 40 |
| UD3-LX: | UD3-LX 60<br>UD3-LX 51<br>UD3-LX 50 |
| UD5-LX: | UD5-LX 50                           |
| UD6-LX: | UD6-LX 51                           |
| UD7-LX: | UD7-LX 20<br>UD7-LX 11<br>UD7-LX 10 |



|         |                 |
|---------|-----------------|
| UD9-LX: | UD9-LX Touch 41 |
|         | UD9-LX 40       |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>384</sup>.

## Component Versions 11.05.120

### Clients

| Product                               | Version                         |
|---------------------------------------|---------------------------------|
| Chromium (experimental)               | 88.0.4324.150-igel1612763117    |
| CID Key                               | 6.5.0-2                         |
| Cisco JVDI Client                     | 12.9.3                          |
| Cisco Webex Teams VDI Client          | 41.1.0.17621                    |
| Cisco Webex Meetings VDI Client       | 41.2.0.142                      |
| Zoom Media Plugin                     | 5.4.59458.0109                  |
| Citrix HDX Realtime Media Engine      | 2.9.200-2506                    |
| Citrix Workspace App                  | 19.12.0.19                      |
| Citrix Workspace App                  | 20.12.0.12                      |
| Citrix Workspace App                  | 21.03.0.38                      |
| deskMate Client                       | 2.1.3                           |
| deviceTRUST Citrix Channel            | 20.1.200.0                      |
| Crossmatch DP Citrix Channel          | 0125                            |
| Ericom PowerTerm                      | 12.0.1.0.20170219.2-_dev_-34574 |
| Ericom PowerTerm                      | 14.0.0.45623                    |
| Evidian AuthMgr                       | 1.5.7617                        |
| Evince PDF Viewer                     | 3.28.4-0ubuntu1.2               |
| FabulaTech USB for Remote Desktop     | 6.0.28                          |
| FabulaTech Scanner for Remote Desktop | 2.7.0.1                         |
| FabulaTech Webcam for Remote Desktop  | 2.8.10                          |

<sup>384</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



|                                        |                                           |
|----------------------------------------|-------------------------------------------|
| Firefox                                | 78.6.1                                    |
| IBM iAccess Client Solutions           | 1.1.8.1                                   |
| IGEL RDP Client                        | 2.2igel1605251065                         |
| IGEL WVD Client                        | 1.0.22igel1612537530                      |
| Imprivata OneSign ProveID Embedded     | onesign-bootstrap-loader_1.0.523630_amd64 |
| deviceTRUST RDP Channel                | 20.1.200.0                                |
| NCP Secure Enterprise Client           | 5.10_rev40552                             |
| NX Client                              | 6.11.2-1igel8                             |
| Open VPN                               | 2.5.0-1igel1606475118                     |
| Zulu JRE                               | 8.48.0.51-2                               |
| Parallels Client (64 bit)              | 17.1.2.1                                  |
| Spice GTK (Red Hat Virtualization)     | 0.39-1igel106                             |
| Remote Viewer (Red Hat Virtualization) | 8.0-2git20191213.e4bacb8igel83            |
| Usbredir (Red Hat Virtualization)      | 0.8.0-1+b1igel71                          |
| SpeechWrite                            | 1.0                                       |
| Teradici PCoIP Software Client         | 20.10.0-18.04                             |
| ThinLinc Client                        | 4.12.0-6517                               |
| ThinPrint Client                       | 7-7.6.126                                 |
| Totem Media Player                     | 2.30.2-0ubuntu1igel55                     |
| Parole Media Player                    | 1.0.5-1igel1583919770                     |
| VNC Viewer                             | 1.10.1+dfsg-9igel17                       |
| VMware Horizon Client                  | 2012-8.1.0-17349998                       |
| Voip Client Ekiga                      | 4.0.1-9build1igel6                        |

## Dictation

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20201118 |



|                       |        |
|-----------------------|--------|
| Philips Speech driver | 12.9.1 |
|-----------------------|--------|

## Signature

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.9    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.4.2    |

## Smartcard

|                                           |                        |
|-------------------------------------------|------------------------|
| PKCS#11 Library A.E.T SafeSign            | 3.6.0.0-AET.000        |
| PKCS#11 Library Athena IDProtect          | 7                      |
| PKCS#11 Library cryptovision sc/interface | 7.3.1                  |
| PKCS#11 Library Gemalto SafeNet           | 10.7.77                |
| PKCS#11 Library OpenSC                    | 0.21.0-1igel39         |
| PKCS#11 Library SecMaker NetID            | 6.8.3.21               |
| PKCS#11 Library 90meter                   | 20190522               |
| Reader Driver ACS CCID                    | 1.1.6-1igel2           |
| Reader Driver Gemalto eToken              | 10.7.77                |
| Reader Driver HID Global Omnikey          | 4.3.3                  |
| Reader Driver Identive CCID               | 5.0.35                 |
| Reader Driver Identive eHealth200         | 1.0.5                  |
| Reader Driver Identive SCRKBC             | 5.0.24                 |
| Reader Driver MUSCLE CCID                 | 1.4.31-1igel12         |
| Reader Driver REINER SCT cyberJack        | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite               | 1.9.0-1igel16          |



|                      |         |
|----------------------|---------|
| Cherry USB2LAN Proxy | 3.2.0.3 |
|----------------------|---------|

## System Components

|                                         |                               |
|-----------------------------------------|-------------------------------|
| OpenSSL                                 | 1.0.2n-1ubuntu5.5             |
| OpenSSL                                 | 1.1.1-1ubuntu2.1~18.04.7      |
| OpenSSH Client                          | 8.4p1-3igel4                  |
| OpenSSH Server                          | 8.4p1-3igel4                  |
| Bluetooth stack (bluez)                 | 5.55-0ubuntu1.1igel10         |
| MESA OpenGL stack                       | 20.2.6-1igel131               |
| VAAPI ABI Version                       | 0.40                          |
| VDPAU Library version                   | 1.4-3igel1099                 |
| Graphics Driver INTEL                   | 2.99.917+git20200515-igel1013 |
| Graphics Driver ATI/RADEON              | 19.1.0-2igel1066              |
| Graphics Driver ATI/AMDGPU              | 19.1.0-2+git20200828igel1064  |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867               |
| Graphics Driver Nvidia                  | 450.102.04-0ubuntu0.20.04.1   |
| Graphics Driver VMware                  | 13.3.0-2igel857               |
| Graphics Driver QXL (Spice)             | 0.1.5-2build2-igel925         |
| Graphics Driver FBDEV                   | 0.5.0-1igel1012               |
| Graphics Driver VESA                    | 2.4.0-1igel1010               |
| Input Driver Evdev                      | 2.10.6-2igel1037              |
| Input Driver Elographics                | 1.4.1-1+b6igel952             |
| Input Driver eGalax                     | 2.5.8825                      |
| Input Driver Synaptics                  | 1.9.1-1ubuntu1igel1009        |
| Input Driver VMMouse                    | 13.1.0-1ubuntu2igel957        |
| Input Driver Wacom                      | 0.39.0-0ubuntu1igel1036       |
| Input Driver ELO Multitouch             | 3.0.0                         |
| Input Driver ELO Singletouch            | 5.1.0                         |



|                                      |                                   |
|--------------------------------------|-----------------------------------|
| Kernel                               | 5.9.16 #mainline-lxos-g1615563496 |
| Xorg X11 Server                      | 1.20.10-2igel1100                 |
| Xorg Xephyr                          | 1.20.10-2igel1100                 |
| CUPS printing daemon                 | 2.2.7-1ubuntu2.8igel32            |
| PrinterLogic                         | 25.1.0.425                        |
| Lightdm Graphical Login Manager      | 1.26.0-0ubuntu1igel13             |
| XFCE4 Window Manager                 | 4.14.2-1~18.04igel1600339249      |
| ISC DHCP Client                      | 4.3.5-3ubuntu7.1                  |
| NetworkManager                       | 1.20.4-2ubuntu2.2igel109          |
| ModemManager                         | 1.10.0-1~ubuntu18.04.2            |
| GStreamer 0.10                       | 0.10.36-2ubuntu0.1igel201         |
| GStreamer 0.10 Fluendo aacdec        | 0.10.42                           |
| GStreamer 0.10 Fluendo asfdemux      | 0.10.90                           |
| GStreamer 0.10 Fluendo h264dec       | 0.10.58                           |
| GStreamer 0.10 Fluendo mp3dec        | 0.10.40                           |
| GStreamer 0.10 Fluendo mpegdemux     | 0.10.85                           |
| GStreamer 0.10 Fluendo mpeg4videodec | 0.10.44                           |
| GStreamer 0.10 Fluendo vadec         | 0.10.224                          |
| GStreamer 0.10 Fluendo wmadec        | 0.10.70                           |
| GStreamer 0.10 Fluendo wmvdec        | 0.10.66                           |
| GStreamer 1.x                        | 1.18.3-1igel283                   |
| GStreamer 1.0 Fluendo aacdec         | 0.10.42.2-8d6d                    |
| GStreamer 1.0 Fluendo asfdemux       | 0.10.90                           |
| GStreamer 1.0 Fluendo h264dec        | 0.10.58                           |
| GStreamer 1.0 Fluendo mp3dec         | 0.10.40                           |
| GStreamer 1.0 Fluendo mpeg4videodec  | 0.10.44                           |
| GStreamer 1.0 Fluendo vadec          | 0.10.224                          |
| GStreamer 1.0 Fluendo wmadec         | 0.10.70                           |
| GStreamer 1.0 Fluendo wmvdec         | 0.10.66                           |
| WebKit2Gtk                           | 2.30.4-1igel40                    |
| Python2                              | 2.7.17                            |
| Python3                              | 3.6.9                             |



## VM Guest Support Components

|                            |                         |
|----------------------------|-------------------------|
| Virtualbox Guest Utils     | 6.1.18-dfsg-3igel52     |
| Virtualbox X11 Guest Utils | 6.1.18-dfsg-3igel52     |
| Open VM Tools              | 11.0.5-4ubuntu0.18.04.1 |
| Open VM Desktop Tools      | 11.0.5-4ubuntu0.18.04.1 |
| Xen Guest Utilities        | 7.10.0-0ubuntu1         |
| Spice Vdagent              | 0.20.0-2igel104         |
| Qemu Guest Agent           | 5.2+dfsg-3igel17        |

## Features with Limited IGEL Support

|                                    |                     |
|------------------------------------|---------------------|
| Mobile Device Access USB (MTP)     | 1.1.17-3igel5       |
| Mobile Device Access USB (imobile) | 1.3.0-5igel11       |
| Mobile Device Access USB (gphoto)  | 2.5.26-2igel7       |
| VPN OpenConnect                    | 8.10-2igel6         |
| Scanner support                    | 1.0.27-1            |
| VirtualBox                         | 6.1.18-dfsg-3igel52 |

## Services

| Service                                    | Size    | Reduced Firmware |
|--------------------------------------------|---------|------------------|
| Asian Language Support                     | 22.5 M  | Included         |
| Java SE Runtime Environment                | 36.0 M  | Included         |
| Citrix Appliance                           | 329.0M  | Included         |
| Citrix Workspace app                       |         |                  |
| Citrix StoreFront                          |         |                  |
| Ericom PowerTerm InterConnect              | 15.5 M  | Included         |
| Media Player                               | 512.0 K | Included         |
| Local Browser (Firefox)                    | 76.5 M  | Included         |
| Citrix Appliance                           |         |                  |
| VMware Horizon                             | 4.5 M   | Included         |
| RDP                                        |         |                  |
| Cendio ThinLinc                            | 10.0 M  | Included         |
| Printing (Internet printing protocol CUPS) | 22.2 M  | Included         |
| NoMachine NX                               | 26.8 M  | Included         |
| VMware Horizon                             | 131.2 M | Included         |
| Voice over IP (Ekiga)                      | 6.5 M   | Included         |



|                                            |         |              |
|--------------------------------------------|---------|--------------|
| Citrix Appliance                           | 768.0 K | Included     |
| NCP Enterprise VPN Client                  | 27.0 M  | Not included |
| Fluendo GStreamer Codec Plugins            | 6.5 M   | Included     |
| IBM i Access Client Solutions              | 72.5 M  | Not included |
| Red Hat Enterprise Virtualization          | 3.0 M   | Included     |
| Parallels Client                           | 5.5 M   | Included     |
| NVIDIA graphics driver                     | 126.8 M | Not included |
| Imprivata Appliance                        | 10.8 M  | Included     |
| Evidian AuthMgr                            | 2.5 M   | Included     |
| Hardware Video Acceleration                | 13.5 M  | Included     |
| Extra Font Package                         | 1.0 M   | Included     |
| Fluendo GStreamer AAC Decoder              | 1.2 M   | Included     |
| x32 Compatibility Support                  | 3.5 M   | Included     |
| Cisco JVDI client                          | 45.8 M  | Included     |
| PrinterLogic                               | 40.8 M  | Not included |
| Biosec BS Login                            | 10.0 M  | Not included |
| Login VSI Login Enterprise                 | 28.8 M  | Not included |
| Stratusphere UX CID Key software           | 2.8 M   | Not included |
| Elastic Filebeat                           | 15.8 M  | Not included |
| WVD                                        | 88.2 M  | Included     |
| Local Browser (Chromium)                   | 87.8 M  | Not included |
| deskMate client                            | 5.8 M   | Included     |
| Cisco Webex Teams VDI                      | 36.8 M  | Not included |
| Cisco Webex Meetings VDI                   | 32.2 M  | Not included |
| Zoom VDI Media Plugin                      | 42.2 M  | Not included |
| DriveLock                                  | 13.2 M  | Included     |
| SpeechWrite Client                         | 256.0 K | Included     |
| Teradici PCoIP Client                      | 14.5 M  | Included     |
| 90meter Smart Card Support                 | 256.0 K | Included     |
| Virtualbox (Limited support)               | 256.0K  | Not included |
| Mobile Device Access USB (Limited support) |         |              |
| VPN OpenConnect (Limited support)          |         |              |
| Scanner support / SANE (Limited support)   |         |              |
| Limited Support Features                   |         |              |



|                                            |         |              |
|--------------------------------------------|---------|--------------|
| Mobile Device Access USB (Limited support) | 256.0 K | Not included |
| VPN OpenConnect (Limited support)          | 1.0 M   | Not included |
| Scanner support / SANE (Limited support)   | 2.5 M   | Not included |
| VirtualBox (Limited support)               | 63.8 M  | Not included |

## General Information 11.05.120

To be beneficial to all new features and implementations, it is recommended to use UMS 6.07.100 or higher and update the corresponding profiles.

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

## Known Issues 11.05.120

### Citrix

- For using **multiple desktop sessions** with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key must be enabled.

[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Value     | enabled / <u>disabled</u>                                        |

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** while the session is ongoing does not work. The reader is visible, but **cannot be used due to permanently unknown reader status**.



- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1, and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with activated DRI3 and hardware-accelerated H.264 deep compression codec.
- With activated DRI3 and an AMD GPU, **Citrix H.264 acceleration plugin could freeze**. Selective H.264 mode (API v2) is not affected by this issue.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.

#### VMware Horizon

- **Client drive mapping** and **USB redirection** for storage devices **should not be enabled both at the same time**.
  - On the one hand, when using USB redirection for storage devices:  
The USB on-insertion feature is only working when the client drive mapping is switched off.  
In the IGEL Setup client drive mapping can be found in:  
**Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**.  
It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules.  
Furthermore, Horizon Client relies on the OS to mount the storage devices themselves.  
Enable local `Storage Hotplug` on setup page **Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection do not appear in the remote desktop.  
Workaround: **map the directory /media as a drive**. Then the external devices will show up inside the media drive.
- After disconnect of an RDP-based session, the **Horizon main window** which contains the server or sessions overview, **cannot be resized anymore**.
- **Copying Text from Horizon Blast sessions** isn't possible.
- The **on-screen keyboard in Horizon appliance mode** does not work correctly with the local logon.  
You have to switch off the local logon and switch on these two keys in the IGEL registry:  
`userinterface.softkeyboard.autoshow`  
`userinterface.softkeyboard.autohide`
- **Zoom VDI Media Plugin makes Horizon Client crash** upon connection to the remote desktop in cases when TCSetup is running at the same time.
- **When using the PCoIP protocol the virtual channel provided by VMware used for serial port and scanner redirection can make Horizon client hang** on logout from the remote session.  
This happens if you enable only one of scanner or serial port redirection. The freeze does not occur if both redirection methods are enabled or none of them. The Blast Protocol isn't affected by this bug  
The respective settings can be found here in the IGEL Registry:



`vmware.view.enable-serial-port-redir`  
`vmware.view.enable-scanner-redir`

#### Parallels Client

- **Native USB redirection** does not work with Parallels Client.

#### Chromium

- **H.264 decoding is not supported anymore / in this release.**

#### WiFi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.  
 Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

#### Cisco JVDI Client

- There may be a **segfault** shown in the logs (during log out of Citrix Desktop session). Occurs only when using **Citrix Workspace app 20.10** and **Cisco JVDI**.

#### Base system

- **Hyper-V (Generation 2) needs a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.
- **Update from memory stick requires network online state** (at least when multiple update stages are involved)
- **Unreliable messages** in user dialog for applying settings during boot. Could occur when new settings were fetched from the UMS.

#### deskMate

- Some **stability issues** may remain.

#### Firmware update

- On **devices with 2 GB of flash** storage, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit [Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher<sup>385</sup>](#) for a possible solution and additional information.

#### Appliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice instead of once.
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported.  
 The **Console Invocation** has to allow **Native** client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

#### VirtualBox

- The current **VirtualBox Guest Tools/Drivers will not work with VirtualBox 5.2.x or older hosts**.  
 This results in a black screen and non-working graphic.

---

<sup>385</sup><https://kb.igel.com/igelos-11.04/en/error-not-enough-%C2%A0space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.html>



Possible workaround: Installation with **Failsafe Installation + Recovery** and set of `x.drivers.force_vesa` registry key to true.

#### Audio

- **IGEL UD2 (D220)** fails to restore the **volume level** of the speaker when the device used firmware version 11.01.110 before.
- **Audio jack detection** on **Advantec POC-W243L** does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.

#### Multimedia

- Multimedia redirection with **GStreamer** could fail with the Nouveau GPU driver.

#### Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work on INTEL-based devices.

#### Remote Management

- **AIT feature** with **IGEL Starter License** is only supported by UMS version 6.05.100 or newer.

### New Features 11.05.120

#### OSC Installer

- Enhanced OSC Installer for **creating so-called factory preload images** (master images)
- Added possibility to **add initial settings** to OSC Installer ISO.

#### Citrix

- Added **automatic configuration of the Citrix webcam redirection** in ICA sessions.

[More...](#)

|            |                                                                    |
|------------|--------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; HDX Multimedia</b> |
| Parameter  | Automatic HDX webcam configuration                                 |
| Registry   | <code>ica.igel_hdxwebcam.enabled</code>                            |
| Value      | <u>enabled</u> / disabled                                          |
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; HDX Multimedia</b> |
| Parameter  | Resolution grade                                                   |
| Registry   | <code>ica.igel_hdxwebcam.quality</code>                            |
| Range      | [Very low][Low][ <u>Normal</u> ] [High][Very high][Best]           |
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; HDX Multimedia</b> |
| Parameter  | Minimal frame rate                                                 |
| Registry   | <code>ica.igel_hdxwebcam.framerate</code>                          |



|       |    |
|-------|----|
| Value | 15 |
|-------|----|

- Added **configuration for h264 encoding** in the Citrix webcam redirection.

[More...](#)

|           |                                  |
|-----------|----------------------------------|
| Parameter | HDX Webcam H264 encoding         |
| Registry  | ica.wfclient.hdxh264inputenabled |
| Value     | enabled / <u>disabled</u>        |

- Added configuration for **native h264 encoding** provided by webcam and used in the Citrix webcam redirection. This parameter requires the `ica.wfclient.hdxh264inputenabled` to be set to true.

[More...](#)

|           |                                  |
|-----------|----------------------------------|
| Parameter | HDX Webcam H264 native           |
| Registry  | ica.wfclient.hdxh264enablenative |
| Value     | enabled / <u>disabled</u>        |

- Available **Citrix Workspace apps** in this release: **21.03(default), 20.12 and 19.12**
- Added new Citrix feature for an enhanced experience of **multi-monitor scenarios**. You can save the selection for a multi-monitor screen layout. Pinning helps to relaunch a session with the selected layout, resulting in an optimized user experience.

Note: Works only with Self Service.

[More...](#)

|           |                                                |
|-----------|------------------------------------------------|
| Parameter | Enhanced Experience of Multi-Monitor scenarios |
| Registry  | ica.authman.screenpinenabled                   |
| Value     | enabled / <u>disabled</u>                      |

- All parameters of the **Citrix set log program** are now available via setup under `ica.logging.setlog`. Logging can be set easier and permanent. Therefore, changed the structure of parameters to show the inheritance.

#### VMware Horizon

- Fixed **broken session handling** when using Webex Teams, Horizon session could only be started once.

#### WVD

- New **WVD icon**.

#### Network

- Added **Realtek RTL8125 2.5Gigabit Ethernet** driver.

#### WiFi



- Added support for **Realtek RTW8852AE WiFi** device.

#### Hardware

- Added hardware support for **LG 34CN650N AiO**.

#### Resolved Issues 11.05.120

##### OSC Installer

- Fixed OSC 11.05.xxx **not deployable with Deployment Appliance (ODA)**.

##### Citrix

- Fixed link to icacontrol
- Fixed: **Several audio device problems** through an enabled registry key `ica.module.vdcamversion4support`. The default was changed to disabled. This ensures that Citrix CWA behaves as before.

**More...**

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Multiple Audio Device support                |
| Registry  | <code>ica.module.vdcamversion4support</code> |
| Value     | <u>enabled</u> / <u>disabled</u>             |

- Fixed **Citrix logging**, the log file is written as expected.

##### RDP/IGEL RDP Client 2

- Added parameter to enable **serverside audio for RDP sessions**.

**More...**

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Enable serverside audio                                          |
| Registry  | <code>sessions.winconnect%.option.enable-serverside-audio</code> |
| Value     | <u>enabled</u> / <u>disabled</u>                                 |

##### Parallels Client

- Fixed an issue where the **post-session command** got triggered too early when using the Parallels Client.

##### Network

- Fixed network device order for **LG 34CN650W** and **CL600W** devices.
- Fixed a **graphics distortion in Setup Assistant**

##### WiFi

- Added registry key for **tweaking the WPA supplicant**. In general, the value is a comma-separated list of names. If it contains LATESUCCESS, a late EAP-Success message will be ignored.

**More...**

|           |             |
|-----------|-------------|
| Parameter | IGEL Tweaks |
|-----------|-------------|



|          |                                                            |
|----------|------------------------------------------------------------|
| Registry | network.interfaces.wirelesslan.device0.wpa.<br>igel_tweaks |
| Value    | " "                                                        |

- Added registry key to **activate the use of Broadcom sta driver** (needed for older Broadcom WiFi devices).

**More...**

|           |                                                 |
|-----------|-------------------------------------------------|
| Parameter | Use Broadcom sta driver instead of b43 for WLAN |
| Registry  | network.drivers.broadcom.use_broadcom_sta       |
| Value     | enabled / <u>disabled</u>                       |

#### NCP VPN

- Fixed **NCP session start**.

#### Smartcard

- Fixed: Usage of **Nexus Personal** smartcard in combination with **Gemalto IDBridge CT30** reader, in Citrix and RDP

#### Base system

- Fixed **custom environment variables** when an administrator password is set.
- Fixed **boot problems** due to 2 partitions are marked active (legacy boot with GPT partition table).
- Fixed **RDP not triggering the post-session command** on session disconnect.
- Fixed **grub boot code and boot error message**: Unknown TPM error.
- Fixed **Demo License browser crashes after EULA**.

#### X11 system

- Fixed **taskbar hide/show delay** has no effect

#### VirtualBox

- Fixed **screen resolution issues with SINA OS 3.5.1 version**.
- Fixed **screen remains black after started multi-monitor configuration in VirtualBox**.
- Fixed **second screen in VirtualBox environment only is configured with 1024x768**.
- Fixed issue when getting **screen resolution from special VirtualBox version**.

#### Audio

- Improved **playback function** in the **ALSA Pulse PCM** - for applications using ALSA API (e.g. Citrix Workspace App).

#### Hardware

- Fixed **microphone detection on Dell Optiplex devices**.

#### Remote Management

- Fixed WOL proxy command.



### 7.3.2 IGEL OS Creator (OSC)

#### Supported Devices

|         |                                     |
|---------|-------------------------------------|
| UD2-LX: | UD2-LX 51<br>UD2-LX 50<br>UD2-LX 40 |
| UD3-LX: | UD3-LX 60<br>UD3-LX 51<br>UD3-LX 50 |
| UD5-LX: | UD5-LX 50                           |
| UD6-LX: | UD6-LX 51                           |
| UD7-LX: | UD7-LX 20<br>UD7-LX 11<br>UD7-LX 10 |
| UD9-LX: | UD9-LX Touch 41<br>UD9-LX 40        |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>386</sup>.

- 
- [Component Versions 11.05.120](#)(see page 1511)
  - [New Features 11.05.120](#)(see page 1512)
  - [Resolved Issues 11.05.120](#)(see page 1512)

---

<sup>386</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



## Component Versions 11.05.120

## Clients

| Product  | Version     |
|----------|-------------|
| Zulu JRE | 8.48.0.51-2 |

## System Components

|                                         |                                   |
|-----------------------------------------|-----------------------------------|
| OpenSSL                                 | 1.0.2n-1ubuntu5.5                 |
| OpenSSL                                 | 1.1.1-1ubuntu2.1~18.04.7          |
| Bluetooth stack (bluez)                 | 5.55-0ubuntu1.1igel10             |
| MESA OpenGL stack                       | 20.2.6-1igel131                   |
| VDPAU Library version                   | 1.4-3igel1099                     |
| Graphics Driver INTEL                   | 2.99.917+git20200515-igel1013     |
| Graphics Driver ATI/Radeon              | 19.1.0-2igel1066                  |
| Graphics Driver ATI/AMDGPU              | 19.1.0-2+git20200828igel1064      |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867                   |
| Graphics Driver Nvidia                  | 450.102.04-0ubuntu0.20.04.1       |
| Graphics Driver VMware                  | 13.3.0-2igel857                   |
| Graphics Driver QXL (Spice)             | 0.1.5-2build2-igel925             |
| Graphics Driver FBDEV                   | 0.5.0-1igel1012                   |
| Graphics Driver VESA                    | 2.4.0-1igel1010                   |
| Input Driver Evdev                      | 2.10.6-2igel1037                  |
| Input Driver Elographics                | 1.4.1-1+b6igel952                 |
| Input Driver Synaptics                  | 1.9.1-1ubuntu1igel1009            |
| Input Driver VMMouse                    | 13.1.0-1ubuntu2igel957            |
| Input Driver Wacom                      | 0.39.0-0ubuntu1igel1036           |
| Kernel                                  | 5.9.16 #mainline-lxos-g1615563496 |



|                                 |                              |
|---------------------------------|------------------------------|
| Xorg X11 Server                 | 1.20.10-2igel1100            |
| Lightdm Graphical Login Manager | 1.26.0-0ubuntu1igel13        |
| XFCE4 Window Manager            | 4.14.2-1~18.04igel1600339249 |
| ISC DHCP Client                 | 4.3.5-3ubuntu7.1             |
| Python3                         | 3.6.9                        |

#### VM Guest Support Components

|                            |                         |
|----------------------------|-------------------------|
| Virtualbox Guest Utils     | 6.1.18-dfsg-3igel52     |
| Virtualbox X11 Guest Utils | 6.1.18-dfsg-3igel52     |
| Open VM Tools              | 11.0.5-4ubuntu0.18.04.1 |
| Open VM Desktop Tools      | 11.0.5-4ubuntu0.18.04.1 |
| Xen Guest Utilities        | 7.10.0-0ubuntu1         |
| Spice Vdagent              | 0.20.0-2igel104         |
| Qemu Guest Agent           | 5.2+dfsg-3igel17        |

#### Services

| Service                     | Size    | Reduced Firmware |
|-----------------------------|---------|------------------|
| Java SE Runtime Environment | 36.0 M  | Included         |
| NVIDIA graphics driver      | 122.5 M | Included         |

#### New Features 11.05.120

##### OSC Installer

- Enhanced OSC Installer for **creating so-called factory preload images** (master images)
- Added possibility to **add initial settings to OSC Installer ISO**.

#### Resolved Issues 11.05.120

##### OSC Installer

- Fixed OSC 11.05.xxx **not deployable with Deployment Appliance (ODA)**.

## 7.4 Notes for Release 11.05.100

|                      |            |           |
|----------------------|------------|-----------|
| <b>Software:</b>     | Version    | 11.05.100 |
| <b>Release Date:</b> | 2021-02-25 |           |



|                       |            |              |
|-----------------------|------------|--------------|
| <b>Release Notes:</b> | Version    | RN-1105100-1 |
| <b>Last update:</b>   | 2021-03-08 |              |

- [IGEL OS 11](#)(see page 1513)
- [IGEL OS Creator \(OSC\)](#)(see page 1554)

#### 7.4.1 IGEL OS 11

- [Supported Devices 11.05.100](#)(see page 1513)
- [Component Versions 11.05.100](#)(see page 1514)
- [General Information 11.05.100](#)(see page 1520)
- [Known Issues 11.05.100](#)(see page 1521)
- [Security Fixes 11.05.100](#)(see page 1523)
- [New Features 11.05.100](#)(see page 1527)
- [Resolved Issues 11.05.100](#)(see page 1538)
- [CA Certificates Contained in IGEL OS 11.05](#)(see page 1546)

#### Supported Devices 11.05.100

|         |                                             |
|---------|---------------------------------------------|
| UD2-LX: | UD2-LX 51<br><br>UD2-LX 50<br><br>UD2-LX 40 |
| UD3-LX: | UD3-LX 60<br><br>UD3-LX 51<br><br>UD3-LX 50 |
| UD5-LX: | UD5-LX 50                                   |
| UD6-LX: | UD6-LX 51                                   |
| UD7-LX: | UD7-LX 20<br><br>UD7-LX 11<br><br>UD7-LX 10 |



|         |                 |
|---------|-----------------|
| UD9-LX: | UD9-LX Touch 41 |
|         | UD9-LX 40       |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>387</sup>.

## Component Versions 11.05.100

### Clients

| Product                               | Version                         |
|---------------------------------------|---------------------------------|
| Chromium                              | 88.0.4324.150-igel1612763117    |
| CID Key                               | 6.5.0-2                         |
| Cisco JVDI Client                     | 12.9.3                          |
| Cisco Webex Teams VDI Client          | 41.1.0.17621                    |
| Cisco Webex Meetings VDI Client       | 41.2.0.142                      |
| Zoom Media Plugin                     | 5.4.59458.0109                  |
| Citrix HDX Realtime Media Engine      | 2.9.200-2506                    |
| Citrix Workspace App                  | 19.12.0.19                      |
| Citrix Workspace App                  | 20.10.0.6                       |
| Citrix Workspace App                  | 20.12.0.12                      |
| deskMate Client                       | 2.1.3                           |
| deviceTRUST Citrix Channel            | 20.1.200.0                      |
| Crossmatch DP Citrix Channel          | 0125                            |
| Ericom PowerTerm                      | 12.0.1.0.20170219.2-_dev_-34574 |
| Ericom PowerTerm                      | 14.0.0.45623                    |
| Evidian AuthMgr                       | 1.5.7617                        |
| Evince PDF Viewer                     | 3.28.4-0ubuntu1.2               |
| FabulaTech USB for Remote Desktop     | 6.0.28                          |
| FabulaTech Scanner for Remote Desktop | 2.7.0.1                         |
| FabulaTech Webcam for Remote Desktop  | 2.8.10                          |

<sup>387</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



|                                        |                                           |
|----------------------------------------|-------------------------------------------|
| Firefox                                | 78.6.1                                    |
| IBM iAccess Client Solutions           | 1.1.8.1                                   |
| IGEL RDP Client                        | 2.2igel1605251065                         |
| IGEL WVD Client                        | 1.0.22igel1612537530                      |
| Imprivata OneSign ProveID Embedded     | onesign-bootstrap-loader_1.0.523630_amd64 |
| deviceTRUST RDP Channel                | 20.1.200.0                                |
| NCP Secure Enterprise Client           | 5.10_rev40552                             |
| NX Client                              | 6.11.2-1igel8                             |
| Open VPN                               | 2.5.0-1igel1606475118                     |
| Zulu JRE                               | 8.48.0.51-2                               |
| Parallels Client (64 bit)              | 17.1.2.1                                  |
| Spice GTK (Red Hat Virtualization)     | 0.39-1igel106                             |
| Remote Viewer (Red Hat Virtualization) | 8.0-2git20191213.e4bacb8igel83            |
| Usbredir (Red Hat Virtualization)      | 0.8.0-1+b1igel71                          |
| SpeechWrite                            | 1.0                                       |
| Teradici PCoIP Software Client         | 20.10.0-18.04                             |
| ThinLinc Client                        | 4.12.0-6517                               |
| ThinPrint Client                       | 7-7.6.126                                 |
| Totem Media Player                     | 2.30.2-0ubuntu1igel55                     |
| Parole Media Player                    | 1.0.5-1igel1583919770                     |
| VNC Viewer                             | 1.10.1+dfsg-9igel17                       |
| VMware Horizon Client                  | 2012-8.1.0-17349998                       |
| Voip Client Ekiga                      | 4.0.1-9build1igel6                        |

## Dictation

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20201118 |



|                       |        |
|-----------------------|--------|
| Philips Speech driver | 12.9.1 |
|-----------------------|--------|

## Signature

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.9    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.4.2    |

## Smartcard

|                                           |                        |
|-------------------------------------------|------------------------|
| PKCS#11 Library A.E.T SafeSign            | 3.6.0.0-AET.000        |
| PKCS#11 Library Athena IDProtect          | 7                      |
| PKCS#11 Library cryptovision sc/interface | 7.3.1                  |
| PKCS#11 Library Gemalto SafeNet           | 10.7.77                |
| PKCS#11 Library OpenSC                    | 0.21.0-1igel39         |
| PKCS#11 Library SecMaker NetID            | 6.8.3.21               |
| PKCS#11 Library 90meter                   | 20190522               |
| Reader Driver ACS CCID                    | 1.1.6-1igel2           |
| Reader Driver Gemalto eToken              | 10.7.77                |
| Reader Driver HID Global Omnikey          | 4.3.3                  |
| Reader Driver Identive CCID               | 5.0.35                 |
| Reader Driver Identive eHealth200         | 1.0.5                  |
| Reader Driver Identive SCRKBC             | 5.0.24                 |
| Reader Driver MUSCLE CCID                 | 1.4.31-1igel11         |
| Reader Driver REINER SCT cyberJack        | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite               | 1.9.0-1igel16          |



|                      |         |
|----------------------|---------|
| Cherry USB2LAN Proxy | 3.2.0.3 |
|----------------------|---------|

## System Components

|                                         |                               |
|-----------------------------------------|-------------------------------|
| OpenSSL                                 | 1.0.2n-1ubuntu5.5             |
| OpenSSL                                 | 1.1.1-1ubuntu2.1~18.04.7      |
| OpenSSH Client                          | 8.4p1-3igel4                  |
| OpenSSH Server                          | 8.4p1-3igel4                  |
| Bluetooth stack (bluez)                 | 5.55-0ubuntu1.1igel10         |
| MESA OpenGL stack                       | 20.2.6-1igel131               |
| VAAPI ABI Version                       | 0.40                          |
| VDPAU Library version                   | 1.4-3igel1099                 |
| Graphics Driver INTEL                   | 2.99.917+git20200515-igel1013 |
| Graphics Driver ATI/RADEON              | 19.1.0-2igel1066              |
| Graphics Driver ATI/AMDGPU              | 19.1.0-2+git20200828igel1064  |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867               |
| Graphics Driver Nvidia                  | 450.102.04-0ubuntu0.20.04.1   |
| Graphics Driver VMware                  | 13.3.0-2igel857               |
| Graphics Driver QXL (Spice)             | 0.1.5-2build2-igel925         |
| Graphics Driver FBDEV                   | 0.5.0-1igel1012               |
| Graphics Driver VESA                    | 2.4.0-1igel1010               |
| Input Driver Evdev                      | 2.10.6-2igel1037              |
| Input Driver Elographics                | 1.4.1-1+b6igel952             |
| Input Driver eGalax                     | 2.5.8825                      |
| Input Driver Synaptics                  | 1.9.1-1ubuntu1igel1009        |
| Input Driver VMMouse                    | 13.1.0-1ubuntu2igel957        |
| Input Driver Wacom                      | 0.39.0-0ubuntu1igel1036       |
| Input Driver ELO Multitouch             | 3.0.0                         |
| Input Driver ELO Singletouch            | 5.1.0                         |



|                                      |                                   |
|--------------------------------------|-----------------------------------|
| Kernel                               | 5.9.16 #mainline-lxos-g1613995475 |
| Xorg X11 Server                      | 1.20.10-2igel1100                 |
| Xorg Xephyr                          | 1.20.10-2igel1100                 |
| CUPS printing daemon                 | 2.2.7-1ubuntu2.8igel32            |
| PrinterLogic                         | 25.1.0.425                        |
| Lightdm Graphical Login Manager      | 1.26.0-0ubuntu1igel13             |
| XFCE4 Window Manager                 | 4.14.2-1~18.04igel1600339249      |
| ISC DHCP Client                      | 4.3.5-3ubuntu7.1                  |
| NetworkManager                       | 1.20.4-2ubuntu2.2igel105          |
| ModemManager                         | 1.10.0-1~ubuntu18.04.2            |
| GStreamer 0.10                       | 0.10.36-2ubuntu0.1igel201         |
| GStreamer 0.10 Fluendo aacdec        | 0.10.42                           |
| GStreamer 0.10 Fluendo asfdemux      | 0.10.90                           |
| GStreamer 0.10 Fluendo h264dec       | 0.10.58                           |
| GStreamer 0.10 Fluendo mp3dec        | 0.10.40                           |
| GStreamer 0.10 Fluendo mpegdemux     | 0.10.85                           |
| GStreamer 0.10 Fluendo mpeg4videodec | 0.10.44                           |
| GStreamer 0.10 Fluendo vadec         | 0.10.224                          |
| GStreamer 0.10 Fluendo wmadec        | 0.10.70                           |
| GStreamer 0.10 Fluendo wmvdec        | 0.10.66                           |
| GStreamer 1.x                        | 1.18.3-1igel283                   |
| GStreamer 1.0 Fluendo aacdec         | 0.10.42.2-8d6d                    |
| GStreamer 1.0 Fluendo asfdemux       | 0.10.90                           |
| GStreamer 1.0 Fluendo h264dec        | 0.10.58                           |
| GStreamer 1.0 Fluendo mp3dec         | 0.10.40                           |
| GStreamer 1.0 Fluendo mpeg4videodec  | 0.10.44                           |
| GStreamer 1.0 Fluendo vadec          | 0.10.224                          |
| GStreamer 1.0 Fluendo wmadec         | 0.10.70                           |
| GStreamer 1.0 Fluendo wmvdec         | 0.10.66                           |
| WebKit2Gtk                           | 2.30.4-1igel40                    |
| Python2                              | 2.7.17                            |
| Python3                              | 3.6.9                             |



## VM Guest Support Components

|                            |                         |
|----------------------------|-------------------------|
| Virtualbox Guest Utils     | 6.1.18-dfsg-1igel49     |
| Virtualbox X11 Guest Utils | 6.1.18-dfsg-1igel49     |
| Open VM Tools              | 11.0.5-4ubuntu0.18.04.1 |
| Open VM Desktop Tools      | 11.0.5-4ubuntu0.18.04.1 |
| Xen Guest Utilities        | 7.10.0-0ubuntu1         |
| Spice Vdagent              | 0.20.0-2igel104         |
| Qemu Guest Agent           | 5.2+dfsg-3igel17        |

## Features with Limited IGEL Support

|                                    |                     |
|------------------------------------|---------------------|
| Mobile Device Access USB (MTP)     | 1.1.17-3igel5       |
| Mobile Device Access USB (imobile) | 1.3.0-5igel11       |
| Mobile Device Access USB (gphoto)  | 2.5.26-2igel7       |
| VPN OpenConnect                    | 8.10-2igel6         |
| Scanner support                    | 1.0.27-1            |
| VirtualBox                         | 6.1.18-dfsg-1igel49 |

## Services

| Service                                    | Size    | Reduced Firmware |
|--------------------------------------------|---------|------------------|
| Asian Language Support                     | 22.5 M  | Included         |
| Java SE Runtime Environment                | 36.0 M  | Included         |
| Citrix Appliance                           | 235.8 M | Included         |
| Citrix Workspace app                       |         |                  |
| Citrix StoreFront                          |         |                  |
| Ericom PowerTerm InterConnect              | 15.5 M  | Included         |
| Media Player                               | 512.0 K | Included         |
| Local Browser (Firefox)                    | 76.5 M  | Included         |
| Citrix Appliance                           |         |                  |
| VMware Horizon                             | 4.5 M   | Included         |
| RDP                                        |         |                  |
| Cendio ThinLinc                            | 10.0 M  | Included         |
| Printing (Internet printing protocol CUPS) | 22.2 M  | Included         |
| NoMachine NX                               | 26.8 M  | Included         |
| VMware Horizon                             | 131.2 M | Included         |
| Voice over IP (Ekiga)                      | 6.5 M   | Included         |



|                                            |         |              |
|--------------------------------------------|---------|--------------|
| Citrix Appliance                           | 768.0 K | Included     |
| NCP Enterprise VPN Client                  | 27.0 M  | Not included |
| Fluendo GStreamer Codec Plugins            | 6.5 M   | Included     |
| IBM i Access Client Solutions              | 72.5 M  | Not included |
| Red Hat Enterprise Virtualization          | 3.0 M   | Included     |
| Parallels Client                           | 5.5 M   | Included     |
| NVIDIA graphics driver                     | 126.8 M | Not included |
| Imprivata Appliance                        | 10.8 M  | Included     |
| Evidian AuthMgr                            | 2.5 M   | Included     |
| Hardware Video Acceleration                | 13.5 M  | Included     |
| Extra Font Package                         | 1.0 M   | Included     |
| Fluendo GStreamer AAC Decoder              | 1.2 M   | Included     |
| x32 Compatibility Support                  | 3.5 M   | Included     |
| Cisco JVDI client                          | 45.8 M  | Included     |
| PrinterLogic                               | 40.8 M  | Not included |
| Biosec BS Login                            | 10.0 M  | Not included |
| Login VSI Login Enterprise                 | 28.8 M  | Not included |
| Stratusphere UX CID Key software           | 2.8 M   | Not included |
| Elastic Filebeat                           | 15.8 M  | Not included |
| WVD                                        | 88.2 M  | Included     |
| Local Browser (Chromium)                   | 87.8 M  | Not included |
| deskMate client                            | 5.8 M   | Included     |
| Cisco Webex Teams VDI                      | 36.8 M  | Not included |
| Cisco Webex Meetings VDI                   | 32.2 M  | Not included |
| Zoom VDI Media Plugin                      | 42.2 M  | Not included |
| DriveLock                                  | 13.2 M  | Included     |
| SpeechWrite Client                         | 256.0 K | Included     |
| Teradici PCoIP Client                      | 14.5 M  | Included     |
| 90meter Smart Card Support                 | 256.0 K | Included     |
| Mobile Device Access USB (Limited support) | 256.0 K | Not included |
| VPN OpenConnect (Limited support)          | 1.0 M   | Not included |
| Scanner support / SANE (Limited support)   | 2.5 M   | Not included |
| VirtualBox (Limited support)               | 63.8 M  | Not included |

## General Information 11.05.100

To be beneficial to all new features and implementations, it is recommended to use UMS 6.07.100 or higher and update the corresponding profiles.



Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

## Known Issues 11.05.100

### Firmware Update

- On **devices with 2 GB of flash storage**, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Check [Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher<sup>388</sup>](#) for a solution.

### Citrix

- With activated **DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1 and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264** acceleration plugin, the following registry key must be enabled.

[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Value     | <u>enabled</u> / <u>disabled</u>                                 |

<sup>388</sup> <https://kb.igel.com/display/igelos1105/Updating+to+IGEL+OS+11.04+or+Higher+on+a+Device+with+Small+Storage>



This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

- **Adding smartcard readers** while the **session is ongoing** does not work. The **reader is visible, but cannot be used** due to permanently unknown reader status.

#### VMware Horizon

- **Client drive mapping** and **USB redirection** for storage devices should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Enable local **Storage Hotplug** on Setup page **Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection do not appear in the **remote desktop**.  
Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- **After the disconnect of an RDP-based session**, the Horizon main **window** which contains the server or sessions overview **cannot be resized anymore**.
- **Copying a text from Horizon Blast sessions** is not possible.
- The **on-screen keyboard** in **Horizon appliance mode** does not work correctly with local logon.  
Workaround: **Switch off local logon** and switch on the corresponding two keys via IGEL registry:
  - userinterface.softkeyboard.autoshow
  - userinterface.softkeyboard.autohide
- **Zoom VDI Media Plugin makes Horizon Client crash** upon connection to the remote desktop in cases **when TC Setup is running at the same time**.

#### Chromium

- **H.264 decoding is not supported** anymore.

#### Wi-Fi

- **TP-Link Archer T2UH Wi-Fi adapters** do not work after system suspend/resume. Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

#### Parallels Client

- **Native USB redirection** does not work with Parallels Client.

#### Cisco JVDI Client

- There may be a **segfault shown in the logs** (during logout of Citrix Desktop session). This occurs only when using **Citrix Workspace app 20.10 and Cisco JVDI**.

#### Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.



## Hyper-V

- **Hyper-V (Generation 2)** needs **a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.

## VirtualBox

- The current **VirtualBox Guest Tools/Drivers** will not work with **VirtualBox 5.2.x or older** hosts which leads to a black screen and non-working graphics.  
**Possible workaround:** Install with 'Failsafe Installation + Recovery' and set the registry key `x.drivers.force_vesa` to 'true'.

## Audio

- **Audio jack detection on Advantech POC-W243L** doesn't work. Therefore, sound output goes through a possibly connected headset and the internal speakers.
- **IGEL UD2 (D220)** fails to restore the volume level of the speaker when the device used **firmware version 11.01.110** before.

## Hardware

- Some newer **Delock 62599 active DisplayPort-to-DVI (4k)** adapters only work with INTEL devices.

## Remote Management

- **AIT feature with IGEL Starter License** is only **supported** by **UMS version 6.05.100 or newer**.

## Base system

- **Update from memory stick** requires network online state (at least when multiple update stages are involved).
- **Unreliable messages in user dialog for applying settings during boot**. Could occur when new settings were fetched from the UMS.

## deskMate

- Some stability issues may remain.

## Appliance Mode

- When **ending a Citrix session** in browser appliance mode, the **browser is restarted twice** instead of once.
- Appliance mode **RHEV/Spice: spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

## Security Fixes 11.05.100

### Citrix

- Fixed file properties for `/var/log/.ctxlogconf` adjusted, **so no code can be executed by the user**.

### Firefox



- **Added** `view-source:file:///` **to the blocklist** in case the browser should not have random access to the local file system.

#### Base system

- Fixed **bluez** security issue CVE-2020-0556.
- Fixed **librsvg** security issue CVE-2019-20446.
- Fixed **ppp** security issue CVE-2020-15704.
- Fixed **chromium-browser** security issues:

[More...](#)

CVE-2020-6541, CVE-2020-6540,  
CVE-2020-6539, CVE-2020-6538, CVE-2020-6537, CVE-2020-6536, CVE-2020-6535,  
CVE-2020-6534, CVE-2020-6533, CVE-2020-6532, CVE-2020-6531, CVE-2020-6530,  
CVE-2020-6529, CVE-2020-6528, CVE-2020-6527, CVE-2020-6526, CVE-2020-6525,  
CVE-2020-6524, CVE-2020-6523, CVE-2020-6522, CVE-2020-6521, CVE-2020-6520,  
CVE-2020-6519, CVE-2020-6518, CVE-2020-6517, CVE-2020-6516, CVE-2020-6515,  
CVE-2020-6514, CVE-2020-6513, CVE-2020-6512, CVE-2020-6511, CVE-2020-6510,  
CVE-2020-6509, CVE-2020-6507, CVE-2020-6506, CVE-2020-6505, CVE-2020-6496,  
CVE-2020-6495, CVE-2020-6494, CVE-2020-6493, CVE-2020-6571, CVE-2020-6570,  
CVE-2020-6569, CVE-2020-6568, CVE-2020-6567, CVE-2020-6566, CVE-2020-6565,  
CVE-2020-6564, CVE-2020-6563, CVE-2020-6562, CVE-2020-6561, CVE-2020-6560,  
CVE-2020-6559, CVE-2020-6558, CVE-2020-6556, CVE-2020-6555, CVE-2020-6554,  
CVE-2020-6553, CVE-2020-6552, CVE-2020-6551, CVE-2020-6550, CVE-2020-6549,  
CVE-2020-6548, CVE-2020-6547, CVE-2020-6546, CVE-2020-6545, CVE-2020-6544,  
CVE-2020-6543, CVE-2020-6542, CVE-2020-6576, CVE-2020-6575, CVE-2020-6574,  
CVE-2020-6573, CVE-2020-15966, CVE-2020-15965, CVE-2020-15964, CVE-2020-15963,  
CVE-2020-15962, CVE-2020-15961, CVE-2020-15960, CVE-2020-15959, CVE-2020-6557,  
CVE-2020-15992, CVE-2020-15991, CVE-2020-15990, CVE-2020-15989,  
CVE-2020-15988, CVE-2020-15987, CVE-2020-15986, CVE-2020-15985,  
CVE-2020-15984, CVE-2020-15983, CVE-2020-15982, CVE-2020-15981,  
CVE-2020-15980, CVE-2020-15979, CVE-2020-15978, CVE-2020-15977,  
CVE-2020-15976, CVE-2020-15975, CVE-2020-15974, CVE-2020-15973,  
CVE-2020-15972, CVE-2020-15971, CVE-2020-15970, CVE-2020-15969,  
CVE-2020-15968, CVE-2020-15967, CVE-2020-16017, CVE-2020-16013,  
CVE-2020-16011, CVE-2020-16009, CVE-2020-16008, CVE-2020-16007,  
CVE-2020-16006, CVE-2020-16005, CVE-2020-16003, CVE-2020-16002,  
CVE-2020-16001, CVE-2020-16000, CVE-2020-15999, CVE-2020-16036,  
CVE-2020-16035, CVE-2020-16034, CVE-2020-16033, CVE-2020-16032,  
CVE-2020-16031, CVE-2020-16030, CVE-2020-16029, CVE-2020-16028,  
CVE-2020-16027, CVE-2020-16026, CVE-2020-16025, CVE-2020-16024,  
CVE-2020-16023, CVE-2020-16022, CVE-2020-16021, CVE-2020-16020,  
CVE-2020-16019, CVE-2020-16018, CVE-2020-16015, CVE-2020-16014,  
CVE-2020-16012, CVE-2019-8075, CVE-2020-16042, CVE-2020-16041, CVE-2020-16040,  
CVE-2020-16039, CVE-2020-16038, CVE-2020-16037, CVE-2021-21116,  
CVE-2021-21115, CVE-2021-21114, CVE-2021-21113, CVE-2021-21112,  
CVE-2021-21111, CVE-2021-21110, CVE-2021-21109, CVE-2021-21108,  
CVE-2021-21107, CVE-2021-21106, CVE-2020-16043, CVE-2020-15995,  
CVE-2021-21148, CVE-2021-21147, CVE-2021-21146, CVE-2021-21145,  
CVE-2021-21144, CVE-2021-21143, CVE-2021-21142, CVE-2021-21141,  
CVE-2021-21140, CVE-2021-21139, CVE-2021-21138, CVE-2021-21137,  
CVE-2021-21136, CVE-2021-21135, CVE-2021-21134, CVE-2021-21133,



CVE-2021-21132, CVE-2021-21131, CVE-2021-21130, CVE-2021-21129, CVE-2021-21128, CVE-2021-21127, CVE-2021-21126, CVE-2021-21125, CVE-2021-21124, CVE-2021-21123, CVE-2021-21122, CVE-2021-21121, CVE-2021-21120, CVE-2021-21119, CVE-2021-21118, CVE-2021-21117, and CVE-2020-16044.

- Fixed **ffmpeg** security issues CVE-2020-14212, CVE-2020-13904, CVE-2020-35965, and CVE-2020-35964.
- Fixed **pulseaudio** security issues CVE-2020-11931 and CVE-2020-16123.
- Fixed **nss** security issues CVE-2020-6829, CVE-2020-12401, CVE-2020-12400, and CVE-2020-12403.
- Fixed libvirt security issues CVE-2020-14301, CVE-2020-12430, CVE-2020-10701, and CVE-2020-14339.
- Fixed **libslirp** security issues CVE-2020-10756, CVE-2020-29130, and CVE-2020-29129.
- Fixed **samba** security issues:  
**More...**

CVE-2020-14303, CVE-2020-1472, CVE-2020-1472, CVE-2020-14383, CVE-2020-14323, and CVE-2020-14318.

- Fixed **qemu** security issues:  
**More...**
- CVE-2020-16092, CVE-2020-14364, CVE-2020-15863, CVE-2020-13800, CVE-2020-13791, CVE-2020-13754, CVE-2020-13659, CVE-2020-13362, CVE-2020-13361, CVE-2020-13253, CVE-2020-12829, CVE-2020-10761, CVE-2020-28916, CVE-2020-27821, CVE-2020-27661, CVE-2020-27617, CVE-2020-27616, CVE-2020-25723, CVE-2020-25707, CVE-2020-25625, CVE-2020-25624, CVE-2020-25085, CVE-2020-25084, and CVE-2020-15859.

- Fixed **bind9** security issues CVE-2020-8624, CVE-2020-8623, and CVE-2020-8622.
- Fixed **grub2** security issues:  
**More...**

CVE-2020-10713, CVE-2020-14308, CVE-2020-14309, CVE-2020-14310, CVE-2020-14311, CVE-2020-15706, and CVE-2020-15707.

- Fixed **sane-backends** security issues:  
**More...**
- CVE-2020-12867, CVE-2020-12866, CVE-2020-12865, CVE-2020-12864, CVE-2020-12863, CVE-2020-12862, and CVE-2020-12861.

- Fixed **ghostscript** security issues:  
**More...**
- CVE-2020-17538, CVE-2020-16310, CVE-2020-16309, CVE-2020-16308, CVE-2020-16307, CVE-2020-16306, CVE-2020-16305, CVE-2020-16304, CVE-2020-16303, CVE-2020-16302, CVE-2020-16301, CVE-2020-16300, CVE-2020-16299, CVE-2020-16298, CVE-2020-16297, CVE-2020-16296, CVE-2020-16295, CVE-2020-16294, CVE-2020-16293, CVE-2020-16292, CVE-2020-16291, CVE-2020-16290, CVE-2020-16289, CVE-2020-16288, CVE-2020-16287, CVE-2020-16, CVE-2020-8112, CVE-2020-6851, CVE-2020-27845, CVE-2020-27843, CVE-2020-27842, CVE-2020-27841, CVE-2020-27824, CVE-2020-27814, and CVE-2018-5727.



- Fixed **net-snmp** security issues CVE-2020-15862 and CVE-2020-15861.
- Fixed **curl** security issues:  
[More...](#)

CVE-2020-8231, CVE-2020-8177, CVE-2020-8169, CVE-2020-8286, CVE-2020-8285, and CVE-2020-8284.
- Fixed **chrony** security issue CVE-2020-14367.
- Fixed **libx11** security issue CVE-2020-14344.
- Fixed **xorg-server** security issues:  
[More...](#)

CVE-2020-14347, CVE-2020-25712, CVE-2020-14360, CVE-2020-14362, CVE-2020-14361, CVE-2020-14346, and CVE-2020-14345.
- Fixed **cairo** security issues CVE-2018-19876 and CVE-2020-35492.
- Fixed **openssl1.0** security issues:  
[More...](#)

CVE-2020-1968, CVE-2019-1563, CVE-2019-1551, CVE-2019-1547, and CVE-2020-1971.
- Fixed **libproxy** security issues CVE-2020-25219 and CVE-2020-26154.
- Fixed **gnupg2** security issue CVE-2019-14855.
- Fixed **util-linux** security issue CVE-2018-7738.
- Fixed **ntp** security issue CVE-2019-8936.
- Fixed **tigervnc** security issue CVE-2020-26117.
- Fixed **brotli** security issue CVE-2020-8927.
- Fixed **vim** security issue CVE-2019-20807.
- Fixed **python2.7** security issue CVE-2020-26116.
- Fixed **python3.6** security issue CVE-2020-26116.
- Fixed **freetype** security issue CVE-2020-15999.
- Fixed **perl** security issues CVE-2020-12723, CVE-2020-10878 and CVE-2020-10543.
- Fixed **spice** security issue CVE-2020-14355.
- Fixed **glibc** security issue CVE-2017-18269.
- Fixed **python-cryptography** security issue CVE-2020-25659.
- Fixed **openldap** security issues CVE-2020-25692, CVE-2020-25710, and CVE-2020-25709.
- Fixed **libexif** security issue CVE-2020-0452.
- Fixed **krb5** security issue CVE-2020-28196.
- Fixed **libvncserver** security issues CVE-2018-21247, and CVE-2020-14396.
- Fixed **poppler** security issues CVE-2020-27778, CVE-2019-9959, CVE-2019-10871, and CVE-2018-21009.
- Fixed **xdg-utils** security issue CVE-2020-27748.
- Fixed **wpa** security issue CVE-2020-12695.
- Fixed **x11vnc** security issue CVE-2020-29074.
- Fixed **spice-gtk** security issue CVE-2020-14355.
- Fixed **libssh2** security issues CVE-2019-17498 and CVE-2019-13115.
- Fixed **spice-vdagent** security issues:  
[More...](#)



CVE-2020-25653, CVE-2020-25652, CVE-2020-25651, CVE-2020-25650, and CVE-2020-2565.

- Fixed **openssl** security issue CVE-2020-1971.
- Fixed **libxml2** security issue CVE-2020-24977.
- Fixed **webkit2gtk** security issues:  
[More...](#)

CVE-2020-9983, CVE-2020-9952, CVE-2020-9951, CVE-2020-9948, and CVE-2020-13584.

- Fixed **lxml** security issue CVE-2020-27783.
- Fixed **p11-kit** security issues CVE-2020-29363, CVE-2020-29362, and CVE-2020-29361.
- Fixed **wavpack** security issue CVE-2020-35738.
- Fixed **nvidia-graphics-drivers-450** security issues CVE-2021-1053 and CVE-2021-1052.
- Fixed **tar** security issues CVE-2019-9923 and CVE-2018-20482.
- Fixed **pillow** security issues CVE-2020-35655 and CVE-2020-35653.
- Fixed **dnsmasq** security issues:  
[More...](#)

CVE-2020-25687, CVE-2020-25686, CVE-2020-25685, CVE-2020-25684, CVE-2020-25683, CVE-2020-25682, CVE-2020-25681 and CVE-2019-14834.

- Fixed **sudo** security issues CVE-2021-3156 and CVE-2021-23239.
- Fixed **privilege escalation via** environment variable PATH in /bin/usershell binary.
- Fixed **privilege escalation via** environment variables in the /bin/update binary.
- Fixed **BleedingTooth** security issue which means CVE-2020-12351, CVE-2020-12352 and CVE-2020-24490.
- Fixed **kernel** security issues named **Platypus** (CVE-2020-8694 and CVE-2020-8695).
- Fixed possible security issue
- Fixed a **local command injection with SSH** session.

## Remote Management

- Added **secure channel** for following commands  
show\_message, get\_file\_from\_url, write\_file\_to\_url  
and upload\_tc\_support\_information  
sends all relevant data in a secured way.

## VNC

- Fixed a **secure terminal** and **secure VNC shadowing** remote code execution vulnerability.

## New Features 11.05.100

### Citrix

- The new "**screen pinning**" feature **for Citrix desktop sessions** has been integrated. With this feature, it is possible to **start multiple Citrix desktop sessions on different screens**.  
The following parameters have been added for this purpose:



- This parameter **defines** the **session name** on which the settings are to be used. Also the known **wildcards like \* and ? are possible** here.

[More...](#)

|            |                                                            |
|------------|------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Window</b> |
| Parameter  | Citrix session name                                        |
| Registry   | ica.destination_window.session%.name                       |
| Value      | ""                                                         |

- The parameter **defines** which **mode** should be **used**.

[More...](#)

|            |                                                                                                                                                                   |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Window</b>                                                                                                        |
| Parameter  | Multimonitor full-screen mode                                                                                                                                     |
| Registry   | ica.destination_window.session%.multimonitor_mode                                                                                                                 |
| Range      | [Restrict full-screen session to one monitor]<br>[Expand full-screen session across all monitors]<br>[Expand the session over a self-selected number of monitors] |

- For "**Restrict full-screen session to one monitor**"

also ica.destination\_window.session%.monitor needs **to be set**.

For "**Expand the session over a self-selected number of monitors**"

also ica.destination\_window.session%.multimonitor\_selection needs **to be set**.

**Further information** is also offered **via tooltip**.

[More...](#)

|            |                                                            |
|------------|------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Window</b> |
| Parameter  | Desktop session start monitor                              |
| Registry   | ica.destination_window.session%.monitor                    |
| Range      | [1st Monitor][2nd Monitor][3rd Monitor][4rd ...]           |
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Window</b> |
| Parameter  | Monitor selection                                          |
| Registry   | ica.destination_window.session%.multimonitor_selection     |
| Value      | ""                                                         |

- Integrated **HDX RTME 2.9.200** for the usage of SfB (Skype for Business).
- Available **Citrix Workspace apps** in this release: **20.12 (default)**, **20.10** and **19.12**.
- Added new feature, where **multiple audio devices could be mapped inside the sessions**. This will display audio devices with their device name and not only HDX audio.

[More...](#)



|           |                                 |
|-----------|---------------------------------|
| Parameter | Multiple Audio Device support   |
| Registry  | ica.module.vdcamversion4support |
| Value     | <u>true/false</u>               |

- Note: **Bluetooth devices** are currently **not supported for Device Redirection**.
- New **centralized Citrix logging in IGEL OS**, only one parameter is needed to activate logging.  
[More...](#)

|           |                                    |
|-----------|------------------------------------|
| Parameter | Enable logging for Citrix sessions |
| Registry  | ica.logging.debug                  |
| Value     | on/off                             |

- Since **Workspace app 20.09**, the tool **setlog** is **used to configure the logging**. For this purpose, parameters are provided in the registry `ica.logging.setlog`, but usually nothing needs to be changed.
- Fixed issue: **mic** and **webcam** devices can be **redirected using Browser Content Redirection**.  
[More...](#)

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Enables mic and webcam redirection using BCR |
| Registry  | ica.allregions.cefenablemediadevices         |
| Value     | [Factory default is "***"] [False][True]     |

- Added new parameter **Readers Status Poll Period** to **specify the delay**, in milliseconds, **for reading information from a smartcard** after the card is inserted or removed, or a reader is disconnected, etc.  
[More...](#)

|           |                                      |
|-----------|--------------------------------------|
| Parameter | Readers Status Poll Period           |
| Registry  | ica.wfclient.ReadersStatusPollPeriod |
| Type      | Integer                              |
| Value     | <u>250</u> /Range 100..5000          |

- Integrated **Zoom Media Plugin 5.4.59458.0109**
- The **default** value of the parameter `ica.module.vdcamversion4support` was **set to "true"**.

## WVD

- Added option to **always prompt for password upon session host connection**.  
[More...](#)

|           |                                                          |
|-----------|----------------------------------------------------------|
| Parameter | Always prompt for password upon session host connection  |
| Registry  | sessions.wvd%.options.always-prompt-for-session-password |
| Type      | bool                                                     |
| Value     | <u>enabled</u> / <u>disabled</u>                         |



|       |                                                                                                                              |
|-------|------------------------------------------------------------------------------------------------------------------------------|
| Note: | The same can be achieved on the server side by setting the RDP group policy of "Always prompt for password upon connection". |
|-------|------------------------------------------------------------------------------------------------------------------------------|

- Added options to configure **Fabulatech for WVD**. This includes **Webcam redirection**, **Scanner redirection**, and **USB redirection**.
- The **USB redirection** configuration is **still to be done** via **Sessions > RDP > RDP Global > Fabulatech USB Redirection**. Later releases should mirror that under WVD as well.
- There are **global WVD settings** to select which redirections (Webcam, Scanner, USB) should be enabled for WVD.
- There is a **switch per WVD session** that allows **to enable/disable Fabulatech for that sessions** respectively.
- Note: Technically, the **Fabulatech redirections** are **selected system-wide**. That means, when **Scanner redirection** is enabled for Citrix and **Webcam redirection** is enabled for WVD, both these redirections are visible in Citrix and in WVD sessions. Only disabling Fabulatech support in general for a WVD session is possible.

[More...](#)

|            |                                                                                          |
|------------|------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; WVD &gt; WVD Global &gt; Plugins &gt; Fabulatech</b>                    |
| Parameter  | Fabulatech Webcam Redirection                                                            |
| Registry   | wvd.plugins.fabulatech.webcam                                                            |
| Value      | enabled / <u>disabled</u>                                                                |
| IGEL Setup | <b>Sessions &gt; WVD &gt; WVD Global &gt; Plugins &gt; Fabulatech</b>                    |
| Parameter  | Fabulatech Scanner Redirection                                                           |
| Registry   | wvd.plugins.fabulatech.scanner                                                           |
| Value      | enabled / <u>disabled</u>                                                                |
| IGEL Setup | <b>Sessions &gt; WVD &gt; WVD Global &gt; Plugins &gt; Fabulatech</b>                    |
| Parameter  | Fabulatech USB Redirection                                                               |
| Registry   | wvd.plugins.fabulatech.usb                                                               |
| Value      | enabled / <u>disabled</u>                                                                |
| IGEL Setup | <b>Sessions &gt; WVD &gt; WVD Sessions &gt; WVD Session &gt; Plugins &gt; Fabulatech</b> |
| Parameter  | Fabulatech Webcam/Scanner/USB Redirection                                                |
| Registry   | sessions.wvd%.plugins.fabulatech                                                         |
| Value      | enabled / <u>disabled</u>                                                                |

- Integrated **Zoom Media Plugin 5.4.59458.0109** with support for WVD.

[More...](#)

|            |                                                                                          |
|------------|------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; WVD &gt; WVD Sessions &gt; WVD Session &gt; Plugins &gt; Fabulatech</b> |
| Parameter  | Zoom VDI Media Plugin                                                                    |



|          |                                            |
|----------|--------------------------------------------|
| Registry | <code>sessions.wvd%.plugins.zoomvdi</code> |
| Value    | <u>enabled</u> / <u>disabled</u>           |

- Added option to **always prompt for username and password upon session host connection.**  
[More...](#)

|           |                                                                                    |
|-----------|------------------------------------------------------------------------------------|
| Parameter | Always prompt for username and password upon session host connection               |
| Registry  | <code>sessions.wvd%.options.always-prompt-for-session-username-and-password</code> |
| Type      | bool                                                                               |
| Value     | <u>enabled</u> / <u>disabled</u>                                                   |

- Added option to **preset the workspace view zoom**

[More...](#)

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | Initial workspace zoom                           |
| Registry  | <code>sessions.wvd%.options.workspacezoom</code> |
| Type      | string                                           |
| Value     | <u>100</u>                                       |

- Added option to **select specific monitors in a multimonitor session.**

**Only monitors matching this mask** are used.

- Monitors start with zero (0).
- If empty all monitors are enabled, which is the default.
- Can be one or a comma-separated list of the following specifiers without the quotes:
  - "1-2": An inclusive range of monitor indexes.
  - "-2": An inclusive range beginning from 0 to the given monitor index.
  - "2-": An inclusive range beginning with the specified monitor up to index 63, which is the maximum monitor index supported.
  - "2,3,5": A comma-separated list of monitor indexes.

[More...](#)

|           |                                                     |
|-----------|-----------------------------------------------------|
| Parameter | Multimonitor enable mask                            |
| Registry  | <code>sessions.wvd%.options.multimonitormask</code> |
| Type      | string                                              |
| Value     | (empty by default)                                  |

- If the **username** is **preset with a string that starts with "@"**, the **rest of the string is taken as a preset domain** name. The user then only needs to enter her/his username and the domain name is automatically appended for AAD login.
- Additionally, the following parameter has been added to **allow/disallow the preset domain being overwritten when the username enters a name that contains an @ symbol itself**. If this



option is enabled, the entered domain is accepted. Otherwise, the entered domain is replaced by the preset domain.

[More...](#)

|           |                                                     |
|-----------|-----------------------------------------------------|
| Parameter | Allow preset domain overwrite                       |
| Registry  | sessions.wvd%.options.allow-preset-domain-overwrite |
| Type      | bool                                                |
| Value     | enabled / <u>disabled</u>                           |

- Added **company logo customization**, but the download of custom images to the local filesystem needs to be defined. So **at the moment, the settings are not really useful, except for disabling the IGEL logo** maybe.

[More...](#)

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Disable company logo                          |
| Registry  | sessions.wvd%.options.no <sup>389</sup> -logo |
| Type      | bool                                          |
| Value     | enabled / <u>disabled</u>                     |
| Parameter | Logo image filename                           |
| Registry  | sessions.wvd%.options.logo-image              |
| Type      | string                                        |
| Value     | (empty by default)                            |

- Added **background customization**, but download of custom images to the local filesystem needs to be defined. So **at the moment, the settings are not really useful, except for disabling the background image or defining a solid color for the background**.

[More...](#)

|           |                                                     |
|-----------|-----------------------------------------------------|
| Parameter | Disable background image                            |
| Registry  | sessions.wvd%.options.no <sup>390</sup> -background |
| Type      | bool                                                |
| Value     | enabled / <u>disabled</u>                           |
| Parameter | Background image filename or color (#rrggbba)       |
| Registry  | sessions.wvd%.options.background-image              |
| Type      | string                                              |
| Value     | (empty by default) / filename / #rrggbba            |

## VMware Horizon

- Updated **Horizon Client** to version **2012-8.1.0-17349998**
- Integrated **Zoom Media Plugin 5.4.59458.0109**
- Fixed failure to **start Horizon serial port redirection service at boot time**

## Chromium

---

<sup>389</sup> <http://options.no>

<sup>390</sup> <http://options.no>



- Updated **Chromium** browser to version **88.0.4324.150**.
- **H.264 decoding** is **not supported** anymore.
- **Custom preferences** setup is **not supported** anymore.
- Reworked **custom commandline** setup: Enter **all commandline parameters in a single entry field**.

## Wi-Fi

- Added support for **WPS push button connect method**

## Imprivata

- Added: The **FUS Username** is an **editable combobox with prefilled values** now. Set of an **own string** is also **possible**.

- Hostname of the endpoint
- MAC address of the endpoint
- Serial number of the endpoint

[More...](#)

|            |                                                    |
|------------|----------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Appliance mode &gt; Imprivata</b> |
| Parameter  | FUS User                                           |
| Registry   | imprivata.fus.user                                 |

## Smartcard

- Updated **A.E.T. Europe SafeSign Identity Client** to version **3.6.0.0**.
- Added **Smartcard PIN passthrough** in **Firefox** and **Chromium**. The PIN will be cached while logging on via Active Directory/Kerberos with smartcard. In Firefox and Chromium, no further PIN input is necessary to use the smartcard.

[More...](#)

|           |                                  |
|-----------|----------------------------------|
| Parameter | Smartcard PIN caching            |
| Registry  | scard.pkcs11.pin_cache.enable    |
| Value     | <u>enabled</u> / <u>disabled</u> |

- Updated **SecMaker Net iD** to version **6.8.3**. New features are:

- Support for Thales IDPrime 940 SIS & IDPrime 3940 SIS
  - Support for FIPS level 3 versions of Thales IDPrime MD smart cards (based on MD830B and MD840)
  - Support for FINEID 3.0
  - Updated support for Yubico YubiKey serial numbers (version 5 and later)
  - Updated support for Feitian ePass FIDO serial numbers (version 99 and later)
- For detailed release information, see <https://docs.secmaker.com/net-id-enterprise/6.8/nie-release-notes/nie-683-release-notes.html>.

## ThinPrint

- Added **ezeep by ThinPrint** support for **WVD**

[More...](#)

|            |                                                                                                   |
|------------|---------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; WVD &gt; WVD Sessions &gt; WVD Session &gt; Printing &gt; ezeep by ThinPrint</b> |
|------------|---------------------------------------------------------------------------------------------------|



|           |                                                                                                                                                                                                                                                                                                                                         |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter | Printing with ezeep                                                                                                                                                                                                                                                                                                                     |
| Registry  | sessions.wvd%.printing.thinprint-ezeep                                                                                                                                                                                                                                                                                                  |
| Value     | <u>enabled</u> / <u>disabled</u>                                                                                                                                                                                                                                                                                                        |
| Note      | <ul style="list-style-type: none"> <li>Ezeep is directly related to the ThinPrint configuration under <b>Devices &gt; Printer &gt; ThinPrint &gt; ...</b></li> <li>When ThinPrint configuration is changed, you need to close running WVD sessions and reconnect to make ThinPrint/Ezeep work again for the related session.</li> </ul> |

#### Application Launcher

- Added **optional custom message in 'About' page of application launcher**. The message is displayed **below** the **License Information** section. The text can be plain text or HTML, supported HTML subset are mentioned in Qt RichText.

[More...](#)

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Custom message                        |
| Registry  | userinterface.launcher.custom_message |
| Value     | <u>empty</u>                          |

#### Cisco Webex

- Integrated **Cisco Webex Meetings 41.2.0.142**
- Integrated **Cisco Webex Teams 41.1.0.17621**

#### Cisco JVDI Client

- Integrated **Cisco JVDI 12.9.3** client

#### Base system

- Added **post-session command** support **for WVD** sessions.
- Updated **OpenVPN** to version **2.5.0**.
- Updated **OpenSSH** to version **8.4p1-2**.
- Added **warning at boot time if Workspace Edition maintenance has expired**.
- Updated **Fluendo multimedia codecs**.
- Updated **Linux kernel** to version **5.9.16**.
- Added **inhibit screensaver** when **Zoom, Teams or Skype for Business** meeting is **active**. Possible for native clients and Citrix optimization plugins.

[More...](#)

|           |                                                   |
|-----------|---------------------------------------------------|
| Parameter | Enable debug logging for igel-screensaver-monitor |
| Registry  | debug.tools.igel-screensaver-monitor.enable       |
| Value     | <u>enabled</u> / <u>disabled</u>                  |

- Added functionality to **change the desktop icon font color** via new Setup parameter.

[More...](#)

|            |                                    |
|------------|------------------------------------|
| IGEL Setup | <b>User Interface &gt; Desktop</b> |
| Parameter  | Desktop Icon Font Color            |



|          |                                                   |
|----------|---------------------------------------------------|
| Registry | windowmanager.defaulttheme.desktop.iconfont_color |
|----------|---------------------------------------------------|

## CID Key Agent

- Update of **CID Key Agent** to version **6.5.0-2**

## Driver

- Updated **Olympus dictation driver** for **Citrix** and **RDP** to version **20201118**.

The changes are:

- Support motion events for Olympus RecMic devices
- Support integration with the Olympus AudioSDK for limited server-side device communication

- Updated **Crossmatch driver** to version **0125**.

The changes are:

- Improved USB encryption for the 4500 readers
- Support for the 5300-101 reader (the 5300-100 was already supported)

- Updated **deviceTRUST** client plugin for **Citrix** and **RDP** to version **20.1.200.0**. Detailed release notes can be found at <https://docs.devicetrust.com/docs/releases-igel-20.1.200/>.

## X11 system

- Enhanced `x.xserver%.mirror_mode` registry key with new **Scaling down mode** (Scales all monitors to the monitor with the lowest resolution)

[More...](#)

|           |                                                                                   |
|-----------|-----------------------------------------------------------------------------------|
| Parameter | Choose the mode which should be used for mirroring monitors if resolution differs |
| Registry  | <code>x.xserver%.mirror_mode</code>                                               |
| Range     | [Default] [Biggest common resolution] [Scaling] [Scaling down]                    |

## Audio

- Added **EPOS Connect 5.0.1.2795**

[More...](#)

|            |                                                                              |
|------------|------------------------------------------------------------------------------|
| IGEL Setup | <b>Devices &gt; Unified Communications &gt; EPOS Audio &gt; EPOS Connect</b> |
| Parameter  | Enable EPOS Connect                                                          |
| Registry   | <code>devices.epos.connect.enable</code>                                     |
| Type       | bool                                                                         |
| Value      | enabled / disabled                                                           |
| IGEL Setup | <b>Devices &gt; Unified Communications &gt; EPOS Audio &gt; EPOS Connect</b> |
| Parameter  | Tenant ID                                                                    |
| Registry   | <code>devices.epos.connect.tenant_id</code>                                  |
| Type       | string                                                                       |



|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| Value      | "                                                                             |
| IGEL Setup | <b>Devices &gt; Unified Communications &gt; EPOS Audio &gt; EPOS Connect</b>  |
| Parameter  | Backend Endpoint                                                              |
| Registry   | devices.epos.connect.tenant_url                                               |
| Type       | string                                                                        |
| Value      | "                                                                             |
| IGEL Setup | <b>Devices &gt; Unified Communications &gt; EPOS Audio &gt; EPOS Connect</b>  |
| Parameter  | Proxy                                                                         |
| Registry   | devices.epos.connect.proxy                                                    |
| Type       | string                                                                        |
| Value      | "                                                                             |
| Registry   | devices.epos.connect.log_level                                                |
| Value      | Trace / Debug / <u>Information</u> / Warnings / Errors / Exceptions / No logs |

- **Pulseaudio** upgraded to the **13.99** version.
- Added parameter to **differentiate sound volume for applications**. If the parameter is set to true, each application can set its own volume level. Otherwise, the sound volume is set to the same value as the default volume for output and input device respectively.

[More...](#)

|          |                                     |
|----------|-------------------------------------|
| Registry | userinterface.sound.app_volume_ctrl |
| Value    | true / false                        |

## Misc

- Added **DriveLock Agent 20.1.4.30482** for USB device access control.

[More...](#)

|            |                                                    |
|------------|----------------------------------------------------|
| IGEL Setup | <b>Devices &gt; Storage Devices &gt; DriveLock</b> |
| Parameter  | Enable DriveLock agent                             |
| Registry   | devices.drivelock.enable                           |
| Value      | enabled / <u>disabled</u>                          |
| IGEL Setup | <b>Devices &gt; Storage Devices &gt; DriveLock</b> |
| Parameter  | DES server URL                                     |
| Registry   | devices.drivelock.server                           |
| Value      | (empty)                                            |
| IGEL Setup | <b>Devices &gt; Storage Devices &gt; DriveLock</b> |
| Parameter  | Tenant                                             |
| Registry   | devices.drivelock.tenant                           |
| Value      | <u>root</u>                                        |

## Evidian



- Added new session type **RD Web Access**.
- Updated **Evidian** to version **1.5.7617**.

## Hardware

- Added hardware support for new **IGEL UD7-LX 20 (H860C)**.
- Added hardware support for **LG 34CN650N AiO**.
- Added hardware support for **Dell Wyse Z Class thin client**.
- Added hardware support for **Lenovo ThinkCentre M70q**.
- Added hardware support for **Dell Wyse 5470**.
- Added hardware support for **Lenovo L14**.
- Added hardware support for **Lenovo ThinkCentre M75n**.
- Added hardware support for **Lenovo 14w**.
- Added hardware support for **LG CN65 All in one**.
- Added hardware support for **DELL LATITUDE 5510**.
- Added hardware support for **ELO i2 Touch all-in-one (15 and 22) inch**.
- Added detection of **UD Pocket UC5-LX 2**.
- Added support for headset **Jabra Evolve2 65**.

## Remote Management

- Added support for **Reportable Heartbeats to the UMS**.
- Added support for **exchanging ICG certificates**.
- The remote management of the endpoint device automatically installs TLS certificates provided by the UMS into the local trusted CA certificates storage. **The automatic deployment of TLS certificates to endpoint devices requires UMS 6.06.100 or higher**. This feature allows verifying certificates used in downloading files from the UMS, downloading of a firmware update and custom partition archives over HTTPS or FTPS protocols. **The verifying of certificates must be enabled by** the parameter `system.security.remote_management.tls_verify_peer`.

[More...](#)

|          |                                                                        |
|----------|------------------------------------------------------------------------|
| Registry | <code>system.security.remote_management.tls_verify_peer</code>         |
| Value    | <u>true</u> / <u>false</u>                                             |
| Registry | <code>system.security.remote_management.tls_hostname_validation</code> |
| Value    | <u>true</u> / <u>false</u>                                             |

- Added support for UMS commands to **store and remove ICG configuration**.
- Introduced parameters for **ICG WebSocket connections: debug log, network timeout** (in seconds) and **ping-pong interval** (in seconds). The parameters are applied on the next established ICG agent connection and ICG tunnel connections: VNC and Secure Terminal.

[More...](#)

|          |                                                        |
|----------|--------------------------------------------------------|
| Registry | <code>system.icg.websocket.debug</code>                |
| Value    | <u>off</u> / <u>all</u> / <u>tunnel</u> / <u>agent</u> |
| Registry | <code>system.icg.websocket.network_timeout</code>      |
| Value    | <u>30</u>                                              |
| Registry | <code>system.icg.websocket.pingpong_interval</code>    |



|       |            |
|-------|------------|
| Value | <u>120</u> |
|-------|------------|

- IGEL Remote Management agent sends now **keep-alive packets to the ICG server to prevent the Websocket connection to the ICG server from being closed by networking infrastructure.** The Websocket's ping-pong mechanism is used for that purpose (see RFC6455). The **keep-alive interval** in seconds can be **configured by** the parameter `system.icg.websocket.pingpong_interval`, 0 disables the keep-alive mechanism.
- More...**

|          |                                                     |
|----------|-----------------------------------------------------|
| Registry | <code>system.icg.websocket.pingpong_interval</code> |
| Value    | <u>120</u>                                          |

#### Fabulatech

- Updated **FabulaTech USB for Remote Desktop** to version **6.0.28**
- Updated **FabulaTech Scanner for Remote Desktop** to version **2.7.0.1**
- Fixed **FabulaTech scanner redirection not working for Citrix** if it's exclusively enabled in IGEL Setup.

#### Resolved Issues 11.05.100

##### Citrix

- Fixed the problem with **apparmor** and the **Citrix MS Teams** workaround
- Following registry keys help to **edit horizontal and vertical window size** (works only for desktops not for applications).

**More...**

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Set desired horizontal window dimension      |
| Registry  | <code>ica.allregions.desiredhres</code>      |
| Value     | <u>[**] [640] [800] [1024] [1280] [1600]</u> |
| Parameter | Set desired vertical window dimension        |
| Registry  | <code>ica.allregions.desiredvres</code>      |
| Value     | <u>[**] [480] [600] [768] [1024] [1200]</u>  |

- Citrix **Desktop** sessions **have a sound device** again, when using **smartcard watch daemon**. `scard.swatchd.insert_action = su user -c /config/sessions/pnlogin0`
- Parameter `ica.module.virtualdrivers.vdwebrtc.keyboard_workaround` has been removed. This workaround is no longer needed because the problem is **solved as of CWA 20.10**.
- Added new parameters to **add config parameters** for **Citrix USB devices**: the parameter string is appended to the config line in `usb.conf`, when the **device is explicitly allowed**. Citrix introduced this to handle special behavior with single devices, e.g. to set "disableselectconfig=1".

**More...**

|           |                                                                                      |
|-----------|--------------------------------------------------------------------------------------|
| Parameter | Extra Config                                                                         |
| Registry  | <code>ica.usbredirection.devicepolicy.product_rule</code><br><code>%parameter</code> |
| Type      | String                                                                               |
| Value     | <u>""</u>                                                                            |



|           |                                                               |
|-----------|---------------------------------------------------------------|
| Parameter | Extra Config                                                  |
| Registry  | ica.usb redirection.devicepolicy.product_rule_igel%.parameter |
| Type      | String                                                        |
| Value     | <u>""</u>                                                     |

- Improved **Fabulatech USB Redirection** and **Scanner Support**

- New parameter added:

**More...**

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | Fabulatech loglevel                              |
| Registry  | ica.module.virtualdriver.fabulatech.loglev<br>el |
| Value     | <u>1</u>                                         |

- Added new parameter **AckDelayThresh**: Max time (in milliseconds) between sending "resource free" message if any resources free. Default=350

**More...**

|           |                           |
|-----------|---------------------------|
| Parameter | AckDelayThresh            |
| Registry  | ica.module.AckDelayThresh |
| Type      | Integer                   |
| Value     | <u>350</u>                |

- Added new parameter **AudioBufferSizeMilliseconds**: Audio buffer size, in ms. Default=200 ms

**More...**

|           |                                            |
|-----------|--------------------------------------------|
| Parameter | AudioBufferSizeMilliseconds                |
| Registry  | ica.module.AudioBufferSizeMilli<br>seconds |
| Type      | Integer                                    |
| Value     | <u>200</u>                                 |

- Added new parameter **AudioLatencyControlEnabled**: Enables latency control. Default=False

**More...**

|           |                                       |
|-----------|---------------------------------------|
| Parameter | AudioLatencyControlEnabled            |
| Registry  | ica.module.AudioLatencyControlEnabled |
| Type      | Boolean                               |
| Value     | <u>true / false</u>                   |

- Added new parameter **AudioMaxLatency**: Sets the maximum latency (in ms) before trying to discard audio data. Default=300 ms

**More...**

|           |                            |
|-----------|----------------------------|
| Parameter | AudioMaxLatency            |
| Registry  | ica.module.AudioMaxLatency |
| Type      | Integer                    |
| Value     | <u>300</u>                 |



- Added new parameter **AudioLatencyCorrectionInterval**: Defines how often to correct the latency (in ms). Default=300 ms

**More...**

|           |                                           |
|-----------|-------------------------------------------|
| Parameter | AudioLatencyCorrectionInterval            |
| Registry  | ica.module.AudioLatencyCorrectionInterval |
| Type      | Integer                                   |
| Value     | 300                                       |

- Added new parameter **AudioTempLatencyBoost**: Sets the higher latency band (in ms) above the lower PlaybackDelayThresh band. Default=300 ms

**More...**

|           |                                  |
|-----------|----------------------------------|
| Parameter | AudioTempLatencyBoost            |
| Registry  | ica.module.AudioTempLatencyBoost |
| Type      | Integer                          |
| Value     | 300                              |

- Added new parameter **CommandAckThresh**: Number of free client command buffers causing a "resource free" message to be sent to the server. Default=10

**More...**

|           |                             |
|-----------|-----------------------------|
| Parameter | CommandAckThresh            |
| Registry  | ica.module.CommandAckThresh |
| Type      | Integer                     |
| Value     | 10                          |

- Added new parameter **DataAckThresh**: Number of free client data buffers causing a "resource free" message to be sent to the server. Default=10

**More...**

|           |                          |
|-----------|--------------------------|
| Parameter | DataAckThresh            |
| Registry  | ica.module.DataAckThresh |
| Type      | Integer                  |
| Value     | 10                       |

- Added new parameter **MaxDataBufferSize**: Maximum size of each data buffer. Default=2048 bytes

**More...**

|           |                              |
|-----------|------------------------------|
| Parameter | MaxDataBufferSize            |
| Registry  | ica.module.MaxDataBufferSize |
| Type      | Integer                      |
| Value     | 2048                         |

- Added new parameter **NumCommandBuffers**: Number of client buffers to use for audio commands. Default=64

**More...**

|           |                              |
|-----------|------------------------------|
| Parameter | NumCommandBuffers            |
| Registry  | ica.module.NumCommandBuffers |
| Type      | Integer                      |



|       |    |
|-------|----|
| Value | 64 |
|-------|----|

- Added new parameter **PlaybackDelayThresh**: Delay (in ms) between being asked to start audio playback and actually starting audio playback in order to build up a backlog of sound. Default=150  
[More...](#)

|           |                                |
|-----------|--------------------------------|
| Parameter | PlaybackDelayThresh            |
| Registry  | ica.module.PlaybackDelayThresh |
| Type      | Integer                        |
| Value     | 150                            |

- Fixed: **ICA Connection Center** starts again as expected.
- Fixed **Citrix Kerberos Passthrough** authentication.
- Added: When the **password has expired** but the **password change is not allowed** on the Citrix server, the **Citrix error message** is displayed.
- Added: The parameter for mouseinput `ica.wfclient.mousesendcontrolv` is available with this release on the Setup page **Sessions > Citrix > Citrix Global > Keyboard**.
- Added: The parameter for the **Citrix Connection bar** `ica.allregions.connectionbar` is available on the Setup page **Sessions > Citrix > Citrix Global > Window**.
- Fixed **Citrix sessions with H.264 hardware acceleration on and DRI3 off** that crashed with error message: The X Request 130.1 caused error: 10 BadAccess.

#### OSC Installer

- Fixed **warning message after feature deselection for installations on 2 GB flashes**.
- Fixed a **display** issue with **Intel and Nvidia GPU**.

#### RDP/IGEL RDP Client 2

- Fixed **USB redirection** for RDP sessions.
- Added new parameter to enable/disable **dynamic drive mapping**.

[More...](#)

|          |                                                         |
|----------|---------------------------------------------------------|
| Registry | rdp.winconnect.enable-dynamic-drivemapping              |
| Value    | <u>enabled</u> / disabled                               |
| Registry | sessions.winconnect%.option.enable-dynamic-drivemapping |
| Range    | <u>Global Setting</u> / On / Off                        |

- Fixed **login information not being set after reboot**.
- Improved **error logging**.

#### WVD

- WVD now comes with **Qt 5.12.10** in order **to get fixes mainly for QWebEngine**. This should fix issues with **.htaccess protected login pages**.
- Fixed **proxy usage** for WVD feed download.

#### RD Web Access

- Fixed **RD Web Access Login** not working with **user@domain**.
- Fixed **RD Web Access username** not being set correctly **after reboot**.

#### VMware Horizon



- Fixed **remember last user** functionality in Horizon **local logon**
- Fixed **Local Logon Window** for visibility in **appliance mode**
- When using the **PCoIP** protocol, the **virtual channel** provided by VMware used **for both serial port and scanner redirection** may **hang on logout**.

The virtual channel is not used when both redirection methods are set to "false" which is the default.

For the usage of either one of these redirection methods, enable the corresponding parameter below **to prevent the logout freeze**.

These settings can be found here in the IGEL Registry:

`vmware.view.enable-serial-port-redir`

`vmware.view.enable-scanner-redir`

## Firefox

- Fixed **smartcard access** in Firefox. Before this fix, smartcards were not recognized in seldom cases.
- Fixed possibility to use the **pre-installed spellcheckers** in Firefox input fields.

## Chromium

- Fixed **browser** and **download history not being cleared**.
- Fixed Chromium browser was not clearing browsing history properly.
- Fixed: **Custom Chromium Policies** datatypes now written in the correct way to policies.json
- Fixed **resetting kiosk mode** would only work **after reboot**
- Fixed: Chromium settings were **parent settings did not influence the child settings**

## Network

- Added registry keys for enabling/disabling **sending of hostname in DHCPv4 and DHCPv6 requests**.

**More...**

|           |                                          |
|-----------|------------------------------------------|
| Parameter | Send hostname in DHCP requests           |
| Registry  | <code>network.dhcp.send_hostname</code>  |
| Range     | [Disabled][Network Manager default]      |
| Value     | <u>Network Manager default</u>           |
| Parameter | Send hostname in DHCPv6 requests         |
| Registry  | <code>network.dhcp6.send_hostname</code> |
| Range     | [Disabled][Network Manager default]      |
| Value     | <u>Network Manager default</u>           |

- Fixed: **SCEP** failed when scep\_getca received only a single certificate.
- Added registry key specifying **the number of 802.1X authentication attempts on Ethernet**.

**More...**

|          |                                                                          |
|----------|--------------------------------------------------------------------------|
| Registry | <code>network.interfaces.ethernet.device%.ieee8021x.auth_attempts</code> |
| Type     | Integer                                                                  |
| Value    | 1                                                                        |



- The **default** value of `network.interfaces.ethernet.device%.nm_disable_link_config` (forbidding Network Manager to modify Ethernet link settings) has been **changed to "true"**.
- Fixed handling of **DNS default domain**
- Added registry key for **disabling Ethernet link reconfiguration by Network Manager**.

[More...](#)

|           |                                                                         |
|-----------|-------------------------------------------------------------------------|
| Parameter | Disable NetworkManager link configuration                               |
| Registry  | <code>network.interfaces.ethernet.device%.nm_disable_link_config</code> |
| Type      | <code>bool</code>                                                       |
| Value     | <code>true / false</code>                                               |

- Setting this to "true"** can be **beneficial when 802.1X authentication is disturbed**. It is currently enforced automatically in the case of e1000e drivers.
- Changed default value of minimum size of a TCP packet** from 750 **to 500 bytes** as a result this would allow a **minimal MTU size of 576 bytes**.

## Wi-Fi

- Added missing **iwlwifi-6000-4 firmware file**.
- Fixed issues with **D-Link DWA-131 WLAN dongle**.
- Removed** `network.drivers.use_backport_drivers` IGEL registry key as this is not used anymore.
- Added some missing **iwlwifi firmware files** to IGEL OS.

## Open VPN

- Fixed **segmentation fault** when nameserver is used.  
Now it is allowed to use an empty password for the private key. **Important: Not enter a password** when the private key doesn't have one.
- OpenConnect VPN: Different protocols are selectable:

[More...](#)

|           |                                                                             |
|-----------|-----------------------------------------------------------------------------|
| Parameter | <code>protocol</code>                                                       |
| Registry  | <code>sessions.openconnect%.vpnopts.protocol</code>                         |
| Value     | <u>Cisco AnyConnect</u> / Juniper Network / Junos Pulse / PAN GlobalProtect |

## Imprivata

- Fixed: Usage the **Horizon Window Size** settings
- Fixed: Set **keyboard repeat rate** correctly on Horizon session end
- Added Imprivatas "**grid-theme**" feature

[More...](#)

|           |                                     |
|-----------|-------------------------------------|
| Parameter | PIE Application Launcher for Citrix |
| Registry  | <code>imprivata.grid_theme</code>   |
| Value     | <code>enabled / disabled</code>     |

## Smartcard



- Added parameter to **disable HID Global OMNIKEY smartcard reader driver**. If this driver is **disabled**, some of the readers are **handled by the MUSCLE CCID driver**. This can help when problems with OMNIKEY reader driver occur.

[More...](#)

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | HID Global OMNIKEY driver for smart card readers |
| Registry  | scard.pcscd.omnikey_enable                       |
| Value     | <u>enabled</u> / disabled                        |

#### HID

- Fixing **double tapping of desktop icons** on **touchscreen** devices.

#### CUPS Printing

- Fixed **CUPS printer spooling configuration** where printjob files were preserved in the spooling directory too long and could fill up the file system.

#### Logging

- Fixed: **Filebeat** now **starts after the hostnames are set** so they will be shown in the logs.

#### Base system

- Fixed problems with **hostnames containing one or more "\_" characters**.
- Post-session command binaries and return codes are now customizable** via registry. Allows post-session commands if a binary doesn't return 0.
  - Name of the binary:

[More...](#)

|           |                                 |
|-----------|---------------------------------|
| Parameter | Binary                          |
| Registry  | pcom.valid_return_codes%.binary |
| Value     | binary name                     |

- Comma-separated return codes (e.g. 7,99) or/and return code ranges (e.g. 3..5 for 3,4,5) to be accepted:

[More...](#)

| Parameter | Return Codes                              |
|-----------|-------------------------------------------|
| Registry  | pcom.valid_return_codes%.return codes     |
| Value     | e.g. 3,5,10..15 for 3,5,10,11,12,13,14,15 |

- Improved **post-session** command parameter pcom.valid\_return\_codes%.returncodes to handle **ranges a la 1..255** (see tooltip).
- Fixed **remembering last user name with Active Directory/Kerberos** logon. Before this fix, the user name could not be stored in UMS to appear again after a reboot.
- Fixed possibility to **add certificates to Chromium and Firefox** which are given **in DER format**.
- Fixed **default browser** not being set properly **after reboot**.
- Fix **GtkMessage** dialog localization.
- Fixed: **Fluendo vadec codec** update closed a **memory leak** with AMD devices using VAAPI acceleration.
- Fixed possible USB issues with **suspend/resume on IGEL M350C** devices.



- Fixed: **Shutdown delay** when post-session command is enabled.
- Fixed **NetworkManager** could not create **ipv6 pid/lease file** while **apparmor** is active.
- Bugfix for missing **bluetooth tray icon** after suspend

#### Storage Devices

- Fixed display of **hotplug eject menu in appliance mode**

#### X11 system

- Fixed display **hotplug detection** not working in some situations.
- Fixed **Display Switch** sometimes **losing config** after reboot.
- Fixed missing **custom background image after migration** from OS 10.
- Fixed **sporadic hang in logoff session restart**.
- Updated **Display Switch rotate buttons** to have usable size.
- Added registry key to solve an issue with **buggy monitors connected over a DP-to-DVI adapter** (only works for Radeon devices like UD3 LX50).

[More...](#)

|           |                                                              |
|-----------|--------------------------------------------------------------|
| Parameter | Fix issues with buggy monitors connected over DP-DVI adapter |
| Registry  | x.drivers.ati.dp_dvi_probe_workaround                        |
| Type      | bool                                                         |
| Value     | enabled / disabled                                           |

- Fixed **touchpad** enable and disable **with hotkey**.
- Fixed issues if **2 DisplayPort MST Hubs** are connected behind each other.
- Fixed **notifications** not being hidden properly when **in do-not-disturb mode**.
- Fixed **monitor configuration** issues with **DisplayLink-based Dockingstations** with more than one independent monitor output.
- Fixed issue with non-correctly working **default mirror mode**.
- Fixed **screen** configuration issues with **Nvidia and Intel graphics cards in one device**.
- Added: Allowance of **up to 8** different **custom wallpapers** (was limited to 4 up to now).
- Added notification mute-all parameter in Setup to **mute all notifications including urgent ones**.

#### X server

- Fixed tearing issue of **UD7 with additional graphic card**.

#### Window manager

- Fixed **desktop icons not** being **restricted to one monitor**.
- Fixed a bug where **icons** were **missing or miss-aligned** in some multiscreen setups.
- Fixed **notify window width** not remaining constant.
- Fixed **crash of start menu** when it is not populated with any items.
- Fixed **start monitor mapping for Firefox**.
- Fixed **notification urgency for critical background color**.

#### VirtualBox

- Fixed **authentication window popup** if screen configuration is changed in Virtualbox.

#### Audio



- Fixed erroneous **closing of the Pulse PCM device** as well as a possible **deadlock in the ALSA Pulse PCM**.
- Fixed the ALSA Pulse PCM - a possible deadlock while writing audio data and closing Pulse PCM.
- Fixed audio for **HP Elitebook TRRS 840 G7**
- Fixed **internal microphone** in **Elitebook TRRS 840 G7**
- Fixed **headset not** properly **detected** if connected on boot in **UD2-LX50**.
- Fixed microphone issues with **UD3-LX60** device.
- Fixed a **sporadic aborting of an application** on closing **ALSA Pulse PCM**. The problem concerns only applications using ALSA API directly, like Citrix Receiver.
- Added **debug output to the ALSA Pulse PCM** which must be **enabled by** the environment variable `ALSA_PULSE_PCM_DEBUG=1`, the debug output is collected then by the system logging facility (`journald`).
- Fixed **missing audio tray icon** after suspend

#### Evidian

- Fixed **error on restart**.

#### Hardware

- Added script to fix issues with **DP MST KVM** and **connected DaisyChaining monitors**.
- Fixed: When KVM is used, **mishandling of connectors** can occur.  
Added **possible workaround** via adding `/etc/igel/kms/kvm-workaround.sh` to the `userinterface.rccustom.custom_cmd_x11_init` registry key.

#### TC Setup (Java)

- Fixed problems with **passwords** of a length **longer than 127 characters**.

#### Remote Management

- Fixed **automatic establishment of the configured ICG connection** if the UMS Server is unreachable.
- Fixed **sending the user logoff message** to the UMS.
- Fixed: Disabled **Nagle caching algorithm** on the underlying TCP socket used for SSL connection between IGEL rmagent and UMS.
- Fixed **sporadic failures while retrieving the Unit ID** by the IGEL Remote Management agent.
- Fixed **ICG HA functionality** broken in the **11.04.100 release**.

#### VNC

- Fixed handling of **CapsLock status in VNC server**. Keyboard input now appears correctly also when CapsLock is active on the client or server side. This especially fixes upper case "umlaut" characters with Swiss German keyboard layout.

#### CA Certificates Contained in IGEL OS 11.05

IGEL OS 11.05 contains the following CA certificates:

| <b>Certificate name</b> | <b>Expiry date</b>          | <b>File in /etc/ssl/certs</b> |
|-------------------------|-----------------------------|-------------------------------|
| ACCVRAIZ1               | Dec 31 09:37:37 2030<br>GMT | ACCVRAIZ1.crt                 |



| Certificate name                                             | Expiry date                 | File in /etc/ssl/certs                                                |
|--------------------------------------------------------------|-----------------------------|-----------------------------------------------------------------------|
| AC RAIZ FNMT-RCM                                             | Jan 1 00:00:00 2030 GMT     | AC_RAIZ_FNMT-RCM.crt                                                  |
| Actalis Authentication Root CA                               | Sep 22 11:22:02 2030<br>GMT | Actalis_Authentication_Ro<br>ot_CA.crt                                |
| AffirmTrust Commercial                                       | Dec 31 14:06:06 2030<br>GMT | AffirmTrust_Commercial.cr<br>t                                        |
| AffirmTrust Networking                                       | Dec 31 14:08:24 2030<br>GMT | AffirmTrust_Networking.cr<br>t                                        |
| AffirmTrust Premium                                          | Dec 31 14:10:36 2040<br>GMT | AffirmTrust_Premium.crt                                               |
| AffirmTrust Premium ECC                                      | Dec 31 14:20:24 2040<br>GMT | AffirmTrust_Premium_ECC.c<br>rt                                       |
| Amazon Root CA 1                                             | Jan 17 00:00:00 2038<br>GMT | AmazonRootCA1.pem                                                     |
| Amazon Root CA 1                                             | Jan 17 00:00:00 2038<br>GMT | Amazon_Root_CA_1.crt                                                  |
| Amazon Root CA 2                                             | May 26 00:00:00 2040<br>GMT | Amazon_Root_CA_2.crt                                                  |
| Amazon Root CA 3                                             | May 26 00:00:00 2040<br>GMT | Amazon_Root_CA_3.crt                                                  |
| Amazon Root CA 4                                             | May 26 00:00:00 2040<br>GMT | Amazon_Root_CA_4.crt                                                  |
| Atos TrustedRoot 2011                                        | Dec 31 23:59:59 2030<br>GMT | Atos_TrustedRoot_2011.crt                                             |
| Autoridad de Certificacion<br>Firmaprofesional CIF A62634068 | Dec 31 08:38:15 2030<br>GMT | Autoridad_de_Certificacio<br>n_Firmaprofesional_CIF_A6<br>2634068.crt |
| Baltimore CyberTrust Root                                    | May 12 23:59:00 2025<br>GMT | BTCTRoot.pem                                                          |
| Baltimore CyberTrust Root                                    | May 12 23:59:00 2025<br>GMT | Baltimore_CyberTrust_Root<br>.crt                                     |
| Buypass Class 2 Root CA                                      | Oct 26 08:38:03 2040<br>GMT | Buypass_Class_2_Root_CA.c<br>rt                                       |
| Buypass Class 3 Root CA                                      | Oct 26 08:28:58 2040<br>GMT | Buypass_Class_3_Root_CA.c<br>rt                                       |
| CA Disig Root R2                                             | Jul 19 09:15:30 2042 GMT    | CA_Disig_Root_R2.crt                                                  |
| CFCA EV ROOT                                                 | Dec 31 03:07:01 2029<br>GMT | CFCA_EV_ROOT.crt                                                      |
| COMODO Certification Authority                               | Dec 31 23:59:59 2029<br>GMT | COMODO_Certification_Auth<br>ority.crt                                |



| <b>Certificate name</b>                                                                                                      | <b>Expiry date</b>          | <b>File in /etc/ssl/certs</b>          |
|------------------------------------------------------------------------------------------------------------------------------|-----------------------------|----------------------------------------|
| COMODO ECC Certification Authority                                                                                           | Jan 18 23:59:59 2038<br>GMT | COMODO_ECC_Certification_Authority.crt |
| COMODO RSA Certification Authority                                                                                           | Jan 18 23:59:59 2038<br>GMT | COMODO_RSA_Certification_Authority.crt |
| Certigna                                                                                                                     | Jun 29 15:13:05 2027<br>GMT | Certigna.crt                           |
| Certigna Root CA                                                                                                             | Oct 1 08:32:27 2033 GMT     | Certigna_Root_CA.crt                   |
| Certum Trusted Network CA                                                                                                    | Dec 31 12:07:37 2029<br>GMT | Certum_Trusted_Network_CA.crt          |
| Certum Trusted Network CA 2                                                                                                  | Oct 6 08:39:56 2046 GMT     | Certum_Trusted_Network_CA_2.crt        |
| Chambers of Commerce Root - 2008                                                                                             | Jul 31 12:29:50 2038 GMT    | Chambers_of_Commerce_Root_--2008.crt   |
| Class 3 Public Primary Certification Authority - G2 (c) 1998 VeriSign, Inc. - For authorized use only VeriSign Trust Network | Aug 1 23:59:59 2028 GMT     | Class3PCA_G2_v2.pem                    |
| Class 4 Public Primary Certification Authority - G2 (c) 1998 VeriSign, Inc. - For authorized use only VeriSign Trust Network | Aug 1 23:59:59 2028 GMT     | Class4PCA_G2_v2.pem                    |
| AAA Certificate Services                                                                                                     | Dec 31 23:59:59 2028<br>GMT | Comodo AAA Services root.crt           |
| Cybertrust Global Root                                                                                                       | Dec 15 08:00:00 2021<br>GMT | Cybertrust_Global_Root.crt             |
| D-TRUST Root Class 3 CA 2 2009                                                                                               | Nov 5 08:35:58 2029 GMT     | D-TRUST_Root_Class_3_CA_2_2009.crt     |
| D-TRUST Root Class 3 CA 2 EV 2009                                                                                            | Nov 5 08:50:46 2029 GMT     | D-TRUST_Root_Class_3_CA_2_EV_2009.crt  |
| DST Root CA X3                                                                                                               | Sep 30 14:01:15 2021<br>GMT | DST_Root_CA_X3.crt                     |
| DigiCert Global Root CA                                                                                                      | Nov 10 00:00:00 2031<br>GMT | DigiCertGlobalRootCA.pem               |
| DigiCert Global Root CA                                                                                                      | Mar 8 12:00:00 2023 GMT     | DigiCertSHA2SecureServerCA.pem         |
| DigiCert Assured ID Root CA                                                                                                  | Nov 10 00:00:00 2031<br>GMT | DigiCert_Assured_ID_Root_CA.crt        |
| DigiCert Assured ID Root G2                                                                                                  | Jan 15 12:00:00 2038<br>GMT | DigiCert_Assured_ID_Root_G2.crt        |



| Certificate name                                          | Expiry date                 | File in /etc/ssl/certs                         |
|-----------------------------------------------------------|-----------------------------|------------------------------------------------|
| DigiCert Assured ID Root G3                               | Jan 15 12:00:00 2038<br>GMT | DigiCert_Assured_ID_Root_G3.crt                |
| DigiCert Global Root CA                                   | Nov 10 00:00:00 2031<br>GMT | DigiCert_Global_Root_CA.crt                    |
| DigiCert Global Root G2                                   | Jan 15 12:00:00 2038<br>GMT | DigiCert_Global_Root_G2.crt                    |
| DigiCert Global Root G3                                   | Jan 15 12:00:00 2038<br>GMT | DigiCert_Global_Root_G3.crt                    |
| DigiCert High Assurance EV Root CA                        | Nov 10 00:00:00 2031<br>GMT | DigiCert_High_Assurance_EV_Root_CA.crt         |
| DigiCert Trusted Root G4                                  | Jan 15 12:00:00 2038<br>GMT | DigiCert_Trusted_Root_G4.crt                   |
| E-Tugra Certification Authority                           | Mar 3 12:09:48 2023 GMT     | E-Tugra_Certification_Authority.crt            |
| EC-ACC                                                    | Jan 7 22:59:59 2031 GMT     | EC-ACC.crt                                     |
| Entrust.net <sup>391</sup> Certification Authority (2048) | Jul 24 14:15:12 2029 GMT    | Entrust.net_Premium_2048_Secure_Server_CA.crt  |
| Entrust Root Certification Authority                      | Nov 27 20:53:42 2026<br>GMT | Entrust_Root_Certification_Authority.crt       |
| Entrust Root Certification Authority - EC1                | Dec 18 15:55:36 2037<br>GMT | Entrust_Root_Certification_Authority_-_EC1.crt |
| Entrust Root Certification Authority - G2                 | Dec 7 17:55:54 2030 GMT     | Entrust_Root_Certification_Authority_-_G2.crt  |
| Entrust Root Certification Authority - G4                 | Dec 27 11:41:16 2037<br>GMT | Entrust_Root_Certification_Authority_-_G4.crt  |
| GDCA TrustAUTH R5 ROOT                                    | Dec 31 15:59:59 2040<br>GMT | GDCA_TrustAUTH_R5_ROOT.crt                     |
| GlobalSign                                                | Dec 15 08:00:00 2021<br>GMT | GSR2.pem                                       |
| GTE CyberTrust Global Root                                | Aug 13 23:59:00 2018<br>GMT | GTECTGlobalRoot.pem                            |
| GTS Root R1                                               | Jun 22 00:00:00 2036<br>GMT | GTS_Root_R1.crt                                |
| GTS Root R2                                               | Jun 22 00:00:00 2036<br>GMT | GTS_Root_R2.crt                                |
| GTS Root R3                                               | Jun 22 00:00:00 2036<br>GMT | GTS_Root_R3.crt                                |

<sup>391</sup> <http://Entrust.net>



| <b>Certificate name</b>                                     | <b>Expiry date</b>          | <b>File in /etc/ssl/certs</b>                                   |
|-------------------------------------------------------------|-----------------------------|-----------------------------------------------------------------|
| GTS Root R4                                                 | Jun 22 00:00:00 2036<br>GMT | GTS_Root_R4.crt                                                 |
| GeoTrust Global CA                                          | May 21 04:00:00 2022<br>GMT | GeoTrust_Global_CA.pem                                          |
| GeoTrust Primary Certification Authority - G2               | Jan 18 23:59:59 2038<br>GMT | GeoTrust_Primary_Certification_Authority_-_G2.crt               |
| GlobalSign                                                  | Jan 19 03:14:07 2038<br>GMT | GlobalSign_ECC_Root_CA_-_R4.crt                                 |
| GlobalSign                                                  | Jan 19 03:14:07 2038<br>GMT | GlobalSign_ECC_Root_CA_-_R5.crt                                 |
| GlobalSign Root CA                                          | Jan 28 12:00:00 2028<br>GMT | GlobalSign_Root_CA.crt                                          |
| GlobalSign                                                  | Dec 15 08:00:00 2021<br>GMT | GlobalSign_Root_CA_-_R2.crt                                     |
| GlobalSign                                                  | Mar 18 10:00:00 2029<br>GMT | GlobalSign_Root_CA_-_R3.crt                                     |
| GlobalSign                                                  | Dec 10 00:00:00 2034<br>GMT | GlobalSign_Root_CA_-_R6.crt                                     |
| Global Chambersign Root - 2008                              | Jul 31 12:31:40 2038 GMT    | Global_Chambersign_Root_-_2008.crt                              |
| Go Daddy Class 2 Certification Authority                    | Jun 29 17:06:20 2034<br>GMT | Go_Daddy_Class_2_CA.crt                                         |
| Go Daddy Root Certificate Authority - G2                    | Dec 31 23:59:59 2037<br>GMT | Go_Daddy_Root_Certificate_Authority_-_G2.crt                    |
| Hellenic Academic and Research Institutions ECC RootCA 2015 | Jun 30 10:37:12 2040<br>GMT | Hellenic_Academic_and_Research_Institutions_ECC_RootCA_2015.crt |
| Hellenic Academic and Research Institutions RootCA 2011     | Dec 1 13:49:52 2031 GMT     | Hellenic_Academic_and_Research_Institutions_RootCA_2011.crt     |
| Hellenic Academic and Research Institutions RootCA 2015     | Jun 30 10:11:21 2040<br>GMT | Hellenic_Academic_and_Research_Institutions_RootCA_2015.crt     |
| Hongkong Post Root CA 1                                     | May 15 04:52:29 2023<br>GMT | Hongkong_Post_Root_CA_1.crt                                     |
| Hongkong Post Root CA 3                                     | Jun 3 02:29:46 2042 GMT     | Hongkong_Post_Root_CA_3.crt                                     |
| ISRG Root X1                                                | Jun 4 11:04:38 2035 GMT     | ISRG_Root_X1.crt                                                |
| IdenTrust Commercial Root CA 1                              | Jan 16 18:12:23 2034<br>GMT | IdenTrust_Commercial_Root_CA_1.crt                              |



| Certificate name                               | Expiry date                 | File in /etc/ssl/certs                            |
|------------------------------------------------|-----------------------------|---------------------------------------------------|
| IdenTrust Public Sector Root CA 1              | Jan 16 17:53:32 2034<br>GMT | IdenTrust_Public_Sector_Root_CA_1.crt             |
| Imprivata Embedded Code Signing CA             | Sep 7 16:20:00 2033 GMT     | Imprivata.crt                                     |
| Izenpe.com <sup>392</sup>                      | Dec 13 08:27:25 2037<br>GMT | Izenpe.com.crt                                    |
| Microsec e-Szigno Root CA 2009                 | Dec 30 11:30:18 2029<br>GMT | Microsec_e-Szigno_Root_CA_2009.crt                |
| Microsoft ECC Root Certificate Authority 2017  | Jul 18 23:16:04 2042 GMT    | Microsoft_ECC_Root_Certificate_Authority_2017.crt |
| Microsoft RSA Root Certificate Authority 2017  | Jul 18 23:00:23 2042 GMT    | Microsoft_RSA_Root_Certificate_Authority_2017.crt |
| NAVER Global Root Certification Authority      | Aug 18 23:59:59 2037<br>GMT | NAVER_Global_Root_Certification_Authority.crt     |
| NetLock Arany (Class Gold)<br>Főtanúsítvány    | Dec 6 15:08:21 2028 GMT     | NetLock_Arany_=Class_Gold=_Főtanúsítvány.crt      |
| Network Solutions Certificate Authority        | Dec 31 23:59:59 2029<br>GMT | Network_Solutions_Certificate_Authority.crt       |
| OISTE WISeKey Global Root GB CA                | Dec 1 15:10:31 2039 GMT     | OISTE_WISeKey_Global_Root_GB_CA.crt               |
| OISTE WISeKey Global Root GC CA                | May 9 09:58:33 2042 GMT     | OISTE_WISeKey_Global_Root_GC_CA.crt               |
| Class 3 Public Primary Certification Authority | Aug 1 23:59:59 2028 GMT     | Pcs3ss_v4.pem                                     |
| QuoVadis Root Certification Authority          | Mar 17 18:33:33 2021<br>GMT | QuoVadis_Root_CA.crt                              |
| QuoVadis Root CA 1 G3                          | Jan 12 17:27:44 2042<br>GMT | QuoVadis_Root_CA_1_G3.crt                         |
| QuoVadis Root CA 2                             | Nov 24 18:23:33 2031<br>GMT | QuoVadis_Root_CA_2.crt                            |
| QuoVadis Root CA 2 G3                          | Jan 12 18:59:32 2042<br>GMT | QuoVadis_Root_CA_2_G3.crt                         |
| QuoVadis Root CA 3                             | Nov 24 19:06:44 2031<br>GMT | QuoVadis_Root_CA_3.crt                            |
| QuoVadis Root CA 3 G3                          | Jan 12 20:26:32 2042<br>GMT | QuoVadis_Root_CA_3_G3.crt                         |

<sup>392</sup> <http://Izenpe.com>



| Certificate name                                              | Expiry date                 | File in /etc/ssl/certs                               |
|---------------------------------------------------------------|-----------------------------|------------------------------------------------------|
| SSL.com <sup>393</sup> EV Root Certification Authority ECC    | Feb 12 18:15:23 2041<br>GMT | SSL.com_EV_Root_Certification_Authority_ECC.crt      |
| SSL.com <sup>394</sup> EV Root Certification Authority RSA R2 | May 30 18:14:37 2042<br>GMT | SSL.com_EV_Root_Certification_Authority_RSA_R2.crt   |
| SSL.com <sup>395</sup> Root Certification Authority ECC       | Feb 12 18:14:03 2041<br>GMT | SSL.com_Root_Certification_Authority_ECC.crt         |
| SSL.com <sup>396</sup> Root Certification Authority RSA       | Feb 12 17:39:39 2041<br>GMT | SSL.com_Root_Certification_Authority_RSA.crt         |
| SZAFIR ROOT CA2                                               | Oct 19 07:43:30 2035<br>GMT | SZAFIR_ROOT_CA2.crt                                  |
| SecureSign RootCA11                                           | Apr 8 04:56:47 2029 GMT     | SecureSign_RootCA11.crt                              |
| SecureTrust CA                                                | Dec 31 19:40:55 2029<br>GMT | SecureTrust_CA.crt                                   |
| Secure Global CA                                              | Dec 31 19:52:06 2029<br>GMT | Secure_Global_CA.crt                                 |
| Security Communication RootCA2                                | May 29 05:00:39 2029<br>GMT | Security_Communication_RootCA2.crt                   |
| Security Communication RootCA1                                | Sep 30 04:20:49 2023<br>GMT | Security_Communication_Root_CA1.crt                  |
| Sonera Class2 CA                                              | Apr 6 07:29:40 2021 GMT     | Sonera_Class_2_Root_CA.crt                           |
| Staat der Nederlanden EV Root CA                              | Dec 8 11:10:28 2022 GMT     | Staat_der_Nederlanden_EV_Root_CA.crt                 |
| Staat der Nederlanden Root CA - G3                            | Nov 13 23:00:00 2028<br>GMT | Staat_der_Nederlanden_Root_CA_G3.crt                 |
| Starfield Class 2 Certification Authority                     | Jun 29 17:39:16 2034<br>GMT | Starfield_Class_2_CA.crt                             |
| Starfield Root Certificate Authority - G2                     | Dec 31 23:59:59 2037<br>GMT | Starfield_Root_Certificate_Authority_G2.crt          |
| Starfield Services Root Certificate Authority - G2            | Dec 31 23:59:59 2037<br>GMT | Starfield_Services_Root_Certificate_Authority_G2.crt |
| SwissSign Gold CA - G2                                        | Oct 25 08:30:35 2036<br>GMT | SwissSign_Gold_CA_G2.crt                             |
| SwissSign Silver CA - G2                                      | Oct 25 08:32:46 2036<br>GMT | SwissSign_Silver_CA_G2.crt                           |

<sup>393</sup> <http://SSL.com><sup>394</sup> <http://SSL.com><sup>395</sup> <http://SSL.com><sup>396</sup> <http://SSL.com>



| Certificate name                                  | Expiry date              | File in /etc/ssl/certs                                |
|---------------------------------------------------|--------------------------|-------------------------------------------------------|
| T-TeleSec GlobalRoot Class 2                      | Oct 1 23:59:59 2033 GMT  | T-<br>TeleSec_GlobalRoot_Class_2.crt                  |
| T-TeleSec GlobalRoot Class 3                      | Oct 1 23:59:59 2033 GMT  | T-<br>TeleSec_GlobalRoot_Class_3.crt                  |
| TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1     | Oct 25 08:25:55 2043 GMT | TUBITAK_Kamu_SM_SSL_Kok_Sertifikasi_-_Surum_1.crt     |
| TWCA Global Root CA                               | Dec 31 15:59:59 2030 GMT | TWCA_Global_Root_CA.crt                               |
| TWCA Root Certification Authority                 | Dec 31 15:59:59 2030 GMT | TWCA_Root_Certification_Authority.crt                 |
| TeliaSonera Root CA v1                            | Oct 18 12:00:50 2032 GMT | TeliaSonera_Root_CA_v1.crt                            |
| TrustCor ECA-1                                    | Dec 31 17:28:07 2029 GMT | TrustCor_ECA-1.crt                                    |
| TrustCor RootCert CA-1                            | Dec 31 17:23:16 2029 GMT | TrustCor_RootCert_CA-1.crt                            |
| TrustCor RootCert CA-2                            | Dec 31 17:26:39 2034 GMT | TrustCor_RootCert_CA-2.crt                            |
| Trustis FPS Root CA                               | Jan 21 11:36:54 2024 GMT | Trustis_FPS_Root_CA.crt                               |
| Trustwave Global Certification Authority          | Aug 23 19:34:12 2042 GMT | Trustwave_Global_Certification_Authority.crt          |
| Trustwave Global ECC P256 Certification Authority | Aug 23 19:35:10 2042 GMT | Trustwave_Global_ECC_P256_Certification_Authority.crt |
| Trustwave Global ECC P384 Certification Authority | Aug 23 19:36:43 2042 GMT | Trustwave_Global_ECC_P384_Certification_Authority.crt |
| UCA Extended Validation Root                      | Dec 31 00:00:00 2038 GMT | UCA_Extended_Validation_Root.crt                      |
| UCA Global G2 Root                                | Dec 31 00:00:00 2040 GMT | UCA_Global_G2_Root.crt                                |
| USERTrust ECC Certification Authority             | Jan 18 23:59:59 2038 GMT | USERTrust_ECC_Certification_Authority.crt             |
| USERTrust RSA Certification Authority             | Jan 18 23:59:59 2038 GMT | USERTrust_RSA_Certification_Authority.crt             |
| VeriSign Universal Root Certification Authority   | Dec 1 23:59:59 2037 GMT  | VeriSign_Universal_Root_Certification_Authority.crt   |



| <b>Certificate name</b>              | <b>Expiry date</b>          | <b>File in /etc/ssl/certs</b>         |
|--------------------------------------|-----------------------------|---------------------------------------|
| XRamp Global Certification Authority | Jan 1 05:37:19 2035 GMT     | XRamp_Global_CA_Root.crt              |
| certSIGN ROOT CA                     | Jul 4 17:20:04 2031 GMT     | certSIGN_ROOT_CA.crt                  |
| certSIGN ROOT CA G2                  | Feb 6 09:27:35 2042 GMT     | certSIGN_Root_CA_G2.crt               |
| e-Szigno Root CA 2017                | Aug 22 12:07:06 2042<br>GMT | e-Szigno_Root_CA_2017.crt             |
| ePKI Root Certification Authority    | Dec 20 02:31:27 2034<br>GMT | ePKI_Root_Certification_Authority.crt |
| emSign ECC Root CA - C3              | Feb 18 18:30:00 2043<br>GMT | emSign_ECC_Root_CA_-C3.crt            |
| emSign ECC Root CA - G3              | Feb 18 18:30:00 2043<br>GMT | emSign_ECC_Root_CA_-G3.crt            |
| emSign Root CA - C1                  | Feb 18 18:30:00 2043<br>GMT | emSign_Root_CA_-C1.crt                |
| emSign Root CA - G1                  | Feb 18 18:30:00 2043<br>GMT | emSign_Root_CA_-G1.crt                |

#### 7.4.2 IGEL OS Creator (OSC)

##### Supported Devices

|         |                                             |
|---------|---------------------------------------------|
| UD2-LX: | UD2-LX 51<br><br>UD2-LX 50<br><br>UD2-LX 40 |
| UD3-LX: | UD3-LX 60<br><br>UD3-LX 51<br><br>UD3-LX 50 |
| UD5-LX: | UD5-LX 50                                   |
| UD6-LX: | UD6-LX 51                                   |



|         |                                     |
|---------|-------------------------------------|
| UD7-LX: | UD7-LX 20<br>UD7-LX 11<br>UD7-LX 10 |
| UD9-LX: | UD9-LX Touch 41<br>UD9-LX 40        |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>397</sup>.

- [Component Versions 11.05.100](#)(see page 1555)
- [New Features 11.05.100](#)(see page 1557)
- [Resolved Issues 11.05.100](#)(see page 1557)

## Component Versions 11.05.100

### Clients

| Product  | Version     |
|----------|-------------|
| Zulu JRE | 8.48.0.51-2 |

### System Components

|                                         |                               |
|-----------------------------------------|-------------------------------|
| OpenSSL                                 | 1.0.2n-1ubuntu5.5             |
| OpenSSL                                 | 1.1.1-1ubuntu2.1~18.04.7      |
| Bluetooth stack (bluez)                 | 5.55-0ubuntu1.1igel10         |
| MESA OpenGL stack                       | 20.2.6-1igel131               |
| VDPAU Library version                   | 1.4-3igel1099                 |
| Graphics Driver INTEL                   | 2.99.917+git20200515-igel1013 |
| Graphics Driver ATI/Radeon              | 19.1.0-2igel1066              |
| Graphics Driver ATI/AMDGPU              | 19.1.0-2+git20200828igel1064  |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867               |
| Graphics Driver Nvidia                  | 450.102.04-0ubuntu0.20.04.1   |

<sup>397</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



|                                 |                                   |
|---------------------------------|-----------------------------------|
| Graphics Driver VMware          | 13.3.0-2igel857                   |
| Graphics Driver QXL (Spice)     | 0.1.5-2build2-igel925             |
| Graphics Driver FBDEV           | 0.5.0-1igel1012                   |
| Graphics Driver VESA            | 2.4.0-1igel1010                   |
| Input Driver Evdev              | 2.10.6-2igel1037                  |
| Input Driver Elographics        | 1.4.1-1+b6igel952                 |
| Input Driver Synaptics          | 1.9.1-1ubuntu1igel1009            |
| Input Driver VMMouse            | 13.1.0-1ubuntu2igel957            |
| Input Driver Wacom              | 0.39.0-0ubuntu1igel1036           |
| Kernel                          | 5.9.16 #mainline-lxos-g1613995475 |
| Xorg X11 Server                 | 1.20.10-2igel1100                 |
| Lightdm Graphical Login Manager | 1.26.0-0ubuntu1igel13             |
| XFCE4 Window Manager            | 4.14.2-1~18.04igel1600339249      |
| ISC DHCP Client                 | 4.3.5-3ubuntu7.1                  |
| Python3                         | 3.6.9                             |

## VM Guest Support Components

|                            |                         |
|----------------------------|-------------------------|
| Virtualbox Guest Utils     | 6.1.18-dfsg-1igel49     |
| Virtualbox X11 Guest Utils | 6.1.18-dfsg-1igel49     |
| Open VM Tools              | 11.0.5-4ubuntu0.18.04.1 |
| Open VM Desktop Tools      | 11.0.5-4ubuntu0.18.04.1 |
| Xen Guest Utilities        | 7.10.0-0ubuntu1         |
| Spice Vdagent              | 0.20.0-2igel104         |
| Qemu Guest Agent           | 5.2+dfsg-3igel17        |

## Services

| Service                     | Size    | Reduced Firmware |
|-----------------------------|---------|------------------|
| Java SE Runtime Environment | 36.0 M  | Included         |
| NVIDIA graphics driver      | 122.5 M | Included         |



## New Features 11.05.100

### Base system

- Updated **Linux kernel** to version **5.9.16**.

### Hardware

- Added hardware support for new **IGEL UD7-LX 20 (H860C)**.
- Added hardware support for **LG 34CN650N AiO**.
- Added hardware support for **Dell Wyse Z Class thin client**.
- Added hardware support for **Lenovo ThinkCentre M70q**.
- Added hardware support for **Dell Wyse 5470**.
- Added hardware support for **Lenovo L14**.
- Added hardware support for **Lenovo ThinkCentre M75n**.
- Added hardware support for **Lenovo 14w**.
- Added hardware support for **LG CN65 All in one**.
- Added hardware support for **DELL LATITUDE 5510**.
- Added hardware support for **ELO i2 Touch all-in-one (15 and 22) inch**.
- Added detection of **UD Pocket UC5-LX 2**.

## Resolved Issues 11.05.100

### OSC Installer

- Fixed **warning message after feature deselection for installations on 2 GB flashes**.
- Fixed a **display issue with Intel and Nvidia GPU**.

## 7.5 Notes for Release 11.04.270

|                       |            |              |
|-----------------------|------------|--------------|
| <b>Software:</b>      | Version    | 11.04.270    |
| <b>Release Date:</b>  | 2021-02-11 |              |
| <b>Release Notes:</b> | Version    | RN-1104270-1 |
| <b>Last update:</b>   | 2021-02-10 |              |

- 
- Supported Devices 11.04.270(see page 1558)
  - Component Versions 11.04.270(see page 1558)
  - General Information 11.04.270(see page 1565)
  - Known Issues 11.04.270(see page 1565)
  - Security Fixes 11.04.270(see page 1569)
  - New Features 11.04.270(see page 1569)
  - Resolved Issues 11.04.270(see page 1570)



### 7.5.1 Supported Devices 11.04.270

|         |                                     |
|---------|-------------------------------------|
| UD2-LX: | UD2-LX 51<br>UD2-LX 50<br>UD2-LX 40 |
| UD3-LX: | UD3-LX 60<br>UD3-LX 51<br>UD3-LX 50 |
| UD5-LX: | UD5-LX 50                           |
| UD6-LX: | UD6-LX 51                           |
| UD7-LX: | UD7-LX 11<br>UD7-LX 10              |
| UD9-LX: | UD9-LX Touch 41<br>UD9-LX 40        |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>398</sup>.

### 7.5.2 Component Versions 11.04.270

#### Clients

| Product                         | Version                       |
|---------------------------------|-------------------------------|
| Chromium                        | 83.0.4103.61-0ubuntu0.18.04.1 |
| Cisco JVDI Client               | 12.9.3                        |
| Cisco Webex Teams VDI Client    | 41.1.0.17621                  |
| Cisco Webex Meetings VDI Client | 41.2.0.142                    |
| Zoom Media Plugin               | 5.4.53376                     |

<sup>398</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



|                                        |                                           |
|----------------------------------------|-------------------------------------------|
| Citrix HDX Realtime Media Engine       | 2.9.0-2330                                |
| Citrix Workspace App                   | 19.12.0.19                                |
| Citrix Workspace App                   | 20.10.0.6                                 |
| Citrix Workspace App                   | 20.12.0.12                                |
| deviceTRUST Citrix Channel             | 20.1.200.0                                |
| Crossmatch DP Citrix Channel           | 0515.2                                    |
| Ericom PowerTerm                       | 12.0.1.0.20170219.2-_dev_-34574           |
| Ericom PowerTerm                       | 14.0.0.45623                              |
| Evidian AuthMgr                        | 1.5.7617                                  |
| Evince PDF Viewer                      | 3.28.4-0ubuntu1.2                         |
| FabulaTech USB for Remote Desktop      | 6.0.28                                    |
| Firefox                                | 68.12.0                                   |
| IBM iAccess Client Solutions           | 1.1.8.1                                   |
| IGEL RDP Client                        | 2.2igel1600249269                         |
| IGEL WVD Client                        | 1.0.21igel1608136172                      |
| Imprivata OneSign ProveID Embedded     | onesign-bootstrap-loader_1.0.523630_amd64 |
| deviceTRUST RDP Channel                | 20.1.200.0                                |
| NCP Secure Enterprise Client           | 5.10_rev40552                             |
| NX Client                              | 6.11.2-1igel8                             |
| Open VPN                               | 2.4.4-2ubuntu1.3                          |
| Zulu JRE                               | 8.48.0.51-2                               |
| Parallels Client (64 bit)              | 17.1.2.1                                  |
| Spice GTK (Red Hat Virtualization)     | 0.38-2igel93                              |
| Remote Viewer (Red Hat Virtualization) | 8.0-2git20191213.e4bach8igel83            |
| Usbredir (Red Hat Virtualization)      | 0.8.0-1+b1igel71                          |
| Teradici PCoIP Software Client         | 20.10.0-18.04                             |
| ThinLinc Client                        | 4.12.0-6517                               |



|                       |                       |
|-----------------------|-----------------------|
| ThinPrint Client      | 7.5.88                |
| Totem Media Player    | 2.30.2-0ubuntu1igel55 |
| Parole Media Player   | 1.0.5-1igel1583919770 |
| VNC Viewer            | 1.10.1+dfsg-4igel13   |
| VMware Horizon Client | 5.5.0-16946361        |
| Voip Client Ekiga     | 4.0.1-9build1igel6    |

## Dictation

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20200323 |
| Philips Speech driver                     | 12.9.1   |

## Signature

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.9    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.4.2    |

## Smartcard

|                                           |                 |
|-------------------------------------------|-----------------|
| PKCS#11 Library A.E.T SafeSign            | 3.6.0.0-AET.000 |
| PKCS#11 Library Athena IDProtect          | 7               |
| PKCS#11 Library cryptovision sc/interface | 7.3.1           |
| PKCS#11 Library Gemalto SafeNet           | 10.7.77         |
| PKCS#11 Library OpenSC                    | 0.20.0-3igel37  |
| PKCS#11 Library SecMaker NetID            | 6.8.1.31        |



|                                    |                        |
|------------------------------------|------------------------|
| PKCS#11 Library 90meter            | 20190522               |
| Reader Driver ACS CCID             | 1.1.6-1igel2           |
| Reader Driver Gemalto eToken       | 10.7.77                |
| Reader Driver HID Global Omnikey   | 4.3.3                  |
| Reader Driver Identive CCID        | 5.0.35                 |
| Reader Driver Identive eHealth200  | 1.0.5                  |
| Reader Driver Identive SCRKBC      | 5.0.24                 |
| Reader Driver MUSCLE CCID          | 1.4.31-1igel11         |
| Reader Driver REINER SCT cyberJack | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite        | 1.8.26-3igel14         |
| Cherry USB2LAN Proxy               | 3.2.0.3                |

## System Components

|                                         |                               |
|-----------------------------------------|-------------------------------|
| OpenSSL                                 | 1.0.2n-1ubuntu5.3             |
| OpenSSL                                 | 1.1.1-1ubuntu2.1~18.04.6      |
| OpenSSH Client                          | 7.6p1-4ubuntu0.3              |
| OpenSSH Server                          | 7.6p1-4ubuntu0.3              |
| Bluetooth stack (bluez)                 | 5.52-1igel6                   |
| MESA OpenGL stack                       | 20.0.8-1igel117               |
| VAAPI ABI Version                       | 0.40                          |
| VDPAU Library version                   | 1.4-1igel1003                 |
| Graphics Driver INTEL                   | 2.99.917+git20200515-igel1013 |
| Graphics Driver ATI/RADEON              | 19.1.0-1+git20200220igel987   |
| Graphics Driver ATI/AMDGPU              | 19.1.0-1+git20200318igel986   |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867               |



|                                 |                                   |
|---------------------------------|-----------------------------------|
| Graphics Driver Nvidia          | 440.100-0ubuntu0.20.04.1          |
| Graphics Driver VMware          | 13.3.0-2igel857                   |
| Graphics Driver QXL (Spice)     | 0.1.5-2build2-igel925             |
| Graphics Driver FBDEV           | 0.5.0-1igel819                    |
| Graphics Driver VESA            | 2.4.0-1igel855                    |
| Input Driver Evdev              | 2.10.6-1igel975                   |
| Input Driver Elographics        | 1.4.1-1+b6igel952                 |
| Input Driver eGalax             | 2.5.8825                          |
| Input Driver Synaptics          | 1.9.1-1ubuntu1igel866             |
| Input Driver VMMouse            | 13.1.0-1ubuntu2igel957            |
| Input Driver Wacom              | 0.36.1-0ubuntu2igel888            |
| Input Driver ELO Multitouch     | 3.0.0                             |
| Input Driver ELO Singletouch    | 5.1.0                             |
| Kernel                          | 5.4.48 #mainline-lxos-g1607354578 |
| Xorg X11 Server                 | 1.20.8-2igel1016                  |
| Xorg Xephyr                     | 1.20.8-2igel1016                  |
| CUPS printing daemon            | 2.2.7-1ubuntu2.8igel32            |
| PrinterLogic                    | 25.1.0.425                        |
| Lightdm Graphical Login Manager | 1.26.0-0ubuntu1igel13             |
| XFCE4 Window Manager            | 4.14.2-1~18.04igel1600339249      |
| ISC DHCP Client                 | 4.3.5-3ubuntu7.1                  |
| NetworkManager                  | 1.20.4-2ubuntu2.2igel105          |
| ModemManager                    | 1.10.0-1~ubuntu18.04.2            |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.1igel201         |
| GStreamer 0.10 Fluendo aacdec   | 0.10.42                           |
| GStreamer 0.10 Fluendo asfdemux | 0.10.90                           |
| GStreamer 0.10 Fluendo h264dec  | 0.10.58                           |



|                                      |                 |
|--------------------------------------|-----------------|
| GStreamer 0.10 Fluendo mp3dec        | 0.10.40         |
| GStreamer 0.10 Fluendo mpegdemux     | 0.10.85         |
| GStreamer 0.10 Fluendo mpeg4videodec | 0.10.44         |
| GStreamer 0.10 Fluendo vadec         | 0.10.224        |
| GStreamer 0.10 Fluendo wmadec        | 0.10.70         |
| GStreamer 0.10 Fluendo wmvdec        | 0.10.66         |
| GStreamer 1.x                        | 1.16.2-4igel239 |
| GStreamer 1.0 Fluendo aacdec         | 0.10.42.2-8d6d  |
| GStreamer 1.0 Fluendo asfdemux       | 0.10.90         |
| GStreamer 1.0 Fluendo h264dec        | 0.10.58         |
| GStreamer 1.0 Fluendo mp3dec         | 0.10.40         |
| GStreamer 1.0 Fluendo mpeg4videodec  | 0.10.44         |
| GStreamer 1.0 Fluendo vadec          | 0.10.224        |
| GStreamer 1.0 Fluendo wmadec         | 0.10.70         |
| GStreamer 1.0 Fluendo wmvdec         | 0.10.66         |
| WebKit2Gtk                           | 2.28.3-2igel36  |
| Python2                              | 2.7.17          |
| Python3                              | 3.6.9           |

## VM Guest Support Components

|                            |                         |
|----------------------------|-------------------------|
| Virtualbox Guest Utils     | 6.1.10-dfsg-1igel41     |
| Virtualbox X11 Guest Utils | 6.1.10-dfsg-1igel41     |
| Open VM Tools              | 11.0.5-4ubuntu0.18.04.1 |
| Open VM Desktop Tools      | 11.0.5-4ubuntu0.18.04.1 |
| Xen Guest Utilities        | 7.10.0-0ubuntu1         |
| Spice Vdagent              | 0.20.0-1igel95          |
| Qemu Guest Agent           | 5.0-5igel12             |

## Features with Limited IGEL Support

|                                    |                                     |
|------------------------------------|-------------------------------------|
| Mobile Device Access USB (MTP)     | 1.1.17-3igel5                       |
| Mobile Device Access USB (imobile) | 1.2.1~git20191129.9f79242-1+b1igel8 |
| Mobile Device Access USB (gphoto)  | 2.5.25-2igel4                       |
| VPN OpenConnect                    | 8.10-1igel4                         |
| Scanner support                    | 1.0.27-1                            |
| VirtualBox                         | 6.1.10-dfsg-1igel41                 |



## Services

| <b>Service</b>                             | <b>Size</b> | <b>Reduced Firmware</b> |
|--------------------------------------------|-------------|-------------------------|
| Asian Language Support                     | 22.5 M      | Included                |
| Java SE Runtime Environment                | 36.0 M      | Included                |
| Citrix Appliance                           | 235.5 M     | Included                |
| Citrix Workspace app                       |             |                         |
| Citrix StoreFront                          |             |                         |
| Ericom PowerTerm InterConnect              | 15.5 M      | Included                |
| Media Player                               | 512.0 K     | Included                |
| Local Browser (Firefox)                    | 70.5 M      | Included                |
| Citrix Appliance                           |             |                         |
| VMware Horizon                             | 4.2. M      | Included                |
| RDP                                        |             |                         |
| Cendio ThinLinc                            | 10.0 M      | Included                |
| Printing (Internet printing protocol CUPS) | 22.2 M      | Included                |
| NoMachine NX                               | 26.8 M      | Included                |
| VMware Horizon                             | 123.2 M     | Included                |
| Voice over IP (Ekiga)                      | 6.5 M       | Included                |
| Citrix Appliance                           | 768.0 K     | Included                |
| NCP Enterprise VPN Client                  | 27.0 M      | Not included            |
| Fluendo GStreamer Codec Plugins            | 7.5 M       | Included                |
| IBM i Access Client Solutions              | 72.5 M      | Not included            |
| Red Hat Enterprise Virtualization          | 3.0 M       | Included                |
| Parallels Client                           | 5.5 M       | Included                |
| NVIDIA graphics driver                     | 115.0 M     | Not included            |
| Imprivata Appliance                        | 10.8 M      | Included                |
| Evidian AuthMgr                            | 2.5 M       | Included                |
| Hardware Video Acceleration                | 13.0 M      | Included                |
| Extra Font Package                         | 1.0 M       | Included                |
| Fluendo GStreamer AAC Decoder              | 1.2 M       | Included                |
| x32 Compatibility Support                  | 48.0 M      | Included                |
| Cisco JVDI client                          | 45.8 M      | Included                |
| PrinterLogic                               | 40.8 M      | Not included            |
| Biosec BS Login                            | 10.0 M      | Not included            |
| Login VSI Login Enterprise                 | 28.8 M      | Not included            |
| Stratusphere UX CID Key software           | 2.8 M       | Not included            |
| Elastic Filebeat                           | 15.8 M      | Not included            |



|                                            |         |              |
|--------------------------------------------|---------|--------------|
| WVD                                        | 14.0 M  | Included     |
| Local Browser (Chromium)                   | 81.2 M  | Not included |
| deskMate client                            | 5.8 M   | Included     |
| Cisco Webex Teams VDI                      | 36.8 M  | Not included |
| Cisco Webex Meetings VDI                   | 32.2 M  | Not included |
| Zoom Media Plugin                          | 40.5 M  | Not included |
| Teradici PCoIP Client                      | 14.5 M  | Included     |
| 90meter Smart Card Support                 | 256.0 K | Included     |
| Mobile Device Access USB (Limited support) | 256.0 K | Not included |
| VPN OpenConnect (Limited support)          | 1.5 M   | Not included |
| Scanner support / SANE (Limited support)   | 2.5 M   | Not included |
| VirtualBox (Limited support)               | 62.5 M  | Not included |

### 7.5.3 General Information 11.04.270

To be beneficial to all new features and implementations, it is recommended to use UMS 6.06.100 or higher and update the corresponding profiles.

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

### 7.5.4 Known Issues 11.04.270

Firmware Update



- On **devices with 2 GB of flash storage**, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Check [Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher<sup>399</sup>](#) for a solution.

## Firefox

- Firefox IGEL extensions are not updated automatically** under some circumstances. After an update from 11.03.xxx to 11.04.100, the IGEL extensions will stay on the old version. In this case, the following settings concerning **kiosk mode** cannot be executed:
  - Switch off hotkey for new window/tab
  - Blocking of internal browser pages like preferences, file picker, specific local directories

As a workaround:

- a **reset to defaults** should be performed
- or the **browser's mimetype template** can be switched **from "Standard" to "Minimal"** by registry key `browserglobal.app.mimetypes_template`. There, the browser profile is renewed as well.

After the TC received the new setting, **reboot** and **set** the `mimetypes_template` registry key to **"Standard"** again.

## Citrix

- With activated **DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1 and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
- Citrix StoreFront login** with **Gemalto smartcard** middleware does not detect smartcard correctly if the card is inserted after start of login.  
Workaround: Insert the smartcard before starting the StoreFront login.
- Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264** acceleration plugin, the following registry key must be enabled.

[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | <code>ica.workaround-dual-rtme</code>                            |
| Value     | <u>enabled</u> / <u>disabled</u>                                 |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

- During the running **Microsoft Teams Optimization of Citrix Workspace App 20.09, webcam redirection or screen sharing** may lead to **display errors** like black stripes or flickering.

<sup>399</sup> <https://kb.igel.com/display/igelos1104/Updating+to+IGEL+OS+11.04+or+Higher+on+a+Device+with+Small+Storage>



## VMware Horizon

- **Client drive mapping** and **USB redirection** for storage devices should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Enable local `Storage Hotplug` on Setup page **Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection do not appear in the **remote desktop**.  
Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- **After the disconnect of an RDP-based session**, the Horizon main **window** which contains the server or sessions overview **cannot be resized anymore**.
- **Seamless application windows in Horizon Client may not be displayed correctly**. When starting the first seamless app, a new iconified window appears in the taskbar, and only if you click on it, the application will show up.  
On some hardware (UD7-H850, UD2-M250, UD2-D220), however, the client aborts when this new window is de-iconified.
- When using the **RDP protocol**, the remote session has a fixed offset of approximately the height of the menu bar. That means you have a black bar on top of the window and as a result of that, the **Windows panel on the bottom is cut off**.
- **Modifier keys** (Shift/Ctrl/Win/Alt) in session windows using **RDP protocol** do not send the keyup event and **keep being pressed**, even when actually released. Only when closing the session with a mouse, the modifiers are reset.
- **Copying a text from Horizon Blast sessions** is not possible.
- The **on-screen keyboard** in **Horizon appliance mode** does not work correctly with local logon.  
Workaround: **Switch off local logon** and switch on the corresponding two keys via IGEL registry:
  - userinterface.softkeyboard.autoshow
  - userinterface.softkeyboard.autohide

## Wi-Fi

- TP-Link Archer T2UH Wi-Fi adapters does not work after system suspend/resume. Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

## Parallels Client

- **Native USB redirection** does not work with Parallels Client.

## Smartcard

- **Citrix Certificate Identity Declaration login** does not work with **SecMaker** smartcards.

## Cisco JVDI Client



- There may be a **segfault shown in the logs** (during logout of Citrix Desktop session). This occurs only when using **Citrix Workspace app 20.10 and Cisco JVDI**.

#### Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.

#### Hyper-V

- **Hyper-V** (Generation 2) needs **a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.

#### VirtualBox

- The current **VirtualBox Guest Tools/Drivers** will not work with **VirtualBox 5.2.x or older** hosts which leads to a black screen and non-working graphics.  
**Possible workaround:** Install with 'Failsafe Installation + Recovery' and set the registry key `x.drivers.force_vesa` to 'true'.
- When running in VirtualBox virtualization, **resizing the window will not automatically change desktop resolution** of IGEL OS guest.

#### Audio

- **Audio jack detection on Advantech POC-W243L** doesn't work. Therefore, sound output goes through a possibly connected headset and the internal speakers.
- **IGEL UD2 (D220)** fails to restore the volume level of the speaker when the device used **firmware version 11.01.110** before.

#### Hardware

- **HP t730** could freeze when monitors with **different resolutions** are connected (1920x1200 + 2560x1440 + 3840x1600 for example). When this occurs, the registry key `x.drivers.kms.best_console_mode` has to be set to **disabled**.
- Some newer **Delock 62599 active DisplayPort-to-DVI (4k)** adapters only work with INTEL devices.

#### Remote Management

- **AIT feature with IGEL Starter License** is only **supported** by **UMS version 6.05.100 or newer**.

#### Base system

- **Update from memory stick** requires network online state (at least when multiple update stages are involved).

#### deskMate

- Some stability issues may remain.

#### Appliance Mode

- When **ending a Citrix session** in browser appliance mode, the **browser is restarted twice** instead of once.
- Appliance mode **RHEV/Spice: spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.



## 7.5.5 Security Fixes 11.04.270

### VNC

- Fixed **Secure Terminal** and **Secure VNC Shadowing** remote code execution vulnerability.

## 7.5.6 New Features 11.04.270

### Citrix

- Integrated **Zoom Media Plugin 5.4.53376.1029**
- Integrated **Citrix Workspace App 20.12**  
Available Citrix Workspace apps in this release: **20.12** (default), **20.10**, and 19.12.
- New Feature: **App Protection [Experimental]**. App Protection is an add-on feature that provides **enhanced security when using Citrix Virtual Apps and Desktops**. The feature **restricts the ability of clients to be compromised by keylogging and screen capturing malware**.

[More...](#)

|           |                                                                                                     |
|-----------|-----------------------------------------------------------------------------------------------------|
| Parameter | Citrix App Protection                                                                               |
| Registry  | ica.appprotection                                                                                   |
| Value     | enabled / <u>disabled</u>                                                                           |
| Note:     | Experimental feature<br>This feature is <b>currently only available for Self-Service sessions</b> . |

- Fixed Issue: **mic** and **webcam** devices can be **redirected using Browser Content Redirection**.

[More...](#)

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Enables mic and webcam redirection using BCR |
| Registry  | ica.allregions.cefenablemediadevices         |
| Value     | [Factory default is "*"] [False][True]       |

### VMware Horizon

- Integrated **Zoom Media Plugin 5.4.53376.1029**
- Updated VMware Horizon Client to version **5.5.0-16946361**

### Smartcard

- Added **Smartcard PIN passthrough in Firefox and Chromium**. The PIN will be **cached while logging on via Active Directory/Kerberos** with a smartcard. In Firefox and Chromium, no further PIN input is necessary to use the smartcard.

[More...](#)

|           |                               |
|-----------|-------------------------------|
| Parameter | Smartcard PIN caching         |
| Registry  | scard.pkcs11.pin_cache.enable |
| Value     | enabled / <u>disabled</u>     |

### Cisco JVDI Client

- Integrated **Cisco JVDI 12.9.3** client



## Cisco Webex

- Integrated **Cisco Webex Meetings 41.2.0.142**
- Integrated **Cisco Webex Teams 41.1.0.17621**

## Evidian

- New session type **RD Web Access**.
- Updated Evidian to version **1.5.7617**.

## Audio

- Added parameter to **control applying of sound volume to application's streams**. If the parameter is set to "true", each application can set its own volume level. Otherwise, the sound volume is set to the same value as the default volume for output and input device respectively.

**More...**

|          |                                               |
|----------|-----------------------------------------------|
| Registry | <code>userinterface.sound.app_volume_c</code> |
|          | <code>trl</code>                              |
| Value    | <u>enabled</u> / disabled                     |

## 7.5.7 Resolved Issues 11.04.270

## Citrix

- Fixed Citrix **Kerberos Passthrough authentication**.
- The parameter `ica.module.virtualdrivers.vdwebrtc.keyboard_workaround` has been **removed**. This workaround is **no longer needed** because **the problem is solved as of CWA 20.10**.

## VMware Horizon

- Fixed failure to start Horizon **serial port redirection service at boot time**.
- Fixed **remember last user functionality in Horizon local logon**.
- Fixed **VMware integrated printing**.

## RDP/IGEL RDP Client 2

- Added **new parameter** to enable/disable **dynamic drive mapping**.

**More...**

|          |                                                                      |
|----------|----------------------------------------------------------------------|
| Registry | <code>rdp.winconnect.enable-dynamic-drivemapping</code>              |
| Value    | <u>enabled</u> / disabled                                            |
| Registry | <code>sessions.winconnect%.option.enable-dynamic-drivemapping</code> |
| Range    | <u>Global setting</u> / on / off                                     |

- Fixed **login information** not being set after reboot.

## RD Web Access

- Fixed RD Web Access **login not working with user@domain**.

## WVD

- Fixed **proxy usage for WVD feed download**.



## Parallels Client

- Fixed a bug with Parallels not working if the **Parallels RAS omits the machine name in the application list.**

## Evidian

- Fixed **error on restart.**

## Firefox

- Fixed usage of a **pre-installed spellchecker in Firefox** input fields.
- Added **TLS 1.3** to the range of "**Maximum supported encryption protocol**" from **Sessions > Firefox Browser > Firefox Browser Global > Encryption.**

[More...](#)

|           |                                                |
|-----------|------------------------------------------------|
| Parameter | Maximum supported encryption protocol          |
| Registry  | browserglobal.app.security_tls_version_max     |
| Range     | [SSL3] [TLS 1.0] [TLS 1.1] [TLS 1.2] [TLS 1.3] |

## Chromium

- Fixed: **Custom Chromium Policies** datatypes now **written** in the correct way to **policies.json**.
- Fixed **browser** and **download history not** being **cleared**.

## Audio

- Fixed a **sporadic aborting** of an application **on closing ALSA Pulse PCM**. The problem affects only applications using ALSA API directly like Citrix Workspace App.
- Added **debug output to the ALSA Pulse PCM** which **must be enabled by** the environment variable `ALSA_PULSE_PCM_DEBUG=1`, the debug output is collected by the system logging facility (`journaldctl`).
- Fixed **missing default setup device** after **reboot**.

## VNC

- Fixed handling of **CapsLock status in VNC server**. Keyboard input now appears correctly, also if CapsLock is active on the client or server side. **This especially fixes upper case 'umlaut' characters** with Swiss and German keyboard layouts.

## Network

- Fixed bug: **SCEP failed** when `scep_getca` **received only a single certificate**.

## Base system

- Fixed issue with early **IGEL UD3-LX 60** (M350C) revisions that can lead to **read error from MMC**.
- Fixed **crash of IGEL monitoring agent**.
- Fixed possibility to **add certificates to Chromium** and **Firefox** which are given in **DER format**.
- The **Options dialog** keeps the **settings** that were **previously set**.
- Fix **GtkMessage dialog localization**.
- Fixed: **Shutdown delay** when **Post-session command** is enabled.
- Fixed **remembering last user name with Active Directory/Kerberos logon**. Before this fix, the user name could not be stored in the UMS to appear again after a reboot.

## X11 system



- Added registry key to solve an issue with **buggy screens connected over a DP-to-DVI adapter** (only works for Radeon devices like IGEL UD3-LX 50).

**More...**

|           |                                                              |
|-----------|--------------------------------------------------------------|
| Parameter | Fix issues with buggy monitors connected over DP-DVI adapter |
| Registry  | x.drivers.ati.dp_dvi_probe_workaround                        |
| Value     | enabled / <u>disabled</u>                                    |

- Updated **Display Switch rotate buttons** to usable size.
- Fixed **notifications not being hidden properly** when in **do-not-disturb mode**.

#### Window manager

- Fixed notifyd window **width not remaining constant**.
- Fixed **notification urgency critical background color**.

#### OS Converter

- Fixed **language chooser** in installations via **Deployment Appliance**.

## 7.6 Notes for Release 11.04.240

|                       |            |              |
|-----------------------|------------|--------------|
| <b>Software:</b>      | Version    | 11.04.240    |
| <b>Release Date:</b>  | 2020-11-16 |              |
| <b>Release Notes:</b> | Version    | RN-1104240-1 |
| <b>Last update:</b>   | 2020-11-16 |              |

- [Supported Devices 11.04.240](#)(see page 1572)
- [Component Versions 11.04.240](#)(see page 1573)
- [General Information 11.04.240](#)(see page 1580)
- [Known Issues 11.04.240](#)(see page 1580)
- [Security Fixes 11.04.240](#)(see page 1583)
- [New Features 11.04.240](#)(see page 1584)
- [Resolved Issues 11.04.240](#)(see page 1585)

### 7.6.1 Supported Devices 11.04.240

|         |           |
|---------|-----------|
| UD2-LX: | UD2-LX 51 |
|         | UD2-LX 50 |
|         | UD2-LX 40 |



|         |                                     |
|---------|-------------------------------------|
| UD3-LX: | UD3-LX 60<br>UD3-LX 51<br>UD3-LX 50 |
| UD5-LX: | UD5-LX 50                           |
| UD6-LX: | UD6-LX 51                           |
| UD7-LX: | UD7-LX 11<br>UD7-LX 10              |
| UD9-LX: | UD9-LX Touch 41<br>UD9-LX 40        |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>400</sup>.

## 7.6.2 Component Versions 11.04.240

### Clients

| Product                          | Version                       |
|----------------------------------|-------------------------------|
| Chromium                         | 83.0.4103.61-0ubuntu0.18.04.1 |
| Cisco JVDI Client                | 12.9.1                        |
| Cisco Webex Teams VDI Client     | 3.0.16605.0                   |
| Cisco Webex Meetings VDI Client  | 40.10.5.2377                  |
| Zoom Media Plugin                | 5.4.53376                     |
| Citrix HDX Realtime Media Engine | 2.9.0-2330                    |
| Citrix Workspace App             | 19.12.0.19                    |
| Citrix Workspace App             | 20.09.0.15                    |
| Citrix Workspace App             | 20.10.0.6                     |
| deviceTRUST Citrix Channel       | 20.1.200.0                    |
| Crossmatch DP Citrix Channel     | 0515.2                        |

<sup>400</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



|                                        |                                           |
|----------------------------------------|-------------------------------------------|
| Ericom PowerTerm                       | 12.0.1.0.20170219.2-_dev_-34574           |
| Ericom PowerTerm                       | 14.0.0.45623                              |
| Evidian AuthMgr                        | 1.5.7116                                  |
| Evince PDF Viewer                      | 3.28.4-0ubuntu1.2                         |
| FabulaTech USB for Remote Desktop      | 6.0.28                                    |
| Firefox                                | 68.12.0                                   |
| IBM iAccess Client Solutions           | 1.1.8.1                                   |
| IGEL RDP Client                        | 2.2igel1600249269                         |
| IGEL WVD Client                        | 1.0.16igel1605091446                      |
| Imprivata OneSign ProveID Embedded     | onesign-bootstrap-loader_1.0.523630_amd64 |
| deviceTRUST RDP Channel                | 20.1.200.0                                |
| NCP Secure Enterprise Client           | 5.10_rev40552                             |
| NX Client                              | 6.11.2-1igel8                             |
| Open VPN                               | 2.4.4-2ubuntu1.3                          |
| Zulu JRE                               | 8.48.0.51-2                               |
| Parallels Client (64 bit)              | 17.1.2.1                                  |
| Spice GTK (Red Hat Virtualization)     | 0.38-2igel93                              |
| Remote Viewer (Red Hat Virtualization) | 8.0-2git20191213.e4bacb8igel83            |
| Usbredir (Red Hat Virtualization)      | 0.8.0-1+b1igel71                          |
| Teradici PCoIP Software Client         | 20.10.0-18.04                             |
| ThinLinc Client                        | 4.12.0-6517                               |
| ThinPrint Client                       | 7.5.88                                    |
| Totem Media Player                     | 2.30.2-0ubuntu1igel55                     |
| Parole Media Player                    | 1.0.5-1igel1583919770                     |
| VNC Viewer                             | 1.10.1+dfsg-4igel13                       |
| VMware Horizon Client                  | 5.4.1-15988340                            |
| Voip Client Ekiga                      | 4.0.1-9build1igel6                        |



## Dictation

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20200323 |
| Philips Speech driver                     | 12.9.1   |

## Signature

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.9    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.4.2    |

## Smartcard

|                                           |                 |
|-------------------------------------------|-----------------|
| PKCS#11 Library A.E.T SafeSign            | 3.6.0.0-AET.000 |
| PKCS#11 Library Athena IDProtect          | 7               |
| PKCS#11 Library cryptovision sc/interface | 7.3.1           |
| PKCS#11 Library Gemalto SafeNet           | 10.7.77         |
| PKCS#11 Library OpenSC                    | 0.20.0-3igel37  |
| PKCS#11 Library SecMaker NetID            | 6.8.1.31        |
| PKCS#11 Library 90meter                   | 20190522        |
| Reader Driver ACS CCID                    | 1.1.6-1igel2    |
| Reader Driver Gemalto eToken              | 10.7.77         |
| Reader Driver HID Global Omnikey          | 4.3.3           |



|                                    |                        |
|------------------------------------|------------------------|
| Reader Driver Identive CCID        | 5.0.35                 |
| Reader Driver Identive eHealth200  | 1.0.5                  |
| Reader Driver Identive SCRKBC      | 5.0.24                 |
| Reader Driver MUSCLE CCID          | 1.4.31-1igel11         |
| Reader Driver REINER SCT cyberJack | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite        | 1.8.26-3igel14         |
| Cherry USB2LAN Proxy               | 3.2.0.3                |

### System Components

|                                         |                               |
|-----------------------------------------|-------------------------------|
| OpenSSL                                 | 1.0.2n-1ubuntu5.3             |
| OpenSSL                                 | 1.1.1-1ubuntu2.1~18.04.6      |
| OpenSSH Client                          | 7.6p1-4ubuntu0.3              |
| OpenSSH Server                          | 7.6p1-4ubuntu0.3              |
| Bluetooth stack (bluez)                 | 5.52-1igel6                   |
| MESA OpenGL stack                       | 20.0.8-1igel117               |
| VAAPI ABI Version                       | 0.40                          |
| VDPAU Library version                   | 1.4-1igel1003                 |
| Graphics Driver INTEL                   | 2.99.917+git20200515-igel1013 |
| Graphics Driver ATI/RADEON              | 19.1.0-1+git20200220igel987   |
| Graphics Driver ATI/AMDGPU              | 19.1.0-1+git20200318igel986   |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867               |
| Graphics Driver Nvidia                  | 440.100-0ubuntu0.20.04.1      |
| Graphics Driver VMware                  | 13.3.0-2igel857               |
| Graphics Driver QXL (Spice)             | 0.1.5-2build2-igel925         |
| Graphics Driver FBDEV                   | 0.5.0-1igel819                |
| Graphics Driver VESA                    | 2.4.0-1igel855                |
| Input Driver Evdev                      | 2.10.6-1igel975               |



|                                      |                                   |
|--------------------------------------|-----------------------------------|
| Input Driver Elographics             | 1.4.1-1+b6igel952                 |
| Input Driver eGalax                  | 2.5.8825                          |
| Input Driver Synaptics               | 1.9.1-1ubuntu1igel866             |
| Input Driver VMMouse                 | 13.1.0-1ubuntu2igel957            |
| Input Driver Wacom                   | 0.36.1-0ubuntu2igel888            |
| Input Driver ELO Multitouch          | 3.0.0                             |
| Input Driver ELO Singletouch         | 5.1.0                             |
| Kernel                               | 5.4.48 #mainline-lxos-g1605521351 |
| Xorg X11 Server                      | 1.20.8-2igel1016                  |
| Xorg Xephyr                          | 1.20.8-2igel1016                  |
| CUPS printing daemon                 | 2.2.7-1ubuntu2.8igel32            |
| PrinterLogic                         | 25.1.0.425                        |
| Lightdm Graphical Login Manager      | 1.26.0-0ubuntu1igel13             |
| XFCE4 Window Manager                 | 4.14.2-1~18.04igel1600339249      |
| ISC DHCP Client                      | 4.3.5-3ubuntu7.1                  |
| NetworkManager                       | 1.20.4-2ubuntu2.2igel105          |
| ModemManager                         | 1.10.0-1~ubuntu18.04.2            |
| GStreamer 0.10                       | 0.10.36-2ubuntu0.1igel201         |
| GStreamer 0.10 Fluendo aacdec        | 0.10.42                           |
| GStreamer 0.10 Fluendo asfdemux      | 0.10.90                           |
| GStreamer 0.10 Fluendo h264dec       | 0.10.58                           |
| GStreamer 0.10 Fluendo mp3dec        | 0.10.40                           |
| GStreamer 0.10 Fluendo mpegdemux     | 0.10.85                           |
| GStreamer 0.10 Fluendo mpeg4videodec | 0.10.44                           |
| GStreamer 0.10 Fluendo vadec         | 0.10.224                          |
| GStreamer 0.10 Fluendo wmadec        | 0.10.70                           |
| GStreamer 0.10 Fluendo wmvdec        | 0.10.66                           |
| GStreamer 1.x                        | 1.16.2-4igel239                   |



|                                     |                |
|-------------------------------------|----------------|
| GStreamer 1.0 Fluendo aacdec        | 0.10.42.2-8d6d |
| GStreamer 1.0 Fluendo asfdemux      | 0.10.90        |
| GStreamer 1.0 Fluendo h264dec       | 0.10.58        |
| GStreamer 1.0 Fluendo mp3dec        | 0.10.40        |
| GStreamer 1.0 Fluendo mpeg4videodec | 0.10.44        |
| GStreamer 1.0 Fluendo vadec         | 0.10.224       |
| GStreamer 1.0 Fluendo wmadec        | 0.10.70        |
| GStreamer 1.0 Fluendo wmvdec        | 0.10.66        |
| WebKit2Gtk                          | 2.28.3-2igel36 |
| Python2                             | 2.7.17         |
| Python3                             | 3.6.9          |

### VM Guest Support Components

|                            |                         |
|----------------------------|-------------------------|
| Virtualbox Guest Utils     | 6.1.10-dfsg-1igel41     |
| Virtualbox X11 Guest Utils | 6.1.10-dfsg-1igel41     |
| Open VM Tools              | 11.0.5-4ubuntu0.18.04.1 |
| Open VM Desktop Tools      | 11.0.5-4ubuntu0.18.04.1 |
| Xen Guest Utilities        | 7.10.0-0ubuntu1         |
| Spice Vdagent              | 0.20.0-1igel95          |
| Qemu Guest Agent           | 5.0-5igel12             |

### Features with Limited IGEL Support

|                                    |                                     |
|------------------------------------|-------------------------------------|
| Mobile Device Access USB (MTP)     | 1.1.17-3igel5                       |
| Mobile Device Access USB (imobile) | 1.2.1~git20191129.9f79242-1+b1igel8 |
| Mobile Device Access USB (gphoto)  | 2.5.25-2igel4                       |
| VPN OpenConnect                    | 8.10-1igel4                         |
| Scanner support                    | 1.0.27-1                            |
| VirtualBox                         | 6.1.10-dfsg-1igel41                 |

### Services

| Service                     | Size   | Reduced Firmware |
|-----------------------------|--------|------------------|
| Asian Language Support      | 22.5 M | Included         |
| Java SE Runtime Environment | 36.0 M | Included         |



|                                            |         |              |
|--------------------------------------------|---------|--------------|
| Citrix Appliance                           | 235.8 M | Included     |
| Citrix Workspace app                       |         |              |
| Citrix StoreFront                          |         |              |
| Ericom PowerTerm InterConnect              | 15.5 M  | Included     |
| Media Player                               | 512.0 K | Included     |
| Local Browser (Firefox)                    | 70.5 M  | Included     |
| Citrix Appliance                           |         |              |
| VMware Horizon                             | 4.2. M  | Included     |
| RDP                                        |         |              |
| Cendio ThinLinc                            | 10.0 M  | Included     |
| Printing (Internet printing protocol CUPS) | 22.2 M  | Included     |
| NoMachine NX                               | 26.8 M  | Included     |
| VMware Horizon                             | 116.0 M | Included     |
| Voice over IP (Ekiga)                      | 6.5 M   | Included     |
| Citrix Appliance                           | 768.0 K | Included     |
| NCP Enterprise VPN Client                  | 27.0 M  | Not included |
| Fluendo GStreamer Codec Plugins            | 7.5 M   | Included     |
| IBM i Access Client Solutions              | 72.5 M  | Not included |
| Red Hat Enterprise Virtualization          | 3.0 M   | Included     |
| Parallels Client                           | 5.5 M   | Included     |
| NVIDIA graphics driver                     | 115.0 M | Not included |
| Imprivata Appliance                        | 10.8 M  | Included     |
| Evidian AuthMgr                            | 2.8 M   | Included     |
| Hardware Video Acceleration                | 13.0 M  | Included     |
| Extra Font Package                         | 1.0 M   | Included     |
| Fluendo GStreamer AAC Decoder              | 1.2 M   | Included     |
| x32 Compatibility Support                  | 48.0 M  | Included     |
| Cisco JVDI client                          | 45.8 M  | Included     |
| PrinterLogic                               | 40.8 M  | Not included |
| Biosec BS Login                            | 10.0 M  | Not included |
| Login VSI Login Enterprise                 | 28.8 M  | Not included |
| Stratusphere UX CID Key software           | 2.8 M   | Not included |
| Elastic Filebeat                           | 15.8 M  | Not included |
| WVD                                        | 14.0 M  | Included     |
| Local Browser (Chromium)                   | 81.2 M  | Not included |
| deskMate client                            | 5.8 M   | Included     |
| Cisco Webex Teams VDI                      | 33.2 M  | Not included |
| Cisco Webex Meetings VDI                   | 40.8 M  | Not included |
| Zoom Media Plugin                          | 40.5 M  | Not included |
| Teradici PCoIP Client                      | 14.5 M  | Included     |



|                                            |         |              |
|--------------------------------------------|---------|--------------|
| 90meter Smart Card Support                 | 256.0 K | Included     |
| Mobile Device Access USB (Limited support) | 256.0 K | Not included |
| VPN OpenConnect (Limited support)          | 1.5 M   | Not included |
| Scanner support / SANE (Limited support)   | 2.5 M   | Not included |
| VirtualBox (Limited support)               | 62.5 M  | Not included |

### 7.6.3 General Information 11.04.240

To be beneficial to all new features and implementations, it is recommended to use UMS 6.06.100 or higher and update the corresponding profiles.

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

### 7.6.4 Known Issues 11.04.240

#### Firmware Update

- On **devices with 2 GB of flash storage**, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Check [Error: "Not enough space on local drive"](#) when [Updating to IGEL OS 11.04 or Higher](#)<sup>401</sup> for a solution.

#### Firefox

- **Firefox IGEL extensions are not updated automatically** under some circumstances. After an update from 11.03.xxx to 11.04.100, the IGEL extensions will stay on the old version. In this case, the following settings concerning **kiosk mode** cannot be executed:
  - Switch off hotkey for new window/tab
  - Blocking of internal browser pages like preferences, file picker, specific local directories

<sup>401</sup> <https://kb.igel.com/display/igelos1104/Updating+to+IGEL+OS+11.04+or+Higher+on+a+Device+with+Small+Storage>



As a workaround:

- a **reset to defaults** should be performed
- or the **browser's mimetype template** can be switched **from "Standard" to "Minimal"** by registry key `browserglobal.app.mimetypes_template`. There, the browser profile is renewed as well.

After the TC received the new setting, **reboot** and **set** the `mimetypes_template` registry key to **"Standard"** again.

## Citrix

- With activated **DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1 and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix StoreFront login** with **Gemalto smartcard** middleware does not detect smartcard correctly if the card is inserted after start of login.  
Workaround: Insert the smartcard before starting the StoreFront login.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264** acceleration plugin, the following registry key must be enabled.

[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | <code>ica.workaround-dual-rtme</code>                            |
| Value     | <code>enabled / disabled</code>                                  |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

- During the running **Microsoft Teams Optimization of Citrix Workspace App 20.09, webcam redirection or screen sharing** may lead to **display errors** like black stripes or flickering.
- The **performance** of Citrix sessions when using **Workspace App 20.06** may be lower on some devices.

A possible **workaround** is to **disable the virtual channels for Microsoft Teams** and **NSAP** or to set the **HDX transport protocol** to **TCP** only.

- `ica.module.virtualdriver.vdwebrtc.enable`
- `ica.module.virtualdriver.nsap.enable`

The protocol can be set via the Setup parameter **Sessions > Citrix > Citrix Global > Options > HDX Adaptive Transport over EDT** or via the **server policy** 'HDX Adaptive Transport'.

## VMware Horizon

- **Client drive mapping** and **USB redirection** for storage devices should not be enabled both at the same time.



- On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
- On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Enable local `Storage Hotplug` on Setup page **Devices > Storage Devices > Storage Hotplug**.
- External drives** mounted already before connection do not appear in the **remote desktop**.  
Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- After the disconnect of an RDP-based session**, the Horizon main **window** which contains the server or sessions overview **cannot be resized anymore**.
- Seamless application windows in Horizon Client may not be displayed correctly**. When starting the first seamless app, a new iconified window appears in the taskbar, and only if you click on it, the application will show up.  
On some hardware (UD7-H850, UD2-M250, UD2-D220), however, the client aborts when this new window is de-iconified.
- When using the **RDP protocol**, the remote session has a fixed offset of approximately the height of the menu bar. That means you have a black bar on top of the window and as a result of that, the **Windows panel on the bottom is cut off**.
- Modifier keys** (Shift/Ctrl/Win/Alt) in session windows using **RDP protocol** do not send the keyup event and **keep being pressed**, even when actually released. Only when closing the session with a mouse, the modifiers are reset.
- Copying a text from Horizon Blast sessions** is not possible.
- The **on-screen keyboard** in **Horizon appliance mode** does not work correctly with local logon.  
Workaround: **Switch off local logon** and switch on the corresponding two keys via IGEL registry:
  - userinterface.softkeyboard.autoshow
  - userinterface.softkeyboard.autohide

#### Wi-Fi

- TP-Link Archer T2UH Wi-Fi adapters does not work after system suspend/resume. Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

#### Parallels Client

- Native USB redirection** does not work with Parallels Client.

#### Smartcard

- Citrix Certificate Identity Declaration login** does not work with **SecMaker** smartcards.

#### Cisco JVDI Client

- There may be a **segfault shown in the logs** (during logout of Citrix Desktop session). This occurs only when using **Citrix Workspace app 20.10 and Cisco JVDI**.

#### Multimedia



- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.

#### Hyper-V

- **Hyper-V** (Generation 2) needs **a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.

#### VirtualBox

- The current **VirtualBox Guest Tools/Drivers** will not work with **VirtualBox 5.2.x or older** hosts which leads to a black screen and non-working graphics.  
**Possible workaround:** Install with 'Failsafe Installation + Recovery' and set the registry key `x.drivers.force_vesa` to 'true'.
- When running in VirtualBox virtualization, **resizing the window will not automatically change desktop resolution** of IGEL OS guest.

#### Audio

- **Audio jack detection on Advantech POC-W243L** doesn't work. Therefore, sound output goes through a possibly connected headset and the internal speakers.
- **IGEL UD2 (D220)** fails to restore the volume level of the speaker when the device used **firmware version 11.01.110** before.

#### Hardware

- **HP t730** could freeze when monitors with **different resolutions** are connected (1920x1200 + 2560x1440 + 3840x1600 for example). When this occurs, the registry key `x.drivers.kms.best_console_mode` has to be set to **disabled**.
- Some newer **Delock 62599 active DisplayPort-to-DVI (4k)** adapters only work with INTEL devices.

#### Remote Management

- **AIT feature with IGEL Starter License** is only **supported** by **UMS version 6.05.100 or newer**.

#### Base system

- **Update from memory stick** requires network online state (at least when multiple update stages are involved).

#### deskMate

- Some stability issues may remain.

#### Appliance Mode

- When **ending a Citrix session** in browser appliance mode, the **browser is restarted twice** instead of once.
- Appliance mode **RHEV/Spice: spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

## 7.6.5 Security Fixes 11.04.240

#### Base system



- Fixed **BleedingTooth** security issue which means CVE-2020-12351, CVE-2020-12352, and CVE-2020-24490.

## 7.6.6 New Features 11.04.240

Citrix

- Integrated **Citrix Workspace app 20.10**. Available Citrix Workspace apps in this release: **20.10 (default)**, **20.09**, and **19.12**
- Added: **Multiple audio devices can be mapped inside the sessions**. This will display audio devices with their device name and not only HDX audio anymore:  
[More...](#)

|           |                                 |
|-----------|---------------------------------|
| Parameter | Multiple Audio Device support   |
| Registry  | ica.module.vdcamversion4support |
| Type      | bool                            |
| Value     | enabled / <u>disabled</u>       |

**Note:** Bluetooth devices are currently not supported for device redirection.

- Updates **Zoom Media Plugin** to version **5.4.53376.1029**

VMware Horizon

- Updated **Zoom Media Plugin** to version **5.4.53376.1029**
- Added support for **VMware Integrated Printing**.  
[More...](#)

|           |                                 |
|-----------|---------------------------------|
| Parameter | Integrated Printing             |
| Registry  | vmware.view.integrated-printing |
| Type      | bool                            |
| Value     | enabled / <u>disabled</u>       |

WVD

- New parameter to set **HTTP user agent string for AAD login requests**.  
[More...](#)

|           |                                                                           |
|-----------|---------------------------------------------------------------------------|
| Parameter | HTTP user agent string                                                    |
| Registry  | sessions.wvd%.options.http-user-agent                                     |
| Type      | editable                                                                  |
| Value     | <u>System Default</u> / Windows / Android / iOS / macOS / <custom-string> |

Cisco Webex VDI

- Updated **Cisco Webex Teams VDI** to version **3.0.16605.0**
- Updated **Cisco Webex Meetings VDI** to version **40.10**

Cisco JVDI Client

- Updated **Cisco JVDI client** to version **12.9.1**



## Fabulatech

- Updated **FabulaTech USB for Remote Desktop** to version **6.0.28**
- Updated **FabulaTech Scanner for Remote Desktop** to version **2.5.0.7**

## Driver

- Updated **deviceTRUST** client plugin for Citrix and RDP to version **20.1.200.0**. Detailed release notes can be found at <https://docs.devicetrust.com/docs/releases-igel-20.1.200/>

## Remote Management

- Added **support for exchanging ICG certificates**.
  - The remote management of the endpoint device **automatically installs TLS certificates provided by the UMS into the local trusted CA certificates storage**. The **automatic deployment** of TLS certificates to endpoint devices **requires UMS 6.06.100 or higher**. This feature allows verifying certificates used when downloading files from the UMS, downloading a firmware update and custom partition archives over HTTPS or FTPS protocols. **The verifying of certificates must be enabled** by the parameter `system.security.remote_management.tls_verify_peer`.
- More...**

|          |                                                                        |
|----------|------------------------------------------------------------------------|
| Registry | <code>system.security.remote_management.tls_verify_peer</code>         |
| Value    | <u>enabled / disabled</u>                                              |
| Registry | <code>system.security.remote_management.tls_hostname_validation</code> |
| Value    | <u>enabled / disabled</u>                                              |

- Added support for **UMS commands to store and remove ICG configuration**.
- Introduced parameters for **ICG WebSocket connections**: debug log, network timeout (in seconds), and ping-pong interval (in seconds). The **parameters** are **applied on the next** established **ICG agent connection** and **ICG tunnel connections**: VNC and Secure Terminal. The **ping-pong** mechanism is supported **only for ICG tunnel connections**.

**More...**

|          |                                                     |
|----------|-----------------------------------------------------|
| Registry | <code>system.icg.websocket.debug</code>             |
| Value    | <u>off / all / tunnel / agent</u>                   |
| Registry | <code>system.icg.websocket.network_timeout</code>   |
| Value    | <u>30</u>                                           |
| Registry | <code>system.icg.websocket.pingpong_interval</code> |
| Value    | <u>120</u>                                          |

## 7.6.7 Resolved Issues 11.04.240

## Citrix

- Fixed issue with **Workspace app 2010: Screen flickering** while running a video call or sharing the screen in Microsoft Teams.
- Fixed Issue with **Workspace app 2010: Microsoft Teams** calls are now working with **different keyboard layouts**.



- Fixed: **Improved pcom** parameter pcom.valid\_return\_codes%.returncodes to handle ranges a la 1..255 (see tooltip).

#### Wi-Fi

- Fixed issues with **D-Link DWA-131 WLAN dongle**.

#### X11 system

- Fixed a problem with **display hotplug detection** when the display switch is not used.
- Fixed issues if **2 DisplayPort MST Hubs** are connected behind each other.

#### WVD

- **WVD memory leak(s)** fixed.
- Switched back to **the local login mask when the AAD login fails** for whatever reason. At the moment, there is no error message shown. This will come in one of the next versions.

#### VMware Horizon

- Fixed **post-session behavior** for VMware Horizon sessions where some **exit codes of the client were discarded** and therefore did not trigger the post-session action.
- Fixed **Local Logon Window** in that now we prevent it to get iconified because it always needs to be visible, especially in appliance mode where there is no panel to de-iconify it.

#### CID Key Agent

- Update of **CID Key Agent** to version **6.5.0-1**

#### Teradici PCoIP Client

- Updated **Teradici PCoIP** client to version **20.10**

#### Network

- Changed: Usage of **r8168** as default network driver **on Lenovo M75 Nano**.
- Added support for some newer **Intel e1000e network cards**.
- Fixed **logon by 802.1X authentication**.
- Fixed: Failing **Ethernet connection does not delay online state** reached by other means anymore.
- Added registry keys for enabling/disabling **sending of hostname in DHCPv4 and DHCPv6** requests.

**More...**

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Send hostname in DHCP requests               |
| Registry  | network.dhcp.send_hostname                   |
| Range     | [Disabled][ <u>Network Manager default</u> ] |
| Parameter | Send hostname in DHCPv6 requests             |
| Registry  | network.dhcp6.send_hostname                  |
| Range     | [Disabled][ <u>Network Manager default</u> ] |

- Added registry key for **disabling Ethernet link reconfiguration by Network Manager**.

**More...**

|           |                                           |
|-----------|-------------------------------------------|
| Parameter | Disable NetworkManager link configuration |
|-----------|-------------------------------------------|



|          |                                                                                                                                                           |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Registry | <code>network.interfaces.ethernet.device%.nm_disable_link_config</code>                                                                                   |
| Type     | <code>bool</code>                                                                                                                                         |
| Value    | <code>true / false</code>                                                                                                                                 |
| Note     | Setting this to "true" can be beneficial when 802.1X authentication is disturbed by link. It is currently set automatically when e1000e drivers are used. |

#### Open VPN

- Fixed **segmentation fault** if the nameserver is used.  
Now it is allowed to use an empty password for the private key. Not needed to enter a password when the private key does not have one.

#### Base system

- Fixed: The **fluendo vadec** update closed a **memory leak with AMD devices** using VAAPI acceleration.
- **Updated Fluendo multimedia codecs** to the following versions:  
[More...](#)

|                                     |            |
|-------------------------------------|------------|
| <code>gst-fluendo-aacdec</code>     | 8/10/2020  |
| <code>gst-fluendo-asfdemux</code>   | 17/9/2020  |
| <code>gst-fluendo-h264dec</code>    | 22/9/2020  |
| <code>gst-fluendo-mp3</code>        | 17/9/2020  |
| <code>gst-fluendo-mpeg4video</code> | 18/9/2020  |
| <code>gst-fluendo-vadec</code>      | 02/11/2020 |
| <code>gst-fluendo-wmadec</code>     | 17/9/2020  |
| <code>gst-fluendo-wmvdec</code>     | 17/9/2020  |

- Fixed possible **USB issues with suspend/resume on IGEL M350C** devices.
- Fixed: **Custom applications** did not run **while being offline** even if they did not need network.

#### Audio

- Fixed the **ALSA Pulse PCM** - a possible **deadlock** while writing audio data and closing Pulse PCM.
- Fixed **microphone** issues with **UD3-LX60** device.

#### Remote Management

- Fixed sporadic **failures while retrieving the Unit ID** by the IGEL Remote Management agent.
- Fixed **sending the user logoff message to the UMS**.

#### HID

- Updated **eGTouch (eGalax) drivers and xorg** configuration.
- Fixing **double tapping of desktop icons on touchscreen** devices.

#### Window manager

- Fixed **desktop icons** not being restricted to one monitor at all.



## 7.7 Notes for Release 11.04.200

|                       |            |              |
|-----------------------|------------|--------------|
| <b>Software:</b>      | Version    | 11.04.200    |
| <b>Release Date:</b>  | 2020-10-08 |              |
| <b>Release Notes:</b> | Version    | RN-1104200-1 |
| <b>Last update:</b>   | 2020-10-08 |              |

- [Supported Devices 11.04.200](#)(see page 1588)
- [Component Versions 11.04.200](#)(see page 1589)
- [General Information 11.04.200](#)(see page 1595)
- [Known Issues 11.04.200](#)(see page 1595)
- [Security Fixes 11.04.200](#)(see page 1599)
- [New Features 11.04.200](#)(see page 1599)
- [Resolved Issues 11.04.200](#)(see page 1601)

### 7.7.1 Supported Devices 11.04.200

|         |                                     |
|---------|-------------------------------------|
| UD2-LX: | UD2-LX 51<br>UD2-LX 50<br>UD2-LX 40 |
| UD3-LX: | UD3-LX 60<br>UD3-LX 51<br>UD3-LX 50 |
| UD5-LX: | UD5-LX 50                           |
| UD6-LX: | UD6-LX 51                           |
| UD7-LX: | UD7-LX 11<br>UD7-LX 10              |



|         |                 |
|---------|-----------------|
| UD9-LX: | UD9-LX Touch 41 |
|         | UD9-LX 40       |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>402</sup>.

## 7.7.2 Component Versions 11.04.200

### Clients

| Product                           | Version                         |
|-----------------------------------|---------------------------------|
| Chromium                          | 83.0.4103.61-0ubuntu0.18.04.1   |
| Cisco JVDI Client                 | 12.9.0                          |
| Cisco Webex Teams VDI Client      | 3.0.15711.0                     |
| Cisco Webex Meetings VDI Client   | 40.10.0.171                     |
| Zoom Media Plugin                 | 5.2.456413                      |
| Citrix HDX Realtime Media Engine  | 2.9.0-2330                      |
| Citrix Workspace App              | 19.12.0.19                      |
| Citrix Workspace App              | 20.06.0.15                      |
| Citrix Workspace App              | 20.09.0.15                      |
| deviceTRUST Citrix Channel        | 19.1.200.2                      |
| Crossmatch DP Citrix Channel      | 0515.2                          |
| Ericom PowerTerm                  | 12.0.1.0.20170219.2-_dev_-34574 |
| Ericom PowerTerm                  | 14.0.0.45623                    |
| Evidian AuthMgr                   | 1.5.7116                        |
| Evince PDF Viewer                 | 3.28.4-0ubuntu1.2               |
| FabulaTech USB for Remote Desktop | 5.2.29                          |
| Firefox                           | 68.12.0                         |
| IBM iAccess Client Solutions      | 1.1.8.1                         |

<sup>402</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



|                                        |                                           |
|----------------------------------------|-------------------------------------------|
| IGEL RDP Client                        | 2.2igel1600249269                         |
| IGEL WVD Client                        | 1.0.13igel1596142398                      |
| Imprivata OneSign ProveID Embedded     | onesign-bootstrap-loader_1.0.523630_amd64 |
| deviceTRUST RDP Channel                | 19.1.200.2                                |
| NCP Secure Enterprise Client           | 5.10_rev40552                             |
| NX Client                              | 6.11.2-1igel8                             |
| Open VPN                               | 2.4.4-2ubuntu1.3                          |
| Zulu JRE                               | 8.48.0.51-2                               |
| Parallels Client (64 bit)              | 17.1.2.1                                  |
| Spice GTK (Red Hat Virtualization)     | 0.38-2igel93                              |
| Remote Viewer (Red Hat Virtualization) | 8.0-2git20191213.e4bacb8igel83            |
| Usbredir (Red Hat Virtualization)      | 0.8.0-1+b1igel71                          |
| Teradici PCoIP Software Client         | 20.04.2-18.04                             |
| ThinLinc Client                        | 4.12.0-6517                               |
| ThinPrint Client                       | 7.5.88                                    |
| Totem Media Player                     | 2.30.2-0ubuntu1igel55                     |
| Parole Media Player                    | 1.0.5-1igel1583919770                     |
| VNC Viewer                             | 1.10.1+dfsg-4igel13                       |
| VMware Horizon Client                  | 5.4.1-15988340                            |
| Voip Client Ekiga                      | 4.0.1-9build1igel6                        |

## Dictation

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20200323 |
| Philips Speech driver                     | 12.9.1   |



## Signature

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.9    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.4.2    |

## Smartcard

|                                           |                        |
|-------------------------------------------|------------------------|
| PKCS#11 Library A.E.T SafeSign            | 3.6.0.0-AET.000        |
| PKCS#11 Library Athena IDProtect          | 7                      |
| PKCS#11 Library cryptovision sc/interface | 7.3.1                  |
| PKCS#11 Library Gemalto SafeNet           | 10.7.77                |
| PKCS#11 Library OpenSC                    | 0.20.0-3igel37         |
| PKCS#11 Library SecMaker NetID            | 6.8.1.31               |
| PKCS#11 Library 90meter                   | 20190522               |
| Reader Driver ACS CCID                    | 1.1.6-1igel2           |
| Reader Driver Gemalto eToken              | 10.7.77                |
| Reader Driver HID Global Omnikey          | 4.3.3                  |
| Reader Driver Identive CCID               | 5.0.35                 |
| Reader Driver Identive eHealth200         | 1.0.5                  |
| Reader Driver Identive SCRKBC             | 5.0.24                 |
| Reader Driver MUSCLE CCID                 | 1.4.31-1igel11         |
| Reader Driver REINER SCT cyberJack        | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite               | 1.8.26-3igel14         |



|                      |         |
|----------------------|---------|
| Cherry USB2LAN Proxy | 3.2.0.3 |
|----------------------|---------|

### System Components

|                                         |                               |
|-----------------------------------------|-------------------------------|
| OpenSSL                                 | 1.0.2n-1ubuntu5.3             |
| OpenSSL                                 | 1.1.1-1ubuntu2.1~18.04.6      |
| OpenSSH Client                          | 7.6p1-4ubuntu0.3              |
| OpenSSH Server                          | 7.6p1-4ubuntu0.3              |
| Bluetooth stack (bluez)                 | 5.52-1igel6                   |
| MESA OpenGL stack                       | 20.0.8-1igel117               |
| VAAPI ABI Version                       | 0.40                          |
| VDPAU Library version                   | 1.4-1igel1003                 |
| Graphics Driver INTEL                   | 2.99.917+git20200515-igel1013 |
| Graphics Driver ATI/RADEON              | 19.1.0-1+git20200220igel987   |
| Graphics Driver ATI/AMDGPU              | 19.1.0-1+git20200318igel986   |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867               |
| Graphics Driver Nvidia                  | 440.100-0ubuntu0.20.04.1      |
| Graphics Driver VMware                  | 13.3.0-2igel857               |
| Graphics Driver QXL (Spice)             | 0.1.5-2build2-igel925         |
| Graphics Driver FBDEV                   | 0.5.0-1igel819                |
| Graphics Driver VESA                    | 2.4.0-1igel855                |
| Input Driver Evdev                      | 2.10.6-1igel975               |
| Input Driver Elographics                | 1.4.1-1+b6igel952             |
| Input Driver eGalax                     | 2.5.7413                      |
| Input Driver Synaptics                  | 1.9.1-1ubuntu1igel866         |
| Input Driver VMMouse                    | 13.1.0-1ubuntu2igel957        |
| Input Driver Wacom                      | 0.36.1-0ubuntu2igel888        |
| Input Driver ELO Multitouch             | 3.0.0                         |
| Input Driver ELO Singletouch            | 5.1.0                         |



|                                 |                                       |
|---------------------------------|---------------------------------------|
| Kernel                          | 5.4.48 #mainline-lxos_dev-g1595410170 |
| Xorg X11 Server                 | 1.20.8-2igel1016                      |
| Xorg Xephyr                     | 1.20.8-2igel1016                      |
| CUPS printing daemon            | 2.2.7-1ubuntu2.8igel32                |
| PrinterLogic                    | 25.1.0.425                            |
| Lightdm Graphical Login Manager | 1.26.0-0ubuntu1igel13                 |
| XFCE4 Window Manager            | 4.14.2-1~18.04.0igel1600339249        |
| ISC DHCP Client                 | 4.3.5-3ubuntu7.1                      |
| NetworkManager                  | 1.20.4-2ubuntu2.2igel100              |
| ModemManager                    | 1.10.0-1~ubuntu18.04.2                |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.1igel201             |
| GStreamer 1.x                   | 1.16.2-4igel239                       |
| WebKit2Gtk                      | 2.28.3-2igel36                        |
| Python2                         | 2.7.17                                |
| Python3                         | 3.6.9                                 |

### VM Guest Support Components

|                            |                         |
|----------------------------|-------------------------|
| Virtualbox Guest Utils     | 6.1.10-dfsg-1igel41     |
| Virtualbox X11 Guest Utils | 6.1.10-dfsg-1igel41     |
| Open VM Tools              | 11.0.5-4ubuntu0.18.04.1 |
| Open VM Desktop Tools      | 11.0.5-4ubuntu0.18.04.1 |
| Xen Guest Utilities        | 7.10.0-0ubuntu1         |
| Spice Vdagent              | 0.20.0-1igel95          |
| Qemu Guest Agent           | 5.0-5igel12             |

### Features with Limited IGEL Support

|                                    |                                     |
|------------------------------------|-------------------------------------|
| Mobile Device Access USB (MTP)     | 1.1.17-3igel5                       |
| Mobile Device Access USB (imobile) | 1.2.1~git20191129.9f79242-1+b1igel8 |
| Mobile Device Access USB (gphoto)  | 2.5.25-2igel4                       |
| VPN OpenConnect                    | 8.10-1igel4                         |



|                 |                     |
|-----------------|---------------------|
| Scanner support | 1.0.27-1            |
| VirtualBox      | 6.1.10-dfsg-1igel41 |

## Services

| Service                                    | Size    | Reduced Firmware |
|--------------------------------------------|---------|------------------|
| Asian Language Support                     | 24.8 M  | Included         |
| Java SE Runtime Environment                | 42.8 M  | Included         |
| Citrix Appliance                           | 258.5 M | Included         |
| Citrix Workspace app                       |         |                  |
| Citrix StoreFront                          |         |                  |
| Ericom PowerTerm InterConnect              | 17.8 M  | Included         |
| Media Player                               | 768.0 K | Included         |
| Local Browser (Firefox)                    | 81.8 M  | Included         |
| Citrix Appliance                           |         |                  |
| VMware Horizon                             | 5.5. M  | Included         |
| RDP                                        |         |                  |
| Cendio ThinLinc                            | 11.5 M  | Included         |
| Printing (Internet printing protocol CUPS) | 23.8 M  | Included         |
| NoMachine NX                               | 31.5 M  | Included         |
| VMware Horizon                             | 193.2 M | Included         |
| Voice over IP (Ekiga)                      | 7.2 M   | Included         |
| Citrix Appliance                           | 768.0 K | Included         |
| NCP Enterprise VPN Client                  | 30.8 M  | Not included     |
| Fluendo GStreamer Codec Plugins            | 8.5 M   | Included         |
| IBM i Access Client Solutions              | 96.2 M  | Not included     |
| Red Hat Enterprise Virtualization          | 3.5 M   | Included         |
| Parallels Client                           | 6.2 M   | Included         |
| NVIDIA graphics driver                     | 128.5 M | Not included     |
| Imprivata Appliance                        | 16.0 M  | Included         |
| Evidian AuthMgr                            | 3.0 M   | Included         |
| Hardware Video Acceleration                | 15.0 M  | Included         |
| Extra Font Package                         | 1.2 M   | Included         |
| Fluendo GStreamer AAC Decoder              | 1.2 M   | Included         |
| x32 Compatibility Support                  | 54.8 M  | Included         |
| Cisco JVDI client                          | 56.0 M  | Included         |
| PrinterLogic                               | 50.8 M  | Not included     |
| Biosec BS Login                            | 10.2 M  | Not included     |
| Login VSI Login Enterprise                 | 32.8 M  | Not included     |



|                                            |         |              |
|--------------------------------------------|---------|--------------|
| Stratusphere UX CID Key software           | 3.2 M   | Not included |
| Elastic Filebeat                           | 25.0 M  | Not included |
| WVD                                        | 16.2 M  | Included     |
| Local Browser (Chromium)                   | 91.0 M  | Not included |
| deskMate client                            | 6.5 M   | Included     |
| Cisco Webex Teams VDI                      | 40.2 M  | Not included |
| Cisco Webex Meetings VDI                   | 46.0 M  | Not included |
| Zoom Media Plugin                          | 42.0 M  | Not included |
| Teradici PCoIP Client                      | 8.8 M   | Included     |
| 90meter Smart Card Support                 | 256.0 K | Included     |
| Mobile Device Access USB (Limited support) | 512.0 K | Not included |
| VPN OpenConnect (Limited support)          | 1.8 M   | Not included |
| Scanner support / SANE (Limited support)   | 2.8 M   | Not included |
| VirtualBox (Limited support)               | 69.0 M  | Not included |

### 7.7.3 General Information 11.04.200

To be beneficial to all new features and implementations, it is recommended to use UMS 6.05.110 or higher and update the corresponding profiles.

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

### 7.7.4 Known Issues 11.04.200

Firmware Update



- On **devices with 2 GB of flash storage**, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Check [Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher\(see page 231\)](#) for a solution.

#### Firefox

- **Firefox IGEL extensions are not updated automatically** under some circumstances. After an update from 11.03.xxx to 11.04.100, the IGEL extensions will stay on the old version. In this case, the following settings concerning **kiosk mode** cannot be executed:
  - Switch off hotkey for new window/tab
  - Blocking of internal browser pages like preferences, file picker, specific local directories

As a workaround:

- a **reset to defaults** should be performed
  - or the **browser's mimetype template** can be switched **from "Standard" to "Minimal"** by registry key `browserglobal.app.mimetypes_template`. There, the browser profile is renewed as well.
- After the TC received the new setting, **reboot** and **set** the `mimetypes_template` registry key to **"Standard"** again.

#### Citrix

- With activated **DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1 and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix StoreFront login** with **Gemalto smartcard** middleware does not detect smartcard correctly if the card is inserted after start of login.  
Workaround: Insert the smartcard before starting the StoreFront login.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264** acceleration plugin, the following registry key must be enabled.

[More...](#)

|                |                                                                           |
|----------------|---------------------------------------------------------------------------|
| Parameter      | Activate workaround for dual RTME sessions and H264 acceleration          |
| Registry Value | <code>ica.workaround-dual-rtme</code><br><u>enabled</u> / <u>disabled</u> |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

- During the running **Microsoft Teams Optimization of Citrix Workspace App 20.06/20.09, webcam redirection or screen sharing** may lead to **display errors** like black stripes or flickering.
- The **performance** of Citrix sessions when using **Workspace App 20.06** may be lower on some devices.



A possible **workaround** is to **disable** the **virtual channels for Microsoft Teams** and **NSAP** or to set the **HDX transport protocol** to **TCP** only.

- ica.module.virtualdriver.vdwebrtc.enable
- ica.module.virtualdriver.nsap.enable

The protocol can be set via the Setup parameter **Sessions > Citrix > Citrix Global > Options > HDX Adaptive Transport over EDT** or via the **server policy** 'HDX Adaptive Transport'.

#### VMware Horizon

- **Client drive mapping** and **USB redirection** for storage devices should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Enable local `Storage Hotplug` on Setup page **Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection do not appear in the **remote desktop**.  
Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- **After the disconnect of an RDP-based session**, the Horizon main **window** which contains the server or sessions overview **cannot be resized anymore**.
- **Seamless application windows in Horizon Client may not be displayed correctly**. When starting the first seamless app, a new iconified window appears in the taskbar, and only if you click on it, the application will show up.  
On some hardware (UD7-H850, UD2-M250, UD2-D220), however, the client aborts when this new window is de-iconified.
- When using the **RDP protocol**, the remote session has a fixed offset of approximately the height of the menu bar. That means you have a black bar on top of the window and as a result of that, the **Windows panel on the bottom is cut off**.
- **Modifier keys** (Shift/Ctrl/Win/Alt) in session windows using **RDP protocol** do not send the keyup event and thus **keep being pressed even when actually released**. Only when you leave the session with the mouse, the modifiers are reset.
- **Copying a text from Horizon Blast sessions** is not possible.
- The **on-screen keyboard** in **Horizon appliance mode** doesn't work correctly with local logon. You have to switch off the local logon and switch on these two keys in the IGEL registry:
  - userinterface.softkeyboard.autoshow
  - userinterface.softkeyboard.autohide

#### Wi-Fi

- TP-Link Archer T2UH Wi-Fi adapters does not work after system suspend/resume. Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

#### Parallels Client



- **Native USB redirection** does not work with Parallels Client.

#### Smartcard

- **Citrix Certificate Identity Declaration login** does not work with **SecMaker** smartcards.

#### Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.

#### Hyper-V

- **Hyper-V** (Generation 2) needs **a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.

#### VirtualBox

- The current **VirtualBox Guest Tools/Drivers** will not work with **VirtualBox 5.2.x or older** hosts which leads to a black screen and non-working graphics.

**Possible workaround:** Install with 'Failsafe Installation + Recovery' and set the registry key `x.drivers.force_vesa` to 'true'.

- When running in VirtualBox virtualization, **resizing the window will not automatically change desktop resolution** of IGEL OS guest.

#### Audio

- **Audio jack detection on Advantech POC-W243L** doesn't work. Therefore, sound output goes through a possibly connected headset and the internal speakers.
- **IGEL UD2 (D220)** fails to restore the volume level of the speaker when the device used **firmware version 11.01.110** before.

#### Hardware

- **HP t730** could freeze when monitors with **different resolutions** are connected (1920x1200 + 2560x1440 + 3840x1600 for example). When this occurs, the registry key `x.drivers.kms.best_console_mode` has to be set to **disabled**.
- Some newer **Delock 62599 active DisplayPort-to-DVI (4k)** adapters only work with INTEL devices.

#### Remote Management

- **AIT feature with IGEL Starter License** is supported by the **UMS version 6.05.100**.

#### Base system

- **Update from memory stick** requires network online state (when multiple update stages are involved).

#### deskMate

- Some stability issues may remain.

#### Appliance Mode

- When **ending a Citrix session** in browser appliance mode, the **browser is restarted twice** instead of once.



- Appliance mode **RHEV/Spice: spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

## 7.7.5 Security Fixes 11.04.200

### Firefox

- Updated Mozilla Firefox to **68.12.0esr**:
  - Fixes for **mfsa2020-11**, also known as CVE-2020-6819, CVE-2020-6820.
    - Fixes for **mfsa2020-13**, also known as  
[More...](#)

CVE-2020-6828, CVE-2020-6827, CVE-2020-6821,  
CVE-2020-6822, and CVE-2020-6825
    - Fixes for **mfsa2020-17** also known as:
      - [More...](#)

CVE-2020-12387, CVE-2020-12388, CVE-2020-12389,  
CVE-2020-6831, CVE-2020-12392, CVE-2020-12393,  
and CVE-2020-1239
    - Fixes for **mfsa2020-21** also known as:
      - [More...](#)

CVE-2020-12399, CVE-2020-12405,  
CVE-2020-12406, CVE-2020-12410
    - Fixes for **mfsa2020-25** also known as:
      - [More...](#)

CVE-2020-12417, CVE-2020-12418, CVE-2020-12419,  
CVE-2020-12420, CVE-2020-12421
    - Fixes for **mfsa2020-31** also known as:
      - [More...](#)

CVE-2020-15652, CVE-2020-6514, CVE-2020-6463,  
CVE-2020-15650, CVE-2020-15649, and CVE-2020-15659
    - Fixes for **mfsa2020-37** also known as: CVE-2020-15663, CVE-2020-15664, and  
CVE-2020-15669

### Base system

- Fixed privilege escalation via environment variables in the /bin/update binary.
- Fixed privilege escalation via environment variable PATH in /bin/usershell binary.
- Fixed privilege escalation via PATH environment variable in the /bin/update binary.

## 7.7.6 New Features 11.04.200

### Citrix



- Integrated **Citrix Workspace app 20.09. Removed** Citrix Workspace app **18.10**. Available Citrix Workspace apps in this release: **20.09 (default)**, **20.06** and **19.12**. The **performance** of the Citrix Workspace app **20.09** was **improved** and a **more detailed logging** was implemented.
- Citrix **logging** was **summarized**. Now, only **one parameter** is needed to **activate logging**.  
**More...**

|           |                                    |
|-----------|------------------------------------|
| Parameter | Enable logging for Citrix sessions |
| Registry  | ica.logging.debug                  |
| Value     | on / off                           |

- Since Workspace app 20.09, the tool **setlog** is used to **configure the logging**. For this purpose, parameters are provided in the registry `ica.logging.setlog`; usually, nothing needs to be changed.
- After **disabling logging**, the system must be **restarted** once.
- Integrated **Zoom Media Plugin 5.2.456413.0902**
- Added **PAC proxy auto configuration support** for Zoom Media Plugin (ZoomVDI). To configure, the following parameters need to be set:
  - `network.proxy.settings.sys_proxy_type="Automatic proxy configuration"`
  - `network.proxy.settings.sys_proxy_autoconfig_url="http://..."`

Alternatively, the **manual HTTP/HTTPS proxy setting** configured at **IGEL Setup > Network > Proxy** is now used for Zoom Media Plugin.

- **Improved** configuration of **ZoomVDI** client.

#### Cisco Webex

- Integrated **Cisco Webex Meetings 40.10**.

#### Parallels Client

- Updated **Parallels** Client to version **17.1.2.1**. Fixed security vulnerability issue disclosed in the Parallels KB article <https://kb.parallels.com/en/125112>.

#### Audio

- Added **EPOS Connect 5.0.1.2795**.

**More...**

|            |                                                                              |
|------------|------------------------------------------------------------------------------|
| IGEL Setup | <b>Devices &gt; Unified Communications &gt; EPOS Audio &gt; EPOS Connect</b> |
| Parameter  | Enable EPOS Connect                                                          |
| Registry   | <code>devices.epos.connect.enable</code>                                     |
| Type       | bool                                                                         |
| Value      | enabled / disabled                                                           |
| IGEL Setup | <b>Devices &gt; Unified Communications &gt; EPOS Audio &gt; EPOS Connect</b> |
| Parameter  | Tenant ID                                                                    |
| Registry   | <code>devices.epos.connect.tenant_id</code>                                  |



|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| Type       | string                                                                        |
| Value      | "                                                                             |
| IGEL Setup | <b>Devices &gt; Unified Communications &gt; EPOS Audio &gt; EPOS Connect</b>  |
| Parameter  | Backend Endpoint                                                              |
| Registry   | devices.epos.connect.tenant_url                                               |
| Type       | string                                                                        |
| Value      | "                                                                             |
| IGEL Setup | <b>Devices &gt; Unified Communications &gt; EPOS Audio &gt; EPOS Connect</b>  |
| Parameter  | Proxy                                                                         |
| Registry   | devices.epos.connect.proxy                                                    |
| Type       | string                                                                        |
| Value      | "                                                                             |
| Registry   | devices.epos.connect.log_level                                                |
| Value      | Trace / Debug / <u>Information</u> / Warnings / Errors / Exceptions / No logs |

#### Smartcard

- Updated **A.E.T. Europe SafeSign Identity Client** to version **3.6.0.0**.

#### Multimedia

- Added possibility to fetch **log files of the Zoom Media Plugin (ZoomVDI)** via **UMS support information**.

#### Hardware

- Added detection of **UD Pocket UC5-LX 2**.

#### Misc

- Updated **Login Enterprise** to version **4.2**.

### 7.7.7 Resolved Issues 11.04.200

#### Citrix

- Fixed the problem with **apparmor** and the **Citrix MS Teams workaround**.
- Fixed: In some Citrix sessions, there have been **sporadic appearances of black rectangles** when the feature "**Accelerated H.264 Deep Compression Codec**" is active.
- Integrated parameter to activate the workaround for the **keyboard language issue with MS Teams Optimization**.  
**More...**

|           |                                                           |
|-----------|-----------------------------------------------------------|
| Parameter | Microsoft Teams optimization keyboard language workaround |
|-----------|-----------------------------------------------------------|



|          |                                                                     |
|----------|---------------------------------------------------------------------|
| Registry | <code>ica.module.virtualdriver.vdwebrtc.keyboard_eworkaround</code> |
| Value    | <u>on</u> / <u>off</u>                                              |

## RDP/IGEL RDP Client 2

- Improved **error logging**.
- Fixed **USB redirection** for RDP sessions.

## Firefox

- Fixed **smartcard access in Firefox**. Before this fix, **smartcards** were **not recognized occasionally**.

## Network

- Fixed handling of **DNS default domain**.
- Added **registry** key specifying the **number of 802.1X authentication attempts on Ethernet**.  
[More...](#)

|          |                                                                          |
|----------|--------------------------------------------------------------------------|
| Registry | <code>network.interfaces.ethernet.device%.ieee8021x.auth_attempts</code> |
| Type     | integer                                                                  |
| Value    | <u>1</u>                                                                 |

- **SCEP**: Fixed derivation of **802.1X identity** from client certificate.

## Window manager

- Fixed **crash of start menu**, where it was not populated with any items.
- Fixed **start monitor mapping for Firefox**.

## Wi-Fi

- **Added** missing **iwlwifi-6000-4 firmware file**.

## Open VPN

- Fixed **segmentation fault** when **nameserver was used**.
- Added: **Different protocols** are now **selectable**:  
[More...](#)

|           |                                                                             |
|-----------|-----------------------------------------------------------------------------|
| Parameter | protocol                                                                    |
| Registry  | <code>sessions.openconnect%.vpnopts.protocol</code>                         |
| Value     | <u>Cisco AnyConnect</u> / Juniper Network / Junos Pulse / PAN GlobalProtect |

## Base system

- Fixed **panels clock format** via registry key `windowmanager.wm%.variables.clock_time`.
- **Post-session command binaries** and **return codes** are **now customizable** via registry. Allows post-session commands if a binary doesn't return 0.

Name of the binary:

[More...](#)



|           |                                    |
|-----------|------------------------------------|
| Parameter | Binary                             |
| Registry  | pcom.valid_return_codes<NR>.binary |
| Value     | binary name                        |

**Comma seperated** return codes (e.g. **7,99**) or/and **return code ranges** (e.g. **3..5** for 3,4,5) to be accepted:

**More...**

|           |                                           |
|-----------|-------------------------------------------|
| Parameter | Return Codes                              |
| Registry  | pcom.valid_return_codes<NR>.returncodes   |
| Value     | e.g. 3,5,10..15 for 3,5,10,11,12,13,14,15 |

- Fixed problems with **hostnames containing one or more "\_" characters.**
- Added: Show **AMD Memory Guard in Boot Mode**, when enabled.

#### Storage Devices

- Fixed **display of hotplug eject menu** in appliance mode.

#### Remote Management

- Fixed **ICG HA functionality broken in 11.04.100.**
- Fixed **automatic establishment of the configured ICG connection** if the UMS Server is unreachable.

## 7.8 Notes for Release 11.04.100

|                       |            |              |
|-----------------------|------------|--------------|
| <b>Software:</b>      | Version    | 11.04.100    |
| <b>Release Date:</b>  | 2020-08-05 |              |
| <b>Release Notes:</b> | Version    | RN-1104100-1 |
| <b>Last update:</b>   | 2020-08-05 |              |

- 
- [IGEL OS 11](#)(see page 1603)
  - [IGEL OS Creator \(OSC\)](#)(see page 1646)

### 7.8.1 IGEL OS 11

- [Supported Devices 11.04.100](#)(see page 1604)
- [Component Versions 11.04.100](#)(see page 1604)
- [General Information 11.04.100](#)(see page 1610)
- [Known Issues 11.04.100](#)(see page 1611)



- Security Fixes 11.04.100(see page 1614)
- New Features 11.04.100(see page 1615)
- Resolved Issues 11.04.100(see page 1631)
- CA Certificates Contained in IGEL OS 11.04.100(see page 1638)

## Supported Devices 11.04.100

|         |                                     |
|---------|-------------------------------------|
| UD2-LX: | UD2-LX 51<br>UD2-LX 50<br>UD2-LX 40 |
| UD3-LX: | UD3-LX 60<br>UD3-LX 51<br>UD3-LX 50 |
| UD5-LX: | UD5-LX 50                           |
| UD6-LX: | UD6-LX 51                           |
| UD7-LX: | UD7-LX 11<br>UD7-LX 10              |
| UD9-LX: | UD9-LX Touch 41<br>UD9-LX 40        |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>403</sup>.

## Component Versions 11.04.100

### Clients

| Product                      | Version                       |
|------------------------------|-------------------------------|
| Chromium                     | 83.0.4103.61-0ubuntu0.18.04.1 |
| Cisco JVDI Client            | 12.9.0                        |
| Cisco Webex Teams VDI Client | 3.0.15711.0                   |

<sup>403</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



|                                        |                                                                                         |
|----------------------------------------|-----------------------------------------------------------------------------------------|
| Cisco Webex Meetings VDI Client        | 40.7.0.375                                                                              |
| Citrix HDX Realtime Media Engine       | 2.9.0-2330                                                                              |
| Citrix Workspace App                   | 18.10.0.11                                                                              |
| Citrix Workspace App                   | 19.12.0.19                                                                              |
| Citrix Workspace App                   | 20.06.0.15                                                                              |
| deviceTRUST Citrix Channel             | 19.1.200.2                                                                              |
| Crossmatch DP Citrix Channel           | 0515.2                                                                                  |
| Ericom PowerTerm                       | 12.0.1.0.20170219.2-_dev_-34574                                                         |
| Ericom PowerTerm                       | 14.0.0.45623                                                                            |
| Evidian AuthMgr                        | 1.5.7116                                                                                |
| Evince PDF Viewer                      | 3.28.4-0ubuntu1.2                                                                       |
| FabulaTech USB for Remote Desktop      | 5.2.29                                                                                  |
| Firefox                                | 68.10.0                                                                                 |
| IBM iAccess Client Solutions           | 1.1.8.1                                                                                 |
| IGEL RDP Client                        | 2.2                                                                                     |
| IGEL WVD Client                        | 1.0.13igel1596142398                                                                    |
| Imprivata OneSign ProveID Embedded     | onesign-bootstrap-loader_1.0.523630_amd64<br><br>Qualification at Imprivata in progress |
| deviceTRUST RDP Channel                | 19.1.200.2                                                                              |
| NCP Secure Enterprise Client           | 5.10_rev40552                                                                           |
| NX Client                              | 6.11.2-1igel8                                                                           |
| Open VPN                               | 2.4.4-2ubuntu1.3                                                                        |
| Zulu JRE                               | 8.48.0.51-2                                                                             |
| Parallels Client (64 bit)              | 17.1.1                                                                                  |
| Spice GTK (Red Hat Virtualization)     | 0.38-2igel93                                                                            |
| Remote Viewer (Red Hat Virtualization) | 8.0-2git20191213.e4bach8igel83                                                          |
| Usbredir (Red Hat Virtualization)      | 0.8.0-1+b1igel71                                                                        |



|                                |                       |
|--------------------------------|-----------------------|
| Teradici PCoIP Software Client | 20.04.2-18.04         |
| ThinLinc Client                | 4.12.0-6517           |
| ThinPrint Client               | 7.5.88                |
| Totem Media Player             | 2.30.2                |
| Parole Media Player            | 1.0.5-1igel1583919770 |
| VNC Viewer                     | 1.10.1+dfsg-4igel13   |
| VMware Horizon Client          | 5.4.1-15988340        |
| Voip Client Ekiga              | 4.0.1                 |

## Dictation

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20200323 |
| Philips Speech driver                     | 12.9.1   |

## Signature

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.9    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.4.2    |

## Smartcard

|                                           |                |
|-------------------------------------------|----------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101        |
| PKCS#11 Library Athena IDProtect          | 7              |
| PKCS#11 Library cryptovision sc/interface | 7.3.1          |
| PKCS#11 Library Gemalto SafeNet           | 10.7.77        |
| PKCS#11 Library OpenSC                    | 0.20.0-3igel37 |



|                                    |                        |
|------------------------------------|------------------------|
| PKCS#11 Library SecMaker NetID     | 6.8.1.31               |
| PKCS#11 Library 90meter            | 20190522               |
| Reader Driver ACS CCID             | 1.1.6-1igel2           |
| Reader Driver Gemalto eToken       | 10.7.77                |
| Reader Driver HID Global Omnikey   | 4.3.3                  |
| Reader Driver Identive CCID        | 5.0.35                 |
| Reader Driver Identive eHealth200  | 1.0.5                  |
| Reader Driver Identive SCRKBC      | 5.0.24                 |
| Reader Driver MUSCLE CCID          | 1.4.31-1igel11         |
| Reader Driver REINER SCT cyberJack | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite        | 1.8.26-3igel14         |
| Cherry USB2LAN Proxy               | 3.2.0.3                |

## System Components

|                            |                               |
|----------------------------|-------------------------------|
| OpenSSL                    | 1.0.2n-1ubuntu5.3             |
| OpenSSL                    | 1.1.1-1ubuntu2.1~18.04.6      |
| OpenSSH Client             | 7.6p1-4ubuntu0.3              |
| OpenSSH Server             | 7.6p1-4ubuntu0.3              |
| Bluetooth stack (bluez)    | 5.52-1igel6                   |
| MESA OpenGL stack          | 20.0.8-1igel117               |
| VAAPI ABI Version          | 0.40                          |
| VDPAU Library version      | 1.4-1igel1003                 |
| Graphics Driver INTEL      | 2.99.917+git20200515-igel1013 |
| Graphics Driver ATI/RADEON | 19.1.0-1+git20200220igel987   |
| Graphics Driver ATI/AMDGPU | 19.1.0-1+git20200318igel986   |



|                                         |                                   |
|-----------------------------------------|-----------------------------------|
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867                   |
| Graphics Driver Nvidia                  | 440.100-0ubuntu0.20.04.1          |
| Graphics Driver VMware                  | 13.3.0-2igel857                   |
| Graphics Driver QXL (Spice)             | 0.1.5-2build2-igel925             |
| Graphics Driver FBDEV                   | 0.5.0-1igel819                    |
| Graphics Driver VESA                    | 2.4.0-1igel855                    |
| Input Driver Evdev                      | 2.10.6-1igel975                   |
| Input Driver Elographics                | 1.4.1-1+b6igel952                 |
| Input Driver eGalax                     | 2.5.7413                          |
| Input Driver Synaptics                  | 1.9.1-1ubuntu1igel866             |
| Input Driver VMMouse                    | 13.1.0-1ubuntu2igel957            |
| Input Driver Wacom                      | 0.36.1-0ubuntu2igel888            |
| Input Driver ELO Multitouch             | 3.0.0                             |
| Input Driver ELO Singletouch            | 5.1.0                             |
| Kernel                                  | 5.4.48 #mainline-lxos-g1595410170 |
| Xorg X11 Server                         | 1.20.8-2igel1016                  |
| Xorg Xephyr                             | 1.20.8-2igel1016                  |
| CUPS printing daemon                    | 2.2.7-1ubuntu2.8igel32            |
| PrinterLogic                            | 25.1.0.425                        |
| Lightdm Graphical Login Manager         | 1.26.0-0ubuntu1igel13             |
| XFCE4 Window Manager                    | 4.14.2-1~18.04igel1595331607      |
| ISC DHCP Client                         | 4.3.5-3ubuntu7.1                  |
| NetworkManager                          | 1.20.4-2ubuntu2.2igel100          |
| ModemManager                            | 1.10.0-1~ubuntu18.04.2            |
| GStreamer 0.10                          | 0.10.36-2ubuntu0.1igel201         |
| GStreamer 1.x                           | 1.16.2-4igel239                   |
| WebKit2Gtk                              | 2.28.3-2igel36                    |



|         |        |
|---------|--------|
| Python2 | 2.7.17 |
| Python3 | 3.6.9  |

## VM Guest Support Components

|                            |                          |
|----------------------------|--------------------------|
| Virtualbox Guest Utils     | 6.1.10-dfsg-1igel41      |
| Virtualbox X11 Guest Utils | 6.1.10-dfsg-1igel41      |
| Open VM Tools              | 11.0.5-4ubuntu0.18.04.13 |
| Open VM Desktop Tools      | 11.0.5-4ubuntu0.18.04.1  |
| Xen Guest Utilities        | 7.10.0-0ubuntu1          |
| Spice Vdagent              | 0.20.0-1igel95           |
| Qemu Guest Agent           | 5.0-5igel12              |

## Features with Limited IGEL Support

|                                    |                                     |
|------------------------------------|-------------------------------------|
| Mobile Device Access USB (MTP)     | 1.1.17-3igel5                       |
| Mobile Device Access USB (imobile) | 1.2.1~git20191129.9f79242-1+b1igel8 |
| Mobile Device Access USB (gphoto)  | 2.5.25-2igel4                       |
| VPN OpenConnect                    | 8.10-1igel4                         |
| Scanner support                    | 1.0.27-1                            |
| VirtualBox                         | 6.1.10-dfsg-1igel41                 |

## Services

| Service                                    | Size    | Reduced Firmware |
|--------------------------------------------|---------|------------------|
| Asian Language Support                     | 22.5 M  | Included         |
| Java SE Runtime Environment                | 36.0 M  | Included         |
| Citrix Workspace app                       | 219.5 M | Included         |
| Citrix Appliance                           |         |                  |
| Citrix StoreFront                          |         |                  |
| Ericom PowerTerm InterConnect              | 15.5 M  | Included         |
| Media Player                               | 512.0 K | Included         |
| Citrix Appliance                           | 70.2 M  | Included         |
| Local Browser (Firefox)                    |         |                  |
| RDP                                        | 4.2 M   | Included         |
| VMware Horizon                             |         |                  |
| Cendio ThinLinc                            | 10.0 M  | Included         |
| Printing (Internet printing protocol CUPS) | 22.2 M  | Included         |
| NoMachine NX                               | 26.8 M  | Included         |
| VMware Horizon                             | 114.5 M | Included         |



|                                            |         |              |
|--------------------------------------------|---------|--------------|
| Voice over IP (Ekiga)                      | 6.5 M   | Included     |
| Citrix Appliance                           | 768.0 K | Included     |
| NCP Enterprise VPN Client                  | 27.0 M  | Not included |
| Fluendo GStreamer Codec Plugins            | 6.8 M   | Included     |
| IBM i Access Client Solutions              | 72.5 M  | Not included |
| Red Hat Enterprise Virtualization          | 3.0 M   | Included     |
| Parallels Client                           | 5.5 M   | Included     |
| NVIDIA graphics driver                     | 115.0 M | Not included |
| Imprivata Appliance                        | 10.8 M  | Included     |
| Evidian AuthMgr                            | 2.8 M   | Included     |
| Hardware Video Acceleration                | 13.0 M  | Included     |
| Extra Font Package                         | 1.0 M   | Included     |
| Fluendo GStreamer AAC Decoder              | 1.2 M   | Included     |
| x32 Compatibility Support                  | 48.0 M  | Included     |
| Cisco JVDI client                          | 45.8 M  | Included     |
| PrinterLogic                               | 40.8 M  | Not included |
| Biosec BS Login                            | 10.0 M  | Not included |
| Login VSI Login Enterprise                 | 28.8 M  | Not included |
| Stratusphere UX CID Key software           | 2.8 M   | Not included |
| Elastic Filebeat                           | 15.8 M  | Not included |
| WVD                                        | 13.8 M  | Included     |
| Local Browser (Chromium)                   | 81.2 M  | Not included |
| deskMate client                            | 5.8 M   | Included     |
| Cisco Webex Teams VDI                      | 32.0 M  | Not included |
| Cisco Webex Meetings VDI                   | 36.8 M  | Not included |
| Zoom Media Plugin                          | 39.8 M  | Not included |
| Teradici PCoIP Client                      | 7.8 M   | Included     |
| 90meter Smart Card Support                 | 256.0 K | Included     |
| Mobile Device Access USB (Limited support) | 256.0 K | Not included |
| VPN OpenConnect (Limited support)          | 1.5 M   | Not included |
| Scanner support / SANE (Limited support)   | 2.5 M   | Not included |
| VirtualBox (Limited support)               | 62.5 M  | Not included |

## General Information 11.04.100

To be beneficial to all new features and implementations, it is recommended to use UMS 6.05.100 or higher and update the corresponding profiles.



Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

## Known Issues 11.04.100

### Firmware Update

- On **devices with 2 GB of flash storage**, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs and unused features must be disabled in IGEL Setup under **System > Firmware Customization > Features** to perform the firmware update. For instructions on how to prevent issues with updating, see [Adapting IGEL OS 11.04 or Higher for Devices with Small Storage](#)(see page 69).

### Firefox

- **Firefox IGEL extensions are not updated automatically** under some circumstances. After an update from 11.03.xxx to 11.04.100, the IGEL extensions will stay on the old version.  
In this case, the following settings concerning **kiosk mode** cannot be executed:
  - Switch off hotkey for new window/tab
  - Blocking of internal browser pages like preferences, file picker, specific local directories

As a workaround:

- a **reset to defaults** should be performed
- or the **browser's mimetype template** can be switched **from "Standard" to "Minimal"** by registry key `browserglobal.app.mimetypes_template`. There, the browser profile is renewed as well.  
After the TC received the new setting, **reboot** and **set** the `mimetypes_template` registry key to **"Standard"** again.

### Citrix

- With activated **DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.



- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1 and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix StoreFront login** with **Gemalto smartcard** middleware does not detect smartcard correctly if the card is inserted after start of login.  
Workaround: Insert the smartcard before starting the StoreFront login.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264** acceleration plugin, the following registry key must be enabled.

[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Value     | enabled / <u>disabled</u>                                        |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

- Using **CWA 19.x** sometimes **freezes the session** while session logoff from a published desktop.  
Workaround: **Use CWA 18.10.0**.
- During the running **Microsoft Teams Optimization of Citrix Workspace App 20.06, webcam redirection or screen sharing** may lead to **display errors** like black stripes or flickering.
- The **performance** of Citrix sessions when using **Workspace App 20.06** may be lower on some devices.  
A possible **workaround** is to **disable the virtual channels for Microsoft Teams** and **NSAP** or to set the **HDX transport protocol** to **TCP** only.
  - ica.module.virtualdriver.vdwebrtc.enable
  - ica.module.virtualdriver.nsap.enable
  - The protocol can be set via the Setup parameter **Sessions > Citrix > Citrix Global > Options > HDX Adaptive Transport over EDT** or via the **server policy** 'HDX Adaptive Transport'.

#### VMware Horizon

- **Client drive mapping** and **USB redirection** for storage devices should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself.



Enable local `Storage Hotplug` on Setup page **Devices > Storage Devices > Storage Hotplug**.

- **External drives** mounted already before connection do not appear in the **remote desktop**.  
Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- **After the disconnect of an RDP-based session**, the Horizon main **window** which contains the server or sessions overview **cannot be resized anymore**.
- **Seamless application windows in Horizon Client may not be displayed correctly**. When starting the first seamless app, a new iconified window appears in the taskbar, and only if you click on it, the application will show up.  
On some hardware (UD7-H850, UD2-M250, UD2-D220), however, the client aborts when this new window is de-iconified.

#### Imprivata

- On **devices with 2 GB of flash storage**, it could happen that there is not enough space to enable the **Imprivata partition after the update to 11.04.100**. In this case, a corresponding error message occurs and **unused features must be disabled** (in IGEL Setup under **System > Firmware Customization > Features**). Imprivata has to be (re-)enabled after a reboot then.

#### Wi-Fi

- TP-Link Archer T2UH Wi-Fi adapters does not work after system suspend/resume. Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

#### Parallels Client

- **Native USB redirection** does not work with Parallels Client.

#### Smartcard

- **Citrix Certificate Identity Declaration login** does not work with **SecMaker** smartcards.
- In seldom cases, the **authentication** hung when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice: spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

#### Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.

#### Hyper-V

- **Hyper-V** (Generation 2) needs **a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.

#### VirtualBox

- The current **VirtualBox Guest Tools/Drivers** will not work with **VirtualBox 5.2.x or older** hosts which leads to a black screen and non-working graphics.

Possible workaround: Install with 'Failsafe Installation + Recovery' and set the registry key `x.drivers.force_vesa` to 'true'.



- When running in VirtualBox virtualization, **resizing the window will not automatically change desktop resolution** of IGEL OS guest.

#### Audio

- **Audio jack detection on Advantech POC-W243L** doesn't work. Therefore, sound output goes through a possibly connected headset and the internal speakers.
- **IGEL UD2 (D220)** fails to restore the volume level of the speaker when the device used **firmware version 11.01.110** before.

#### Hardware

- **HP t730** could freeze when monitors with **different resolutions** are connected (1920x1200 + 2560x1440 + 3840x1600 for example). When this occurs, the registry key `x.drivers.kms.best_console_mode` has to be set to **disabled**.
- Some newer **Delock 62599 active DisplayPort-to-DVI (4k)** adapters only work with INTEL devices.

#### Remote Management

- **AIT feature with IGEL Starter License is supported** by the **UMS version 6.05.100**.

#### Base system

- **Update from memory stick** requires network online state (when multiple update stages are involved).

#### deskMate

- Integrated deskMate solution. Some stability issues may remain.

## Security Fixes 11.04.100

#### Firefox

- Updated Mozilla **Firefox** to **68.10.0esr**:
  - Fixes for **mfsa2020-11**, also known as CVE-2020-6819 and CVE-2020-6820
  - Fixes for **mfsa2020-13**, also known as:  
[More...](#)  
CVE-2020-6828, CVE-2020-6827, CVE-2020-6821, CVE-2020-6822, and CVE-2020-6825
  - Fixes for **mfsa2020-17** also known as:  
[More...](#)  
CVE-2020-12387, CVE-2020-12388, CVE-2020-12389, CVE-2020-6831, CVE-2020-12392, CVE-2020-12393, and CVE-2020-1239
  - Fixes for **mfsa2020-21** also known as:  
[More...](#)  
CVE-2020-12399, CVE-2020-12405, CVE-2020-12406, and CVE-2020-12410
  - Fixes for **mfsa2020-25** also known as:



[More...](#)

CVE-2020-12417, CVE-2020-12418, CVE-2020-12419,  
CVE-2020-12420, and CVE-2020-12421

- Changed option to **deny local file browsing** via file:// URI per default now.

[More...](#)

|            |                                                                |
|------------|----------------------------------------------------------------|
| IGEL Setup | <b>Firefox Browser &gt; Firefox Browser Global &gt; Window</b> |
| Parameter  | Hide local filesystem                                          |
| Registry   | browserglobal.app.filepicker_dialog_hidden                     |
| Value      | <u>enabled</u> / disabled                                      |

Base system

- SSH protocol version 1 is now disabled.** All remote connections via SSH must use SSHv2.

Driver

- Updated **Nvidia driver** to version **440.100**.

New Features 11.04.100

Citrix

- Integrated **Citrix Workspace App 20.06**. Available Citrix Workspace Apps in this release: **20.06** (default), **19.12**, and **18.10**
- Added a registry key to enable optimization for **Microsoft Teams**.

[More...](#)

|            |                                                                                               |
|------------|-----------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; VDI Solutions</b> |
| Parameter  | Microsoft Teams optimization                                                                  |
| Registry   | ica.module.virtualdriver.vdwebrtc.enable                                                      |
| Value      | <u>on</u> / off                                                                               |

- Added a registry key to enable support for **NetScaler App Experience (NSAP)** virtual channel.

[More...](#)

|           |                                      |
|-----------|--------------------------------------|
| Parameter | HDX uses the NSAP virtual channel    |
| Registry  | ica.module.virtualdriver.nsap.enable |
| Value     | <u>on</u> / off                      |

- Integrated **Citrix HDX/RTME 2.9**.
- Integrated **ZOOM Media Plugin for Citrix** to optimize performance for ZOOM video calls and conferences.
- IGEL x64: 5.0.415463.0619 requires Windows x86 or x64: 5.0.24002.0619. <https://support.zoom.us/hc/en-us/articles/360031096531-Getting-Started-with-VDI>

[More...](#)



|            |                                                                                               |
|------------|-----------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; VDI Solutions</b> |
| Parameter  | Zoom Media Plugin                                                                             |
| Registry   | ica.module.virtualdriver.vdzoom.enable                                                        |
| Value      | <u>enabled</u> / <u>disabled</u>                                                              |

- Updated **signotec Virtual Channel** to version **8.0.9**.

The corresponding changes are:

- Logging has been improved.
- A problem with the communication with the signature pads was fixed.
- USB communication via bulk transfer is model-independent (improved speed).
- Removed parameter **Content redirection** / ica.wfclient.crenabled from TC Setup (**Sessions > Citrix > Citrix Global > HDX Multimedia**).

#### OSC Installer

- Added **dialog "Feature Selection"** in **IGEL OS Creator** for the selection of features to be installed on the target device. It interactively shows if the current selection of features fits onto the device. The selection of features is saved on the OSC installer medium (when allowed) and set as the default selection for the next installation. If "**Migrate Old Settings**" is selected, the set of features of the old installation is set as the default selection.
- Reduced memory requirements** of OSC installer for **machines without Nvidia graphic card**.

#### WVD

- Added **AAC Codec support** to Audio Output redirection.  
[More...](#)

|          |                                  |
|----------|----------------------------------|
| Registry | sessions.wvd%.options.enable-aac |
| Value    | <u>enabled</u> / <u>disabled</u> |

#### RDP/IGEL RDP Client 2

- Added the **possibility to add a black background** to the RDP auto-reconnect window.  
[More...](#)

|          |                                                 |
|----------|-------------------------------------------------|
| Registry | sessions.rdp.options.reconnect-black-fullscreen |
| Type     | bool                                            |
| Value    | <u>enabled</u> / <u>disabled</u>                |

- Added configuration option for the **amount of RDP auto-reconnect retries**. The default value will remain "20". A value of "0" means infinite retries.

[More...](#)

|          |                                                        |
|----------|--------------------------------------------------------|
| Registry | sessions.rdp.winconnect%.options.reconnect-max-retries |
| Type     | Integer                                                |



|       |           |
|-------|-----------|
| Value | <u>20</u> |
|-------|-----------|

## VMware Horizon

- Updated **VMware Horizon** to version **5.4.1**.

For usage with **Blast protocol**, it is recommended to enable **DRI3 graphics mode**:  
[More...](#)

|           |                                  |
|-----------|----------------------------------|
| Parameter | Use DRI3                         |
| Registry  | x.driver.use_dri3                |
| Value     | <u>enabled</u> / <u>disabled</u> |

- Fixed **handling of RDP's fullscreen mode span**, which means to combine all local monitors for one big remote session.

## PowerTerm

- Updated **Ericom PowerTerm** LTC to version **14.0.0.45623**.

## Parallels Client

- Updated **Parallels Client** to version **17.1.1**.

## Teradici PCoIP Client

- Updated **Teradici PCoIP** Client to version **20.04.2-18.04**. The new version supports **hardware-accelerated H.264 decoding with Ultra PCoIP**.
- New parameters:  
[More...](#)

|           |                                                      |
|-----------|------------------------------------------------------|
| Parameter | Log level                                            |
| Registry  | pcoip.log-level                                      |
| Value     | <u>0</u> / <u>1</u> / <u>2</u> / <u>3</u> / <u>4</u> |

PCoIP sessions **can now use the global setting**.

[More...](#)

|           |                                                                                                                                                                                                        |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter | Show codec indicator                                                                                                                                                                                   |
| Registry  | pcoip.codec_indicator                                                                                                                                                                                  |
| Value     | <u>disabled</u> / enabled                                                                                                                                                                              |
| Info      | Show a small dot in the bottom left corner during the session to indicate which codec is being used. Green indicates simple codec; blue indicates tic2 codec. This setting is only available globally. |

## XEN

- Added support to run as **XEN guest system**.



## NX client

- Updated **NoMachine NX Client** to version **6.11.2**.

## ThinLinc

- Updated **ThinLinc** to version **4.12**.

## Network

- **DHCP changes:**

The system now sends a **vendor-class-identifier(option 60)** "igel-dhcp-1". Furthermore, it requests **vendor-encapsulated-options (43)**. Those can be used to transfer IGEL-specific options **igelrmserver(224)** and **umsstructuretag(226)** in the vendor namespace (with the same option numbers and types) instead of in the global namespace.

The former way is also still functional, but values transferred in the new way override those which were transferred the old way.

Apart from 224 and 226 one more option is defined in the vendor space: "**exclusive**", **option 1, type byte**. Its presence means that global options 224 and 226 shall not be interpreted in the traditional way and only settings in the vendor space apply.

IPv6 is not involved.

- Added support for **LTE module HP lt4132**.
- Updated **Network Manager** to version **1.20.4**.
  - The range of **network.interfaces.wirelesslan.device0.bgscan.module** now includes "**default**" for using original upstream Network Manager settings.
- Added some **additional Ethernet network drivers**.

**More...**

- amd-xgbe : AMD 10 Gigabit Ethernet driver
- ec\_bhf : Beckhoff EtherCAT
- liquidio\_vf : Cavium LiquidIO Intelligent Server Adapter Virtual Function driver
- liquidio : Cavium LiquidIO Intelligent Server Adapter driver
- thunder\_bgx : Cavium Thunder BGX/MAC driver
- nicvf : Cavium Thunder NIC Virtual Function driver
- nicpf : Cavium Thunder NIC Physical Function driver
- thunder\_xcv : Cavium Thunder RGX/XCV driver
- atlantic : aQuantia Corporation(R) network driver
- be2net : Emulex OneConnect NIC driver 12.0.0.0
- ixgb : Intel(R) PRO/10GbE network driver
- igc : Intel(R) 2.5G Ethernet Linux driver
- ice : Intel(R) Ethernet Connection E800 Series Linux driver
- i40e : Intel(R) Ethernet Connection XL710 network driver
- iavf : Intel(R) Ethernet Adaptive Virtual Function network driver
- ixgbe : Intel(R) 10 Gigabit PCI Express network driver
- igbvf : Intel(R) Gigabit Virtual Function network driver
- ixgbefv : Intel(R) 10 Gigabit Virtual Function network driver
- ena : Elastic Network Adapter (ENA)
- nfp : The Netronome Flow Processor (NFP) driver
- bna : QLogic BR-series 10G PCIe Ethernet driver
- enic : Cisco VIC Ethernet NIC driver



- mlx5\_core : Mellanox 5th generation network adapters (ConnectX series) core driver
  - mlx4\_en : Mellanox ConnectX HCA Ethernet driver
  - ionic : Pensando Ethernet NIC driver
  - sfc-falcon : Solarflare Falcon network driver
  - sfc : Solarflare network driver
  - dwc-xlgmac : Synopsys DWC XLGMAC driver
  - hinic : Huawei Intelligent NIC driver
  - cassini : Sun Cassini Ethernet driver
  - niu : NIU Ethernet driver
  - samsung-sxgb : SAMSUNG 10G/2.5G/1G Ethernet PLATFORM driver
  - cxgb : Chelsio 10Gb Ethernet driver
  - qede : QLogic FastLinQ 4xxxx Ethernet driver
  - qlcnic : QLogic 1/10 GbE Converged/Intelligent Ethernet driver
  - qed : QLogic FastLinQ 4xxxx Core module
  - netxen\_nic : QLogic/NetXen (1/10) GbE Intelligent Ethernet driver
  - vxge : Neterion's X3100 Series 10GbE PCIe I/OVirtualized Server adapter
  - myri10ge : Myricom 10G driver (10GbE)
  - tehuti : Tehuti Networks(R) network driver
  - bnxt\_en : Broadcom BCM573xx network driver
  - bnx2x : QLogic BCM57710/57711/57711E/57712/57712\_MF/57800/57800\_MF/57810/57810\_MF/57840/57840\_MF driver
  - Added a registry key for specifying a **space-separated list of DNS resolver options**. See "**man resolv.conf**".
- More...**

| Parameter | Option list         |
|-----------|---------------------|
| Registry  | network.dns.options |
| Type      | string              |
| Value     | <u>empty</u>        |

## Wi-Fi

- Added support for **WPA3 Personal network authentication**.
  - Added a registry key for **preferring WPA3 Personal** (i.e. SAE) or **WPA2 Personal** at the time a connection is created with Wireless Manager when the access point offers both:
- More...**

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Prefer WPA3 Personal to WPA2 Personal |
| Registry  | network.applet.wireless.prefer_sae    |
| Range     | [default] [yes] [no]                  |
| Info      | "default" currently means "no"        |

- Added **captive portal support for Wi-Fi**. Passing through a captive portal (which is basically a web application) is sometimes **necessary to achieve full network connectivity** (here also referred to as online state).



- The **feature is disabled when** the following **registry key** is **empty**. Otherwise, it should be a **URI** that is **suitable for NetworkManager connectivity check**.

[More...](#)

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Online check URI                             |
| Registry  | network.global.onlinecheck.uri               |
| Range     | [] [http://connectivity-check.ubuntu.com/]   |
| Value     | <u>http://connectivity-check.ubuntu.com/</u> |

- The following key specifies the **conditions of the online check**. It is also required that **no Ethernet cable is plugged in** and **DHCP is not set** in the UMS.

[More...](#)

|           |                                                                      |
|-----------|----------------------------------------------------------------------|
| Parameter | Condition for online check                                           |
| Registry  | network.global.onlinecheck.condition                                 |
| Range     | [None] [ <u>Network is user-defined</u> ] [ <u>Network is open</u> ] |

- This key determines **how many seconds to wait for full network connectivity** before the network connection is considered complete with incomplete connectivity. The timeout should allow a user to do what is necessary for passing through the captive portal.

[More...](#)

|           |                                    |
|-----------|------------------------------------|
| Parameter | Online check timeout               |
| Registry  | network.global.onlinecheck.timeout |
| Type      | integer                            |
| Value     | <u>120</u>                         |

- Enabled **use of 802.11r**, also known as **fast BSS transition** or FT. This is confirmed to work at least in the **mode "over the air"**.

## Smartcard

- Updated **OpenSC** to version **0.20.0**. See <https://github.com/OpenSC/OpenSC/releases/tag/0.20.0> for detailed release notes.

## Cisco JVDI Client

- Updated **Cisco JVDI** client to version **12.9.0**.

## Cisco Webex VDI

- Integrated the new feature **Cisco Webex Teams VDI for Citrix** and **Horizon** sessions.  
**Cisco Webex Teams** version: **3.0.15711.0**
- Added a parameter to activate the feature within **Citrix**:  
[More...](#)

|            |                                                                                       |
|------------|---------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; Cisco</b> |
| Parameter  | Cisco Webex Teams VDI                                                                 |
| Registry   | ica.module.virtualdriver.vdciscoteams.enable                                          |
| Value      | <u>enabled</u> / <u>disabled</u>                                                      |

- Added a parameter to activate the feature within **VMware**:



[More...](#)

|            |                                                                                                |
|------------|------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Horizon &gt; Horizon Client Global &gt; Unified Communications &gt; Cisco</b> |
| Parameter  | Cisco Webex Teams VDI - Horizon                                                                |
| Registry   | vmware.view.vdciscoteams.enable                                                                |
| Value      | enabled / <u>disabled</u>                                                                      |

- Integrated the new feature **Cisco Webex Meetings VDI for Citrix** sessions.

Client Version: **40.7.0.375**

- Added a parameter to activate the feature within **Citrix**:

[More...](#)

|            |                                                                                       |
|------------|---------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; Cisco</b> |
| Parameter  | Cisco Webex Meetings VDI                                                              |
| Registry   | ica.module.virtualdriver.vdciscomeetings.enable                                       |
| Value      | enabled / <u>disabled</u>                                                             |

Base system

- Updated base system to **Ubuntu LTS** version **18.04**.
- Updated **kernel** to version **5.4.48**.
- Added **notification for critical system out-of-memory state** when the available **system memory is lower than 40 MB** and **processes were killed** to prevent the system from freezing.
- Display **AMD Memory Guard in Boot Mode** when it's active.
- Added **notification option for Session Autostart** when a autostart delay is configured. It is possible to cancel the session autostart or to start immediately.

[More...](#)

|            |                                   |
|------------|-----------------------------------|
| IGEL Setup | <b>* &gt; Desktop integration</b> |
| Parameter  | Autostart notification            |
| Value      | enabled / <u>disabled</u>         |

- Added correct **UI handling** for **Wacom DTU-1141B**.
- Updated **CA Certificates** to version **20190122** (Mozilla authority bundle version **2.30**). The following authorities were added:

[More...](#)

- "Certigna Root CA"
- "GTS Root R1"
- "GTS Root R2"
- "GTS Root R3"
- "GTS Root R4"
- "UCA Extended Validation Root"
- "UCA Global G2 Root"
- "GlobalSign Root CA - R6"
- "OISTE WISEKey Global Root GC CA"
- "GDCA TrustAUTH R5 ROOT"



- "SSL.com EV Root Certification Authority ECC"
- "SSL.com EV Root Certification Authority RSA R2"
- "SSL.com Root Certification Authority ECC"
- "SSL.com Root Certification Authority RSA"
- "TrustCor ECA-1"
- "TrustCor RootCert CA-1"
- "TrustCor RootCert CA-2"
- The following authorities were removed:  
**More...**
  - "Certplus Root CA G1"
  - "Certplus Root CA G2"
  - "OpenTrust Root CA G1"
  - "OpenTrust Root CA G2"
  - "OpenTrust Root CA G3"
  - "TÜRKTRUST Elektronik Sertifika Hizmet Saglayicisi H5"
  - "Visa eCommerce Root"
  - "ACEDICOM Root"
  - "AddTrust Low-Value Services Root"
  - "AddTrust Public Services Root"
  - "AddTrust Qualified Certificates Root"
  - "CA Disig Root R1"
  - "CNNIC ROOT"
  - "Camerfirma Chambers of Commerce Root"
  - "Camerfirma Global Chambersign Root"
  - "Certinomis - Autorit, Racine"
  - "Certum Root CA"
  - "China Internet Network Information Center EV Certificates Root"
  - "Comodo Secure Services root"
  - "Comodo Trusted Services root"
  - "DST ACES CA X6"
  - "GeoTrust Global CA 2"
  - "PSCPProcert"
  - "Security Communication EV RootCA1"
  - "Swisscom Root CA 1"
  - "Swisscom Root CA 2"
  - "Swisscom Root EV CA 2"
  - "TÜRKTRUST Certificate Services Provider Root 2007"
  - "TUBITAK UEKAE Kok Sertifika Hizmet Saglayicisi - Surum 3"
  - "UTN USERFirst Hardware Root CA"
- Added parameter to override **rate limit of debug messages** in journal. It should be enabled for debugging processes which generate a big amount of messages in order to avoid skipping of messages.  
**More...**

|           |                               |
|-----------|-------------------------------|
| Parameter | No rate limit                 |
| Registry  | system.journald.no_rate_limit |



|       |                    |
|-------|--------------------|
| Value | enabled / disabled |
|-------|--------------------|

- It's possible to **extend the login options of the Kerberos** login window now.

There are several new registry keys:

[More...](#)

|           |                                                |
|-----------|------------------------------------------------|
| Parameter | extended login                                 |
| Registry  | sessions.xlock0.options.login_extension_active |
| Value     | enabled / disabled                             |

If enabled, an "**Associate Type**" **combo box** is shown. The **entries of the combo box** are configured with the following **login\_feature1**, **login\_feature2**, and **login\_feature3** keys.

- Configure the **label of the "Associate Type" combo box**:

[More...](#)

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | login features label                         |
| Registry  | sessions.xlock0.options.login_features_label |
| Value     | Default: empty which means "Associate Type"  |

- The first entry of the "Associate Type" combo box.** To enable the combo box entry, add e.g. the text "Store associate at home store".

[More...](#)

|           |                                        |
|-----------|----------------------------------------|
| Parameter | login_feature1                         |
| Registry  | sessions.xlock0.options.login_feature1 |

**If the entry is selected, the username is expanded by a fixed string** defined in `login_extension_default` registry key.

- The fixed username extension** for the first feature. It can be set e.g. by a script.

[More...](#)

|           |                                                 |
|-----------|-------------------------------------------------|
| Parameter | login extension default value                   |
| Registry  | sessions.xlock0.options.login_extension_default |

- The second entry of the "Associate Type" combo box.** To enable the combo box entry, add e.g. the text "Store associate visiting this store".

[More...](#)

|           |                                        |
|-----------|----------------------------------------|
| Parameter | login_feature2                         |
| Registry  | sessions.xlock0.options.login_feature2 |

**If the entry is selected, the username is expanded by a suffix** that is **entered in a separate entry widget**.

- The label of the entry field for the username suffix.** Set it e.g. to "Store Number".

[More...](#)

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | login_extension_label                         |
| Registry  | sessions.xlock0.options.login_extension_label |
| Value     | Default: empty which means "no label"         |



- **The third entry of the "Associate Type" combo box.** To enable the combo box entry, add e.g. the text "Homeoffice associate visiting this store".

[More...](#)

|           |                                        |
|-----------|----------------------------------------|
| Parameter | login_feature3                         |
| Registry  | sessions.xlock0.options.login_feature3 |

**If the entry is selected, another domain can be selected from an appended domain combo box.**

- The **label for the domain entry field.**

[More...](#)

|           |                                            |
|-----------|--------------------------------------------|
| Parameter | login domain label                         |
| Registry  | sessions.xlock0.options.login_domain_label |
| Value     | Default: empty which means "domain"        |

- The **extension to the username is added after a dot ('.')**.

- For the **domain drop-down box, four different domains are configurable** here:

[More...](#)

|            |                                                                  |
|------------|------------------------------------------------------------------|
| IGEL Setup | <b>Security &gt; Active Directory/Kerberos &gt; Domain 1 - 4</b> |
| Parameter  | Fully qualified domain name                                      |
| Registry   | auth.krb5.realms.realm0.realm                                    |
| Registry   | auth.krb5.realms.realm1.realm                                    |
| Registry   | auth.krb5.realms.realm2.realm                                    |
| Registry   | auth.krb5.realms.realm3.realm                                    |

- There are keys to **add more domain names:**

[More...](#)

|           |                                           |
|-----------|-------------------------------------------|
| Parameter | Domain                                    |
| Registry  | auth.krb5.extended_domain%.name           |
| Info      | Add a new instance for each domain entry. |

- In the Kerberos login window, it's now possible to turn on or off **numlock** and/or **capslock for password input.**

Registry keys:

[More...](#)

|           |                                                                                                              |
|-----------|--------------------------------------------------------------------------------------------------------------|
| Parameter | Handling of numlock                                                                                          |
| Registry  | sessions.xlock0.options.numlock_approach                                                                     |
| Range     | [don't change] [set on] [set off]                                                                            |
| Info      | "set on": force numlock on when password is entered<br>"set off": force numlock off when password is entered |
| Parameter | Handling of capslock                                                                                         |
| Registry  | sessions.xlock0.options.capslock_approach                                                                    |
| Range     | [don't change] [set on] [set off]                                                                            |



|      |                                                                                                                |
|------|----------------------------------------------------------------------------------------------------------------|
| Info | "set on": force capslock on when password is entered<br>"set off": force capslock off when password is entered |
|------|----------------------------------------------------------------------------------------------------------------|

- It's now possible to **show a message in the Kerberos login window**. Registry key:  
[More...](#)

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | banner text                                      |
| Registry  | sessions.xlock0.options.banner_text              |
| Info      | The user will see the message on the top border. |

- In the Kerberos login window, there is a **mode to convert passwords always to upper case**. To turn it on, use:  
[More...](#)

|           |                                                   |
|-----------|---------------------------------------------------|
| Parameter | case-insensitive password                         |
| Registry  | sessions.xlock0.options.case_insensitive_password |
| Value     | enabled / <u>disabled</u>                         |

- With this key, the text for the **case-insensitive indicator** can be modified:  
[More...](#)

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | case-insensitive text                         |
| Registry  | sessions.xlock0.options.case_insensitive_text |
| Value     | Default: empty which means "case-insensitive" |

- Fixed **ThinkPad Brazil keyboard layout**.
- It is possible to **show a custom logo** in the Kerberos login window. Also, the **background and text color is customizable** now.

Registry keys:

[More...](#)

|           |                                                |
|-----------|------------------------------------------------|
| Parameter | path for login image                           |
| Registry  | sessions.xlock0.options.login_image            |
| Value     | /usr/share/pixmaps/greeter-user.svg            |
| Info      | Supported image formats include: PNG, JPG, SVG |

|           |                                   |
|-----------|-----------------------------------|
| Parameter | set specific colors for greeter   |
| Registry  | sessions.xlock0.options.set_color |
| Value     | enabled / <u>disabled</u>         |

|           |                                    |
|-----------|------------------------------------|
| Parameter | text color                         |
| Registry  | sessions.xlock0.options.text_color |
| Value     | #ffffffff                          |

|      |                                                      |
|------|------------------------------------------------------|
| Info | Text color in the format #rrggbb<br>Example: #ff0077 |
|------|------------------------------------------------------|

|           |                                          |
|-----------|------------------------------------------|
| Parameter | background color                         |
| Registry  | sessions.xlock0.options.background_color |



|       |                                                           |
|-------|-----------------------------------------------------------|
| Value | #000000                                                   |
| Info  | Background color in the format #rrggb<br>Example: #7700ff |

- Added **new local logon method "Login with Smart Card Certificate"**. It implements the **pam\_pkcs11 smartcard authentication module**. For a successful configuration, the following has to be provided via **UMS file transfer**:
  - **root and intermediate CA certificates** for verification of the client certificates in folder /etc/pam\_pkcs11/cacerts
  - file /etc/pam\_pkcs11/cn\_map which contains **mappings of Common Names to UPN names**.
    - Each line is in the format \<common name> -> \<logon name>  
where
    - \<common name> is the common name part of the subject of the certificate
    - \<logon name> is
    - in case of **Kerberos Enterprise** (auth.login.krb5\_enterprise) **disabled**: the UPN name of the SubjectAltName extension of the certificate, e.g. user@MY.DOMAIN
    - in case of **Kerberos Enterprise** (auth.login.krb5\_enterprise) **enabled**: the UPN name of the SubjectAltName extension of the certificate with Default Domain (auth.krb5.libdefaults.default\_realm) suffix, e.g. user@[DOMAIN.SUFFIX@DEFAULT.DOMAIN](mailto:DOMAIN.SUFFIX@DEFAULT.DOMAIN)<sup>404</sup>
- The logon method **can either be used standalone or together with Kerberos logon** as a fallback if Kerberos does not succeed.

[More...](#)

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | Login with Smart Card Certificate                |
| Registry  | auth.login.pkcs11                                |
| Value     | <u>false</u> / true                              |
| Parameter | Certificate verification policy                  |
| Registry  | auth.login.pkcs11_cert_policy                    |
| Value     | <u>ca,ocsp_on_signature</u>                      |
| Parameter | Enable Debugging of Smart Card Certificate Logon |
| Registry  | auth.login.pkcs11_debug                          |
| Value     | <u>false</u> / true                              |

- It is possible to expand the store number by a registry key:  
[More...](#)

|           |                                      |
|-----------|--------------------------------------|
| Parameter | expand store                         |
| Registry  | sessions.xlock0.options.expand_store |
| Value     | <u>enabled</u> / <u>disabled</u>     |

- Fixed: The **login screen is adjusted to lower resolutions**.
- It is possible to activate enter key to login on all fields.

<sup>404</sup> mailto:DOMAIN.SUFFIX@DEFAULT.DOMAIN



[More...](#)

|           |                                    |
|-----------|------------------------------------|
| Parameter | auto login on all fields           |
| Registry  | sessions.xlock0.options.auto_login |
| Value     | enabled / <u>disabled</u>          |

X11 system

- Changed: Use **modesetting graphics driver** on **devices with newer intel GPUs**.
- Changed registry key:

[More...](#)

|           |                                                   |
|-----------|---------------------------------------------------|
| Parameter | Use generic modesetting driver for INTEL hardware |
| Registry  | x.drivers.intel.use_modesetting                   |
| Range     | [Auto] [True] [False]                             |

- Updated **DisplayLink driver** to version **5.3.1.34**.
- Added new registry key for **Nvidia cards** (use this **if you want to use PRIME**):

[More...](#)

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | Enable/Disable NVIDIA Kernel Modesetting support |
| Registry  | x.drivers.nvidia.use_modeset                     |
| Range     | [Default] [Enabled] [Disabled]                   |
| Info      | "Default" is currently the same as "disabled"    |

- Updated **florence soft keyboard** to version **0.6.3**.
- **Removed 640x480** from possible **display resolution range**.
- Added possibility to **change the order of primary** and **secondary graphic card**.

New registry key:

[More...](#)

|           |                                                    |
|-----------|----------------------------------------------------|
| Parameter | Make the secondary graphic card to the primary one |
| Registry  | x.drivers.swap_card0_with_card1                    |
| Value     | true / <u>false</u>                                |

- Added possibility to **invert the order of all graphic cards**.

New registry key:

[More...](#)

|           |                                      |
|-----------|--------------------------------------|
| Parameter | Invert default graphic card ordering |
| Registry  | x.drivers.swap_all                   |
| Value     | true / <u>false</u>                  |

- Added possibility to **choose the driver** which should become **the primary graphic card**.

New registry key:

[More...](#)

|           |                                                                             |
|-----------|-----------------------------------------------------------------------------|
| Parameter | Choose which drivers should be preferred to become the primary graphic card |
| Registry  | x.drivers.preferred_driver                                                  |
| Value     |                                                                             |



## X server

- Added possibility to influence **mode used for mirroring screens with different resolutions.** (Notice: here scaling may not always work).

New registry key:

[More...](#)

|           |                                                                                   |
|-----------|-----------------------------------------------------------------------------------|
| Parameter | Choose the mode which should be used for mirroring monitors if resolution differs |
| Registry  | x.xserver0.mirror_mode                                                            |
| Range     | [Default] [Biggest common resolution] [Scaling]                                   |
| Value     | Default (use panning if needed)                                                   |

## Driver

- Updated **Grundig Dictation driver for Citrix and RDP** to version **0.10**.

The changes are:

- Support **third-party USB HID devices** in a more flexible way
- Fixed USB transfer overflow for **Philips LFH 9620**
- Remove **erroneous debug output** in release configuration
- Allow to **control** also "**Headphone**" **volume & switches**

- Updated **Olympus driver for dictation** to version **2020-03-23-143654**.

[Changelog](#):

New:

- DR-1200: PID 0225
- DR-2300: PID 0256

Changed:

- PID 0253 from DR-2100 to DR-1200

- Updated **Philips Speech driver** to version **G12.9**.

The changes are:

- Support for **Philips SpeechLive**
- Faster and more reliable remote session connection status check
- Shutdown of the PSPDispatcher.exe** on the server if it's not in use anymore.

- Updated **StepOver TCP client** and **Citrix plugin** to version **2.4.2**. Fixed **crash of Citrix** session while **using the signature pad**.

## Audio

- Integrated **new sound mixer**.
- New combo box for **audio device selection in TC Setup** available:
  - Accessories > Sound Preferences > Options > Default Sound Output**
  - Accessories > Sound Preferences > Options > Default Sound Input**

## Appliance Mode

- Integrated: The **new Browser Appliance mode** is the successor for the XenDesktop appliance mode. The Browser is configured as in XenDesktop appliance mode, but **does not use the upstream SAS window**.

[More...](#)



|            |                                                  |
|------------|--------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b>              |
| Parameter  | Browser                                          |
| Registry   | xen.xenapp-morph.enabled                         |
| Type       | Bool                                             |
| Value      | enabled / <u>disabled</u>                        |
| IGEL Setup | <b>Sessions &gt; Appliance Mode &gt; Browser</b> |
| Parameter  | Web URL                                          |
| Registry   | xen.xenapp-morph.xendeliveryserverurl            |
| Type       | string                                           |

- A **hyperlink to the "On-screen Keyboard"** is available on the right side under "Related Configurations".

## Multimedia

- Added **ffmpeg support** for following codecs:
  - Added support for **new decoders:**
[More...](#)

flac, gif, libaom\_av1, mjpeg, mjpegb,  
mp1, mp1float, mp2, mp3, mp3adu,  
mp3adufloat, mp3float, opus, theora, vorbis,  
vp2, vp8, vp9, and wavepack
  - Added support for **new encoder:** libopus
  - Added support for **new hwaccels:**
[More...](#)

mjpeg\_vaapi, mpeg1\_vdpau, mpeg2\_vaapi,  
mpeg2\_vdpau, vp8\_vaapi, and vp9\_vaapi
  - Added support for **new parsers:** avi, flac, gif, matroska, mp3, ogg, and wav
  - Added support for **new demuxers:** avi, flac, gif, matroska, ogg, and wav
  - Added support for **new muxers:** ogg and opus

## Chromium Browser

- Integrated **Chromium** browser version **83.0.4103.61** as experimental feature.  
Configurable at **IGEL Setup > Sessions > Chromium Browser > Chromium Browser Global** and **IGEL Setup > Sessions > Chromium Browser > Chromium Browser Sessions**
- Main switch to enable and disable **IGEL configuration:**
[More...](#)

|            |                                                                    |
|------------|--------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Chromium Browser &gt; Chromium Browser Global</b> |
| Parameter  | Use IGEL Setup for configuration                                   |
| Registry   | chromiumglobal.app.igelsetupconfig                                 |
| Value      | disabled / <u>enabled</u>                                          |



|      |                                                                                                                                                                                                                                                                                     |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Info | With disabled IGEL configuration, you can use the generic Custom Setup to configure Chromium.<br>The Custom Setup can be found at <b>IGEL Setup &gt; Sessions &gt; Chromium Browser &gt; Chromium Browser Global &gt; Custom Setup: Policies, Preferences, Commandline Options.</b> |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

- Parameter for **enabling** and **disabling** the **H.264 decoding**:  
[More...](#)

|            |                                                                                                                                |
|------------|--------------------------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Chromium Browser &gt; Chromium Browser Global</b>                                                             |
| Parameter  | H.264 decoding                                                                                                                 |
| Registry   | chromiumglobal.app.h264_decoding                                                                                               |
| Value      | <u>enabled</u> / <u>disabled</u>                                                                                               |
| Info       | Enable Audio/Video playback of non-free codecs (H.264+AAC) - the support is in a beta state and therefore disabled by default. |

## Evidian

- Added the Evidian **built-in option 'Process To Spy'**.  
[More...](#)

|          |                                       |
|----------|---------------------------------------|
| Registry | evidian.processtospy                  |
| Value    | <u>YOUR-PROCESS</u> / <u>disabled</u> |

## ControlUp

- Integrated **ControlUp Monitoring Tool** for **Citrix** and **Horizon** sessions.

## Hardware

- Added hardware support for **Lenovo M625q**.
- Added hardware support for **LG CL600N**.
- Added hardware support for **HP Engage Go Mobile System**.
- Added hardware support for **Fujitsu FUTRO S740**.
- Added hardware support for **OnLogic CL210G-10**.
- Added hardware support for **OnLogic KARBON 300**.
- Added hardware support for **Rein Medical Clinio S 522TCT** and **S 524TCT**.
- Added hardware support for **HP t640 Thin Client**.
- Added basic support for **Macbook models 2018** and **newer**.
- Added support for **Sennheiser MB 660, SC 630, SC 45, SC 160 headsets**.
- Added support for **Plantronics Savi 8245 Office, Voyager 6200 UC, Savi 8220 headsets**.
- Added serial port driver for **Exar UART PCIe card**.
- Added driver for **GSPCA based webcams**.

## TC Setup (Java)

- Added Setup page **Sessions > Horizon Client > Horizon Client Global > Window**. Settings for "**Window size**" and "**Multimonitor full-screen mode**" can be set.



These settings are repeated and originate in RDP Global but are now presented in a more obvious place for Horizon sessions.

#### IGEL Cloud Gateway

- Added support for **Secure Terminal over ICG**.
- Changed default order of connecting to the IGEL Remote Management** - an available UMS Server is preferred now by default. The device establishes a configured ICG connection only if the UMS Server is not reachable. This behavior can be changed by the parameter:  
[More...](#)

|          |                                          |
|----------|------------------------------------------|
| Registry | system.remotemanager.icg_try_ums_connect |
| Value    | <u>true</u> / false                      |

#### Fabulatech

- Updated **FabulaTech Scanner for Remote Desktop** client to version **2.4.0.11**.
- Updated **FabulaTech plugins** to version **3.6.2**.
- Updated **Fabulatech USB for Remote Desktop plugins** to version **3.6.8**.

#### Jabra

- Jabra Xpress** (JDU) is upgraded to the **7.2.0-509** version. List of the newly introduced parameters:  
[More...](#)

|          |                                        |
|----------|----------------------------------------|
| Registry | jabra.xpress.show_jdu_gui              |
| Value    | <u>true</u> / false                    |
| Registry | jabra.xpress.device_dashboard.autopost |
| Value    | <u>true</u> / false                    |

#### Resolved Issues 11.04.100

##### Citrix

- "**Green artifacts**" problem in Citrix sessions (most probably) fixed.
- Citrix **hardware video acceleration** supports the **latest Intel hardware**.

##### OSC Installer

- Fixed issue with **filesystems not** always get detected correctly in **initramfs OSC Installer** (needed for using iso file boot parameter).
- Fixed: **username and password in the error message** are not shown anymore when firmware file could not be downloaded.
- Get **URLs** with **username:password@** working.

##### RDP/IGEL RDP Client 2

- Fixed error when **renaming a non-empty shared folder**.

##### WVD

- Includes **WVD client with** fixed **RDcoreSDK** version.
- Clipboard redirection** has potential privacy and security risks and is therefore **disabled by default**.



- **IGEL WVD Client integrated**

#### VMware Horizon

- Fixed missing **support for ThinPrint** and **Skype for Business** when starting **Horizon from Firefox browser**.

#### Firefox

- Fixed Firefox **block extension missing tabs** created via command line argument.
- Fixed **rtsp media stream** with enabled apparmor.
- **Show "blocked" page instead of closing tab** when blocked page is viewed in Firefox.
- Fixed functionality in the local setup to start the **certificate manager of the Firefox browser**.
- Fixed functionality in the local setup to **start the Firefox browser with the internal page to show the installed plugins**.
- Fixed **restart mechanism in the Firefox** browser where the browser could not be closed on suspend resulting in a superfluous browser window on resume.

#### Network

- Improved **Wi-Fi DHCP lease handling**: Leases are discarded when the network changes. The former behavior caused problems with certain iPhone IOS versions.
- **802.1X failures** now generally **result in falling back to a connection without authentication**, e.g. also in the case of 802.1X settings that don't make sense at all. This only **applies if the fallback is allowed** of course.
- **wpa\_supplicant** now adds **timestamps to entries of its log file**.
- Use **e1000e driver** out of the kernel **as default** instead of the third-party driver.
- Added a registry key that determines whether **lldpd is in receive-only mode**.  
**More...**

|            |                                                                                      |
|------------|--------------------------------------------------------------------------------------|
| Parameter  | Disable sending LLDP packets                                                         |
| Registry   | network.lldp.rxonly                                                                  |
| Value      | <u>true</u>                                                                          |
| Attention: | If the behavior since 10.06.100 shall be preserved, this key must be set to "false". |

- Updated **scep** to version **0.7.0**.

#### Wi-Fi

- Fixed non-working **Marvell WLAN device 8997** (SDIO version).

#### NCP VPN

- Added fix for **NCP Secure Client**.

#### genucard VPN

- **genucard 3 is supported** now.

#### Imprivata

- **Control the visibility** of the **Horizon session control bar** via registry parameter:  
**More...**



|          |                                   |
|----------|-----------------------------------|
| Registry | <code>vmware.view.menu-bar</code> |
| Value    | <u>enabled</u> / disabled         |

- Honor the Citrix Window Configuration in **Imprivata Appliance Mode**.
- Fixed **Lock key** and **Tap out** behavior.
- Fixed **MS RDSH** session.
- Simplified the configuration of **Imprivata FUS**.
- **Enable the following** if you use **Imprivata** versions **above 6.3**:  
[More...](#)

|          |                                        |
|----------|----------------------------------------|
| Registry | <code>imprivata.gain_permission</code> |
| Value    | <u>enabled</u> / disabled              |

- Fixed **bug regarding Imprivata** and **On-Screen Keyboard**.
- **Restore the keyboard map** after Horizon sessions.

## Smartcard

- Fixed not working **90meter in Firefox** when **apparmor is active**.
- Fixed problem in **smartcard resource manager PC/SC-Lite** which caused **disconnects of VMware Horizon sessions** when using smartcards with certain applications.
- Added **driver for smartcard reader Elatec TWN4 CCID** (USB 0x09D8:0x0425).
- Updated **cryptovision scInterface** to version **7.3.1**.

The changes are:

[More...](#)

- Consolidated features of the last versions 7.2 and 7.1
  - Malta eID Release
  - Added Admin Card Gemalto V3
- Updated **PC/SC-Lite smartcard resource manager** to version **1.8.26**.

## HID

- Fixed: **Switching touchpad to other driver** via IGEL registry key.

## CUPS Printing

- Added new version **25.1.0.425 of Printerlogic Printer Installer Client**.
- Added **new printer models** into IGEL OS from the current CUPS drivers.

## Base System

- Fixed bug in **folder generation of the Application Launcher**.
- Fixed **TLS certificate verification** problem of **certificates signed by "USERTrust RSA CA" or "COMODO RSA CA"**. The problem could occur in clients like Citrix Workspace App and VMWare Horizon client.
- Fixed **password change with AD/Kerberos**. Before this fix, the password complexity rules were not enforced for users with the Reset Password permission for their account.
- You can now **connect to Bluetooth devices without pairing**. For this a new registry key is available.

[More...](#)

|           |                                             |
|-----------|---------------------------------------------|
| Parameter | connect devices without pairing             |
| Registry  | <code>devices.bluetooth.connect_only</code> |



| Value | enabled / disabled |
|-------|--------------------|
|-------|--------------------|

- **Some devices do not connect automatically after reboot.** To fix that, bluetoothctl connect \<device-ID> can be executed via script. If the **device is connected (0)** or **not (1)** can be seen in return value.  
**Known devices** that do not connect:
  - dialog semiconductor IoT Multi Sensor DK
- **SSHv1 support is now removed** due to newer openssh libraries.
- **Forcing protocol version 1 via SSH Session > Options is no longer possible.**
- The network.ssh\_server.server\_key\_bits registry key parameter is **removed** due to **deprecation of SSHv1**.
- Updates **systemd** to **Ubuntu Focal version**.
- Improved **stability of mounting network shares** when using a **static network configuration**.
- Fixed **apparmor cache** issue **after update with OSC installer**.
- Bug fix: **touchscreen calibration** on 1 or more normal screen with 1 touch screen environment.
- Fixed **syslog, kern.log, auth.log**, and **daemon.log** entries are **not shown in IGEL System Log Viewer**.
- Updated **Grub2** to current Debian SID/Bullseye version **2.04**.
- **Removed** deprecated registry keys system.idlecommand.
- New **Bluetooth pairing tool** and **Bluetooth tray icon** for Bionic.
- Updated **kernel** to mainline version **5.4.48**.
- If used as master image, the **image will expand itself to full size** (limited to 16 GiB) on flash. This is done only on first boot and never again.
- Possible **rollout of initial settings, certificates or licenses placed on first partition** for this you need to:
  - a. Write image to your USB/Flash medium.
  - b. Mount or simply access the **1. VFAT partition** which is present (should be empty).
  - c. Copy your **setup.ini** and/or **\*\*.lic files** to the 1st partition (no directories).
  - d. Create a ca-certs directory and copy your certificates into it. They will be copied to the /wfs/ca-certs directory on first boot.
  - e. You can now copy the USB/Flash medium several times if needed.
  - f. On first boot, the device will reboot out of the splash screen (reread changed partition table)
  - g. The settings, certificates and/or licenses will get rolled out and deleted from the 1st partition.
- Added initial support for **Thunderbolt devices** (only limited support here, may work but is not guaranteed).
- Updated **IGEL EULA**.
- Updated **AMD Microcode** to version **3.20191218.1**.
- Updated **Intel Microcode** to version **20200520** and a special update for **J1900 devices**.
- Updated **Intel Microcode** to **20200616** version.
- Added a **userspace oom killer** to the firmware.

#### Firmware Update

- An **ongoing firmware update can now be canceled by the user** when the network online status could not be reached after 10 seconds (since start of the firmware update).



- **Citrix hardware video acceleration** supports the latest Intel hardware.

#### Storage Devices

- Fixed mount issues with **Iphone XR/XE/11PRO**.
- **Mobile Device Access** feature respects USB Access Control now.
- Fixed unwanted **ownership change** of automounted Linux filesystem root directories.

#### X11 System

- Fixed **Display Switch not saving settings over reboot**.
  - **Default to settings from Setup** instead of mirror when no Display Switch profile is available.
- Prevent misconfiguration that **picks GPU without render capability as primary** (e.g. Displaylink).
- Improved **Nvidia** with **additional GPU handling**.
- Fixed error with **single-gpu Nvidia card support**.

#### X server

- Fixed a **Xorg crash** due to a **NULL pointer dereference in the Intel driver**.

#### Window Manager

- Fixed **random login** (greeter) **window focus** issues.

#### Shadowing/VNC

- Added the "**snapfb**" option for the VNC server.  
[More...](#)

|          |                                                                                            |
|----------|--------------------------------------------------------------------------------------------|
| Registry | <code>network.vncserver.snapfb</code>                                                      |
| Value    | <u>enabled</u> / <u>disabled</u>                                                           |
| Info     | This option should only be enabled with experienced delays in remote or shadowing session. |

- Improved **security of the password authentication method** - the VNC server does not require anymore a file holding the password. **During client authentication**, the **server retrieves** now the **password from the IGEL Setup**.

#### VNC Viewer

- Fixed **occasional freeze of shadowing session** e.g. when resizing a window. Now **the session gets unlocked again after about 20 seconds**.

[More...](#)

|           |                                                     |
|-----------|-----------------------------------------------------|
| Parameter | Unlock X server in case of shadowing session freeze |
| Registry  | <code>network.vncserver.grab_buster</code>          |
| Type      | bool                                                |
| Value     | <u>enabled</u> / <u>disabled</u>                    |

#### VirtualBox

- Fixed **no automatic resolution changes** as **virtualbox guest** issue.

#### Audio



- Fixed **headset microphone using 3.5mm audio jack** in **Dell Wyse 3040**.
  - Added possibility to **set** some **snd\_hda\_intel kernel module parameter** to overcome possible issues with sound devices.
- New registry keys:  
[More...](#)

|           |                                                                                               |
|-----------|-----------------------------------------------------------------------------------------------|
| Parameter | Enable Message Signaled Interrupt                                                             |
| Registry  | system.sound_driver.snd_hda_intel.enable_ms_i                                                 |
| Type      | bool                                                                                          |
| Value     | enabled / <u>disabled</u>                                                                     |
| Parameter | Force enable device                                                                           |
| Registry  | system.sound_driver.snd_hda_intel.enable                                                      |
| Type      | bool                                                                                          |
| Value     | enabled / <u>disabled</u>                                                                     |
| Parameter | Position fix quirk                                                                            |
| Registry  | system.sound_driver.snd_hda_intel.position_fix                                                |
| Range     | [Default] [Auto (0)] [LPIB (1)] [POSBUF (2)] [VIACOMBO (3)] [COMBO (4)] [SKL+ (5)] [FIFO (6)] |
| Parameter | Change sound card order                                                                       |
| Registry  | system.sound_driver.snd_hda_intel.index                                                       |
| Type      | integer                                                                                       |
| Value     | <u>empty</u>                                                                                  |
| Parameter | Detection of DMIC devices                                                                     |
| Registry  | system.sound_driver.snd_hda_intel.dmic_detect                                                 |
| Range     | [Default] [Disabled] [Enabled]                                                                |
| Parameter | Enable this if you encounter sound card problems                                              |
| Registry  | system.sound_driver.snd_hda_intel.single_cmd                                                  |
| Type      | bool                                                                                          |
| Value     | enabled / <u>disabled</u>                                                                     |
| Parameter | Automatic power save timeout                                                                  |
| Registry  | system.sound_driver.snd_hda_intel.power_save                                                  |
| Type      | integer                                                                                       |
| Value     | <u>empty</u>                                                                                  |
| Parameter | Reset controller in power save mode                                                           |
| Registry  | system.sound_driver.snd_hda_intel.power_save_controller                                       |



|           |                                                                            |
|-----------|----------------------------------------------------------------------------|
| Type      | bool                                                                       |
| Value     | <u>enabled</u> / disabled                                                  |
| Parameter | Choose sound model to use                                                  |
| Registry  | system.sound_driver.snd_hda_intel.model                                    |
| Type      | string                                                                     |
| Value     | <u>Auto</u>                                                                |
| Parameter | If you encounter sound problems try to choose one of the alternative masks |
| Registry  | system.sound_driver.snd_hda_intel.probe_mask                               |
| Range     | [Auto] [1] [8]                                                             |

- Old settings. **Command at startup removed.**

#### Jabra

- **Avoid deploying of the same Jabra Xpress package several times** on the same Jabra device.

#### Evidian

- Evidian now **triggers the regular Horizon session script**.

#### Hardware

- Fixed non-working **Prolific PL2303 USB-to-serial adapters**.

#### TC Setup (Java)

- **Removed "default" button** left of selection box IGEL Setup: **Sessions > Citrix > Citrix Global > Window > Multimonitor full-screen mode**.

#### Remote Management

- Fixed **repeated firmware registering over the ICG** which can occur after a new firmware was successfully registered in the UMS. The device invokes firmware registering again after every settings transfer from the device to the UMS. This behavior lasts until reboot.
- Fixed **syncing settings changed on the device if the UMS wasn't reachable**.
- Fixed handling of the **structure tag** if it was **configured in the system dialog "UMS Registering"**.

#### IGEL Cloud Gateway

- **Maximum waiting time for a response from the ICG server** can now be **configured by** the parameter **system.remotemanager.rmagent\_timeout** (default: 90 seconds).

#### VNC

- **Shadowing notification** is **restricted to primary monitor** and **cannot be moved outside of the monitor's visible range**.
- Fixed **sporadic connection failure** in VNC server.
- Fixed **occasional freeze of shadowing session** e.g. when resizing a window. Now the session gets unlocked again after about 20 seconds.

[More...](#)

|           |                                                     |
|-----------|-----------------------------------------------------|
| Parameter | Unlock X server in case of shadowing session freeze |
| Registry  | network.vncserver.grab_buster                       |



|       |                    |
|-------|--------------------|
| Type  | bool               |
| Value | enabled / disabled |

### CA Certificates Contained in IGEL OS 11.04.100

| Certificate name                                          | Expiry date                 | File in /etc/ssl/certs                                        |
|-----------------------------------------------------------|-----------------------------|---------------------------------------------------------------|
| ACCVRAIZ1                                                 | Dec 31 09:37:37<br>2030 GMT | ACCVRAIZ1.crt                                                 |
| AC RAIZ FNMT-RCM                                          | Jan 1 00:00:00<br>2030 GMT  | AC_RAIZ_FNMT-RCM.crt                                          |
| Actalis Authentication Root CA                            | Sep 22 11:22:02<br>2030 GMT | Actalis_Authentication_Root_CA.crt                            |
| AffirmTrust Commercial                                    | Dec 31 14:06:06<br>2030 GMT | AffirmTrust_Commercial.crt                                    |
| AffirmTrust Networking                                    | Dec 31 14:08:24<br>2030 GMT | AffirmTrust_Networking.crt                                    |
| AffirmTrust Premium                                       | Dec 31 14:10:36<br>2040 GMT | AffirmTrust_Premium.crt                                       |
| AffirmTrust Premium ECC                                   | Dec 31 14:20:24<br>2040 GMT | AffirmTrust_Premium_ECC.crt                                   |
| Amazon Root CA 1                                          | Jan 17 00:00:00<br>2038 GMT | AmazonRootCA1.pem)                                            |
| Amazon Root CA 1                                          | Jan 17 00:00:00<br>2038 GMT | Amazon_Root_CA_1.crt                                          |
| Amazon Root CA 2                                          | May 26 00:00:00<br>2040 GMT | Amazon_Root_CA_2.crt                                          |
| Amazon Root CA 3                                          | May 26 00:00:00<br>2040 GMT | Amazon_Root_CA_3.crt                                          |
| Amazon Root CA 4                                          | May 26 00:00:00<br>2040 GMT | Amazon_Root_CA_4.crt                                          |
| Atos TrustedRoot 2011                                     | Dec 31 23:59:59<br>2030 GMT | Atos_TrustedRoot_2011.crt                                     |
| Autoridad de Certificacion Firmaprofesional CIF A62634068 | Dec 31 08:38:15<br>2030 GMT | Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.crt |
| Baltimore CyberTrust Root                                 | May 12 23:59:00<br>2025 GMT | BTCTRoot.pem)                                                 |
| Baltimore CyberTrust Root                                 | May 12 23:59:00<br>2025 GMT | Baltimore_CyberTrust_Root.crt                                 |
| Buypass Class 2 Root CA                                   | Oct 26 08:38:03<br>2040 GMT | Buypass_Class_2_Root_CA.crt                                   |



| Certificate name                                                                                                                | Expiry date                 | File in /etc/ssl/certs                 |
|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------|----------------------------------------|
| Buypass Class 3 Root CA                                                                                                         | Oct 26 08:28:58<br>2040 GMT | Buypass_Class_3_Root_CA.crt            |
| CA Disig Root R2                                                                                                                | Jul 19 09:15:30<br>2042 GMT | CA_Disig_Root_R2.crt                   |
| CFCA EV ROOT                                                                                                                    | Dec 31 03:07:01<br>2029 GMT | CFCA_EV_ROOT.crt                       |
| COMODO Certification Authority                                                                                                  | Dec 31 23:59:59<br>2029 GMT | COMODO_Certification_Authority.crt     |
| COMODO ECC Certification Authority                                                                                              | Jan 18 23:59:59<br>2038 GMT | COMODO_ECC_Certification_Authority.crt |
| COMODO RSA Certification Authority                                                                                              | Jan 18 23:59:59<br>2038 GMT | COMODO_RSA_Certification_Authority.crt |
| Certigna                                                                                                                        | Jun 29 15:13:05<br>2027 GMT | Certigna.crt                           |
| Certigna Root CA                                                                                                                | Oct 1 08:32:27<br>2033 GMT  | Certigna_Root_CA.crt                   |
| Certinomis - Root CA                                                                                                            | Oct 21 09:17:18<br>2033 GMT | Certinomis_-_Root_CA.crt               |
| Class 2 Primary CA                                                                                                              | Jul 6 23:59:59<br>2019 GMT  | Certplus_Class_2_Primary_CA.crt        |
| Certum Trusted Network CA                                                                                                       | Dec 31 12:07:37<br>2029 GMT | Certum_Trusted_Network_CA.crt          |
| Certum Trusted Network CA 2                                                                                                     | Oct 6 08:39:56<br>2046 GMT  | Certum_Trusted_Network_CA_2.crt        |
| Chambers of Commerce Root - 2008                                                                                                | Jul 31 12:29:50<br>2038 GMT | Chambers_of_Commerce_Root_-_2008.crt   |
| Class 3 Public Primary Certification Authority - G2 (c)<br>1998 VeriSign, Inc. - For authorized use only VeriSign Trust Network | Aug 1 23:59:59<br>2028 GMT  | Class3PCA_G2_v2.pem)                   |
| Class 4 Public Primary Certification Authority - G2 (c)<br>1998 VeriSign, Inc. - For authorized use only VeriSign Trust Network | Aug 1 23:59:59<br>2028 GMT  | Class4PCA_G2_v2.pem)                   |
| AAA Certificate Services                                                                                                        | Dec 31 23:59:59<br>2028 GMT | Comodo_AAA_Services_root.crt           |
| Cybertrust Global Root                                                                                                          | Dec 15 08:00:00<br>2021 GMT | Cybertrust_Global_Root.crt             |



| Certificate name                                          | Expiry date              | File in /etc/ssl/certs                        |
|-----------------------------------------------------------|--------------------------|-----------------------------------------------|
| D-TRUST Root Class 3 CA 2 2009                            | Nov 5 08:35:58 2029 GMT  | D-TRUST_Root_Class_3_CA_2_2009.crt            |
| D-TRUST Root Class 3 CA 2 EV 2009                         | Nov 5 08:50:46 2029 GMT  | D-TRUST_Root_Class_3_CA_2_EV_2009.crt         |
| DST Root CA X3                                            | Sep 30 14:01:15 2021 GMT | DST_Root_CA_X3.crt                            |
| Deutsche Telekom Root CA 2                                | Jul 9 23:59:00 2019 GMT  | Deutsche_Telekom_Root_CA_2.crt                |
| DigiCert Global Root CA                                   | Nov 10 00:00:00 2031 GMT | DigiCertGlobalRootCA.pem)                     |
| DigiCert Global Root CA                                   | Mar 8 12:00:00 2023 GMT  | DigiCertSHA2SecureServerCA.pem)               |
| DigiCert Assured ID Root CA                               | Nov 10 00:00:00 2031 GMT | DigiCert_Assured_ID_Root_CA.crt               |
| DigiCert Assured ID Root G2                               | Jan 15 12:00:00 2038 GMT | DigiCert_Assured_ID_Root_G2.crt               |
| DigiCert Assured ID Root G3                               | Jan 15 12:00:00 2038 GMT | DigiCert_Assured_ID_Root_G3.crt               |
| DigiCert Global Root CA                                   | Nov 10 00:00:00 2031 GMT | DigiCert_Global_Root_CA.crt                   |
| DigiCert Global Root G2                                   | Jan 15 12:00:00 2038 GMT | DigiCert_Global_Root_G2.crt                   |
| DigiCert Global Root G3                                   | Jan 15 12:00:00 2038 GMT | DigiCert_Global_Root_G3.crt                   |
| DigiCert High Assurance EV Root CA                        | Nov 10 00:00:00 2031 GMT | DigiCert_High_Assurance_EV_Root_CA.crt        |
| DigiCert Trusted Root G4                                  | Jan 15 12:00:00 2038 GMT | DigiCert_Trusted_Root_G4.crt                  |
| E-Tugra Certification Authority                           | Mar 3 12:09:48 2023 GMT  | E-Tugra_Certification_Authority.crt           |
| EC-ACC                                                    | Jan 7 22:59:59 2031 GMT  | EC-ACC.crt                                    |
| EE Certification Centre Root CA                           | Dec 17 23:59:59 2030 GMT | EE_Certification_Centre_Root_CA.crt           |
| Entrust.net <sup>405</sup> Certification Authority (2048) | Jul 24 14:15:12 2029 GMT | Entrust.net_Premium_2048_Secure_Server_CA.crt |
| Entrust Root Certification Authority                      | Nov 27 20:53:42 2026 GMT | Entrust_Root_Certification_Authority.crt      |

<sup>405</sup> <http://Entrust.net>



| Certificate name                              | Expiry date              | File in /etc/ssl/certs                            |
|-----------------------------------------------|--------------------------|---------------------------------------------------|
| Entrust Root Certification Authority - EC1    | Dec 18 15:55:36 2037 GMT | Entrust_Root_Certification_Authority_-_EC1.crt    |
| Entrust Root Certification Authority - G2     | Dec 7 17:55:54 2030 GMT  | Entrust_Root_Certification_Authority_-_G2.crt     |
| GDCA TrustAUTH R5 ROOT                        | Dec 31 15:59:59 2040 GMT | GDCA_TrustAUTH_R5_ROOT.crt                        |
| GlobalSign                                    | Dec 15 08:00:00 2021 GMT | GSR2.pem)                                         |
| GTE CyberTrust Global Root                    | Aug 13 23:59:00 2018 GMT | GTECTGlobalRoot.pem)                              |
| GTS Root R1                                   | Jun 22 00:00:00 2036 GMT | GTS_Root_R1.crt                                   |
| GTS Root R2                                   | Jun 22 00:00:00 2036 GMT | GTS_Root_R2.crt                                   |
| GTS Root R3                                   | Jun 22 00:00:00 2036 GMT | GTS_Root_R3.crt                                   |
| GTS Root R4                                   | Jun 22 00:00:00 2036 GMT | GTS_Root_R4.crt                                   |
| GeoTrust Global CA                            | May 21 04:00:00 2022 GMT | GeoTrust_Global_CA.crt                            |
| GeoTrust Global CA                            | May 21 04:00:00 2022 GMT | GeoTrust_Global_CA.pem)                           |
| GeoTrust Primary Certification Authority      | Jul 16 23:59:59 2036 GMT | GeoTrust_Primary_Certification_Authority.crt      |
| GeoTrust Primary Certification Authority - G2 | Jan 18 23:59:59 2038 GMT | GeoTrust_Primary_Certification_Authority_-_G2.crt |
| GeoTrust Primary Certification Authority - G3 | Dec 1 23:59:59 2037 GMT  | GeoTrust_Primary_Certification_Authority_-_G3.crt |
| GeoTrust Universal CA                         | Mar 4 05:00:00 2029 GMT  | GeoTrust_Universal_CA.crt                         |
| GeoTrust Universal CA 2                       | Mar 4 05:00:00 2029 GMT  | GeoTrust_Universal_CA_2.crt                       |
| GlobalSign                                    | Jan 19 03:14:07 2038 GMT | GlobalSign_ECC_Root_CA_-_R4.crt                   |
| GlobalSign                                    | Jan 19 03:14:07 2038 GMT | GlobalSign_ECC_Root_CA_-_R5.crt                   |
| GlobalSign Root CA                            | Jan 28 12:00:00 2028 GMT | GlobalSign_Root_CA.crt                            |
| GlobalSign                                    | Dec 15 08:00:00 2021 GMT | GlobalSign_Root_CA_-_R2.crt                       |



| Certificate name                                            | Expiry date                 | File in /etc/ssl/certs                                          |
|-------------------------------------------------------------|-----------------------------|-----------------------------------------------------------------|
| GlobalSign                                                  | Mar 18 10:00:00<br>2029 GMT | GlobalSign_Root_CA_-_R3.crt                                     |
| GlobalSign                                                  | Dec 10 00:00:00<br>2034 GMT | GlobalSign_Root_CA_-_R6.crt                                     |
| Global Chambersign Root - 2008                              | Jul 31 12:31:40<br>2038 GMT | Global_Chambersign_Root_-_2008.crt                              |
| Go Daddy Class 2 Certification Authority                    | Jun 29 17:06:20<br>2034 GMT | Go_Daddy_Class_2_CA.crt                                         |
| Go Daddy Root Certificate Authority - G2                    | Dec 31 23:59:59<br>2037 GMT | Go_Daddy_Root_Certificate_Authority_-_G2.crt                    |
| Hellenic Academic and Research Institutions ECC RootCA 2015 | Jun 30 10:37:12<br>2040 GMT | Hellenic_Academic_and_Research_Institutions_ECC_RootCA_2015.crt |
| Hellenic Academic and Research Institutions RootCA 2011     | Dec 1 13:49:52<br>2031 GMT  | Hellenic_Academic_and_Research_Institutions_RootCA_2011.crt     |
| Hellenic Academic and Research Institutions RootCA 2015     | Jun 30 10:11:21<br>2040 GMT | Hellenic_Academic_and_Research_Institutions_RootCA_2015.crt     |
| Hongkong Post Root CA 1                                     | May 15 04:52:29<br>2023 GMT | Hongkong_Post_Root_CA_1.crt                                     |
| ISRG Root X1                                                | Jun 4 11:04:38<br>2035 GMT  | ISRG_Root_X1.crt                                                |
| IdenTrust Commercial Root CA 1                              | Jan 16 18:12:23<br>2034 GMT | IdenTrust_Commercial_Root_CA_1.crt                              |
| IdenTrust Public Sector Root CA 1                           | Jan 16 17:53:32<br>2034 GMT | IdenTrust_Public_Sector_Root_CA_1.crt                           |
| Imprivata Embedded Code Signing CA                          | Sep 7 16:20:00<br>2033 GMT  | Imprivata.crt                                                   |
| Izenpe.com <sup>406</sup>                                   | Dec 13 08:27:25<br>2037 GMT | Izenpe.com <sup>407</sup> .crt                                  |
| LuxTrust Global Root 2                                      | Mar 5 13:21:57<br>2035 GMT  | LuxTrust_Global_Root_2.crt                                      |
| Microsec e-Szigno Root CA 2009                              | Dec 30 11:30:18<br>2029 GMT | Microsec_e-Szigno_Root_CA_2009.crt                              |
| NetLock Arany (Class Gold)<br>Főtanúsítvány                 | Dec 6 15:08:21<br>2028 GMT  | NetLock_Arany_=Class_Gold=_F<br>őtanúsítvány.crt                |

<sup>406</sup> <http://Izenpe.com><sup>407</sup> <http://Izenpe.com>



| Certificate name                                              | Expiry date              | File in /etc/ssl/certs                             |
|---------------------------------------------------------------|--------------------------|----------------------------------------------------|
| Network Solutions Certificate Authority                       | Dec 31 23:59:59 2029 GMT | Network_Solutions_Certificate_Authority.crt        |
| OISTE WISEKey Global Root GA CA                               | Dec 11 16:09:51 2037 GMT | OISTE_WISEKey_Global_Root_GA_CA.crt                |
| OISTE WISEKey Global Root GB CA                               | Dec 1 15:10:31 2039 GMT  | OISTE_WISEKey_Global_Root_GB_CA.crt                |
| OISTE WISEKey Global Root GC CA                               | May 9 09:58:33 2042 GMT  | OISTE_WISEKey_Global_Root_GC_CA.crt                |
| Class 3 Public Primary Certification Authority                | Aug 1 23:59:59 2028 GMT  | Pcs3ss_v4.pem)                                     |
| QuoVadis Root Certification Authority                         | Mar 17 18:33:33 2021 GMT | QuoVadis_Root_CA.crt                               |
| QuoVadis Root CA 1 G3                                         | Jan 12 17:27:44 2042 GMT | QuoVadis_Root_CA_1_G3.crt                          |
| QuoVadis Root CA 2                                            | Nov 24 18:23:33 2031 GMT | QuoVadis_Root_CA_2.crt                             |
| QuoVadis Root CA 2 G3                                         | Jan 12 18:59:32 2042 GMT | QuoVadis_Root_CA_2_G3.crt                          |
| QuoVadis Root CA 3                                            | Nov 24 19:06:44 2031 GMT | QuoVadis_Root_CA_3.crt                             |
| QuoVadis Root CA 3 G3                                         | Jan 12 20:26:32 2042 GMT | QuoVadis_Root_CA_3_G3.crt                          |
| SSL.com <sup>408</sup> EV Root Certification Authority ECC    | Feb 12 18:15:23 2041 GMT | SSL.com_EV_Root_Certification_Authority_ECC.crt    |
| SSL.com <sup>409</sup> EV Root Certification Authority RSA R2 | May 30 18:14:37 2042 GMT | SSL.com_EV_Root_Certification_Authority_RSA_R2.crt |
| SSL.com <sup>410</sup> Root Certification Authority ECC       | Feb 12 18:14:03 2041 GMT | SSL.com_Root_Certification_Authority_ECC.crt       |
| SSL.com <sup>411</sup> Root Certification Authority RSA       | Feb 12 17:39:39 2041 GMT | SSL.com_Root_Certification_Authority_RSA.crt       |
| SZAFIR ROOT CA2                                               | Oct 19 07:43:30 2035 GMT | SZAFIR_ROOT_CA2.crt                                |
| SecureSign RootCA11                                           | Apr 8 04:56:47 2029 GMT  | SecureSign_RootCA11.crt                            |
| SecureTrust CA                                                | Dec 31 19:40:55 2029 GMT | SecureTrust_CA.crt                                 |

<sup>408</sup> <http://SSL.com><sup>409</sup> <http://SSL.com><sup>410</sup> <http://SSL.com><sup>411</sup> <http://SSL.com>



| Certificate name                                   | Expiry date                 | File in /etc/ssl/certs                                 |
|----------------------------------------------------|-----------------------------|--------------------------------------------------------|
| Secure Global CA                                   | Dec 31 19:52:06<br>2029 GMT | Secure_Global_CA.crt                                   |
| Security Communication RootCA2                     | May 29 05:00:39<br>2029 GMT | Security_Communication_RootCA2.crt                     |
| Security Communication RootCA1                     | Sep 30 04:20:49<br>2023 GMT | Security_Communication_Root_CA.crt                     |
| Sonera Class2 CA                                   | Apr 6 07:29:40<br>2021 GMT  | Sonera_Class_2_Root_CA.crt                             |
| Staat der Nederlanden EV Root CA                   | Dec 8 11:10:28<br>2022 GMT  | Staat_der_Nederlanden_EV_Root_CA.crt                   |
| Staat der Nederlanden Root CA - G2                 | Mar 25 11:03:10<br>2020 GMT | Staat_der_Nederlanden_Root_CA_-_G2.crt                 |
| Staat der Nederlanden Root CA - G3                 | Nov 13 23:00:00<br>2028 GMT | Staat_der_Nederlanden_Root_CA_-_G3.crt                 |
| Starfield Class 2 Certification Authority          | Jun 29 17:39:16<br>2034 GMT | Starfield_Class_2_CA.crt                               |
| Starfield Root Certificate Authority - G2          | Dec 31 23:59:59<br>2037 GMT | Starfield_Root_Certificate_Authority_-_G2.crt          |
| Starfield Services Root Certificate Authority - G2 | Dec 31 23:59:59<br>2037 GMT | Starfield_Services_Root_Certificate_Authority_-_G2.crt |
| SwissSign Gold CA - G2                             | Oct 25 08:30:35<br>2036 GMT | SwissSign_Gold_CA_-_G2.crt                             |
| SwissSign Silver CA - G2                           | Oct 25 08:32:46<br>2036 GMT | SwissSign_Silver_CA_-_G2.crt                           |
| T-TeleSec GlobalRoot Class 2                       | Oct 1 23:59:59<br>2033 GMT  | T-TeleSec_GlobalRoot_Class_2.crt                       |
| T-TeleSec GlobalRoot Class 3                       | Oct 1 23:59:59<br>2033 GMT  | T-TeleSec_GlobalRoot_Class_3.crt                       |
| TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1      | Oct 25 08:25:55<br>2043 GMT | TUBITAK_Kamu_SM_SSL_Kok_Sertifikasi_-_Surum_1.crt      |
| TWCA Global Root CA                                | Dec 31 15:59:59<br>2030 GMT | TWCA_Global_Root_CA.crt                                |
| TWCA Root Certification Authority                  | Dec 31 15:59:59<br>2030 GMT | TWCA_Root_Certification_Authority.crt                  |
| Government Root Certification Authority            | Dec 5 13:23:33<br>2032 GMT  | Taiwan_GRCA.crt                                        |
| TeliaSonera Root CA v1                             | Oct 18 12:00:50<br>2032 GMT | TeliaSonera_Root_CA_v1.crt                             |
| TrustCor ECA-1                                     | Dec 31 17:28:07<br>2029 GMT | TrustCor_ECA-1.crt                                     |



| Certificate name                                             | Expiry date                 | File in /etc/ssl/certs                                           |
|--------------------------------------------------------------|-----------------------------|------------------------------------------------------------------|
| TrustCor RootCert CA-1                                       | Dec 31 17:23:16<br>2029 GMT | TrustCor_RootCert_CA-1.crt                                       |
| TrustCor RootCert CA-2                                       | Dec 31 17:26:39<br>2034 GMT | TrustCor_RootCert_CA-2.crt                                       |
| Trustis FPS Root CA                                          | Jan 21 11:36:54<br>2024 GMT | Trustis_FPS_Root_CA.crt                                          |
| UCA Extended Validation Root                                 | Dec 31 00:00:00<br>2038 GMT | UCA_Extended_Validation_Root.crt                                 |
| UCA Global G2 Root                                           | Dec 31 00:00:00<br>2040 GMT | UCA_Global_G2_Root.crt                                           |
| USERTrust ECC Certification Authority                        | Jan 18 23:59:59<br>2038 GMT | USERTrust_ECC_Certification_Authority.crt                        |
| USERTrust RSA Certification Authority                        | Jan 18 23:59:59<br>2038 GMT | USERTrust_RSA_Certification_Authority.crt                        |
| VeriSign Class 3 Public Primary Certification Authority - G4 | Jan 18 23:59:59<br>2038 GMT | VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt |
| VeriSign Class 3 Public Primary Certification Authority - G5 | Jul 16 23:59:59<br>2036 GMT | VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt |
| VeriSign Universal Root Certification Authority              | Dec 1 23:59:59<br>2037 GMT  | VeriSign_Universal_Root_Certification_Authority.crt              |
| VeriSign Class 3 Public Primary Certification Authority - G3 | Jul 16 23:59:59<br>2036 GMT | VeriSign_Class_3_Public_Primary_Certification_Authority_-_G3.crt |
| XRamp Global Certification Authority                         | Jan 1 05:37:19<br>2035 GMT  | XRamp_Global_CA_Root.crt                                         |
| certSIGN ROOT CA                                             | Jul 4 17:20:04<br>2031 GMT  | certSIGN_ROOT_CA.crt                                             |
| ePKI Root Certification Authority                            | Dec 20 02:31:27<br>2034 GMT | ePKI_Root_Certification_Authority.crt                            |
| thawte Primary Root CA                                       | Jul 16 23:59:59<br>2036 GMT | thawte_Primary_Root_CA.crt                                       |
| thawte Primary Root CA - G2                                  | Jan 18 23:59:59<br>2038 GMT | thawte_Primary_Root_CA_-_G2.crt                                  |
| thawte Primary Root CA - G3                                  | Dec 1 23:59:59<br>2037 GMT  | thawte_Primary_Root_CA_-_G3.crt                                  |



## 7.8.2 IGEL OS Creator (OSC)

### Supported Devices

|         |                                     |
|---------|-------------------------------------|
| UD2-LX: | UD2-LX 51<br>UD2-LX 50<br>UD2-LX 40 |
| UD3-LX: | UD3-LX 60<br>UD3-LX 51<br>UD3-LX 50 |
| UD5-LX: | UD5-LX 50                           |
| UD6-LX: | UD6-LX 51                           |
| UD7-LX: | UD7-LX 11<br>UD7-LX 10              |
| UD9-LX: | UD9-LX Touch 41<br>UD9-LX 40        |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>412</sup>.

- [Component Versions 11.04.100](#)(see page 1647)
- [General Information 11.04.100](#)(see page 1653)
- [Known Issues 11.04.100](#)(see page 1653)
- [Security Fixes 11.04.100](#)(see page 1656)
- [New Features 11.04.100](#)(see page 1657)
- [Resolved Issues 11.04.100](#)(see page 1673)

<sup>412</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



## Component Versions 11.04.100

## Clients

| <b>Product</b>                     | <b>Version</b>                                                                      |
|------------------------------------|-------------------------------------------------------------------------------------|
| Chromium                           | 83.0.4103.61-0ubuntu0.18.04.1                                                       |
| Cisco JVDI Client                  | 12.9.0                                                                              |
| Cisco Webex Teams VDI Client       | 3.0.15711.0                                                                         |
| Cisco Webex Meetings VDI Client    | 40.7.0.375                                                                          |
| Citrix HDX Realtime Media Engine   | 2.9.0-2330                                                                          |
| Citrix Workspace App               | 18.10.0.11                                                                          |
| Citrix Workspace App               | 19.12.0.19                                                                          |
| Citrix Workspace App               | 20.06.0.15                                                                          |
| deviceTRUST Citrix Channel         | 19.1.200.2                                                                          |
| Crossmatch DP Citrix Channel       | 0515.2                                                                              |
| Ericom PowerTerm                   | 12.0.1.0.20170219.2-_dev_-34574                                                     |
| Ericom PowerTerm                   | 14.0.0.45623                                                                        |
| Evidian AuthMgr                    | 1.5.7116                                                                            |
| Evince PDF Viewer                  | 3.28.4-0ubuntu1.2                                                                   |
| FabulaTech USB for Remote Desktop  | 5.2.29                                                                              |
| Firefox                            | 68.10.0                                                                             |
| IBM iAccess Client Solutions       | 1.1.8.1                                                                             |
| IGEL RDP Client                    | 2.2                                                                                 |
| IGEL WVD Client                    | 1.0.13igel1596142398                                                                |
| Imprivata OneSign ProveID Embedded | onesign-bootstrap-loader_1.0.523630_amd64<br>Qualification at Imprivata in progress |
| deviceTRUST RDP Channel            | 19.1.200.2                                                                          |
| NCP Secure Enterprise Client       | 5.10_rev40552                                                                       |



|                                        |                                |
|----------------------------------------|--------------------------------|
| NX Client                              | 6.11.2-1igel8                  |
| Open VPN                               | 2.4.4-2ubuntu1.3               |
| Zulu JRE                               | 8.48.0.51-2                    |
| Parallels Client (64 bit)              | 17.1.1                         |
| Spice GTK (Red Hat Virtualization)     | 0.38-2igel93                   |
| Remote Viewer (Red Hat Virtualization) | 8.0-2git20191213.e4bacb8igel83 |
| Usbredir (Red Hat Virtualization)      | 0.8.0-1+b1igel71               |
| Teradici PCoIP Software Client         | 20.04.2-18.04                  |
| ThinLinc Client                        | 4.12.0-6517                    |
| ThinPrint Client                       | 7.5.88                         |
| Totem Media Player                     | 2.30.2                         |
| Parole Media Player                    | 1.0.5-1igel1583919770          |
| VNC Viewer                             | 1.10.1+dfsg-4igel13            |
| VMware Horizon Client                  | 5.4.1-15988340                 |
| Voip Client Ekiga                      | 4.0.1                          |

## Dictation

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20200323 |
| Philips Speech driver                     | 12.9.1   |

## Signature

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.9    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.4.2    |



## Smartcard

|                                           |                        |
|-------------------------------------------|------------------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101                |
| PKCS#11 Library Athena IDProtect          | 7                      |
| PKCS#11 Library cryptovision sc/interface | 7.3.1                  |
| PKCS#11 Library Gemalto SafeNet           | 10.7.77                |
| PKCS#11 Library OpenSC                    | 0.20.0-3igel37         |
| PKCS#11 Library SecMaker NetID            | 6.8.1.31               |
| PKCS#11 Library 90meter                   | 20190522               |
| Reader Driver ACS CCID                    | 1.1.6-1igel2           |
| Reader Driver Gemalto eToken              | 10.7.77                |
| Reader Driver HID Global Omnikey          | 4.3.3                  |
| Reader Driver Identive CCID               | 5.0.35                 |
| Reader Driver Identive eHealth200         | 1.0.5                  |
| Reader Driver Identive SCRKBC             | 5.0.24                 |
| Reader Driver MUSCLE CCID                 | 1.4.31-1igel11         |
| Reader Driver REINER SCT cyberJack        | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite               | 1.8.26-3igel14         |
| Cherry USB2LAN Proxy                      | 3.2.0.3                |

## System Components

|                         |                          |
|-------------------------|--------------------------|
| OpenSSL                 | 1.0.2n-1ubuntu5.3        |
| OpenSSL                 | 1.1.1-1ubuntu2.1~18.04.6 |
| OpenSSH Client          | 7.6p1-4ubuntu0.3         |
| OpenSSH Server          | 7.6p1-4ubuntu0.3         |
| Bluetooth stack (bluez) | 5.52-1igel6              |



|                                         |                                   |
|-----------------------------------------|-----------------------------------|
| MESA OpenGL stack                       | 20.0.8-1igel117                   |
| VAAPI ABI Version                       | 0.40                              |
| VDPAU Library version                   | 1.4-1igel1003                     |
| Graphics Driver INTEL                   | 2.99.917+git20200515-igel1013     |
| Graphics Driver ATI/RADEON              | 19.1.0-1+git20200220igel987       |
| Graphics Driver ATI/AMDGPU              | 19.1.0-1+git20200318igel986       |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867                   |
| Graphics Driver Nvidia                  | 440.100-0ubuntu0.20.04.1          |
| Graphics Driver VMware                  | 13.3.0-2igel857                   |
| Graphics Driver QXL (Spice)             | 0.1.5-2build2-igel925             |
| Graphics Driver FBDEV                   | 0.5.0-1igel819                    |
| Graphics Driver VESA                    | 2.4.0-1igel855                    |
| Input Driver Evdev                      | 2.10.6-1igel975                   |
| Input Driver Elographics                | 1.4.1-1+b6igel952                 |
| Input Driver eGalax                     | 2.5.7413                          |
| Input Driver Synaptics                  | 1.9.1-1ubuntu1igel866             |
| Input Driver VMMouse                    | 13.1.0-1ubuntu2igel957            |
| Input Driver Wacom                      | 0.36.1-0ubuntu2igel888            |
| Input Driver ELO Multitouch             | 3.0.0                             |
| Input Driver ELO Singletouch            | 5.1.0                             |
| Kernel                                  | 5.4.48 #mainline-lxos-g1595410170 |
| Xorg X11 Server                         | 1.20.8-2igel1016                  |
| Xorg Xephyr                             | 1.20.8-2igel1016                  |
| CUPS printing daemon                    | 2.2.7-1ubuntu2.8igel32            |
| PrinterLogic                            | 25.1.0.425                        |
| Lightdm Graphical Login Manager         | 1.26.0-0ubuntu1igel13             |



|                      |                              |
|----------------------|------------------------------|
| XFCE4 Window Manager | 4.14.2-1~18.04igel1595331607 |
| ISC DHCP Client      | 4.3.5-3ubuntu7.1             |
| NetworkManager       | 1.20.4-2ubuntu2.2igel100     |
| ModemManager         | 1.10.0-1~ubuntu18.04.2       |
| GStreamer 0.10       | 0.10.36-2ubuntu0.1igel201    |
| GStreamer 1.x        | 1.16.2-4igel239              |
| WebKit2Gtk           | 2.28.3-2igel36               |
| Python2              | 2.7.17                       |
| Python3              | 3.6.9                        |

#### VM Guest Support Components

|                            |                          |
|----------------------------|--------------------------|
| Virtualbox Guest Utils     | 6.1.10-dfsg-1igel41      |
| Virtualbox X11 Guest Utils | 6.1.10-dfsg-1igel41      |
| Open VM Tools              | 11.0.5-4ubuntu0.18.04.13 |
| Open VM Desktop Tools      | 11.0.5-4ubuntu0.18.04.1  |
| Xen Guest Utilities        | 7.10.0-0ubuntu1          |
| Spice Vdagent              | 0.20.0-1igel95           |
| Qemu Guest Agent           | 5.0-5igel12              |

#### Features with Limited IGEL Support

|                                    |                                     |
|------------------------------------|-------------------------------------|
| Mobile Device Access USB (MTP)     | 1.1.17-3igel5                       |
| Mobile Device Access USB (imobile) | 1.2.1~git20191129.9f79242-1+b1igel8 |
| Mobile Device Access USB (gphoto)  | 2.5.25-2igel4                       |
| VPN OpenConnect                    | 8.10-1igel4                         |
| Scanner support                    | 1.0.27-1                            |
| VirtualBox                         | 6.1.10-dfsg-1igel41                 |

#### Services

| Service                     | Size   | Reduced Firmware |
|-----------------------------|--------|------------------|
| Asian Language Support      | 22.5 M | Included         |
| Java SE Runtime Environment | 36.0 M | Included         |



|                                            |         |              |
|--------------------------------------------|---------|--------------|
| Citrix Workspace app                       | 219.5 M | Included     |
| Citrix Appliance                           |         |              |
| Citrix StoreFront                          |         |              |
| Ericom PowerTerm InterConnect              | 15.5 M  | Included     |
| Media Player                               | 512.0 K | Included     |
| Citrix Appliance                           | 70.2 M  | Included     |
| Local Browser (Firefox)                    |         |              |
| RDP                                        | 4.2 M   | Included     |
| VMware Horizon                             |         |              |
| Cendio ThinLinc                            | 10.0 M  | Included     |
| Printing (Internet printing protocol CUPS) | 22.2 M  | Included     |
| NoMachine NX                               | 26.8 M  | Included     |
| VMware Horizon                             | 114.5 M | Included     |
| Voice over IP (Ekiga)                      | 6.5 M   | Included     |
| Citrix Appliance                           | 768.0 K | Included     |
| NCP Enterprise VPN Client                  | 27.0 M  | Not included |
| Fluendo GStreamer Codec Plugins            | 6.8 M   | Included     |
| IBM i Access Client Solutions              | 72.5 M  | Not included |
| Red Hat Enterprise Virtualization          | 3.0 M   | Included     |
| Parallels Client                           | 5.5 M   | Included     |
| NVIDIA graphics driver                     | 115.0 M | Not included |
| Imprivata Appliance                        | 10.8 M  | Included     |
| Evidian AuthMgr                            | 2.8 M   | Included     |
| Hardware Video Acceleration                | 13.0 M  | Included     |
| Extra Font Package                         | 1.0 M   | Included     |
| Fluendo GStreamer AAC Decoder              | 1.2 M   | Included     |
| x32 Compatibility Support                  | 48.0 M  | Included     |
| Cisco JVDI client                          | 45.8 M  | Included     |
| PrinterLogic                               | 40.8 M  | Not included |
| Biosec BS Login                            | 10.0 M  | Not included |
| Login VSI Login Enterprise                 | 28.8 M  | Not included |
| Stratusphere UX CID Key software           | 2.8 M   | Not included |
| Elastic Filebeat                           | 15.8 M  | Not included |
| WVD                                        | 13.8 M  | Included     |
| Local Browser (Chromium)                   | 81.2 M  | Not included |
| deskMate client                            | 5.8 M   | Included     |
| Cisco Webex Teams VDI                      | 32.0 M  | Not included |
| Cisco Webex Meetings VDI                   | 36.8 M  | Not included |
| Zoom Media Plugin                          | 39.8 M  | Not included |
| Teradici PCoIP Client                      | 7.8 M   | Included     |
| 90meter Smart Card Support                 | 256.0 K | Included     |



|                                            |         |              |
|--------------------------------------------|---------|--------------|
| Mobile Device Access USB (Limited support) | 256.0 K | Not included |
| VPN OpenConnect (Limited support)          | 1.5 M   | Not included |
| Scanner support / SANE (Limited support)   | 2.5 M   | Not included |
| VirtualBox (Limited support)               | 62.5 M  | Not included |

## General Information 11.04.100

To be beneficial to all new features and implementations, it is recommended to use UMS 6.04.100 or higher and update the corresponding profiles.

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

## Known Issues 11.04.100

### Firmware Update

- On **devices with 2 GB of flash storage**, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs and unused features must be disabled in IGEL Setup under **System > Firmware Customization > Features** to perform the firmware update.

### Firefox

- **Firefox IGEL extensions are not updated automatically** under some circumstances. After an update from 11.03.xxx to 11.04.100, the IGEL extensions will stay on the old version.  
In this case, the following settings concerning **kiosk mode** cannot be executed:
  - Switch off hotkey for new window/tab
  - Blocking of internal browser pages like preferences, file picker, specific local directories

As a workaround:



- a **reset to defaults** should be performed
- or the **browser's mimetype template** can be switched **from "Standard" to "Minimal"** by registry key `browserglobal.app.mimetypes_template`. There, the browser profile is renewed as well.  
After the TC received the new setting, **reboot** and **set** the `mimetypes_template` registry key to **"Standard"** again.

## Citrix

- With activated **DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1 and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix StoreFront login** with **Gemalto smartcard** middleware does not detect smartcard correctly if the card is inserted after start of login.  
Workaround: Insert the smartcard before starting the StoreFront login.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264** acceleration plugin, the following registry key must be enabled.

[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | <code>ica.workaround-dual-rtme</code>                            |
| Value     | <u>enabled</u> / <u>disabled</u>                                 |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

- Using **CWA 19.x** sometimes **freezes the session** while session logoff from a published desktop.  
Workaround: **Use CWA 18.10.0**.
- During the running **Microsoft Teams Optimization of Citrix Workspace App 20.06, webcam redirection or screen sharing** may lead to **display errors** like black stripes or flickering.
- The **performance** of Citrix sessions when using **Workspace App 20.06** may be lower on some devices.  
A possible **workaround** is to **disable the virtual channels for Microsoft Teams** and **NSAP** or to set the **HDX transport protocol** to **TCP** only.
  - `ica.module.virtualdriver.vdwebrtc.enable`
  - `ica.module.virtualdriver.nsap.enable`
  - The protocol can be set via the Setup parameter **Sessions > Citrix > Citrix Global > Options > HDX Adaptive Transport over EDT** or via the **server policy** 'HDX Adaptive Transport'.

## VMware Horizon



- **Client drive mapping** and **USB redirection** for storage devices should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Enable local `Storage Hotplug` on Setup page **Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection do not appear in the **remote desktop**.  
Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- **After the disconnect of an RDP-based session**, the Horizon main **window** which contains the server or sessions overview **cannot be resized anymore**.
- **Seamless application windows in Horizon Client may not be displayed correctly**. When starting the first seamless app, a new iconified window appears in the taskbar, and only if you click on it, the application will show up.  
On some hardware (UD7-H850, UD2-M250, UD2-D220), however, the client aborts when this new window is de-iconified.

#### Imprivata

- On **devices with 2 GB of flash storage**, it could happen that there is not enough space to enable the **Imprivata partition after the update to 11.04.100**. In this case, a corresponding error message occurs and **unused features must be disabled** (in IGEL Setup under **System > Firmware Customization > Features**). Imprivata has to be (re-)enabled after a reboot then.

#### Wi-Fi

- TP-Link Archer T2UH Wi-Fi adapters does not work after system suspend/resume. Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

#### Parallels Client

- **Native USB redirection** does not work with Parallels Client.

#### Smartcard

- **Citrix Certificate Identity Declaration login** does not work with **SecMaker** smartcards.
- In seldom cases, the **authentication** hung when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice: spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

#### Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.



## Hyper-V

- **Hyper-V (Generation 2)** needs **a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.

## VirtualBox

- The current **VirtualBox Guest Tools/Drivers** will not work with **VirtualBox 5.2.x or older** hosts which leads to a black screen and non-working graphics.  
Possible workaround: Install with 'Failsafe Installation + Recovery' and set the registry key `x.drivers.force_vesa` to 'true'.
- When running in VirtualBox virtualization, **resizing the window will not automatically change desktop resolution** of IGEL OS guest.

## Audio

- **Audio jack detection on Advantech POC-W243L** doesn't work. Therefore, sound output goes through a possibly connected headset and the internal speakers.
- **IGEL UD2 (D220)** fails to restore the volume level of the speaker when the device used **firmware version 11.01.110** before.

## Hardware

- **HP t730** could freeze when monitors with **different resolutions** are connected (1920x1200 + 2560x1440 + 3840x1600 for example). When this occurs, the registry key `x.drivers.kms.best_console_mode` has to be set to **disabled**.
- Some newer **Delock 62599 active DisplayPort-to-DVI (4k)** adapters only work with INTEL devices.

## Remote Management

- **AIT feature with IGEL Starter License** is **supported** by the **UMS version 6.05.100**.

## Base system

- **Update from memory stick** requires network online state (when multiple update stages are involved).

## deskMate

- Integrated deskMate solution. Some stability issues may remain.

## Security Fixes 11.04.100

### Firefox

- Updated Mozilla **Firefox** to **68.10.0esr**:
  - Fixes for **mfsa2020-11**, also known as CVE-2020-6819 and CVE-2020-6820
  - Fixes for **mfsa2020-13**, also known as:  
[More...](#)
  - CVE-2020-6828, CVE-2020-6827, CVE-2020-6821, CVE-2020-6822, and CVE-2020-6825
  - Fixes for **mfsa2020-17** also known as:

**More...**

CVE-2020-12387, CVE-2020-12388, CVE-2020-12389,  
 CVE-2020-6831, CVE-2020-12392,  
 CVE-2020-12393, and CVE-2020-1239

- Fixes for **mfsa2020-21** also known as:

**More...**

CVE-2020-12399, CVE-2020-12405,  
 CVE-2020-12406, and CVE-2020-12410

- Fixes for **mfsa2020-25** also known as:

**More...**

CVE-2020-12417, CVE-2020-12418, CVE-2020-12419,  
 CVE-2020-12420, and CVE-2020-12421

- Changed option to **deny local file browsing** via file:// URI per default now.

**More...**

|            |                                                                |
|------------|----------------------------------------------------------------|
| IGEL Setup | <b>Firefox Browser &gt; Firefox Browser Global &gt; Window</b> |
| Parameter  | Hide local filesystem                                          |
| Registry   | browserglobal.app.filepicker_dialog_hidden                     |
| Value      | <u>enabled</u> / disabled                                      |

## Base system

- **SSH protocol version 1 is now disabled.** All remote connections via SSH must use SSHv2.

## Driver

- Updated **Nvidia driver** to version **440.100**.

## New Features 11.04.100

## Citrix

- Integrated **Citrix Workspace App 20.06**.

Available Citrix Workspace Apps in this release: **20.06** (default), **19.12**, and **18.10**

- Added a registry key to enable optimization for **Microsoft Teams**.

**More...**

|            |                                                                                               |
|------------|-----------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; VDI Solutions</b> |
| Parameter  | Microsoft Teams optimization                                                                  |
| Registry   | ica.module.virtualdriver.vdwebrtc.enable                                                      |
| Value      | <u>on</u> / off                                                                               |

- Added a registry key to enable support for **NetScaler App Experience (NSAP)** virtual channel.

**More...**



|           |                                                   |
|-----------|---------------------------------------------------|
| Parameter | HDX uses the NSAP virtual channel                 |
| Registry  | <code>ica.module.virtualdriver.nsap.enable</code> |
| Value     | <u>on</u> / off                                   |

- Integrated **Citrix HDX/RTME 2.9**.
- Integrated **ZOOM Media Plugin for Citrix** to optimize performance for ZOOM video calls and conferences.
- IGEL x64: 5.0.415463.0619 requires Windows x86 or x64: 5.0.24002.0619. <https://support.zoom.us/hc/en-us/articles/360031096531-Getting-Started-with-VDI>

**More...**

|            |                                                                                               |
|------------|-----------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; VDI Solutions</b> |
| Parameter  | Zoom Media Plugin                                                                             |
| Registry   | <code>ica.module.virtualdriver.vdzoom.enable</code>                                           |
| Value      | <u>enabled</u> / <u>disabled</u>                                                              |

- Updated **signotec Virtual Channel** to version **8.0.9**.

The corresponding changes are:

- Logging has been improved.
- A problem with the communication with the signature pads was fixed.
- USB communication via bulk transfer is model-independent (improved speed).

- Removed parameter **Content redirection** / `ica.wfclient.crenabled` from TC Setup (**Sessions > Citrix > Citrix Global > HDX Multimedia**).

#### OSC Installer

- Added **dialog "Feature Selection"** in **IGEL OS Creator** for the selection of features to be installed on the target device. It interactively shows if the current selection of features fits onto the device. The selection of features is saved on the OSC installer medium (when allowed) and set as the default selection for the next installation. If "**Migrate Old Settings**" is selected, the set of features of the old installation is set as the default selection.
- **Reduced memory requirements** of OSC installer for **machines without Nvidia graphic card**.

#### WVD

- Added **AAC Codec support** to Audio Output redirection.

**More...**

|          |                                               |
|----------|-----------------------------------------------|
| Registry | <code>sessions.wvd%.options.enable-aac</code> |
| Value    | <u>enabled</u> / <u>disabled</u>              |

#### RDP/IGEL RDP Client 2

- Added the **possibility to add a black background** to the RDP auto-reconnect window.

**More...**

|          |                                                              |
|----------|--------------------------------------------------------------|
| Registry | <code>sessions.rdp.options.reconnect-black-fullscreen</code> |
|----------|--------------------------------------------------------------|



|       |                           |
|-------|---------------------------|
| Type  | bool                      |
| Value | enabled / <u>disabled</u> |

- Added configuration option for the **amount of RDP auto-reconnect retries**. The default value will remain "20". A value of "0" means infinite retries.

[More...](#)

|          |                                                        |
|----------|--------------------------------------------------------|
| Registry | sessions.rdp.winconnect%.options.reconnect-max-retries |
| Type     | Integer                                                |
| Value    | <u>20</u>                                              |

#### VMware Horizon

- Updated **VMware Horizon** to version **5.4.1**.

For usage with **Blast protocol**, it is recommended to enable **DRI3 graphics mode**:

[More...](#)

|           |                           |
|-----------|---------------------------|
| Parameter | Use DRI3                  |
| Registry  | x.driver.use_dri3         |
| Value     | enabled / <u>disabled</u> |

- Fixed **handling of RDP's fullscreen mode span**, which means to combine all local monitors for one big remote session.

#### PowerTerm

- Updated **Ericom PowerTerm** LTC to version **14.0.0.45623**.

#### Parallels Client

- Updated **Parallels Client** to version **17.1.1**.

#### Teradici PCoIP Client

- Updated **Teradici PCoIP** Client to version **20.04.2-18.04**. The new version supports **hardware-accelerated H.264 decoding with Ultra PCoIP**.
- New parameters:

[More...](#)

|           |                   |
|-----------|-------------------|
| Parameter | Log level         |
| Registry  | pcoip.log-level   |
| Value     | 0 / 1 / 2 / 3 / 4 |

PCoIP sessions **can now use the global setting**.

[More...](#)

|           |                       |
|-----------|-----------------------|
| Parameter | Show codec indicator  |
| Registry  | pcoip.codec_indicator |



|       |                                                                                                                                                                                                        |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Value | <u>disabled</u> / enabled                                                                                                                                                                              |
| Info  | Show a small dot in the bottom left corner during the session to indicate which codec is being used. Green indicates simple codec; blue indicates tic2 codec. This setting is only available globally. |

## XEN

- Added support to run as **XEN guest system**.

## NX client

- Updated **NoMachine NX Client** to version **6.11.2**.

## ThinLinc

- Updated **ThinLinc** to version **4.12**.

## Network

- DHCP changes:**

The system now sends a **vendor-class-identifier(option 60)** "**igel-dhcp-1**". Furthermore, it requests **vendor-encapsulated-options (43)**. Those can be used to transfer IGEL-specific options **igelrmserver(224)** and **umsstructuretag(226)** in the vendor namespace (with the same option numbers and types) instead of in the global namespace.

The former way is also still functional, but values transferred in the new way override those which were transferred the old way.

Apart from 224 and 226 one more option is defined in the vendor space: **"exclusive"**, **option 1**, **type byte**. Its presence means that global options 224 and 226 shall not be interpreted in the traditional way and only settings in the vendor space apply.

IPv6 is not involved.

- Added support for **LTE module HP lt4132**.
- Updated **Network Manager** to version **1.20.4**.
  - The range of **network.interfaces.wirelesslan.device0.bgscan.module** now includes **"default"** for using original upstream Network Manager settings.
- Added some **additional Ethernet network drivers**.

**More...**

- amd-xgbe : AMD 10 Gigabit Ethernet driver
- ec\_bhf : Beckhoff EtherCAT
- liquidio\_vf : Cavium LiquidIO Intelligent Server Adapter Virtual Function driver
- liquidio : Cavium LiquidIO Intelligent Server Adapter driver
- thunder\_bgx : Cavium Thunder BGX/MAC driver
- nicvf : Cavium Thunder NIC Virtual Function driver
- nicpf : Cavium Thunder NIC Physical Function driver
- thunder\_xcv : Cavium Thunder RGX/XCV driver
- atlantic : aQuantia Corporation(R) network driver
- be2net : Emulex OneConnect NIC driver 12.0.0.0
- ixgb : Intel(R) PRO/10GbE network driver
- igc : Intel(R) 2.5G Ethernet Linux driver



- ice : Intel(R) Ethernet Connection E800 Series Linux driver
- i40e : Intel(R) Ethernet Connection XL710 network driver
- iavf : Intel(R) Ethernet Adaptive Virtual Function network driver
- ixgbe : Intel(R) 10 Gigabit PCI Express network driver
- igbvf : Intel(R) Gigabit Virtual Function network driver
- ixgbefv : Intel(R) 10 Gigabit Virtual Function network driver
- ena : Elastic Network Adapter (ENA)
- nfp : The Netronome Flow Processor (NFP) driver
- bna : QLogic BR-series 10G PCIe Ethernet driver
- enic : Cisco VIC Ethernet NIC driver
- mlx5\_core : Mellanox 5th generation network adapters (ConnectX series) core driver
- mlx4\_en : Mellanox ConnectX HCA Ethernet driver
- ionic : Pensando Ethernet NIC driver
- sfc-falcon : Solarflare Falcon network driver
- sfc : Solarflare network driver
- dwc-xlgmac : Synopsys DWC XLGMAC driver
- hinic : Huawei Intelligent NIC driver
- cassini : Sun Cassini Ethernet driver
- niu : NIU Ethernet driver
- samsung-sxgbe : SAMSUNG 10G/2.5G/1G Ethernet PLATFORM driver
- cxgb : Chelsio 10Gb Ethernet driver
- qede : QLogic FastLinQ 4xxxx Ethernet driver
- qlcnic : QLogic 1/10 GbE Converged/Intelligent Ethernet driver
- qed : QLogic FastLinQ 4xxxx Core module
- netxen\_nic : QLogic/NetXen (1/10) GbE Intelligent Ethernet driver
- vxge : Neterion's X3100 Series 10GbE PCIe I/OVirtualized Server adapter
- myri10ge : Myricom 10G driver (10GbE)
- tehuti : Tehuti Networks(R) network driver
- bnxt\_en : Broadcom BCM573xx network driver
- bnx2x : QLogic BCM57710/57711/57711E/57712/57712\_MF/57800/57800\_MF/57810/57810\_MF/57840/57840\_MF driver
- Added a registry key for specifying a **space-separated list of DNS resolver options**. See "**man resolv.conf**".

[More...](#)

| Parameter | Option list         |
|-----------|---------------------|
| Registry  | network.dns.options |
| Type      | string              |
| Value     | <u>empty</u>        |

## Wi-Fi

- Added support for **WPA3 Personal network authentication**.
- Added a registry key for **preferring WPA3 Personal** (i.e. SAE) or **WPA2 Personal** at the time a connection is created with Wireless Manager when the access point offers both:

[More...](#)



|           |                                       |
|-----------|---------------------------------------|
| Parameter | Prefer WPA3 Personal to WPA2 Personal |
| Registry  | network.applet.wireless.prefer_sae    |
| Range     | [default] [yes] [no]                  |
| Info      | "default" currently means "no"        |

- Added **captive portal support for Wi-Fi**. Passing through a captive portal (which is basically a web application) is sometimes **necessary to achieve full network connectivity** (here also referred to as online state).
  - The **feature is disabled when** the following **registry key is empty**. Otherwise, it should be a **URI** that is **suitable for NetworkManager connectivity check**.
   
**More...**

|           |                                            |
|-----------|--------------------------------------------|
| Parameter | Online check URI                           |
| Registry  | network.global.onlinecheck.uri             |
| Range     | [] [http://connectivity-check.ubuntu.com/] |
| Value     | http://connectivity-check.ubuntu.com/      |

- The following key specifies the **conditions of the online check**. It is also required that **no Ethernet cable is plugged in** and **DHCP is not set** in the UMS.
   
**More...**

|           |                                                    |
|-----------|----------------------------------------------------|
| Parameter | Condition for online check                         |
| Registry  | network.global.onlinecheck.condition               |
| Range     | [None] [Network is user-defined] [Network is open] |

- This key determines **how many seconds to wait for full network connectivity** before the network connection is considered complete with incomplete connectivity. The timeout should allow a user to do what is necessary for passing through the captive portal.
   
**More...**

|           |                                    |
|-----------|------------------------------------|
| Parameter | Online check timeout               |
| Registry  | network.global.onlinecheck.timeout |
| Type      | integer                            |
| Value     | 120                                |

- Enabled **use of 802.11r**, also known as **fast BSS transition** or FT. This is confirmed to work at least in the **mode "over the air"**.

#### Smartcard

- Updated **OpenSC** to version **0.20.0**. See <https://github.com/OpenSC/OpenSC/releases/tag/0.20.0> for detailed release notes.

#### Cisco JVDI Client

- Updated **Cisco JVDI** client to version **12.9.0**.

#### Cisco Webex VDI

- Integrated the new feature **Cisco Webex Teams VDI for Citrix** and **Horizon** sessions.  
**Cisco Webex Teams** version: **3.0.15711.0**



- Added a parameter to activate the feature within **Citrix**:

[More...](#)

|            |                                                                                       |
|------------|---------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; Cisco</b> |
| Parameter  | Cisco Webex Teams VDI                                                                 |
| Registry   | ica.module.virtualdriver.vdciscoteams.enable                                          |
| Value      | enabled / <u>disabled</u>                                                             |

- Added a parameter to activate the feature within **VMware**:

[More...](#)

|            |                                                                                                |
|------------|------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Horizon &gt; Horizon Client Global &gt; Unified Communications &gt; Cisco</b> |
| Parameter  | Cisco Webex Teams VDI - Horizon                                                                |
| Registry   | vmware.view.vdciscoteams.enable                                                                |
| Value      | enabled / <u>disabled</u>                                                                      |

- Integrated the new feature **Cisco Webex Meetings VDI for Citrix** sessions.

Client Version: **40.7.0.375**

- Added a parameter to activate the feature within **Citrix**:

[More...](#)

|            |                                                                                       |
|------------|---------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; Cisco</b> |
| Parameter  | Cisco Webex Meetings VDI                                                              |
| Registry   | ica.module.virtualdriver.vdciscomeetings.enable                                       |
| Value      | enabled / <u>disabled</u>                                                             |

#### Base system

- Updated base system to **Ubuntu LTS** version **18.04**.
- Updated **kernel** to version **5.4.48**.
- Added **notification for critical system out-of-memory state** when the available **system memory is lower than 40 MB** and **processes were killed** to prevent the system from freezing.
- Display **AMD Memory Guard in Boot Mode** when it's active.
- Added **notification option for Session Autostart** when a autostart delay is configured. It is possible to cancel the session autostart or to start immediately.

[More...](#)

|            |                                   |
|------------|-----------------------------------|
| IGEL Setup | <b>* &gt; Desktop integration</b> |
| Parameter  | Autostart notification            |
| Value      | enabled / <u>disabled</u>         |

- Added correct **UI handling** for **Wacom DTU-1141B**.
- Updated **CA Certificates** to version **20190122** (Mozilla authority bundle version **2.30**). The following authorities were added:

[More...](#)

- "Certigna Root CA"



- "GTS Root R1"
- "GTS Root R2"
- "GTS Root R3"
- "GTS Root R4"
- "UCA Extended Validation Root"
- "UCA Global G2 Root"
- "GlobalSign Root CA - R6"
- "OISTE WISEKey Global Root GC CA"
- "GDCA TrustAUTH R5 ROOT"
- "[SSL.com](http://SSL.com)<sup>413</sup> EV Root Certification Authority ECC"
- "[SSL.com](http://SSL.com)<sup>414</sup> EV Root Certification Authority RSA R2"
- "[SSL.com](http://SSL.com)<sup>415</sup> Root Certification Authority ECC"
- "[SSL.com](http://SSL.com)<sup>416</sup> Root Certification Authority RSA"
- "TrustCor ECA-1"
- "TrustCor RootCert CA-1"
- "TrustCor RootCert CA-2"

- The following authorities were removed:

[More...](#)

- "Certplus Root CA G1"
- "Certplus Root CA G2"
- "OpenTrust Root CA G1"
- "OpenTrust Root CA G2"
- "OpenTrust Root CA G3"
- "TÜRKTRUST Elektronik Sertifika Hizmet Saglayicisi H5"
- "Visa eCommerce Root"
- "ACEDICOM Root"
- "AddTrust Low-Value Services Root"
- "AddTrust Public Services Root"
- "AddTrust Qualified Certificates Root"
- "CA Disig Root R1"
- "CNNIC ROOT"
- "Camerfirma Chambers of Commerce Root"
- "Camerfirma Global Chambersign Root"
- "Certinomis - Autorit, Racine"
- "Certum Root CA"
- "China Internet Network Information Center EV Certificates Root"
- "Comodo Secure Services root"
- "Comodo Trusted Services root"
- "DST ACES CA X6"
- "GeoTrust Global CA 2"
- "PSCProcert"

---

<sup>413</sup> <http://SSL.com>

<sup>414</sup> <http://SSL.com>

<sup>415</sup> <http://SSL.com>

<sup>416</sup> <http://SSL.com>



- "Security Communication EV RootCA1"
- "Swisscom Root CA 1"
- "Swisscom Root CA 2"
- "Swisscom Root EV CA 2"
- "TURKTRUST Certificate Services Provider Root 2007"
- "TUBITAK UEKAE Kok Sertifika Hizmet Saglayicisi - Surum 3"
- "UTN USERFirst Hardware Root CA"
- Added parameter to override **rate limit of debug messages** in journal. It should be enabled for debugging processes which generate a big amount of messages in order to avoid skipping of messages.

[More...](#)

|           |                               |
|-----------|-------------------------------|
| Parameter | No rate limit                 |
| Registry  | system.journald.no_rate_limit |
| Value     | enabled / <u>disabled</u>     |

- It's possible to **extend the login options of the Kerberos** login window now.

There are several new registry keys:

[More...](#)

|           |                                                |
|-----------|------------------------------------------------|
| Parameter | extended login                                 |
| Registry  | sessions.xlock0.options.login_extension_active |
| Value     | enabled / <u>disabled</u>                      |

If enabled, an "**Associate Type**" **combo box** is shown. The **entries of the combo box** are **configured with** the following **login\_feature1**, **login\_feature2**, and **login\_feature3** **keys**.

- Configure the **label of the "Associate Type" combo box**:

[More...](#)

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | login features label                         |
| Registry  | sessions.xlock0.options.login_features_label |
| Value     | Default: empty which means "Associate Type"  |

- **The first entry of the "Associate Type" combo box.** To enable the combo box entry, add e.g. the text "Store associate at home store".

[More...](#)

|           |                                        |
|-----------|----------------------------------------|
| Parameter | login_feature1                         |
| Registry  | sessions.xlock0.options.login_feature1 |

**If the entry is selected, the username is expanded by a fixed string** defined in **login\_extension\_default** registry key.

- The **fixed username extension** for the first feature. It can be set e.g. by a script.

[More...](#)

|           |                                                 |
|-----------|-------------------------------------------------|
| Parameter | login extension default value                   |
| Registry  | sessions.xlock0.options.login_extension_default |



- **The second entry of the "Associate Type" combo box.** To enable the combo box entry, add e.g. the text "Store associate visiting this store".

[More...](#)

|           |                                        |
|-----------|----------------------------------------|
| Parameter | login_feature2                         |
| Registry  | sessions.xlock0.options.login_feature2 |

If the entry is selected, the username is expanded by a suffix that is entered in a separate entry widget.

- The **label of the entry field for the username suffix.** Set it e.g. to "Store Number".

[More...](#)

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | login_extension_label                         |
| Registry  | sessions.xlock0.options.login_extension_label |
| Value     | Default: empty which means "no label"         |

- **The third entry of the "Associate Type" combo box.** To enable the combo box entry, add e.g. the text "Homeoffice associate visiting this store".

[More...](#)

|           |                                        |
|-----------|----------------------------------------|
| Parameter | login_feature3                         |
| Registry  | sessions.xlock0.options.login_feature3 |

If the entry is selected, another domain can be selected from an appended domain combo box.

- The **label for the domain entry field.**

[More...](#)

|           |                                            |
|-----------|--------------------------------------------|
| Parameter | login domain label                         |
| Registry  | sessions.xlock0.options.login_domain_label |
| Value     | Default: empty which means "domain"        |

- The **extension to the username is added after a dot ('.')**.
- For the **domain drop-down box, four different domains are configurable** here:

[More...](#)

|            |                                                                  |
|------------|------------------------------------------------------------------|
| IGEL Setup | <b>Security &gt; Active Directory/Kerberos &gt; Domain 1 - 4</b> |
| Parameter  | Fully qualified domain name                                      |
| Registry   | auth.krb5.realms.realm0.realm                                    |
| Registry   | auth.krb5.realms.realm1.realm                                    |
| Registry   | auth.krb5.realms.realm2.realm                                    |
| Registry   | auth.krb5.realms.realm3.realm                                    |

- There are keys to **add more domain names:**

[More...](#)

|           |                                 |
|-----------|---------------------------------|
| Parameter | Domain                          |
| Registry  | auth.krb5.extended_domain%.name |


**Info**

Add a new instance for each domain entry.

- In the Kerberos login window, it's now possible to turn on or off **numlock** and/or **capslock for password input**.

Registry keys:

[More...](#)

|           |                                                                                                                |
|-----------|----------------------------------------------------------------------------------------------------------------|
| Parameter | Handling of numlock                                                                                            |
| Registry  | <code>sessions.xlock0.options.numlock_approach</code>                                                          |
| Range     | [ <u>don't change</u> ] [set on] [set off]                                                                     |
| Info      | "set on": force numlock on when password is entered<br>"set off": force numlock off when password is entered   |
| Parameter | Handling of capslock                                                                                           |
| Registry  | <code>sessions.xlock0.options.capslock_approach</code>                                                         |
| Range     | [ <u>don't change</u> ] [set on] [set off]                                                                     |
| Info      | "set on": force capslock on when password is entered<br>"set off": force capslock off when password is entered |

- It's now possible to **show a message in the Kerberos login window**. Registry key:

[More...](#)

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | banner text                                      |
| Registry  | <code>sessions.xlock0.options.banner_text</code> |
| Info      | The user will see the message on the top border. |

- In the Kerberos login window, there is a **mode to convert passwords always to upper case**. To turn it on, use:

[More...](#)

|           |                                                                |
|-----------|----------------------------------------------------------------|
| Parameter | case-insensitive password                                      |
| Registry  | <code>sessions.xlock0.options.case_insensitive_password</code> |
| Value     | enabled / <u>disabled</u>                                      |

- With this key, the text for the **case-insensitive indicator** can be modified:

[More...](#)

|           |                                                            |
|-----------|------------------------------------------------------------|
| Parameter | case-insensitive text                                      |
| Registry  | <code>sessions.xlock0.options.case_insensitive_text</code> |
| Value     | Default: empty which means "case-insensitive"              |

- Fixed **ThinkPad Brazil keyboard layout**.

- It is possible to **show a custom logo** in the Kerberos login window. Also, the **background and text color is customizable** now.

Registry keys:

[More...](#)

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | path for login image                             |
| Registry  | <code>sessions.xlock0.options.login_image</code> |



|           |                                                             |
|-----------|-------------------------------------------------------------|
| Value     | /usr/share/pixmaps/greeter-user.svg                         |
| Info      | Supported image formats include: PNG, JPG, SVG              |
| Parameter | set specific colors for greeter                             |
| Registry  | sessions.xlock0.options.set_color                           |
| Value     | enabled / <u>disabled</u>                                   |
| Parameter | text color                                                  |
| Registry  | sessions.xlock0.options.text_color                          |
| Value     | #ffffff                                                     |
| Info      | Text color in the format #rrggbba<br>Example: #ff0077       |
| Parameter | background color                                            |
| Registry  | sessions.xlock0.options.background_color                    |
| Value     | #000000                                                     |
| Info      | Background color in the format #rrggbba<br>Example: #7700ff |

- Added **new local logon method "Login with Smart Card Certificate"**. It implements the **pam\_pkcs11 smartccard authentication module**. For a successful configuration, the following has to be provided via **UMS file transfer**:
  - root and intermediate CA certificates** for verification of the client certificates in folder /etc/pam\_pkcs11/cacerts
  - file /etc/pam\_pkcs11/cn\_map which contains **mappings of Common Names to UPN names**.  
Each line is in the format \<common name> -> \<logon name>  
where  
\<common name> is the common name part of the subject of the certificate  
\<logon name> is
  - in case of **Kerberos Enterprise** (auth.login.krb5\_enterprise) **disabled**:  
the UPN name of the SubjectAltName extension of the certificate,  
e.g. [user@MY.DOMAIN](mailto:user@MY.DOMAIN)<sup>417</sup>
  - in case of **Kerberos Enterprise** (auth.login.krb5\_enterprise) **enabled**:  
the UPN name of the SubjectAltName extension of the certificate with Default Domain (auth.krb5.libdefaults.default\_realm) suffix,  
e.g. [user@DOMAIN.SUFFIX@DEFAULT.DOMAIN](mailto:user@DOMAIN.SUFFIX@DEFAULT.DOMAIN)<sup>418</sup>
- The logon method **can either be used standalone or together with Kerberos logon** as a fallback if Kerberos does not succeed.

[More...](#)

|           |                                   |
|-----------|-----------------------------------|
| Parameter | Login with Smart Card Certificate |
| Registry  | auth.login.pkcs11                 |

<sup>417</sup> mailto:[user@MY.DOMAIN](mailto:user@MY.DOMAIN)

<sup>418</sup> mailto:[DOMAIN.SUFFIX@DEFAULT.DOMAIN](mailto:DOMAIN.SUFFIX@DEFAULT.DOMAIN)



|           |                                                  |
|-----------|--------------------------------------------------|
| Value     | <u>false</u> / true                              |
| Parameter | Certificate verification policy                  |
| Registry  | auth.login.pkcs11_cert_policy                    |
| Value     | <u>ca,ocsp_on,signature</u>                      |
| Parameter | Enable Debugging of Smart Card Certificate Logon |
| Registry  | auth.login.pkcs11_debug                          |
| Value     | <u>false</u> / true                              |

- It is possible to expand the store number by a registry key:

[More...](#)

|           |                                      |
|-----------|--------------------------------------|
| Parameter | expand store                         |
| Registry  | sessions.xlock0.options.expand_store |
| Value     | <u>enabled</u> / <u>disabled</u>     |

- Fixed: The **login screen** is **adjusted to lower resolutions**.

- It is possible to activate enter key to login on all fields.

[More...](#)

|           |                                    |
|-----------|------------------------------------|
| Parameter | auto login on all fields           |
| Registry  | sessions.xlock0.options.auto_login |
| Value     | <u>enabled</u> / <u>disabled</u>   |

## X11 system

- Changed: Use **modesetting graphics driver** on **devices with newer intel GPUs**.
- Changed registry key:

[More...](#)

|           |                                                   |
|-----------|---------------------------------------------------|
| Parameter | Use generic modesetting driver for INTEL hardware |
| Registry  | x.drivers.intel.use_modesetting                   |
| Range     | [Auto] [True] [False]                             |

- Updated **DisplayLink driver** to version **5.3.1.34**.

- Added new registry key for **Nvidia cards** (use this **if you want to use PRIME**):

[More...](#)

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | Enable/Disable NVIDIA Kernel Modesetting support |
| Registry  | x.drivers.nvidia.use_modeset                     |
| Range     | [Default] [Enabled] [Disabled]                   |
| Info      | "Default" is currently the same as "disabled"    |

- Updated **florence soft keyboard** to version **0.6.3**.

- Removed 640x480** from possible **display resolution range**.

- Added possibility to **change the order of primary** and **secondary graphic card**.

New registry key:

[More...](#)

|           |                                                    |
|-----------|----------------------------------------------------|
| Parameter | Make the secondary graphic card to the primary one |
| Registry  | x.drivers.swap_card0_with_card1                    |
| Value     | <u>true</u> / <u>false</u>                         |



- Added possibility to **invert the order of all graphic cards**.

New registry key:

[More...](#)

|           |                                      |
|-----------|--------------------------------------|
| Parameter | Invert default graphic card ordering |
| Registry  | x.drivers.swap_all                   |
| Value     | true / false                         |

- Added possibility to **choose the driver** which should become **the primary graphic card**.

New registry key:

[More...](#)

|           |                                                                             |
|-----------|-----------------------------------------------------------------------------|
| Parameter | Choose which drivers should be preferred to become the primary graphic card |
| Registry  | x.drivers.preferred_driver                                                  |
| Value     |                                                                             |

## X server

- Added possibility to influence **mode used for mirroring screens with different resolutions**. (Notice: here scaling may not always work).

New registry key:

[More...](#)

|           |                                                                                   |
|-----------|-----------------------------------------------------------------------------------|
| Parameter | Choose the mode which should be used for mirroring monitors if resolution differs |
| Registry  | x.xserver0.mirror_mode                                                            |
| Range     | [Default] [Biggest common resolution] [Scaling]                                   |
| Value     | Default (use panning if needed)                                                   |

## Driver

- Updated **Grundig Dictation driver for Citrix** and **RDP** to version **0.10**.

The changes are:

- Support **third-party USB HID devices** in a more flexible way
- Fixed USB transfer overflow for **Philips LFH 9620**
- Remove **erroneous debug output** in release configuration
- Allow to **control** also "**Headphone**" **volume & switches**

- Updated **Olympus driver for dictation** to version **2020-03-23-143654**.

**Changelog:**

New:

- DR-1200: PID 0225
- DR-2300: PID 0256

Changed:

- PID 0253 from DR-2100 to DR-1200

- Updated **Philips Speech driver** to version **G12.9**.

The changes are:

- Support for **Philips SpeechLive**



- Faster and more reliable remote session connection status check
- **Shutdown of the PSPDispatcher.exe** on the server if it's not in use anymore.
- Updated **StepOver TCP client** and **Citrix plugin** to version **2.4.2**. Fixed **crash of Citrix** session while **using the signature pad**.

## Audio

- Integrated **new sound mixer**.
- New combo box for **audio device selection in TC Setup** available:
  - **Accessories > Sound Preferences > Options > Default Sound Output**
  - **Accessories > Sound Preferences > Options > Default Sound Input**

## Appliance Mode

- Integrated: The **new Browser Appliance mode** is the successor for the XenDesktop appliance mode. The Browser is configured as in XenDesktop appliance mode, but **does not use the upstream SAS window**.

[More...](#)

|            |                                                  |
|------------|--------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b>              |
| Parameter  | Browser                                          |
| Registry   | xen.xenapp-morph.enabled                         |
| Type       | Bool                                             |
| Value      | enabled / disabled                               |
| IGEL Setup | <b>Sessions &gt; Appliance Mode &gt; Browser</b> |
| Parameter  | Web URL                                          |
| Registry   | xen.xenapp-morph.xendeliveryserverurl            |
| Type       | string                                           |

- A **hyperlink to the "On-screen Keyboard"** is available on the right side under **"Related Configurations"**.

## Multimedia

- Added **ffmpeg support** for following codecs:
  - Added support for **new decoders**:
    - [More...](#)
    - flac, gif, libaom\_av1, mjpeg, mjpegb,  
mp1, mp1float, mp2, mp3, mp3adu,  
mp3adufloat, mp3float, opus, theora, vorbis,  
vp2, vp8, vp9, and wavepack
  - Added support for **new encoder**: libopus
  - Added support for **new hwaccels**:
    - [More...](#)
    - mjpeg\_vaapi, mpeg1\_vdpau, mpeg2\_vaapi,  
mpeg2\_vdpau, vp8\_vaapi, and vp9\_vaapi
  - Added support for **new parsers**: avi, flac, gif, matroska, mp3, ogg, and wav
  - Added support for **new demuxers**: avi, flac, gif, matroska, ogg, and wav
  - Added support for **new muxers**: ogg and opus



## Chromium Browser

- Integrated **Chromium** browser version **83.0.4103.61** as experimental feature.  
Configurable at **IGEL Setup > Sessions > Chromium Browser > Chromium Browser Global** and **IGEL Setup > Sessions > Chromium Browser > Chromium Browser Sessions**
- Main switch to enable and disable **IGEL configuration**:  
[More...](#)

|            |                                                                                                                                                                                                                                                                                                |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Chromium Browser &gt; Chromium Browser Global</b>                                                                                                                                                                                                                             |
| Parameter  | Use IGEL Setup for configuration                                                                                                                                                                                                                                                               |
| Registry   | chromiumglobal.app.igelsetupconfig                                                                                                                                                                                                                                                             |
| Value      | disabled / enabled                                                                                                                                                                                                                                                                             |
| Info       | <p>With disabled IGEL configuration, you can use the generic Custom Setup to configure Chromium.</p> <p>The Custom Setup can be found at <b>IGEL Setup &gt; Sessions &gt; Chromium Browser &gt; Chromium Browser Global &gt; Custom Setup: Policies, Preferences, Commandline Options</b>.</p> |

- Parameter for **enabling** and **disabling** the **H.264 decoding**:  
[More...](#)

|            |                                                                                                                                |
|------------|--------------------------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Chromium Browser &gt; Chromium Browser Global</b>                                                             |
| Parameter  | H.264 decoding                                                                                                                 |
| Registry   | chromiumglobal.app.h264_decoding                                                                                               |
| Value      | enabled / disabled                                                                                                             |
| Info       | Enable Audio/Video playback of non-free codecs (H.264+AAC) - the support is in a beta state and therefore disabled by default. |

## Evidian

- Added the Evidian **built-in option 'Process To Spy'**.  
[More...](#)

|          |                         |
|----------|-------------------------|
| Registry | evidian.processtospy    |
| Value    | YOUR-PROCESS / disabled |

## ControlUp

- Integrated **ControlUp Monitoring Tool for Citrix** and **Horizon** sessions.

## Hardware

- Added hardware support for **Lenovo M625q**.
- Added hardware support for **LG CL600N**.
- Added hardware support for **HP Engage Go Mobile System**.
- Added hardware support for **Fujitsu FUTRO S740**.



- Added hardware support for **OnLogic CL210G-10**.
- Added hardware support for **OnLogic KARBON 300**.
- Added hardware support for **Rein Medical Clinio S 522TCT** and **S 524TCT**.
- Added hardware support for **HP t640 Thin Client**.
- Added basic support for **Macbook models 2018 and newer**.
- Added support for **Sennheiser MB 660, SC 630, SC 45, SC 160 headsets**.
- Added support for **Plantronics Savi 8245 Office, Voyager 6200 UC, Savi 8220 headsets**.
- Added serial port driver for **Exar UART PCIe card**.
- Added driver for **GSPCA based webcams**.

#### TC Setup (Java)

- Added Setup page **Sessions > Horizon Client > Horizon Client Global > Window**. Settings for "**Window size**" and "**Multimonitor full-screen mode**" can be set.  
These settings are repeated and originate in RDP Global but are now presented in a more obvious place for Horizon sessions.

#### IGEL Cloud Gateway

- Added support for **Secure Terminal over ICG**.
- **Changed default order of connecting to the IGEL Remote Management** - an available UMS Server is preferred now by default. The device establishes a configured ICG connection only if the UMS Server is not reachable. This behavior can be changed by the parameter:  
[More...](#)

|          |                                                       |
|----------|-------------------------------------------------------|
| Registry | <code>system.remotemanager.icg_try_ums_connect</code> |
| Value    | <u>true</u> / false                                   |

#### Fabulatech

- Updated **FabulaTech Scanner for Remote Desktop** client to version **2.4.0.11**.
- Updated **FabulaTech plugins** to version **3.6.2**.
- Updated **Fabulatech USB for Remote Desktop plugins** to version **3.6.8**.

#### Jabra

- **Jabra Xpress** (JDU) is upgraded to the **7.2.0-509** version. List of the newly introduced parameters:  
[More...](#)

|          |                                                     |
|----------|-----------------------------------------------------|
| Registry | <code>jabra.xpress.show_jdu_gui</code>              |
| Value    | <u>true</u> / false                                 |
| Registry | <code>jabra.xpress.device_dashboard.autopost</code> |
| Value    | <u>true</u> / false                                 |

#### Resolved Issues 11.04.100

##### Citrix

- "**Green artifacts**" problem in Citrix sessions (most probably) fixed.
- Citrix **hardware video acceleration** supports the **latest Intel hardware**.

##### OSC Installer



- Fixed issue with **filesystems not** always get detected correctly in **initramfs OSC Installer** (needed for using iso file boot parameter).
- Fixed: **username and password in the error message** are not shown anymore when firmware file could not be downloaded.
- Get **URLs** with **username:password@** working.

## RDP/IGEL RDP Client 2

- Fixed error when **renaming a non-empty shared folder**.

## WVD

- Includes **WVD client** with fixed **RDcoreSDK** version.
- **Clipboard redirection** has potential privacy and security risks and is therefore **disabled by default**.
- **IGEL WVD Client** integrated

## VMware Horizon

- Fixed missing **support for ThinPrint** and **Skype for Business** when starting **Horizon from Firefox browser**.

## Firefox

- Fixed Firefox **block extension missing tabs** created via command line argument.
- Fixed **rtsp media stream** with enabled apparmor.
- **Show "blocked" page instead of closing tab** when blocked page is viewed in Firefox.
- Fixed functionality in the local setup to start the **certificate manager of the Firefox browser**.
- Fixed functionality in the local setup to **start the Firefox browser with the internal page to show the installed plugins**.
- Fixed **restart mechanism in the Firefox** browser where the browser could not be closed on suspend resulting in a superfluous browser window on resume.

## Network

- Improved **Wi-Fi DHCP lease handling**: Leases are discarded when the network changes. The former behavior caused problems with certain iPhone IOS versions.
- **802.1X failures** now generally **result in falling back to a connection without authentication**, e.g. also in the case of 802.1X settings that don't make sense at all. This only **applies if the fallback is allowed** of course.
- **wpa\_supplicant** now adds **timestamps to entries of its log file**.
- Use **e1000e driver** out of the kernel **as default** instead of the third-party driver.
- Added a registry key that determines whether **lldpd is in receive-only mode**.  
**More...**

|            |                                                                                      |
|------------|--------------------------------------------------------------------------------------|
| Parameter  | Disable sending LLDP packets                                                         |
| Registry   | network.lldp.rxonly                                                                  |
| Value      | true                                                                                 |
| Attention: | If the behavior since 10.06.100 shall be preserved, this key must be set to "false". |

- Updated **scep** to version **0.7.0**.



## Wi-Fi

- Fixed non-working **Marvell WLAN device 8997** (SDIO version).

## NCP VPN

- Added fix for **NCP Secure Client**.

## genucard VPN

- **genucard 3 is supported** now.

## Imprivata

- **Control the visibility** of the **Horizon session control bar** via registry parameter:

[More...](#)

|          |                           |
|----------|---------------------------|
| Registry | vmware.view.menu-bar      |
| Value    | <u>enabled</u> / disabled |

- Honor the Citrix Window Configuration in **Imprivata Appliance Mode**.

- Fixed **Lock key** and **Tap out** behavior.

- Fixed **MS RDSH** session.

- Simplified the configuration of **Imprivata FUS**.

- **Enable the following** if you use **Imprivata** versions **above 6.3**:

[More...](#)

|          |                                  |
|----------|----------------------------------|
| Registry | imprivata.gain_permission        |
| Value    | <u>enabled</u> / <u>disabled</u> |

- Fixed **bug regarding Imprivata** and **On-Screen Keyboard**.

- **Restore the keyboard map** after Horizon sessions.

## Smartcard

- Fixed not working **90meter in Firefox** when **apparmor** is active.

- Fixed problem in **smartcard resource manager PC/SC-Lite** which caused **disconnects of VMware Horizon sessions** when using smartcards with certain applications.

- Added **driver for smartcard reader Elatec TWN4 CCID** (USB 0x09D8:0x0425).

- Updated **cryptovision scInterface** to version **7.3.1**.

The changes are:

[More...](#)

- Consolidated features of the last versions 7.2 and 7.1

- Malta eID Release

- Added Admin Card Gemalto V3

- Updated **PC/SC-Lite smartcard resource manager** to version **1.8.26**.

## HID

- Fixed: **Switching touchpad to other driver** via IGEL registry key.

## CUPS Printing

- Added new version **25.1.0.425** of **Printerlogic Printer Installer Client**.

- Added **new printer models** into IGEL OS from the current CUPS drivers.

## Base System



- Fixed bug in **folder generation of the Application Launcher**.
- Fixed **TLS certificate verification** problem of **certificates signed by "USERTrust RSA CA" or "COMODO RSA CA"**. The problem could occur in clients like Citrix Workspace App and VMWare Horizon client.
- Fixed **password change with AD/Kerberos**. Before this fix, the password complexity rules were not enforced for users with the Reset Password permission for their account.
- You can now **connect to Bluetooth devices without pairing**. For this a new registry key is available.

**More...**

|           |                                 |
|-----------|---------------------------------|
| Parameter | connect devices without pairing |
| Registry  | devices.bluetooth.connect_only  |
| Value     | enabled / disabled              |

- **Some devices do not connect automatically after reboot**. To fix that, bluetoothctl connect \<device-ID> can be executed via script. If the **device is connected (0)** or **not (1)** can be seen in return value.

**Known devices** that do not connect:

- dialog semiconductor IoT Multi Sensor DK
- **SSHv1 support is now removed** due to newer openssh libraries.
- **Forcing protocol version 1 via SSH Session > Options is no longer possible**.
- The network.ssh\_server.server\_key\_bits registry key parameter is **removed** due to **depreciation of SSHv1**.
- Updates **systemd** to **Ubuntu Focal version**.
- Improved **stability of mounting network shares** when using a **static network configuration**.
- Fixed **apparmor cache issue after update with OSC installer**.
- Bug fix: **touchscreen calibration** on 1 or more normal screen with 1 touch screen environment.
- Fixed **syslog**, **kern.log**, **auth.log**, and **daemon.log** entries are **not shown in IGEL System Log Viewer**.
- Updated **Grub2** to current Debian SID/Bullseye version **2.04**.
- **Removed** deprecated registry keys system.idlecommand.
- New **Bluetooth pairing tool** and **Bluetooth tray icon** for Bionic.
- Updated **kernel** to mainline version **5.4.48**.
- If used as master image, the **image will expand itself to full size** (limited to 16 GiB) on flash. This is done only on first boot and never again.
- Possible **rollout of initial settings, certificates or licenses placed on first partition** for this you need to:
  - a. Write image to your USB/Flash medium.
  - b. Mount or simply access the **1. VFAT partition** which is present (should be empty).
  - c. Copy your **setup.ini** and/or **\*\*.lic files** to the 1st partition (no directories).
  - d. Create a ca-certs directory and copy your certificates into it. They will be copied to the /wfs/ca-certs directory on first boot.
  - e. You can now copy the USB/Flash medium several times if needed.
  - f. On first boot, the device will reboot out of the splash screen (reread changed partition table)
  - g. The settings, certificates and/or licenses will get rolled out and deleted from the 1st partition.



- Added initial support for **Thunderbolt devices** (only limited support here, may work but is not guaranteed).
- Updated IGEL **EULA**.
- Updated **AMD Microcode** to version **3.20191218.1**.
- Updated **Intel Microcode** to version **20200520** and a special update for **J1900 devices**.
- Updated **Intel Microcode** to **20200616** version.
- Added a **userspace oom killer** to the firmware.

#### Firmware Update

- An **ongoing firmware update can now be canceled by the user** when the network online status could not be reached after 10 seconds (since start of the firmware update).

#### H264

- **Citrix hardware video acceleration** supports the latest Intel hardware.

#### Storage Devices

- Fixed mount issues with **Iphone XR/XE/11PRO**.
- **Mobile Device Access** feature respects USB Access Control now.
- Fixed unwanted **ownership change** of automounted Linux filesystem root directories.

#### X11 System

- Fixed **Display Switch not saving settings over reboot**.
  - **Default to settings from Setup** instead of mirror when no Display Switch profile is available.
- Prevent misconfiguration that **picks GPU without render capability as primary** (e.g. Displaylink).
- Improved **Nvidia** with **additional GPU handling**.
- Fixed error with **single-gpu Nvidia card support**.

#### X server

- Fixed a **Xorg crash** due to a **NULL pointer dereference in the Intel driver**.

#### Window Manager

- Fixed **random login** (greeter) **window focus** issues.

#### Shadowing/VNC

- Added the "**snapfb**" option for the VNC server.  
[More...](#)

|          |                                                                                            |
|----------|--------------------------------------------------------------------------------------------|
| Registry | <code>network.vncserver.snapfb</code>                                                      |
| Value    | <u>enabled</u> / <u>disabled</u>                                                           |
| Info     | This option should only be enabled with experienced delays in remote or shadowing session. |

- Improved **security of the password authentication method** - the VNC server does not require anymore a file holding the password. **During client authentication**, the **server retrieves** now the **password from the IGEL Setup**.

#### VNC Viewer



- Fixed **occasional freeze of shadowing session** e.g. when resizing a window. Now **the session gets unlocked again after about 20 seconds.**

**More...**

|           |                                                     |
|-----------|-----------------------------------------------------|
| Parameter | Unlock X server in case of shadowing session freeze |
| Registry  | network.vncserver.grab_buster                       |
| Type      | bool                                                |
| Value     | <u>enabled</u> / disabled                           |

#### VirtualBox

- Fixed **no automatic resolution changes** as **virtualbox guest** issue.

#### Audio

- Fixed **headset microphone using 3.5mm audio jack** in **Dell Wyse 3040**.
- Added possibility to **set** some **snd\_hda\_intel kernel module parameter** to overcome possible issues with sound devices.

New registry keys:

**More...**

|           |                                                                                               |
|-----------|-----------------------------------------------------------------------------------------------|
| Parameter | Enable Message Signaled Interrupt                                                             |
| Registry  | system.sound_driver.snd_hda_intel.enable_ms_i                                                 |
| Type      | bool                                                                                          |
| Value     | <u>enabled</u> / <u>disabled</u>                                                              |
| Parameter | Force enable device                                                                           |
| Registry  | system.sound_driver.snd_hda_intel.enable                                                      |
| Type      | bool                                                                                          |
| Value     | <u>enabled</u> / <u>disabled</u>                                                              |
| Parameter | Position fix quirk                                                                            |
| Registry  | system.sound_driver.snd_hda_intel.position_fix                                                |
| Range     | [Default] [Auto (0)] [LPIB (1)] [POSBUF (2)] [VIACOMBO (3)] [COMBO (4)] [SKL+ (5)] [FIFO (6)] |
| Parameter | Change sound card order                                                                       |
| Registry  | system.sound_driver.snd_hda_intel.index                                                       |
| Type      | integer                                                                                       |
| Value     | <u>empty</u>                                                                                  |
| Parameter | Detection of DMIC devices                                                                     |
| Registry  | system.sound_driver.snd_hda_intel.dmic_detect                                                 |
| Range     | [Default] [Disabled] [Enabled]                                                                |
| Parameter | Enable this if you encounter sound card problems                                              |



|           |                                                                            |
|-----------|----------------------------------------------------------------------------|
| Registry  | system.sound_driver.snd_hda_intel.single_cd                                |
| Type      | bool                                                                       |
| Value     | enabled / <u>disabled</u>                                                  |
| Parameter | Automatic power save timeout                                               |
| Registry  | system.sound_driver.snd_hda_intel.power_save                               |
| Type      | integer                                                                    |
| Value     | <u>empty</u>                                                               |
| Parameter | Reset controller in power save mode                                        |
| Registry  | system.sound_driver.snd_hda_intel.power_save_controller                    |
| Type      | bool                                                                       |
| Value     | enabled / disabled                                                         |
| Parameter | Choose sound model to use                                                  |
| Registry  | system.sound_driver.snd_hda_intel.model                                    |
| Type      | string                                                                     |
| Value     | <u>Auto</u>                                                                |
| Parameter | If you encounter sound problems try to choose one of the alternative masks |
| Registry  | system.sound_driver.snd_hda_intel.probe_mask                               |
| Range     | [ <u>Auto</u> ] [1] [8]                                                    |

- Old settings. **Command at startup removed.**

#### Jabra

- **Avoid deploying of the same Jabra Xpress package several times** on the same Jabra device.

#### Evidian

- Evidian now **triggers the regular Horizon session script**.

#### Hardware

- Fixed non-working **Prolific PL2303 USB-to-serial adapters**.

#### TC Setup (Java)

- **Removed "default" button** left of selection box IGEL Setup: **Sessions > Citrix > Citrix Global > Window > Multimonitor full-screen mode**.

#### Remote Management

- Fixed **repeated firmware registering over the ICG** which can occur after a new firmware was successfully registered in the UMS. The device invokes firmware registering again after every settings transfer from the device to the UMS. This behavior lasts until reboot.
- Fixed **syncing settings changed on the device if the UMS wasn't reachable**.
- Fixed handling of the **structure tag** if it was **configured in the system dialog "UMS Registering"**.



## IGEL Cloud Gateway

- **Maximum waiting time for a response from the ICG server** can now be **configured by** the parameter **system.remotemanager.rmagent\_timeout** (default: 90 seconds).

## VNC

- **Shadowing notification** is **restricted to primary monitor** and **cannot be moved outside of the monitor's visible range**.
- Fixed **sporadic connection failure** in VNC server.
- Fixed **occasional freeze of shadowing session** e.g. when resizing a window. Now the session gets unlocked again after about 20 seconds.

[More...](#)

|           |                                                     |
|-----------|-----------------------------------------------------|
| Parameter | Unlock X server in case of shadowing session freeze |
| Registry  | network.vncserver.grab_buster                       |
| Type      | bool                                                |
| Value     | <u>enabled</u> / disabled                           |

## 7.9 Notes for Release 11.03.500

|                       |            |              |
|-----------------------|------------|--------------|
| <b>Software:</b>      | Version    | 11.03.500    |
| <b>Release Date:</b>  | 2020-04-01 |              |
| <b>Release Notes:</b> | Version    | RN-1103500-1 |
| <b>Last update:</b>   | 2020-04-01 |              |

- [IGEL OS 11](#)(see page 1680)
- [IGEL OS Creator \(OSC\)](#)(see page 1696)

## 7.9.1 IGEL OS 11

- [Supported Devices 11.03.500](#)(see page 1681)
- [Component Versions 11.03.500](#)(see page 1681)
- [General Information 11.03.500](#)(see page 1686)
- [Security Fixes 11.03.500](#)(see page 1686)
- [Known Issues 11.03.500](#)(see page 1687)
- [New Features 11.03.500](#)(see page 1689)
- [Resolved Issues 11.03.500](#)(see page 1693)



## Supported Devices 11.03.500

|         |                                     |
|---------|-------------------------------------|
| UD2-LX: | UD2-LX 51<br>UD2-LX 50<br>UD2-LX 40 |
| UD3-LX: | UD3-LX 60<br>UD3-LX 51<br>UD3-LX 50 |
| UD5-LX: | UD5-LX 50                           |
| UD6-LX: | UD6-LX 51                           |
| UD7-LX: | UD7-LX 11<br>UD7-LX 10              |
| UD9-LX: | UD9-LX Touch 41<br>UD9-LX 40        |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>419</sup>.

## Component Versions 11.03.500

- **Clients**

| Product                          | Version    |
|----------------------------------|------------|
| Cisco JVDI Client                | 12.7.1     |
| Citrix HDX Realtime Media Engine | 2.8.0-2235 |
| Citrix Workspace App             | 18.10.0.11 |
| Citrix Workspace App             | 19.10.0.15 |
| Citrix Workspace App             | 19.12.0.19 |

<sup>419</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



|                                        |                                           |
|----------------------------------------|-------------------------------------------|
| deviceTRUST Citrix Channel             | 19.1.200.2                                |
| Crossmatch DP Citrix Channel           | 0515.2                                    |
| Ericom PowerTerm                       | 12.0.1.0.20170219.2_dev_-34574            |
| Ericom PowerTerm                       | 12.5_x64_20190619_12.5.1.40008            |
| Evidian AuthMgr                        | 1.5.7116                                  |
| Evince PDF Viewer                      | 3.18.2-1ubuntu4.6                         |
| FabulaTech USB for Remote Desktop      | 5.2.29                                    |
| Firefox                                | 68.6.0                                    |
| IBM iAccess Client Solutions           | 1.1.8.1                                   |
| IGEL RDP Client                        | 2.2                                       |
| IGEL WVD Client                        | 1.0.5                                     |
| Imprivata OneSign ProveID Embedded     | onesign-bootstrap-loader_1.0.523630_amd64 |
| deviceTRUST RDP Channel                | 19.1.200.2                                |
| NCP Secure Enterprise Client           | 5.10_rev40552                             |
| NX Client                              | 6.7.6                                     |
| Open VPN                               | 2.3.10-1ubuntu2.2                         |
| Zulu JRE                               | 8.44.0.11                                 |
| Parallels Client (64 bit)              | 17.0.21474                                |
| Spice GTK (Red Hat Virtualization)     | 0.37-1igel62                              |
| Remote Viewer (Red Hat Virtualization) | 8.0-1igel49                               |
| Usbredir (Red Hat Virtualization)      | 0.8.0-1+b1igel71                          |
| Teradici PCoIP Software Client         | 19.05.9-18.04                             |
| ThinLinc Client                        | 4.10.1-6197                               |
| ThinPrint Client                       | 7.5.88                                    |
| Totem Media Player                     | 2.30.2                                    |



|                       |                       |
|-----------------------|-----------------------|
| Parole Media Player   | 1.0.5-1igel1583919770 |
| VNC Viewer            | 1.9.0+dfsg-3igel8     |
| VMware Horizon Client | 5.3.0-15208949        |
| Voip Client Ekiga     | 4.0.1                 |

- **Dictation**

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20180621 |
| Philips Speech driver                     | 12.8.5   |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.8    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.3.2    |

- **Smartcard**

|                                           |                |
|-------------------------------------------|----------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101        |
| PKCS#11 Library Athena IDProtect          | 7              |
| PKCS#11 Library cryptovision sc/interface | 7.1.20         |
| PKCS#11 Library Gemalto SafeNet           | 10.7.77        |
| PKCS#11 Library OpenSC                    | 0.19.0-2igel35 |
| PKCS#11 Library SecMaker NetID            | 6.8.1.31       |
| PKCS#11 Library 90meter                   | 20190522       |
| Reader Driver ACS CCID                    | 1.1.6-1igel2   |
| Reader Driver Gemalto eToken              | 10.7.77        |



|                                    |                        |
|------------------------------------|------------------------|
| Reader Driver HID Global Omnikey   | 4.3.3                  |
| Reader Driver Identive CCID        | 5.0.35                 |
| Reader Driver Identive eHealth200  | 1.0.5                  |
| Reader Driver Identive SCRKBC      | 5.0.24                 |
| Reader Driver MUSCLE CCID          | 1.4.31-1igel10         |
| Reader Driver REINER SCT cyberJack | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite        | 1.8.23-1igel11         |
| Cherry USB2LAN Proxy               | 3.2.0.3                |

- **System Components**

|                                         |                              |
|-----------------------------------------|------------------------------|
| OpenSSL                                 | 1.0.2g-1ubuntu4.15           |
| OpenSSH Client                          | 7.2p2-4ubuntu2.8             |
| OpenSSH Server                          | 7.2p2-4ubuntu2.8             |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5           |
| MESA OpenGL stack                       | 19.2.5-1igel93               |
| VAAPI ABI Version                       | 0.40                         |
| VDPAU Library version                   | 1.2-1igel911                 |
| Graphics Driver INTEL                   | 2.99.917+git20191117-igel939 |
| Graphics Driver ATI/RADEON              | 19.0.1-3igel936              |
| Graphics Driver ATI/AMDGPU              | 19.0.1-5igel924              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867              |
| Graphics Driver Nvidia                  | 418.56-0ubuntu1              |
| Graphics Driver Vboxvideo               | 1.0.0-igel798                |
| Graphics Driver VMware                  | 13.3.0-2igel857              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build2-igel925        |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |
| Graphics Driver VESA                    | 2.4.0-1igel855               |



|                                 |                              |
|---------------------------------|------------------------------|
| Input Driver Evdev              | 2.10.6-1igel975              |
| Input Driver Elographics        | 1.4.1-1build5igel633         |
| Input Driver eGalax             | 2.5.7413                     |
| Input Driver Synaptics          | 1.9.1-1ubuntu1igel866        |
| Input Driver VMMouse            | 13.1.0-1ubuntu2igel635       |
| Input Driver Wacom              | 0.36.1-0ubuntu2igel888       |
| Kernel                          | 4.19.85 #mainline-lxos-r2875 |
| Xorg X11 Server                 | 1.20.5-1igel914              |
| Xorg Xephyr                     | 1.20.5-1igel914              |
| CUPS printing daemon            | 2.1.3-4ubuntu0.10igel29      |
| PrinterLogic                    | 25.1.0.381                   |
| Lightdm Graphical Login Manager | 1.18.3-0ubuntu1.1            |
| XFCE4 Window Manager            | 4.12.3-1ubuntu2igel675       |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7      |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.3igel74 |
| ModemManager                    | 1.10.0-1~ubuntu18.04.2igel3  |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.2           |
| GStreamer 1.x                   | 1.16.1-1igel222              |
| WebKit2Gtk                      | 2.26.2-1igel27               |
| Python2                         | 2.7.12                       |
| Python3                         | 3.5.2                        |

- **Features with Limited IGEL Support**

|                                    |                                  |
|------------------------------------|----------------------------------|
| Mobile Device Access USB (MTP)     | 1.1.16-2igel1                    |
| Mobile Device Access USB (imobile) | 1.2.1~git20191129.9f79242-1igel7 |
| Mobile Device Access USB (gphoto)  | 2.5.23-2igel2                    |



|                 |                     |
|-----------------|---------------------|
| VPN OpenConnect | 7.08-1              |
| Scanner support | 1.0.27-1            |
| VirtualBox      | 6.0.14-dfsg-1igel33 |

## General Information 11.03.500

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

## Security Fixes 11.03.500

### Firefox

- Updated Mozilla Firefox to **68.6.0 ESR**.
- Fixes for **mfsa2020-09**, also known as:

[More...](#)

CVE-2020-6805, CVE-2020-6806, CVE-2020-6807, CVE-2020-6811, CVE-2019-20503, CVE-2020-6812, and CVE-2020-6814

- Fix for **mfsa2020-03**, also known as CVE-2019-17026.
- Fixes for **mfsa2020-02**, also known as:

[More...](#)

CVE-2019-17016, CVE-2019-17017, CVE-2019-17022, and CVE-2019-17024

- Fixes for **mfsa2019-37**, also known as:

[More...](#)

CVE-2019-17008, CVE-2019-11745, CVE-2019-17010, CVE-2019-17005, CVE-2019-17011, and CVE-2019-17012

### Base system

- Fixed **libxml2** security issues CVE-2020-7595 and CVE-2019-19956.



- Fixed **nss** security issues CVE-2019-17007, CVE-2019-17006, and CVE-2019-11745.
  - Fixed **libvncserver** security issue CVE-2019-15681.
  - Fixed **libexif** security issues CVE-2019-9278, CVE-2017-7544, and CVE-2016-6328.
  - Fixed **cyrus-sasl2** security issue CVE-2019-19906.
  - Fixed **samba** security issues CVE-2019-14907, CVE-2019-14870, and CVE-2019-14861.
  - Fixed **zulu** security issues:  
[More...](#)
- CVE-2020-2583, CVE-2020-2590, CVE-2020-2593, CVE-2020-2601,  
CVE-2020-2604, CVE-2020-2659, and CVE-2020-2654

## Known Issues 11.03.500

### Firmware Update

- On **devices with 2 GB of flash storage**, it could happen that there is **too little space for updating all features**. In this case, a corresponding error message occurs and **unused features** must be **disabled** in IGEL Setup **under System > Firmware Customization > Features** to perform the firmware update.

### Firefox

- **Firefox IGEL extensions are not updated automatically** under some circumstances. After an update from 11.03.10x to 11.03.500, the IGEL extensions will stay on the old version.  
In this case, the following settings concerning **kiosk mode** cannot be executed:
  - Switch off Hotkey for new window/tab
  - Blocking of internal browser pages like preferences, file picker, specific local directories

As a workaround:

- a **reset to defaults** should be performed
  - or the **browser's mimetype template** can be switched **from "Standard" to "Minimal"** by registry key `browserglobal.app.mimetypes_template`. There, the browser profile is renewed as well.
- After the TC got the new setting, **reboot** and **set** the `mimetypes_template` registry key **back to "Standard"**.

### Citrix

- With activated **DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.
  - Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1 and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
  - **Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
  - **Citrix StoreFront login** with **Gemalto smartcard** middleware does not detect smartcard correctly if the card is inserted after start of login.
- Workaround: Insert the smartcard before starting the StoreFront login.



- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264** acceleration plugin, the following registry key must be enabled.

[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Value     | enabled / <u>disabled</u>                                        |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

- Using **CWA 19.x** sometimes **freezes the session** while session logoff from a published desktop.  
Workaround: **Use CWA 18.10.0**.

#### VMware Horizon

- **Client drive mapping** and **USB redirection** for storage devices should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Enable local `Storage Hotplug` on setup page **Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection do not appear in the **remote desktop**.  
Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- **After disconnect of an RDP based session**, the Horizon main **window** which contains the server or sessions overview **cannot be resized anymore**.
- **Seamless application windows in Horizon Client may not be displayed correctly**. When starting the first seamless app, a new iconified window appears in the taskbar, and only if you click on it, the application will show up.  
On some hardware (UD7-H850, UD2-M250, UD2-D220), however, the client aborts when this new window is de-iconified.

#### Imprivata

- On **devices with 2 GB of flash storage**, it could happen that there is too little space to enable the **Imprivata partition after the update to 11.03.500**. In this case, a corresponding error message occurs and **unused features must be disabled** (in IGEL Setup under **System > Firmware Customization > Features**). Imprivata has to be (re-)enabled after a reboot then.

#### Wi-Fi



- TP-Link Archer T2UH Wi-Fi adapters does not work after system suspend/resume. Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

#### Parallels Client

- **Native USB redirection** does not work with Parallels Client.

#### Smartcard

- In seldom cases, the **authentication** hung when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice: spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

#### Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.

#### Hyper-V

- **Hyper-V** (Generation 2) needs **a lot of memory**. The machine needs a sufficient amount of memory allocated.

#### VirtualBox

- The current **VirtualBox Guest Tools/Drivers** will not work with **VirtualBox 5.2.x or older** hosts which leads to black screen and non-working graphic.  
Workaround: Install with 'Failsafe Installation + Recovery' and set the registry key `x.drivers.force_vesa` to true.
- When running in VirtualBox virtualization, **resizing the window will not automatically change desktop resolution** of IGEL OS guest.

#### Audio

- **Audio jack detection on Advantech POC-W243L doesn't work**. Sound output goes through the headset connection and the internal speakers.
- **IGEL UD2 (D220)** fails to restore the volume level of the speaker when the device used **firmware version 11.01.110** before.

#### Hardware

- **HP t730** could freeze when monitors with **different resolutions** are connected (1920x1200 + 2560x1440 + 3840x1600 for example). When this occurs, the registry key `x.drivers.kms.best_console_mode` has to be set to **disabled**.
- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work with INTEL devices.

#### Remote Management

- **AIT feature with IGEL Starter License is supported** by the next **UMS version 6.05.100**.

## New Features 11.03.500

#### Citrix



- Integrated **Citrix Workspace App 19.12**
- Available **Citrix Workspace Apps** in this release: **19.12** (default), **19.10**, and **18.10**
- New **registry keys**:
  - Added a registry key for enabling **full-screen banner "Citrix Desktop Viewer"** when starting a Desktop or Application session.

[More...](#)

|           |                                   |
|-----------|-----------------------------------|
| Parameter | Show Citrix Desktop Viewer screen |
| Registry  | ica.module.cdviewerscreen         |
| Value     | <u>off</u> / on                   |

- Added a registry key to enable usage of **Chromium Embedded Framework (CEF) for Browser Content Redirection (BCR)** [Experimental].

[More...](#)

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Use Chromium Embedded Framework (CEF)        |
| Registry  | ica.allregions.usecefbrowser                 |
| Value     | <u>factory default is "*" / false</u> / true |

- "factory default" impact can be set by config file.
- Changed default:

[More...](#)

|           |                                       |
|-----------|---------------------------------------|
| Parameter | VDTUI protocol                        |
| Registry  | ica.module.virtualdriver.vdtui.enable |
| Value     | <u>off</u> / <u>on</u>                |

## WVD

- Integrated **IGEL WVD Client**.

## VMware Horizon

- Updated **VMware Horizon Client** to version **5.3.0**.

## ThinLinc

- Updated **ThinLinc Client** to version **4.11.0**.

## Smartcard

- Updated **Gemalto / Safenet smartcard middleware** to version **10.7.7**.
- Added **support for smartcard reader HP Business Slim Smartcard CCID Keyboard**.
- Added **configuration parameter to disable PIN pad functionality of smartcard readers**, driven by Open Source CCID driver. This might work to solve problems with PIN pads, but lowers security level.

[More...](#)

|           |                                 |
|-----------|---------------------------------|
| Parameter | Disable PIN pad                 |
| Registry  | scard.pcscd.ccid.disable_pinpad |



|       |                           |
|-------|---------------------------|
| Value | <u>disabled</u> / enabled |
|-------|---------------------------|

- Added possibility to **add custom CCID smartcard readers to Open Source CCID driver**. Readers can be specified by USB Vendor, Product Id, and custom name:

[More...](#)

|           |                                          |
|-----------|------------------------------------------|
| Parameter | USB Vendor Id                            |
| Registry  | scard.pcscd.ccid.custom_reader<num>.vid  |
| Value     |                                          |
| Parameter | USB Product Id                           |
| Registry  | scard.pcscd.ccid.custom_reader<num>.pid  |
| Value     |                                          |
| Parameter | Reader name                              |
| Registry  | scard.pcscd.ccid.custom_reader<num>.name |
| Value     |                                          |

- Updated **Athena IDProtect library** to version 7. This version **supports CRYPTAS TicTok V3 cards**. Known issue: The **detection of locked PIN does not work**.

#### CUPS Printing

- Added **CUPS Printer port "USB class printer"**. The USB printer is assigned, in this case, by **matching patterns of USB Manufacturer and Product name strings**. In this way, a single printer definition could work for a class of different USB printer models.

[More...](#)

|            |                                                          |
|------------|----------------------------------------------------------|
| IGEL Setup | <b>Devices &gt; Printer &gt; CUPS &gt; Printers</b>      |
| Parameter  | Printer port                                             |
| Registry   | print.cups.printer<num>.backend                          |
| Value      | USB class printer                                        |
| IGEL Setup | <b>Devices &gt; Printer &gt; CUPS &gt; Printers</b>      |
| Parameter  | Pattern matching mode                                    |
| Registry   | print.cups.printer<num>.usbclass_mode                    |
| Value      | pattern / pattern, case insensitive / regular expression |
| IGEL Setup | <b>Devices &gt; Printer &gt; CUPS &gt; Printers</b>      |
| Parameter  | Manufacturer pattern                                     |
| Registry   | print.cups.printer<num>.usbclass_manufacturer            |
| IGEL Setup | <b>Devices &gt; Printer &gt; CUPS &gt; Printers</b>      |
| Parameter  | Product pattern                                          |
| Registry   | print.cups.printer<num>.product                          |



- Updated **PrinterLogic Printer-Installer-Client** to version **25.1.0.381**. Fixed tray icon functionality.

## Cisco JVDI Client

- Integrated **Cisco JVDI 12.7.1 client**. Cisco JVDI 12.7.0 has been removed.

## Base system

- Added **Starter License functionality**.

This license is now part of every new IGEL OS installation and is **valid for 30 days**. The license will be activated with the first boot after the initial installation. More and detailed information via <https://kb.igel.com/licensing>.

- Added 'Licensing' tool to 'System' in **local Start menu**. Disable the tool by key:  
[More...](#)

| IGEL Setup | <b>Accessories &gt; License Browser</b>    |
|------------|--------------------------------------------|
| Parameter  | Start Menu's System tab                    |
| Registry   | sessions.license_browser0.startmenu_system |
| Value      | <u>enabled</u> / disabled                  |

If there is only the Starter License and no UMS connection, the **Licensing tool is shown on the desktop by default**.

- Added feature **Custom Partition to Workspace Edition license**.
- Updated **Fluendo multimedia codecs** to the following versions: **gst-fluendo-vadec - 30/01/2020 0.10.212**.
- **Kerberos Logon:**  
You can now **turn on/off numlock** and/or **capslock** for password input. Registry keys:  
[More...](#)

|           |                                                                                                                |
|-----------|----------------------------------------------------------------------------------------------------------------|
| Parameter | Handling of numlock                                                                                            |
| Registry  | sessions.xlock0.options.numlock_approach                                                                       |
| Value     | <u>don't change</u> / set on / set off                                                                         |
| Note      | "set on": force numlock on when password is entered<br>"set off": force numlock off when password is entered   |
| Parameter | Handling of capslock                                                                                           |
| Registry  | sessions.xlock0.options.capslock_approach                                                                      |
| Value     | <u>don't change</u> / set on / set off                                                                         |
| Note      | "set on": force capslock on when password is entered<br>"set off": force capslock off when password is entered |

- Added configuration for special **thinkpad keyboard model**:  
[More...](#)

| IGEL Setup | <b>User Interface &gt; Input &gt; Keyboard</b> |
|------------|------------------------------------------------|
| Parameter  | Keyboard type                                  |
| Registry   | userinterface.keyboard.type                    |



|       |                                                                                                                                                                                 |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Range | [Default] [Standard PC Keyboard (105 Keys)] [IBM Keyboard (122 Keys)]<br>[Trimodal Keyboard] [Sun Type 6 Keyboard] [Chromebook]<br>[Macbook] [Macbook international] [Thinkpad] |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Wi-Fi

- Added **driver for Realtek 8822ce** and **8822be** Wi-Fi hardware.
- Added driver for **Realtek 8821cu** Wi-Fi hardware.

## Driver

- Updated **Crossmatch DP driver for fingerprint**. The new version allows the **fingerprint image** to be **sent via the Citrix channel**. With this change, customers will be able to develop their own SW using the Crossmatch DP SDK.

## Misc

- Updated **Login PI 3.6** to the new **Login Enterprise 4.0**.

## Resolved Issues 11.03.500

## Citrix

- Fixed **video playback on BBC websites** redirected via Citrix Browser Content Redirection.
- Fixed **Multimedia redirection** and **HDX RealTime Media Engine** may used concurrently.

## OSC Installer

- Fixed issue with **failed partitioning**.

## RDP/IGEL RDP Client 2

- Added a new parameter to control **audio latency** (in milliseconds) which **defines the amount of buffered audio data in the RDP client**.

[More...](#)

|          |                              |
|----------|------------------------------|
| Registry | rdp.winconnect.sound-latency |
| Value    | <u>125</u> (msec)            |

## WVD

- Improved overall sound quality.
- Fixed issue caused **audio redirection to fail randomly**.
- Clipboard redirection has potential privacy and security risks** and is therefore disabled by default.
- Fixed **dead key support** (key composition).
- Fixed **sound getting choppy** after a while.
- Several **bugfixes** for all kind of **stability issues**.

## VMware Horizon



- Fixed: **Save VMWare Horizon user from last login** when **in appliance mode**. Reduced the options for "**Preset login information**" to either "**from last login**" or "**from session setup**". The redundant option "from appliance mode" **is removed** because the appliance mode is also treated as a session.

[More...](#)

|            |                                                                                 |
|------------|---------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Local Logon</b> |
| Parameter  | Preset login information                                                        |
| Registry   | vmware.login.saveusertype                                                       |
| Range      | [Set user/domain from last login] [Set user/domain from session setup]          |

- Fixed **Skype for Business** integration.

#### Firefox

- Fixed **switching off** firmware feature **PrinterLogic removes browser policies file**.
- Fixed **hiding the URL input** results in **disappearing web content**.
- Fixed **browser startscript** which was waiting for a new window even when browser was not configured to open an extra one.

#### Network

- Use **e1000e driver out-of-the-kernel as default** instead of the third-party driver.

#### Wi-Fi

- Fixed **connection problems by updating the regulatory domain database**.
- Improved **persistence of Wi-Fi switch state** across reboots.
- Fixed problems with **Wi-Fi backports driver** and older **Wi-Fi adapters** or **adapters with external kernel drivers**.

#### Open VPN

- Fixed **timing in OpenVPN credential dialogs** to prevent **focus loss** when started too early at system boot.
- Fixed **session management** where **VPN connections could get stuck when wrong passwords** were entered with no possibility of retry.

#### Imprivata

- Hide the **Imprivata session templates on the desktop** as this is misleading.

#### Smartcard

- Fixed smartcard reader **VASCO/OneSpan Digipass 905. Disabled USB auto suspend** for all smart card readers.
- Added **parameter to control the used smartcard protocol** when connecting with raw and other protocols allowed. Enable to read smartcards using **NHS Identity Agent**.

[More...](#)

|           |                                |
|-----------|--------------------------------|
| Parameter | Avoid raw protocol             |
| Registry  | scard.pcscd.avoid_raw_protocol |



|       |                     |
|-------|---------------------|
| Value | <u>false</u> / true |
|-------|---------------------|

- Fixed use of **IDPrime smartcards inside sessions** with readers driven by **Open Source CCID** smartcard reader driver: implemented attribute SCARD\_ATTR\_CHANNEL\_ID.
- Added parameter to **delay smartcard insertion events** (in milliseconds). This solves issues reading smartcards within the **Citrix Workspace App**. Issue occurred when inserting the card after already started StoreFront login.

**More...**

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Delay smart card insertion event time |
| Registry  | scard.pcscd.card_insert_event_delay   |
| Value     | 0                                     |

#### Base system

- Fixed **NTP sync problem** with some **Windows Timeservers**.

New registry key:

**More...**

|           |                                                                                |
|-----------|--------------------------------------------------------------------------------|
| Parameter | NTP max allowed distance                                                       |
| Tooltip   | Set this to a larger value can help to synchronize with unreliable NTP servers |
| Registry  | system.time.ntp_max_distance                                                   |
| Type      | Integer                                                                        |
| Value     | <u>16</u> (new default 16 seconds instead of 3 before)                         |

- Added **\_diag kernel modules** needed by **Stratusphere IPS**.
- Fixed **Next** button usage in **Setup Assistant** while **registering for an evaluation license**.
- Fixed issue with **mounting USB devices** in the **Licensing tool**.
- If used as a master image, the **image will expand itself to full size** (limited to 16 GiB) on flash. This is done only **on first boot** and never again.
- Possible **rollout of initial settings, certificates, or licenses placed on the first partition**.

The necessary steps are:

- Writing image to USB or Flash medium
- Mount or simply access the 1. VFAT partition which is present (should be empty)
- Copying the modified `setup.ini` and/or `**.lic` files to the 1st partition (no directories)
- For copying certificates, a `ca-certs` directory must be created where the desired certificates can be inserted. These will be copied to the `/wfs/ca-certs` directory on first boot.
- The USB/Flash medium can be copied several times as needed
- With the initial boot, the device will reboot out of the splash screen (re-read changed partition table)
- The settings, certificates and/or licenses will be deployed and also deleted from the 1st partition.

#### Firmware update

- Improve **download speed for SFTP update sources**.

#### Appliance Mode



- Fixed **RHEV/Spice appliance mode**.

X11 system

- Fixed **displays not being automatically set up on boot**.

Media Player (Parole)

- Fixed **handling of player latency** (stream buffering).

Hardware

- Fixed non-working **Prolific PL2303 USB-to-serial adapters**.
- Fixed non-working **keyboard and touchpad on Microsoft Surface 3 Laptop**.

IGEL Cloud Gateway

- Handle **UMS jobs** intended to be executed on the next boot. This feature requires **UMS 6.05.100 or later**.

## 7.9.2 IGEL OS Creator (OSC)

### Supported Devices

|         |                                     |
|---------|-------------------------------------|
| UD2-LX: | UD2-LX 51<br>UD2-LX 50<br>UD2-LX 40 |
| UD3-LX: | UD3-LX 60<br>UD3-LX 51<br>UD3-LX 50 |
| UD5-LX: | UD5-LX 50                           |
| UD6-LX: | UD6-LX 51                           |
| UD7-LX: | UD7-LX 11<br>UD7-LX 10              |
| UD9-LX: | UD9-LX Touch 41<br>UD9-LX 40        |



See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>420</sup>.

- [Component Versions 11.03.500](#)(see page 1697)
- [New Features 11.03.500](#)(see page 1698)
- [Resolved Issues 11.03.500](#)(see page 1698)

## Component Versions 11.03.500

- **Clients**

| Product  | Version   |
|----------|-----------|
| Zulu JRE | 8.44.0.11 |

- **Smartcard**

|                             |                |
|-----------------------------|----------------|
| Reader Driver MUSCLE CCID   | 1.4.31-1igel10 |
| Resource Manager PC/SC Lite | 1.8.23-1igel11 |

- **System Components**

|                                         |                              |
|-----------------------------------------|------------------------------|
| OpenSSL                                 | 1.0.2g-1ubuntu4.15           |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5           |
| MESA OpenGL stack                       | 19.2.5-1igel93               |
| VDPAU Library version                   | 1.2-1igel911                 |
| Graphics Driver INTEL                   | 2.99.917+git20191117-igel939 |
| Graphics Driver ATI/Radeon              | 19.0.1-3igel936              |
| Graphics Driver ATI/AMDGPU              | 19.0.1-5igel924              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867              |
| Graphics Driver Nvidia                  | 418.56-0ubuntu1              |
| Graphics Driver Vboxvideo               | 1.0.0-igel798                |
| Graphics Driver VMware                  | 13.3.0-2igel857              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build2-igel925        |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |
| Graphics Driver VESA                    | 2.4.0-1igel855               |
| Input Driver Evdev                      | 2.10.6-1igel975              |

<sup>420</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



|                                 |                               |
|---------------------------------|-------------------------------|
| Input Driver Elographics        | 1.4.1-1build5igel633          |
| Input Driver Synaptics          | 1.9.1-1ubuntu1igel866         |
| Input Driver VMMouse            | 13.1.0-1ubuntu2igel635        |
| Input Driver Wacom              | 0.36.1-0ubuntu2igel888        |
| Kernel                          | 4.19.85 #mainline-lxos-r2875  |
| Xorg X11 Server                 | 1.20.5-1igel914               |
| Lightdm Graphical Login Manager | 1.18.3-0ubuntu1.1             |
| XFCE4 Window Manager            | 4.12.3-1ubuntu2igel675        |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7       |
| WebKit2Gtk                      | 2.24.2-0ubuntu0.19.04.1igel18 |
| Python2                         | 2.7.12                        |
| Python3                         | 3.5.2                         |

## New Features 11.03.500

### OSC Installer

- Added **Starter License** functionality.

This license is now part of every new IGEL OS installation and is **valid for 30 days**. The license will be **activated with the first boot** after the initial installation. For more information, see <https://kb.igel.com/licensing>.

## Resolved Issues 11.03.500

### OSC Installer

- Fixed issue with **failed partitioning**.



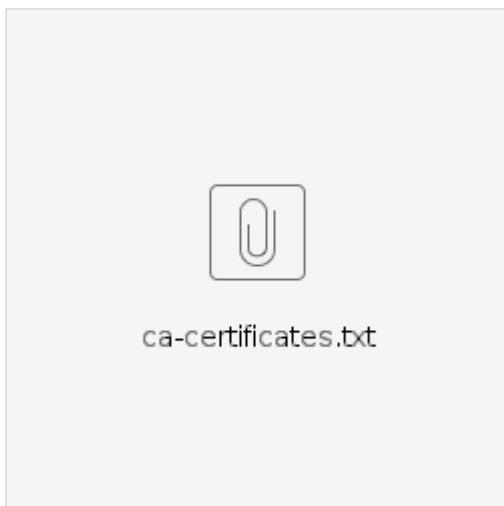
## 7.10 Notes for Release 11.03.110

|                       |            |              |
|-----------------------|------------|--------------|
| <b>Software:</b>      | Version    | 11.03.110    |
| <b>Release Date:</b>  | 2020-01-15 |              |
| <b>Release Notes:</b> | Version    | RN-1103110-1 |
| <b>Last update:</b>   | 2020-01-16 |              |

- [IGEL OS 11](#)(see page 1699)
- [IGEL OS Creator \(OSC\)](#)(see page 1709)

### 7.10.1 IGEL OS 11

See here the list of contained CA certificates:



- [Supported Devices 11.03.110](#)(see page 1700)
- [Component Versions 11.03.110](#)(see page 1700)
- [General Information 11.03.110](#)(see page 1705)
- [Known Issues 11.03.110](#)(see page 1705)
- [Security Fixes 11.03.110](#)(see page 1708)
- [New Features 11.03.110](#)(see page 1708)
- [Resolved Issues 11.03.110](#)(see page 1709)



## Supported Devices 11.03.110

|         |                                     |
|---------|-------------------------------------|
| UD2-LX: | UD2-LX 51<br>UD2-LX 50<br>UD2-LX 40 |
| UD3-LX: | UD3-LX 60<br>UD3-LX 51<br>UD3-LX 50 |
| UD5-LX: | UD5-LX 50                           |
| UD6-LX: | UD6-LX 51                           |
| UD7-LX: | UD7-LX 11<br>UD7-LX 10              |
| UD9-LX: | UD9-LX Touch 41<br>UD9-LX 40        |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>421</sup>.

## Component Versions 11.03.110

• **Clients**

| Product                          | Version    |
|----------------------------------|------------|
| Cisco JVDI Client                | 12.7.0     |
| Citrix HDX Realtime Media Engine | 2.8.0-2235 |
| Citrix Workspace App             | 18.10.0.11 |
| Citrix Workspace App             | 19.10.0.15 |
| Citrix Workspace App             | 19.12.0.19 |

<sup>421</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



|                                        |                                                                        |
|----------------------------------------|------------------------------------------------------------------------|
| deviceTRUST Citrix Channel             | 19.1.200.2                                                             |
| Ericom PowerTerm                       | 12.0.1.0.20170219.2-_dev_-34574                                        |
| Ericom PowerTerm                       | 12.5_x64_20190619_12.5.1.40008                                         |
| Evidian AuthMgr                        | 1.5.7116                                                               |
| Evince PDF Viewer                      | 3.18.2-1ubuntu4.6                                                      |
| FabulaTech USB for Remote Desktop      | 5.2.29                                                                 |
| Firefox                                | 68.4.1                                                                 |
| IBM iAccess Client Solutions           | 1.1.8.1                                                                |
| IGEL RDP Client                        | 2.2                                                                    |
| Imprivata OneSign ProveID Embedded     | onesign-bootstrap-loader_1.0.523630_amd64<br>Qualification in progress |
| deviceTRUST RDP Channel                | 19.1.200.2                                                             |
| NCP Secure Enterprise Client           | 5.10_rev40552                                                          |
| NX Client                              | 6.7.6                                                                  |
| Open VPN                               | 2.3.10-1ubuntu2.2                                                      |
| Zulu JRE                               | 8.42.0.23                                                              |
| Parallels Client (64 bit)              | 17.0.21474                                                             |
| Spice GTK (Red Hat Virtualization)     | 0.37-1igel62                                                           |
| Remote Viewer (Red Hat Virtualization) | 8.0-1igel49                                                            |
| Usbredir (Red Hat Virtualization)      | 0.8.0-1+b1igel71                                                       |
| Teradici PCoIP Software Client         | 19.05.9-18.04                                                          |
| ThinLinc Client                        | 4.10.1-6197                                                            |
| ThinPrint Client                       | 7.5.88                                                                 |
| Totem Media Player                     | 2.30.2                                                                 |
| Parole Media Player                    | 1.0.1-0ubuntu1igel18                                                   |



|                       |                   |
|-----------------------|-------------------|
| VNC Viewer            | 1.9.0+dfsg-3igel8 |
| VMware Horizon Client | 5.2.0-14604769    |
| Voip Client Ekiga     | 4.0.1             |

- **Dictation**

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20180621 |
| Philips Speech driver                     | 12.8.5   |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.8    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.3.2    |

- **Smartcard**

|                                           |                |
|-------------------------------------------|----------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101        |
| PKCS#11 Library Athena IDProtect          | 623.07         |
| PKCS#11 Library cryptovision sc/interface | 7.1.20         |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0      |
| PKCS#11 Library OpenSC                    | 0.19.0-2igel35 |
| PKCS#11 Library SecMaker NetID            | 6.8.1.31       |
| PKCS#11 Library 90meter                   | 20190522       |
| Reader Driver ACS CCID                    | 1.1.6-1igel1   |
| Reader Driver Gemalto eToken              | 10.0.37-0      |
| Reader Driver HID Global Omnikey          | 4.3.3          |



|                                    |                        |
|------------------------------------|------------------------|
| Reader Driver Identive CCID        | 5.0.35                 |
| Reader Driver Identive eHealth200  | 1.0.5                  |
| Reader Driver Identive SCRKBC      | 5.0.24                 |
| Reader Driver MUSCLE CCID          | 1.4.31-1igel6          |
| Reader Driver REINER SCT cyberJack | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite        | 1.8.23-1igel9          |
| Cherry USB2LAN Proxy               | 3.2.0.3                |

- **System Components**

|                                         |                              |
|-----------------------------------------|------------------------------|
| OpenSSL                                 | 1.0.2g-1ubuntu4.15           |
| OpenSSH Client                          | 7.2p2-4ubuntu2.8             |
| OpenSSH Server                          | 7.2p2-4ubuntu2.8             |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5           |
| MESA OpenGL stack                       | 19.2.5-1igel93               |
| VAAPI ABI Version                       | 0.40                         |
| VDPAU Library version                   | 1.2-1igel911                 |
| Graphics Driver INTEL                   | 2.99.917+git20191117-igel939 |
| Graphics Driver ATI/RADEON              | 19.0.1-3igel936              |
| Graphics Driver ATI/AMDGPU              | 19.0.1-5igel924              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867              |
| Graphics Driver Nvidia                  | 418.56-0ubuntu1              |
| Graphics Driver Vboxvideo               | 1.0.0-igel798                |
| Graphics Driver VMware                  | 13.3.0-2igel857              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build2-igel925        |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |
| Graphics Driver VESA                    | 2.4.0-1igel855               |
| Input Driver Evdev                      | 2.10.6-1igel888              |



|                                 |                              |
|---------------------------------|------------------------------|
| Input Driver Elographics        | 1.4.1-1build5igel633         |
| Input Driver eGalax             | 2.5.5814                     |
| Input Driver Synaptics          | 1.9.1-1ubuntu1igel866        |
| Input Driver VMMouse            | 13.1.0-1ubuntu2igel635       |
| Input Driver Wacom              | 0.36.1-0ubuntu2igel888       |
| Kernel                          | 4.19.85 #mainline-lxos-r2872 |
| Xorg X11 Server                 | 1.20.5-1igel914              |
| Xorg Xephyr                     | 1.20.5-1igel914              |
| CUPS printing daemon            | 2.1.3-4ubuntu0.10igel29      |
| PrinterLogic                    | 25.1.0.303                   |
| Lightdm Graphical Login Manager | 1.18.3-0ubuntu1.1            |
| XFCE4 Window Manager            | 4.12.3-1ubuntu2igel675       |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7      |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.3igel74 |
| ModemManager                    | 1.10.0-1~ubuntu18.04.2igel3  |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.2           |
| GStreamer 1.x                   | 1.16.1-1igel222              |
| WebKit2Gtk                      | 2.26.2-1igel27               |
| Python2                         | 2.7.12                       |
| Python3                         | 3.5.2                        |

- **Features with Limited IGEL Support**

|                                    |                                  |
|------------------------------------|----------------------------------|
| Mobile Device Access USB (MTP)     | 1.1.16-2igel1                    |
| Mobile Device Access USB (imobile) | 1.2.1~git20181030.92c5462-1igel5 |
| Mobile Device Access USB (gphoto)  | 2.5.23-2igel2                    |
| VPN OpenConnect                    | 7.08-1                           |
| Scanner support / Sane             | 1.0.27-1                         |



VirtualBox

6.0.14-dfsg-1igel33

## General Information 11.03.110

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

## Known Issues 11.03.110

### Firefox

- **Firefox IGEL extensions are not updated automatically** under some circumstances. After an update from 11.03.10x to 11.03.110, the IGEL extensions will stay on the old version.

In this case, the following settings concerning **kiosk mode** cannot be executed:

- Switch off Hotkey for new window/tab
- Blocking of internal browser pages like preferences, file picker, specific local directories

As a workaround:

- a **reset to defaults** should be performed
- or the **browser's mimetype template** can be switched **from "Standard" to "Minimal"** by registry key browserglobal.app.mimetypes\_template. There, the browser profile is renewed as well.  
After the TC got the new setting, **reboot** and **set** the **mimetypes\_template** registry key **back to "Standard"**.

### Citrix

- With activated **DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1 and MPEG2**. GStreamer1.0 is used if browser content redirection is active.



- **Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix StoreFront login** with **Gemalto smartcard** middleware does not detect smartcard correctly if the card is inserted after start of login.  
Workaround: Insert the smartcard before starting the StoreFront login.
- **Citrix H.264 acceleration plugin** does not work if server policy **Optimize for 3D graphics workload** is enabled together with server policy **Use video codec compression > For the entire screen**.
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264** acceleration plugin a registry key must be enabled.

[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Value     | <u>enabled</u> / <u>disabled</u>                                 |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

- **Multimedia redirection** isn't working if "HDX RealTime Media Engine" is enabled at the same time.

Workaround: Switch off **HDX RealTime Media Engine**.

[More...](#)

|            |                                                                                                    |
|------------|----------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; HDX Multimedia</b>                                 |
|            | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; Skype for Business</b> |
| Parameter  | HDX RealTime Media Engine                                                                          |
| Registry   | ica.module.virtualdriver.hdxrtme.enable                                                            |
| Value      | <u>enabled</u> / <u>disabled</u>                                                                   |

- With Citrix **Workspace App 19.10.0** or **19.8.0** the session sometimes freezes while session logoff from a published desktop:

Workaround: Use **CWA 18.10.0**.

[More...](#)

|            |                                                                             |
|------------|-----------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Citrix Client Selection</b> |
| Parameter  | Citrix client version                                                       |
| Registry   | ica.activeversion                                                           |
| Range      | <u>Default (19.10.0) / 18.10.0 / 19.8.0 / 19.10.0</u>                       |

## VMware Horizon

- **After disconnect of an RDP based session**, the Horizon main **window** which contains the server or sessions overview **cannot be resized anymore**.
- **Seamless application windows in Horizon Client may not be displayed correctly**. When starting the first seamless app a new iconified window appears in the taskbar and only if you click on it the application will show up.



- **Client drive mapping** and **USB redirection** for storage devices should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore Horizon Client relies on the OS to mount the storage devices itself. Enable local `Storage Hotplug` on setup page **Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection do not appear in the **remote desktop**.  
Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.

#### Wi-Fi

- TP-Link Archer T2UH Wi-Fi adapters does not work after system suspend/resume. Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

#### Parallels Client

- **Native USB redirection** does not work with Parallels Client.

#### Smartcard

- In seldom cases the **authentication** hung when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice: spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

#### Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.

#### Audio

- **Audio jack detection on Advantech POC-W243L doesn't work**. Sound output goes through the headset connection and the internal speakers.
- **IGEL UD2 (D220)** fails to restore the volume level of the speaker when the device used **firmware version 11.01.110** before.

#### VirtualBox

- The current **VirtualBox Guest Tools/Drivers** will not work with **VirtualBox 5.2.x or older** hosts which leads to black screen and non working graphic.  
Workaround: Install with 'Failsafe Installation + Recovery' and set registry key `x.drivers.force_vesa` to true.
- When running in VirtualBox virtualization, **resizing the window will not automatically change desktop resolution** of IGEL OS guest.



## Hardware

- **HP t730** could freeze when monitors with **different resolutions** are connected (1920x1200 + 2560x1440 + 3840x1600 for example). When this occurs, the registry key `x.drivers.kms.best_console_mode` has to be set to disabled.
- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work with INTEL devices.

## Security Fixes 11.03.110

### Firefox

- Updated Mozilla Firefox to **68.4.1esr**.
- Fix for **mfsa2020-03**, also known as CVE-2019-17026.
- Fixes for **mfsa2020-02**, also known as: CVE-2019-17016, CVE-2019-17017, CVE-2019-17022, and CVE-2019-17024.
- Fixes for **mfsa2019-37**, also known as:  
[More...](#)  
 CVE-2019-17008, CVE-2019-11745, CVE-2019-17010,  
 CVE-2019-17005, CVE-2019-17011, and CVE-2019-17012.

## New Features 11.03.110

### Citrix

- Integrated **Citrix Workspace App 19.12**
- Available **Citrix Workspace Apps** in this release: **19.12** (default), **19.10**, and **18.10**
- New **registry keys**:
  - Added a registry key for enabling **full-screen banner "Citrix Desktop Viewer"** when starting a Desktop or Application session.  
[More...](#)

|           |                                        |
|-----------|----------------------------------------|
| Parameter | Show Citrix Desktop Viewer screen      |
| Registry  | <code>ica.module.cdviewerscreen</code> |
| Value     | <u>off</u> / on                        |

- Added a registry key to enable usage of **Chromium Embedded Framework (CEF) for Browser Content Redirection (BCR)** [Experimental].  
[More...](#)

|           |                                           |
|-----------|-------------------------------------------|
| Parameter | Use Chromium Embedded Framework (CEF)     |
| Registry  | <code>ica.allregions.usecefbrowser</code> |
| Value     | <u>factory default</u> / false / true     |

- "factory default" means that can be set by config file.
- Changed default:  
[More...](#)

|           |                |
|-----------|----------------|
| Parameter | VDTUI protocol |
|-----------|----------------|



|          |                                       |
|----------|---------------------------------------|
| Registry | ica.module.virtualdriver.vdtui.enable |
| Value    | off / <u>on</u>                       |

## Resolved Issues 11.03.110

### OSC Installer

- Fixed deployment of IGEL OS with **IGEL Deployment Appliance**.

### Firefox

- Fixed **possibility to remove the browser's navigation bar**. In 11.03.100, the whole browser content was invisible without the navigation bar.

### Wi-Fi

- Fixed **support for some newer Wi-Fi chipsets**.
- Fixed **Wi-Fi backport driver** instability problems with updating them to **5.4-rc8-1**.

### Imprivata

- Fixed **race condition** that may lead to unexpected behavior with RDP connections.
- Fixed **VMware Horizon session disconnect**.

### Smartcard

- Fixed bug in **smartcard transaction locking**.

### Cisco JVDI Client

- The **Cisco EULA** must be accepted together with the IGEL EULA before installing IGEL OS and also within IGEL Setup Assistant when requesting an IGEL OS demo license.

### Base system

- Fixed potential **temporary settings loss when resuming from standby**.

### RDP/IGEL RDP Client 2

- Fixed **Fabulotech Scanner Redirection** not working for **RDP Remote Apps**.

## 7.10.2 IGEL OS Creator (OSC)

### Supported Devices

|         |           |
|---------|-----------|
| UD2-LX: | UD2-LX 51 |
|         | UD2-LX 50 |
|         | UD2-LX 40 |



|         |                                     |
|---------|-------------------------------------|
| UD3-LX: | UD3-LX 60<br>UD3-LX 51<br>UD3-LX 50 |
| UD5-LX: | UD5-LX 50                           |
| UD6-LX: | UD6-LX 51                           |
| UD7-LX: | UD7-LX 11<br>UD7-LX 10              |
| UD9-LX: | UD9-LX Touch 41<br>UD9-LX 40        |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>422</sup>.

- [Component Versions 11.03.110](#)(see page 1710)
- [Resolved Issues 11.03.110](#)(see page 1712)

## Component Versions 11.03.110

- **Clients**

| Product  | Version   |
|----------|-----------|
| Zulu JRE | 8.42.0.23 |

- **Smartcard**

|                             |               |
|-----------------------------|---------------|
| Reader Driver MUSCLE CCID   | 1.4.31-1igel6 |
| Resource Manager PC/SC Lite | 1.8.23-1igel9 |

- **System Components**

|                         |                    |
|-------------------------|--------------------|
| OpenSSL                 | 1.0.2g-1ubuntu4.15 |
| Bluetooth Stack (bluez) | 5.50-0ubuntu1igel5 |

<sup>422</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



|                                         |                              |
|-----------------------------------------|------------------------------|
| MESA OpenGL stack                       | 19.2.5-1igel93               |
| VDPAU Library version                   | 1.2-1igel911                 |
| Graphics Driver INTEL                   | 2.99.917+git20191117-igel939 |
| Graphics Driver ATI/RADEON              | 19.0.1-3igel936              |
| Graphics Driver ATI/AMDGPU              | 19.0.1-5igel924              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867              |
| Graphics Driver Nvidia                  | 418.56-0ubuntu1              |
| Graphics Driver Vboxvideo               | 1.0.0-igel798                |
| Graphics Driver VMware                  | 13.3.0-2igel857              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build2-igel925        |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |
| Graphics Driver VESA                    | 2.4.0-1igel855               |
| Input Driver Evdev                      | 2.10.6-1igel888              |
| Input Driver Elographics                | 1.4.1-1build5igel633         |
| Input Driver Synaptics                  | 1.9.1-1ubuntu1igel866        |
| Input Driver VMMouse                    | 13.1.0-1ubuntu2igel635       |
| Input Driver Wacom                      | 0.36.1-0ubuntu2igel888       |
| Kernel                                  | 4.19.85 #mainline-lxos-r2872 |
| Xorg X11 Server                         | 1.20.5-1igel914              |
| Lightdm Graphical Login Manager         | 1.18.3-0ubuntu1.1            |
| XFCE4 Window Manager                    | 4.12.3-1ubuntu2igel675       |
| ISC DHCP Client                         | 4.3.3-5ubuntu12.10igel7      |
| WebKit2Gtk                              | 2.26.2-1igel27               |
| Python2                                 | 2.7.12                       |
| Python3                                 | 3.5.2                        |



## Resolved Issues 11.03.110

### OSC Installer

- Fixed deployment of **IGEL OS with IGEL Deployment Appliance**.

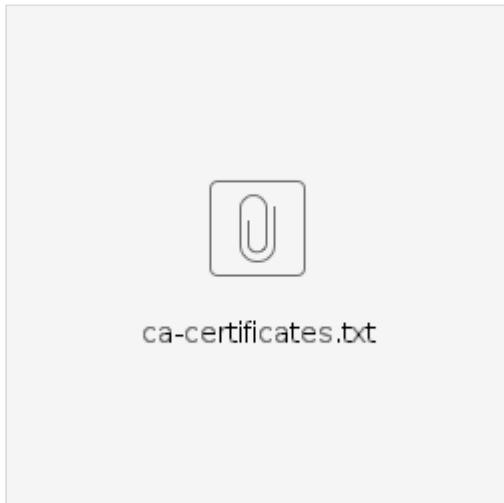
## 7.11 Notes for Release 11.03.100

|                       |            |              |
|-----------------------|------------|--------------|
| <b>Software:</b>      | Version    | 11.03.100    |
| <b>Release Date:</b>  | 2019-12-10 |              |
| <b>Release Notes:</b> | Version    | RN-1103100-1 |
| <b>Last update:</b>   | 2019-12-06 |              |

- 
- [IGEL OS 11](#)(see page 1712)
  - [IGEL OS Creator \(OSC\)](#)(see page 1741)

### 7.11.1 IGEL OS 11

See here the list of contained CA certificates:



- 
- [Supported Devices 11.03.100](#)(see page 1713)
  - [Component Versions 11.03.100](#)(see page 1713)
  - [General Information 11.03.100](#)(see page 1718)
  - [Security Fixes 11.03.100](#)(see page 1718)
  - [Known Issues 11.03.100](#)(see page 1721)



- New Features 11.03.100(see page 1723)
- Resolved Issues 11.03.100(see page 1731)
- CA Certificates Contained in IGEL OS 11.03(see page 1733)

## Supported Devices 11.03.100

|         |                                     |
|---------|-------------------------------------|
| UD2-LX: | UD2-LX 51<br>UD2-LX 50<br>UD2-LX 40 |
| UD3-LX: | UD3-LX 60<br>UD3-LX 51<br>UD3-LX 50 |
| UD5-LX: | UD5-LX 50                           |
| UD6-LX: | UD6-LX 51                           |
| UD7-LX: | UD7-LX 11<br>UD7-LX 10              |
| UD9-LX: | UD9-LX Touch 41<br>UD9-LX 40        |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>423</sup>.

## Component Versions 11.03.100

- **Clients**

| Product                          | Version    |
|----------------------------------|------------|
| Cisco JVDI Client                | 12.7.0     |
| Citrix HDX Realtime Media Engine | 2.8.0-2235 |
| Citrix Workspace App             | 18.10.0.11 |

<sup>423</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



|                                        |                                           |
|----------------------------------------|-------------------------------------------|
| Citrix Workspace App                   | 19.10.0.15                                |
| Citrix Workspace App                   | 19.8.0.20                                 |
| deviceTRUST Citrix Channel             | 19.1.200.2                                |
| Ericom PowerTerm                       | 12.0.1.0.20170219.2-_dev_-34574           |
| Ericom PowerTerm                       | 12.5_x64_20190619_12.5.1.40008            |
| Evidian AuthMgr                        | 1.5.7116                                  |
| Evince PDF Viewer                      | 3.18.2-1ubuntu4.6                         |
| FabulaTech USB for Remote Desktop      | 5.2.29                                    |
| Firefox                                | 68.2.0                                    |
| IBM iAccess Client Solutions           | 1.1.8.1                                   |
| IGEL RDP Client                        | 2.2                                       |
| Imprivata OneSign ProveID Embedded     | onesign-bootstrap-loader_1.0.523630_amd64 |
| deviceTRUST RDP Channel                | 19.1.200.2                                |
| NCP Secure Enterprise Client           | 5.10_rev40552                             |
| NX Client                              | 6.7.6                                     |
| Open VPN                               | 2.3.10-1ubuntu2.2                         |
| Zulu JRE                               | 8.42.0.23                                 |
| Parallels Client (64 bit)              | 17.0.21474                                |
| Spice GTK (Red Hat Virtualization)     | 0.37-1igel62                              |
| Remote Viewer (Red Hat Virtualization) | 8.0-1igel49                               |
| Usbredir (Red Hat Virtualization)      | 0.8.0-1igel49                             |
| Teradici PCoIP Software Client         | 19.05.9-18.04                             |
| ThinLinc Client                        | 4.10.1-6197                               |
| ThinPrint Client                       | 7.5.88                                    |



|                       |                      |
|-----------------------|----------------------|
| Totem Media Player    | 2.30.2               |
| Parole Media Player   | 1.0.1-0ubuntu1igel18 |
| VNC Viewer            | 1.9.0+dfsg-3igel8    |
| VMware Horizon Client | 5.2.0-14604769       |
| Voip Client Ekiga     | 4.0.1                |

- **Dictation**

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20180621 |
| Philips Speech driver                     | 12.8.5   |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.8    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.3.2    |

- **Smartcard**

|                                           |                |
|-------------------------------------------|----------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101        |
| PKCS#11 Library Athena IDProtect          | 623.07         |
| PKCS#11 Library cryptovision sc/interface | 7.1.20         |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0      |
| PKCS#11 Library OpenSC                    | 0.19.0-2igel35 |
| PKCS#11 Library SecMaker NetID            | 6.8.1.31       |
| PKCS#11 Library 90meter                   | 20190522       |
| Reader Driver ACS CCID                    | 1.1.6-1igel1   |



|                                    |                        |
|------------------------------------|------------------------|
| Reader Driver Gemalto eToken       | 10.0.37-0              |
| Reader Driver HID Global Omnikey   | 4.3.3                  |
| Reader Driver Identive CCID        | 5.0.35                 |
| Reader Driver Identive eHealth200  | 1.0.5                  |
| Reader Driver Identive SCRKBC      | 5.0.24                 |
| Reader Driver MUSCLE CCID          | 1.4.31-1igel6          |
| Reader Driver REINER SCT cyberJack | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite        | 1.8.23-1igel8          |
| Cherry USB2LAN Proxy               | 3.2.0.3                |

- **System Components**

|                                         |                              |
|-----------------------------------------|------------------------------|
| OpenSSL                                 | 1.0.2g-1ubuntu4.15           |
| OpenSSH Client                          | 7.2p2-4ubuntu2.8             |
| OpenSSH Server                          | 7.2p2-4ubuntu2.8             |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5           |
| MESA OpenGL stack                       | 19.2.5-1igel93               |
| VAAPI ABI Version                       | 0.40                         |
| VDPAU Library version                   | 1.2-1igel911                 |
| Graphics Driver INTEL                   | 2.99.917+git20191117-igel939 |
| Graphics Driver ATI/Radeon              | 19.0.1-3igel936              |
| Graphics Driver ATI/AMDGPU              | 19.0.1-5igel924              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867              |
| Graphics Driver Nvidia                  | 418.56-0ubuntu1              |
| Graphics Driver Vboxvideo               | 1.0.0-igel798                |
| Graphics Driver VMware                  | 13.3.0-2igel857              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build2-igel925        |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |



|                                             |                                  |
|---------------------------------------------|----------------------------------|
| Graphics Driver VESA                        | 2.4.0-1igel855                   |
| Input Driver Evdev                          | 2.10.6-1igel888                  |
| Input Driver Elographics                    | 1.4.1-1build5igel633             |
| Input Driver eGalax                         | 2.5.5814                         |
| Input Driver Synaptics                      | 1.9.1-1ubuntu1igel866            |
| Input Driver VMMouse                        | 13.1.0-1ubuntu2igel635           |
| Input Driver Wacom                          | 0.36.1-0ubuntu2igel888           |
| Kernel                                      | 4.19.85 #mainline-lxos-r2872     |
| Xorg X11 Server                             | 1.20.5-1igel914                  |
| Xorg Xephyr                                 | 1.20.5-1igel914                  |
| CUPS printing daemon                        | 2.1.3-4ubuntu0.10igel29          |
| PrinterLogic                                | 25.1.0.303                       |
| Lightdm Graphical Login Manager             | 1.18.3-0ubuntu1.1                |
| XFCE4 Window Manager                        | 4.12.3-1ubuntu2igel675           |
| ISC DHCP Client                             | 4.3.3-5ubuntu12.10igel7          |
| NetworkManager                              | 1.2.6-0ubuntu0.16.04.3igel74     |
| ModemManager                                | 1.10.0-1~ubuntu18.04.2igel3      |
| GStreamer 0.10                              | 0.10.36-2ubuntu0.2               |
| GStreamer 1.x                               | 1.16.1-1igel222                  |
| WebKit2Gtk                                  | 2.26.2-1igel27                   |
| Python2                                     | 2.7.12                           |
| Python3                                     | 3.5.2                            |
| <b>• Features with Limited IGEL Support</b> |                                  |
| Mobile Device Access USB (MTP)              | 1.1.16-2igel1                    |
| Mobile Device Access USB (imobile)          | 1.2.1~git20181030.92c5462-1igel5 |



|                                   |                     |
|-----------------------------------|---------------------|
| Mobile Device Access USB (gphoto) | 2.5.23-2igel2       |
| VPN OpenConnect                   | 7.08-1              |
| Scanner support / Sane            | 1.0.27-1            |
| VirtualBox                        | 6.0.14-dfsg-1igel33 |

## General Information 11.03.100

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

## Security Fixes 11.03.100

### Firefox

- Updated Mozilla Firefox to **68.2.0esr**
  - Fixes for **mfsa2019-33**.
  - [More...](#)

CVE-2019-15903, CVE-2019-11757, CVE-2019-11758, CVE-2019-11759,  
 CVE-2019-11760, CVE-2019-11761, CVE-2019-11762, CVE-2019-11763,  
 CVE-2019-11764.

- Fixes for **mfsa2019-26**.
    - [More...](#)
- CVE-2019-11746, CVE-2019-11744, CVE-2019-11742, CVE-2019-11752,  
 CVE-2019-9812, CVE-2019-11743, CVE-2019-11748, CVE-2019-11749,  
 CVE-2019-11750, CVE-2019-11738, CVE-2019-11747, CVE-2019-11735,  
 CVE-2019-11740.

### Base system



- Added **cryptographic signatures** to OS 11 firmware files to prevent reading from corrupt images or disks.
  - Updates to firmwares without valid signatures are blocked.
  - When a signature error on the system partition is detected, the system is halted immediately. For system recovery a reinstallation via the OS Creator tool (OSC) is required. A signature error during early boot is signalized by a beep sequence.
  - When a signature error in another partition is detected the partition is removed and a firmware update is triggered to reinstall the corrupt partition.
  - Added user visible notification about partition signature errors.
- Fixed **admin logout from rescue shell** after suspend.
- Fixed security issue **CVE-2019-15902** in **4.19.x kernel**.
- Updated **Intel microcodes** to version **20191115** to fix various security issues (CVE-2019-11135, CVE-2019-0117 and CVE-2019-11139).
- Fixed **cups** security issues CVE-2019-8696, CVE-2019-8675 and CVE-2019-86.
- Fixed **openjpeg2** security issues CVE-2018-6616, CVE-2018-5785, CVE-2018-18088, CVE-2018-14423 and CVE-2017-17480.
- Fixed **xorg-server** security issue CVE-2018-14665.
- Fixed **expat** security issue CVE-2019-15903.
- Fixed **freetype** security issue CVE-2015-9383.
- Fixed **ghostscript** security issues.  
**More...**

CVE-2019-14817, CVE-2019-14813, CVE-2019-14812,  
CVE-2019-14811, CVE-2019-10216 and CVE-2019-14869.
- Fixed **python2.7** security issues.  
**More...**

CVE-2019-9948, CVE-2019-9947, CVE-2019-9740, CVE-2019-9636,  
CVE-2019-5010, CVE-2019-10160 , CVE-2018-20852, CVE-2019-16935 and CVE-2019-16056.
- Fixed **python3.5** security issues.  
**More...**

CVE-2019-9948, CVE-2019-9947, CVE-2019-9740, CVE-2019-9636,  
CVE-2019-5010, CVE-2019-10160, CVE-2018-20852, CVE-2018-20406, CVE-2019-16935 and CVE-2019-16056.
- Fixed **glib** security issues CVE-2019-15133 and CVE-2018-11490.
- Fixed **libvirt** security issues.  
**More...**

CVE-2019-3886, CVE-2019-11091, CVE-2019-10168, CVE-2019-10167,  
CVE-2019-10166, CVE-2019-10161, CVE-2019-10132, CVE-2018-6764,  
CVE-2018-5748, CVE-2018-12130, CVE-2018-12127, CVE-2018-12126,  
CVE-2018-1064, CVE-2017-2635, CVE-2017-1000256 and CVE-2016-5008.
- Fixed **e2fsprogs** security issue CVE-2019-5094.
- Fixed **rpcbind** security issues CVE-2017-8779 and CVE-2015-7236.
- Fixed **wpa** security issues CVE-2019-16275 and CVE-2019-13377.



- Fixed **tiff** security issues CVE-2019-17546 and CVE-2019-14973.
- Fixed **aspell** security issue CVE-2019-17544.
- Fixed **libsdl1.2** security issues.

[More...](#)

CVE-2019-7638, CVE-2019-7637, CVE-2019-7636,  
 CVE-2019-7635, CVE-2019-7578, CVE-2019-7577,  
 CVE-2019-7576, CVE-2019-7575, CVE-2019-7574,  
 CVE-2019-7573, CVE-2019-7572 and CVE-2019-13616.

- Fixed **libsoup2.4** security issues CVE-2019-17266, CVE-2018-12910 and CVE-2017-2885.
- Fixed **rtlwifi driver** security issue CVE-2019-17666 .
- Fixed **libxslt** security issues CVE-2019-18197, CVE-2019-13118 and CVE-2019-13117.
- Fixed **opus** security issue CVE-2017-0381.
- Fixed **curl** security issues CVE-2019-5482 and CVE-2019-5481.
- Fixed **libidn2** security issues CVE-2019-18224 and CVE-2019-12290.
- Fixed **libarchive** security issue CVE-2019-18408.
- Fixed **samba** security issues CVE-2019-14847 and CVE-2019-10218.
- Fixed **file** security issue CVE-2019-18218.
- Fixed **imagemagick** security issues.

[More...](#)

CVE-2019-16713, CVE-2019-16711, CVE-2019-16710, CVE-2019-16709,  
 CVE-2019-16708, CVE-2019-15140, CVE-2019-15139,  
 CVE-2019-14981, CVE-2019-13454, CVE-2019-13391,  
 CVE-2019-13311, CVE-2019-13310, CVE-2019-13309, CVE-2019-13307,  
 CVE-2019-13306, CVE-2019-13305, CVE-2019-13304, CVE-2019-13301,  
 CVE-2019-13300, CVE-2019-13297, CVE-2019-13295, CVE-2019-13137,  
 CVE-2019-13135, CVE-2019-12979, CVE-2019-12978, CVE-2019-12977,  
 CVE-2019-12976, CVE-2019-12975 and CVE-2019-12974.

- Fixed **libjpeg-turbo** security issues CVE-2019-2201, CVE-2018-20330 and CVE-2018-19664.
- Fixed **python-ecdsa** security issues CVE-2019-14859, CVE-2019-14853 and CVE-2019-1485.
- Restricted access to **journalctl log** file for root only.
- Limit list of allowed **TLS ciphers** according to the Germany BSI recommendation (TR-0210202 Version 2019-01). The functionality is controlled by a parameter.

[More...](#)

|          |                                              |
|----------|----------------------------------------------|
| Registry | system.security.remote_management.tls_policy |
| Value    | Default / BSI                                |

The limited cipher list is applied on TLS (SSL) connections in:

- IGEL RM Agent
- Secure Shadowing
- Secure Terminal
- Firmware Update



- Custom Partition

## Known Issues 11.03.100

### Citrix

- With activated **DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1 and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix StoreFront login** with **Gemalto smartcard** middleware does not detect smartcard correctly if the card is inserted after start of login.  
Workaround: Insert the smartcard before starting the StoreFront login.
- **Citrix H.264 acceleration plugin** does not work if server policy **Optimize for 3D graphics workload** is enabled together with server policy **Use video codec compression > For the entire screen**.
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264** acceleration plugin a registry key must be enabled.

[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Value     | enabled / disabled                                               |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

- **Multimedia redirection** isn't working if "HDX RealTime Media Engine" is enabled at the same time.

Workaround: Switch off **HDX RealTime Media Engine**.

[More...](#)

|            |                                                                                                    |
|------------|----------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; HDX Multimedia</b>                                 |
|            | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; Skype for Business</b> |
| Parameter  | HDX RealTime Media Engine                                                                          |
| Registry   | ica.module.virtualdriver.hdxrtme.enable                                                            |
| Value      | enabled / disabled                                                                                 |

- With Citrix **Workspace App 19.10.0 or 19.8.0** the session sometimes freezes while session logoff from a published desktop. :

Workaround: Use **CWA 18.10.0**.

[More...](#)

|            |                                                                             |
|------------|-----------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Citrix Client Selection</b> |
|            |                                                                             |



|           |                                                       |
|-----------|-------------------------------------------------------|
| Parameter | Citrix client version                                 |
| Registry  | ica.activeversion                                     |
| Range     | <u>Default</u> (19.10.0) / 18.10.0 / 19.8.0 / 19.10.0 |

## VMware Horizon

- **After disconnect of an RDP based session**, the Horizon main **window** which contains the server or sessions overview **cannot be resized anymore**.
- **Seamless application windows in Horizon Client may not be displayed correctly**. When starting the first seamless app a new iconified window appears in the taskbar and only if you click on it the application will show up.
- **Client drive mapping** and **USB redirection** for storage devices should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore Horizon Client relies on the OS to mount the storage devices itself. Enable local `Storage Hotplug` on setup page **Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection do not appear in the **remote desktop**. Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.

## WiFi

- TP-Link Archer T2UH WiFi adapters does not work after system suspend/resume. Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

## Parallels Client

- **Native USB redirection** does not work with Parallels Client.

## Smartcard

- In seldom cases the **authentication** hung when using **A.E.T. SafeSign smartcards**.

## Appliance Mode

- Appliance mode **RHEV/Spice: spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

## Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.

## Audio



- **Audio jack detection on Advantec POC-W243L doesn't work.** Sound output goes through the headset connection and the internal speakers.
- **IGEL UD2 (D220)** fails to restore the volume level of the speaker when the device used **firmware version 11.01.110** before.

#### VirtualBox

- The current **VirtualBox Guest Tools/Drivers** will not work with **VirtualBox 5.2.x or older** hosts which leads to black screen and non working graphic.  
Workaround: Install with 'Failsafe Installation + Recovery' and set registry key `x.drivers.force_vesa` to true.
- When running in VirtualBox virtualization, **resizing the window will not automatically change desktop resolution** of IGEL OS guest.

#### Hardware

- **HP t730** could freeze when monitors with **different resolutions** are connected (1920x1200 + 2560x1440 + 3840x1600 for example). When this occurs, the registry key `x.drivers.kms.best_console_mode` has to be set to disabled.
- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work with INTEL devices.

#### New Features 11.03.100

##### Citrix

- Integrated **Citrix Workspace app 19.10**
- Available Citrix Workspace apps in this release: 19.10 (default), 19.08 and 18.10
- Added a registry key to enable **Transparent User Interface [TUI] Virtual Channel [VC]** protocol.  
**More...**

|           |                                                    |
|-----------|----------------------------------------------------|
| Parameter | Enable VDTUI protocol                              |
| Registry  | <code>ica.module.virtualdriver.vdtui.enable</code> |
| Value     | <code>enabled</code> / <code>disabled</code>       |

- Updated **libwebkit2gtk-4.0-37** to version **2.26.2**. It is now possible to **enable debug output for Citrix Browser Content Redirection** by running the script `/config/bin/install-webkit-debug`. The debug output is written to `/var/log/user/webcontainer.debug`.

Only short sessions with enabled debug output can be tracked, due to the huge amount of debugging data which is written to the log file.

- Added support for **FabulaTech Scanner for Remote Desktop**.  
**More...**

|            |                                                                                    |
|------------|------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Fabulatech Scanner Redirection</b> |
| Parameter  | Fabulatech Scanner for Remote Desktop                                              |
| Registry   | <code>ica.module.virtualdriver.fabulatech_scanner.enable</code>                    |
| Value      | <code>enabled</code> / <code>disabled</code>                                       |



## RDP/IGEL RDP Client 2

- Added support for **FabulaTech Scanner for Remote Desktop**.  
[More...](#)

|            |                                                                              |
|------------|------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; RDP &gt; RDP Global &gt; Fabulatech Scanner Redirection</b> |
| Parameter  | Fabulatech Scanner for Remote Desktop                                        |
| Registry   | rdp.fabulatech_scanner.enable                                                |
| Value      | enabled / <u>disabled</u>                                                    |

## VMware Horizon

- Updated Horizon Client to version **5.2.0-14604769**.
- Added **local scanner redirection** for VMWare Horizon Client.  
[More...](#)

|           |                                  |
|-----------|----------------------------------|
| Parameter | Scanner Redirection              |
| Registry  | vmware.view.enable-scanner-redir |
| Value     | enabled / <u>disabled</u>        |

- Added support for **FabulaTech Scanner for Remote Desktop**.  
[More...](#)

|            |                                                                                                    |
|------------|----------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Fabulatech Scanner Redirection</b> |
| Parameter  | Fabulatech Scanner for Remote Desktop                                                              |
| Registry   | vmware.view.usb.enable-fabulatech-scanner                                                          |
| Value      | enabled / <u>disabled</u>                                                                          |

## ThinLinc

- Updated ThinLinc Client to version **4.10.1**.

## Parallels Client

- Updated Parallels Client to Version **17.0.1**.  
 For using the FIPS 140-2 compliance mode no special handling is needed anymore.

## Teradici PCoIP Client

- Updated Teradici PCoIP client to **19.05.9**.

## Imprivata

- Added: When **available flash** is **bigger than 2GB**, 500 MB will be used for the Imprivata data partition.

## Cisco JVDI Client

- Integrated new **Cisco Jabber Softphone for VDI** (Cisco JVDI Client) version 12.7 in 64bit.  
[More...](#)



|            |                                                                                                                 |
|------------|-----------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix XenDesktop/XenApp &gt; HDX/ICA Global &gt; Unified Communications &gt; Cisco Jabber</b> |
| Parameter  | Cisco JVDI client                                                                                               |
| Registry   | ica.module.virtualdriver.vdcisco.enable                                                                         |
| Value      | enabled / <u>disabled</u>                                                                                       |
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Global &gt; Unified Communications &gt; Cisco Jabber</b>           |
| Parameter  | Cisco JVDI client                                                                                               |
| Registry   | vmware.view.vdcisco.enable                                                                                      |
| Value      | enabled / <u>disabled</u>                                                                                       |

> Registry path for Common JVDI options: multimedia.ciscovxme.\*\*

## Logging

- Added **Elastic Filebeat 7.3.0**. This is a lightweight way to forward and centralize logs and files. There are new registry keys to enable and configure **Elastic Filebeat**.
- More...**

|            |                                                         |
|------------|---------------------------------------------------------|
| IGEL Setup | <b>System &gt; Firmware Customization &gt; Features</b> |
| Parameter  | Elastic Filebeat                                        |
| Registry   | services.elastic_filebeat.enabled                       |
| Value      | enabled / <u>disabled</u>                               |
| Parameter  | Use custom configuration                                |
| Registry   | network.filebeat.custom.enabled                         |
| Value      | <u>enabled</u> / disabled                               |
| Parameter  | Custom Configuration                                    |
| Registry   | network.filebeat.custom.config                          |
| Value      | filebeat.inputs: ...                                    |

## Base system

- Added support for **exFAT filesystem**.
  - Updated **Kernel to version 4.19.85** with **WiFi backport drivers 5.3.6.1**.
  - Updated **Intel microcodes to version 20191115** to fix various security issues (CVE-2019-11135, CVE-2019-0117 and CVE-2019-11139).
  - Updated **Xorg Xserver** from version 1.19.6 to **1.20.5**.
  - Updated **Mesa OpenGL stack** from version 19.0.8 to **19.2.5**.
  - Updated the **X11 video** and **input drivers** to their most current available versions.
  - Added functionality to **enable or disable touchpad with a hotkey**.
- More...**



|                      |                                                                                   |
|----------------------|-----------------------------------------------------------------------------------|
| IGEL Setup Parameter | <b>User Interface &gt; Input &gt; Touchpad</b><br>Enable Touchpad                 |
| Registry Value       | userinterface.touchpad.general.touchpadenable<br><u>enabled</u> / <u>disabled</u> |
| IGEL Setup Parameter | <b>User Interface &gt; Input &gt; Touchpad</b><br>Hotkey                          |
| Registry Value       | userinterface.touchpad.general.usehotkey<br><u>enabled</u> / <u>disabled</u>      |
| IGEL Setup Parameter | <b>User Interface &gt; Input &gt; Touchpad</b><br>Modifiers                       |
| Registry             | userinterface.touchpad.general.hotkeymodifier                                     |
| IGEL Setup Parameter | <b>User Interface &gt; Input &gt; Touchpad</b><br>Hotkey                          |
| Registry             | userinterface.touchpad.general.hotkey                                             |

- Added feature to **log into different files** and to **store log files on a persistent encrypted partition.**  
[More...](#)

|                      |                                                              |
|----------------------|--------------------------------------------------------------|
| IGEL Setup Parameter | <b>System &gt; Logging</b><br>Local logging                  |
| Registry Value       | system.syslog.enabled<br><u>enabled</u> / <u>disabled</u>    |
| IGEL Setup Parameter | <b>System &gt; Logging</b><br>Use persistent log partition   |
| Registry Value       | system.syslog.persistent<br><u>enabled</u> / <u>disabled</u> |
| IGEL Setup Parameter | <b>System &gt; Logging</b><br>Partition size in MB           |
| Registry Value       | system.syslog.partsize<br><u>100</u>                         |

Create /var/log/auth.log:

|                |                                                              |
|----------------|--------------------------------------------------------------|
| Registry Value | system.syslog.sinks.auth<br><u>enabled</u> / <u>disabled</u> |
|----------------|--------------------------------------------------------------|

Create /var/log/daemon.log:



|          |                            |
|----------|----------------------------|
| Registry | system.syslog.sinks.daemon |
| Value    | <u>enabled</u> / disabled  |

Create /var/log/kern.log:

|          |                           |
|----------|---------------------------|
| Registry | system.syslog.sinks.kern  |
| Value    | <u>enabled</u> / disabled |

Create /var/log/syslog:

|          |                            |
|----------|----------------------------|
| Registry | system.syslog.sinks.syslog |
| Value    | <u>enabled</u> / disabled  |

- Updated **Fluendo multimedia codecs** to the following versions:

gst-fluendo-h264dec - 18/09/2019 0.10.54

gst-fluendo-vadec - 16/10/2019 0.10.210

- Added **beep sequence** to signalize a **missing system partition** during early boot.

#### CUPS Printing

- Updated **Printer Installer** client to version **25.1.0.303**.
- Added missing **cups model names** for some printers.

#### Smartcard

- Updated **MUSCLE Open Source CCID** driver to version **1.4.31**. Added additional smartcard reader **Cherry SECURE BOARD**.
- Updated **SecMaker Net iD** smartcard library to version **6.8.1.31**. The changes are:
  - Support for **Gemalto IDPrime 940** and **3940**.
  - Support for new **VRK card** (IDEA IAS ECC, spec: FINEID S1 - FINEID S1 Electronic ID Application v4.0).
  - Support for **Aventra MyEID v4.0** (customer specific card profile with read support only).
  - Fixed problem with **detection of cards in Net iD Card Portal**.
  - Other fixes, see release notes at [SecMaker](#)<sup>424</sup>.

#### WiFi

- Added **backports kernel drivers** with version **5.3.6-1** for better WiFi support.
- Disabled **backports drivers** for **Microsoft Surface** Laptop 3.
- Added new registry key to enable or disable the use of the **backport drivers** (reboot is needed).  
**More...**

|           |                                         |
|-----------|-----------------------------------------|
| Parameter | Use the newer backport drivers for WiFi |
| Registry  | network.drivers.use_backport_drivers    |

<sup>424</sup> <https://service.secmaker.com/releasenotes/>



|       |                                                               |
|-------|---------------------------------------------------------------|
| Range | <u>Default</u> (normally use backport drivers) / False / True |
|-------|---------------------------------------------------------------|

- Added switch for more aggressively search of configured **hidden WiFi networks**.

**More...**

|           |                                                           |
|-----------|-----------------------------------------------------------|
| Parameter | Force connection to hidden network                        |
| Registry  | network.interfaces.wirelesslan.device0.mssid_force_hidden |
| Value     | <u>never</u> / once / continuously                        |

The default value **never** preserves the old behaviour.

Changing can be useful in situations where the system cannot detect any configured WiFi in the environment. If **once** is selected, the system will blindly try to connect to all configured hidden networks once (until the network as a whole gets started again). In the case of **continuously**, it will continue trying to connect to hidden networks.

Remarks: An access point found in this way will be remembered next time and its reconnecting will be faster. Search for hidden networks in the Wireless Manager is not affected.

#### Driver

- Updated **Philips Speech Driver** to version **12.8.5**.
- Added login with **BioSec BS Login Hand Vein Recognition** software. The parameters have to be set in IGEL Setup Registry.

**More...**

|            |                                                         |
|------------|---------------------------------------------------------|
| Parameter  | Login with Biosec BS Login                              |
| Registry   | auth.login.biosec_bslogin                               |
| Value      | <u>enabled</u> / <u>disabled</u>                        |
| Parameter  | URL of LifePassServer                                   |
| Registry   | auth.biosec.lifeppassserverurl                          |
| Value      | <u>localhost:10100</u>                                  |
| IGEL Setup | <b>System &gt; Firmware Customization &gt; Features</b> |
| Parameter  | Biosec BS Login                                         |
| Registry   | services.biosec_bslogin.enabled                         |
| Value      | <u>enabled</u> / <u>disabled</u>                        |

- Added **Broadcom Tigon3** network driver.

#### X11 system

- Added support for secure keyboard input with **Cherry SECURE BOARD 1.0**.

In secure mode all keyboard input devices are suppressed except pre-personalized Cherry SECURE BOARD 1.0 devices. For the encrypted communication certificates and keys in directories /wfs/cherry/ca-certs and /wfs/cherry/client-certs are required.

**More...**

|            |                                                |
|------------|------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Input &gt; Keyboard</b> |
| Parameter  | Secure keyboard input with Cherry SECURE BOARD |
| Registry   | devices.cherry_secureboard.enable              |
| Value      | enabled / <u>disabled</u>                      |
| Parameter  | Debug messages for Cherry SECURE BOARD         |
| Registry   | devices.cherry_secureboard.debug               |
| Value      | enabled / <u>disabled</u>                      |

- Added the possibility to configure the **screen brightness** with registry keys.

**More...**

|           |                                   |
|-----------|-----------------------------------|
| Parameter | Brightness value                  |
| Registry  | x.xserver0.brightness             |
|           | x.xserver0.screen[1-7].brightness |
| Range     | 0.1 - <u>1.0</u> (darker)         |
|           | <u>1.0</u> - 3.0 (brighter)       |

- Added new registry keys to be able to configure some **modesetting graphics driver options** if needed.

**More...**

|           |                                                                       |
|-----------|-----------------------------------------------------------------------|
| Parameter | Use DRI3 PageFlip feature                                             |
| Registry  | x.drivers.modesetting.use_page_flip                                   |
| Range     | <u>Default</u> (normally use page flip feature) / disabled / enabled  |
| Parameter | Use shadow framebuffer layer                                          |
| Registry  | x.drivers.modesetting.use_shadow_fb                                   |
| Range     | <u>Default</u> (normally use shadow framebuffer) / disabled / enabled |
| Parameter | Use double shadow framebuffer to improve VNC performance              |
| Registry  | x.drivers.modesetting.use_double_shadow                               |
| Range     | <u>disabled</u> / enabled                                             |
| Parameter | Use software cursor for modesetting driver                            |
| Registry  | x.drivers.modesetting.use_sw_cursor                                   |
| Range     | <u>Default</u> (normally disabled)                                    |
| Parameter | Choose acceleration method                                            |



|           |                                                                           |
|-----------|---------------------------------------------------------------------------|
| Registry  | <code>x.drivers.modesetting.accel_method</code>                           |
| Range     | <u>Default</u> (normally Glamor is used) / Glamor / None                  |
| Parameter | Force usage of DRI3 regardless of <code>x.drivers.use_dri3</code> setting |
| Registry  | <code>x.drivers.modesetting.force_dri3</code>                             |
| Range     | <u>disabled</u> / enabled                                                 |

## Misc

- Added support for **Stratusphere UX** from Liquidware.

**More...**

|            |                                                             |
|------------|-------------------------------------------------------------|
| IGEL Setup | <b>Accessories &gt; Connector ID Key Software</b>           |
| Parameter  | Enable Stratusphere UX CID Key                              |
| Registry   | <code>stratusphere_ux.cid_key_software.enable</code>        |
| IGEL Setup | <b>Accessories &gt; Connector ID Key Software</b>           |
| Parameter  | Stratusphere hub                                            |
| Registry   | <code>stratusphere_ux.cid_key_software.hub</code>           |
| IGEL Setup | <b>Accessories &gt; Connector ID Key Software</b>           |
| Parameter  | Stratusphere machine group                                  |
| Registry   | <code>stratusphere_ux.cid_key_software.machine_group</code> |
| IGEL Setup | <b>Accessories &gt; Connector ID Key Software</b>           |
| Parameter  | Stratusphere user group                                     |
| Registry   | <code>stratusphere_ux.cid_key_software.user_group</code>    |

- Added the launcher of Login VSI's monitoring tool **Login PI** to the IGEL OS which can be configured from setup via parameters and started from the UMS.

Besides of specifying the parameters given below, a SSL certificate must be provided and deployed via the UMS. This has to be obtained from the Login PI server manually. Given the parameters and the certificate, **the launcher can be started via job from the UMS**.

**More...**

|            |                                                  |
|------------|--------------------------------------------------|
| IGEL Setup | <b>Accessories &gt; Login PI</b>                 |
| Parameter  | Server URL                                       |
| Registry   | <code>debug.tools.login_pi.server_url</code>     |
| IGEL Setup | <b>Accessories &gt; Login PI</b>                 |
| Parameter  | Secret                                           |
| Registry   | <code>debug.tools.login_pi.crypt_password</code> |

## Hardware

- Added recognition for **IGEL UD2 M250C** with **8 GB eMMC** with product id **UD2-LX 51**.
- Added support for **IGEL UD3 M350C** with product id **UD3-LX 60**.
- UD7** with active **AMD Secure Processor** feature uses new product id **UD7-LX 11**.
- Improved support for **ADS-Tec VMT9000** devices:
  - Enable **rs-232 additional power supply** without restart.



- Enable **external wifi antenna** without restart.
  - Enable **shutdown by ignition off**.
  - Enable **watchdog service**.
  - Added hardware support for **LG CL600N**.
  - Added hardware support for **LG CL600W**.
  - Added new registry keys to be able to configure some **new i915 parameter**.
- More...**

|           |                                                          |
|-----------|----------------------------------------------------------|
| Parameter | Disable the use of limited color range for DisplayPort 1 |
| Registry  | x.drivers.intel.dp1_no_limited_color_range               |
| Range     | <u>Default</u> / disabled / enabled                      |

**Info:** Only for M250C the use of limited color range for DP1 is disabled.

- Added support for newer Prolific PL2303 USB serial adapters (used in UD3-LX 60).

## Resolved Issues 11.03.100

### Citrix

- Fixed **video playback** with enabled **Citrix Browser Content Redirection**.

### RDP/IGEL RDP Client 2

- Fixed **RDP graphics issues** with **Windows 2008(R2)** Server (when RemoteFX is not enabled).
- Fixed **RDP Web Access Domain Visibility** not working correctly.
- Fixed **sound glitch** while using **PulseAudio** system. PulseAudio is now the default sound driver.

### VMware Horizon

- Fixed **sound issue in Horizon client 5.x using PCoIP protocol**.

### Firefox

- Fixed: **Homepage** cannot be set
- Fixed: **RTSP media stream** with enabled apparmor.

### Network

- Fixed issue with configuration of more than one **NTP server**.
- Fixed network interface device order for **Dell Wyse 5070 Thin Client** so that the onboard interface always is the first one.

When endpoint is updated from a previous firmware version, network interface device order might change

- Changed **minimal allowed MSS size to 750** to avoid problems with some VPN solutions.
- Added new registry keys to be able to configure the **minimal allowed TCP MSS size**.

**More...**

|           |                               |
|-----------|-------------------------------|
| Parameter | Minimal TCP send MSS size     |
| Registry  | system.sysctl.tcp_min_snd_mss |



|       |     |
|-------|-----|
| Range | 750 |
|-------|-----|

## Smartcard

- Fixed not working **90meter** in **Firefox** when apparmor is enabled.
- Fixed handling of smartcards in **pcsc-lite**: Improved transaction locking. A new parameter was introduced to control the new behavior (enabled by default).

[More...](#)

|           |                                        |
|-----------|----------------------------------------|
| Parameter | Abort stalled transactions             |
| Registry  | scard.pcscd.abort_stalled_transactions |
| Range     | <u>enabled</u> / disabled              |

- Fixed **bug in smartcard transaction locking**.
- Fixed **IGEL Smartcard** to be able to handle **VoIP client Ekiga** sessions.
- Fixed **smartcard usernames displayed on login screen**: non-ASCII characters were not shown correctly before.
- Fixed **error message on login screen**, shown when smart card PIN is locked.

## Base system

- Fixed **license handling**: Add-on licenses can be used on top of Workspace Edition evaluation licenses now.
- Fixed **warnings when evaluation license is about to expire**. In detail, removed warning when **Enterprise Management Pack** is about to expire and WE is already licensed.
- Fixed **ActiveDirectory/Kerberos password** change with **Change Password** accessory for users which are member of many (~300+) AD groups.
- Fixed **IGEL License retrieval via FTP protocol** in **IGEL Setup Assistant** and **Licenses Browser tool**.
- Fixed **bug in reboot message** where not all available translations were used.
- Fixed problems with **missing library** if using **OpenConnect** feature.
- Changed: **Bluetooth is off by default again**. It will be temporary enabled for auto pairing before the initial Setup Assistant runs. Only if a device is paired during this phase, Bluetooth is enabled afterwards. To enable Bluetooth support by configuration use this parameter:

[More...](#)

|            |                                  |
|------------|----------------------------------|
| IGEL Setup | <b>Devices &gt; Bluetooth</b>    |
| Parameter  | Bluetooth                        |
| Registry   | devices.bluetooth.enable         |
| Value      | <u>enabled</u> / <u>disabled</u> |

- Fixed **license information** of Add-On licenses in category evaluation.
- Re-fixed broken **custom bootsplash** when doing a reset to factory defaults via UMS.

## Custom Partition

- Automatic constrain of minimum size for **custom partition to 5MB**.

## Firmware update

- **Automatic firmware update** is now checked after retrieval of UMS settings.



- If there are some not executed changes in the network configuration, these **changes are applied automatically** before performing firmware update.

#### Storage Devices

- Fixed bug: **udiskd mounted storage devices** on behalf of user processes (e.g. parole) even if Storage Hotplug was disabled in the setup.

#### X11 system

- Fixed issue with **Wacom Signing Pads** not being recognized as displays.
- Solved issues with certain **monitors** on **UD2 LX50**.
- Fixed **Multi-GPU NVIDIA** setups with **Display Switch**.
- Prevent configuration of **Display Switch** utility on unlicensed device.
- Fixed an issue with **modesetting driver** and **DisplayLink USB graphic adapters**.

#### X server

- Fixed **Xorg freezes** when usage of **modesetting driver** and **video acceleration**.

#### Shared Workplace

- Fixed broken **Shared Workplace** authentication when ICG is used.

#### Hardware

- Fixed **EFI freeze** problem **after bootcode update** on devices like the HP t630 and probably others too.
- Added: **Bluetooth tool shows now a message when no device is connected**.
- Fixed issue with **limited colors** on the **DisplayPort 1 of UD2-LX50**.

#### Remote Management

- Fixed **automatic registering** in the UMS using DNS entry or DHCP tag during initial rollout.

#### IGEL Cloud Gateway

- Fixed search for an available **buddy update server** when devices are managed over **ICG**.

#### VNC

- Fixed **sporadic connection failure** in VNC server.

#### CA Certificates Contained in IGEL OS 11.03

IGEL OS 11.03 contains the following CA certificates:

| Certificate name               | Expiry date                 | File in /etc/ssl/certs             |
|--------------------------------|-----------------------------|------------------------------------|
| ACCVRAIZ1                      | Dec 31 09:37:37<br>2030 GMT | ACCVRAIZ1.crt                      |
| AC RAIZ FNMT-RCM               | Jan 1 00:00:00<br>2030 GMT  | AC_RAIZ_FNMT-RCM.crt               |
| Actalis Authentication Root CA | Sep 22 11:22:02<br>2030 GMT | Actalis_Authentication_Root_CA.crt |



| <b>Certificate name</b>                                   | <b>Expiry date</b>       | <b>File in /etc/ssl/certs</b>                                 |
|-----------------------------------------------------------|--------------------------|---------------------------------------------------------------|
| AddTrust External CA Root                                 | May 30 10:48:38 2020 GMT | AddTrust_External_Root.crt                                    |
| AffirmTrust Commercial                                    | Dec 31 14:06:06 2030 GMT | AffirmTrust_Commercial.crt                                    |
| AffirmTrust Networking                                    | Dec 31 14:08:24 2030 GMT | AffirmTrust_Networking.crt                                    |
| AffirmTrust Premium                                       | Dec 31 14:10:36 2040 GMT | AffirmTrust_Premium.crt                                       |
| AffirmTrust Premium ECC                                   | Dec 31 14:20:24 2040 GMT | AffirmTrust_Premium_ECC.crt                                   |
| Amazon Root CA 1                                          | Jan 17 00:00:00 2038 GMT | Amazon_Root_CA_1.crt                                          |
| Amazon Root CA 2                                          | May 26 00:00:00 2040 GMT | Amazon_Root_CA_2.crt                                          |
| Amazon Root CA 3                                          | May 26 00:00:00 2040 GMT | Amazon_Root_CA_3.crt                                          |
| Amazon Root CA 4                                          | May 26 00:00:00 2040 GMT | Amazon_Root_CA_4.crt                                          |
| Atos TrustedRoot 2011                                     | Dec 31 23:59:59 2030 GMT | Atos_TrustedRoot_2011.crt                                     |
| Autoridad de Certificacion Firmaprofesional CIF A62634068 | Dec 31 08:38:15 2030 GMT | Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.crt |
| Baltimore CyberTrust Root                                 | May 12 23:59:00 2025 GMT | Baltimore_CyberTrust_Root.crt                                 |
| Buypass Class 2 Root CA                                   | Oct 26 08:38:03 2040 GMT | Buypass_Class_2_Root_CA.crt                                   |
| Buypass Class 3 Root CA                                   | Oct 26 08:28:58 2040 GMT | Buypass_Class_3_Root_CA.crt                                   |
| CA Disig Root R2                                          | Jul 19 09:15:30 2042 GMT | CA_Disig_Root_R2.crt                                          |
| CFCA EV ROOT                                              | Dec 31 03:07:01 2029 GMT | CFCA_EV_ROOT.crt                                              |
| COMODO Certification Authority                            | Dec 31 23:59:59 2029 GMT | COMODO_Certification_Authority.crt                            |
| COMODO ECC Certification Authority                        | Jan 18 23:59:59 2038 GMT | COMODO_ECC_Certification_Authority.crt                        |
| COMODO RSA Certification Authority                        | Jan 18 23:59:59 2038 GMT | COMODO_RSA_Certification_Authority.crt                        |
| Certigna                                                  | Jun 29 15:13:05 2027 GMT | Certigna.crt                                                  |



| <b>Certificate name</b>               | <b>Expiry date</b>          | <b>File in /etc/ssl/certs</b>              |
|---------------------------------------|-----------------------------|--------------------------------------------|
| Certigna Root CA                      | Oct 1 08:32:27<br>2033 GMT  | Certigna_Root_CA.crt                       |
| Certinomis - Root CA                  | Oct 21 09:17:18<br>2033 GMT | Certinomis_-_Root_CA.crt                   |
| Class 2 Primary CA                    | Jul 6 23:59:59<br>2019 GMT  | Certplus_Class_2_Primary_CA.crt            |
| Certum Trusted Network CA             | Dec 31 12:07:37<br>2029 GMT | Certum_Trusted_Network_CA.crt              |
| Certum Trusted Network CA 2           | Oct 6 08:39:56<br>2046 GMT  | Certum_Trusted_Network_CA_2.crt            |
| Chambers of Commerce Root -<br>2008   | Jul 31 12:29:50<br>2038 GMT | Chambers_of_Commerce_Root_-<br>_2008.crt   |
| AAA Certificate Services              | Dec 31 23:59:59<br>2028 GMT | Comodo_AAA_Services_root.crt               |
| Cybertrust Global Root                | Dec 15 08:00:00<br>2021 GMT | Cybertrust_Global_Root.crt                 |
| D-TRUST Root Class 3 CA 2 2009        | Nov 5 08:35:58<br>2029 GMT  | D-TRUST_Root_Class_3_CA_2_2009.crt         |
| D-TRUST Root Class 3 CA 2 EV<br>2009  | Nov 5 08:50:46<br>2029 GMT  | D-<br>TRUST_Root_Class_3_CA_2_EV_2009.crt  |
| DST Root CA X3                        | Sep 30 14:01:15<br>2021 GMT | DST_Root_CA_X3.crt                         |
| Deutsche Telekom Root CA 2            | Jul 9 23:59:00<br>2019 GMT  | Deutsche_Telekom_Root_CA_2.crt             |
| DigiCert Global Root CA               | Nov 10 00:00:00<br>2031 GMT | DigiCertGlobalRootCA.pem                   |
| DigiCert Assured ID Root CA           | Nov 10 00:00:00<br>2031 GMT | DigiCert_Assured_ID_Root_CA.crt            |
| DigiCert Assured ID Root G2           | Jan 15 12:00:00<br>2038 GMT | DigiCert_Assured_ID_Root_G2.crt            |
| DigiCert Assured ID Root G3           | Jan 15 12:00:00<br>2038 GMT | DigiCert_Assured_ID_Root_G3.crt            |
| DigiCert Global Root CA               | Nov 10 00:00:00<br>2031 GMT | DigiCert_Global_Root_CA.crt                |
| DigiCert Global Root G2               | Jan 15 12:00:00<br>2038 GMT | DigiCert_Global_Root_G2.crt                |
| DigiCert Global Root G3               | Jan 15 12:00:00<br>2038 GMT | DigiCert_Global_Root_G3.crt                |
| DigiCert High Assurance EV Root<br>CA | Nov 10 00:00:00<br>2031 GMT | DigiCert_High_Assurance_EV_Root_CA.<br>crt |



| Certificate name                                          | Expiry date                 | File in /etc/ssl/certs                            |
|-----------------------------------------------------------|-----------------------------|---------------------------------------------------|
| DigiCert Trusted Root G4                                  | Jan 15 12:00:00<br>2038 GMT | DigiCert_Trusted_Root_G4.crt                      |
| E-Tugra Certification Authority                           | Mar 3 12:09:48<br>2023 GMT  | E-Tugra_Certification_Authority.crt               |
| EC-ACC                                                    | Jan 7 22:59:59<br>2031 GMT  | EC-ACC.crt                                        |
| EE Certification Centre Root CA                           | Dec 17 23:59:59<br>2030 GMT | EE_Certification_Centre_Root_CA.crt               |
| Entrust.net <sup>425</sup> Certification Authority (2048) | Jul 24 14:15:12<br>2029 GMT | Entrust.net_Premium_2048_Secure_Server_CA.crt     |
| Entrust Root Certification Authority                      | Nov 27 20:53:42<br>2026 GMT | Entrust_Root_Certification_Authority.crt          |
| Entrust Root Certification Authority - EC1                | Dec 18 15:55:36<br>2037 GMT | Entrust_Root_Certification_Authority_-_EC1.crt    |
| Entrust Root Certification Authority - G2                 | Dec 7 17:55:54<br>2030 GMT  | Entrust_Root_Certification_Authority_-_G2.crt     |
| GDCA TrustAUTH R5 ROOT                                    | Dec 31 15:59:59<br>2040 GMT | GDCA_TrustAUTH_R5_ROOT.crt                        |
| GTS Root R1                                               | Jun 22 00:00:00<br>2036 GMT | GTS_Root_R1.crt                                   |
| GTS Root R2                                               | Jun 22 00:00:00<br>2036 GMT | GTS_Root_R2.crt                                   |
| GTS Root R3                                               | Jun 22 00:00:00<br>2036 GMT | GTS_Root_R3.crt                                   |
| GTS Root R4                                               | Jun 22 00:00:00<br>2036 GMT | GTS_Root_R4.crt                                   |
| GeoTrust Global CA                                        | May 21 04:00:00<br>2022 GMT | GeoTrust_Global_CA.crt                            |
| GeoTrust Primary Certification Authority                  | Jul 16 23:59:59<br>2036 GMT | GeoTrust_Primary_Certification_Authority.crt      |
| GeoTrust Primary Certification Authority - G2             | Jan 18 23:59:59<br>2038 GMT | GeoTrust_Primary_Certification_Authority_-_G2.crt |
| GeoTrust Primary Certification Authority - G3             | Dec 1 23:59:59<br>2037 GMT  | GeoTrust_Primary_Certification_Authority_-_G3.crt |
| GeoTrust Universal CA                                     | Mar 4 05:00:00<br>2029 GMT  | GeoTrust_Universal_CA.crt                         |
| GeoTrust Universal CA 2                                   | Mar 4 05:00:00<br>2029 GMT  | GeoTrust_Universal_CA_2.crt                       |

<sup>425</sup> <http://Entrust.net>



| Certificate name                                            | Expiry date              | File in /etc/ssl/certs                                          |
|-------------------------------------------------------------|--------------------------|-----------------------------------------------------------------|
| GlobalSign                                                  | Jan 19 03:14:07 2038 GMT | GlobalSign_ECC_Root_CA_-_R4.crt                                 |
| GlobalSign                                                  | Jan 19 03:14:07 2038 GMT | GlobalSign_ECC_Root_CA_-_R5.crt                                 |
| GlobalSign Root CA                                          | Jan 28 12:00:00 2028 GMT | GlobalSign_Root_CA.crt                                          |
| GlobalSign                                                  | Dec 15 08:00:00 2021 GMT | GlobalSign_Root_CA_-_R2.crt                                     |
| GlobalSign                                                  | Mar 18 10:00:00 2029 GMT | GlobalSign_Root_CA_-_R3.crt                                     |
| GlobalSign                                                  | Dec 10 00:00:00 2034 GMT | GlobalSign_Root_CA_-_R6.crt                                     |
| Global Chambersign Root - 2008                              | Jul 31 12:31:40 2038 GMT | Global_Chambersign_Root_-_2008.crt                              |
| Go Daddy Class 2 Certification Authority                    | Jun 29 17:06:20 2034 GMT | Go_Daddy_Class_2_CA.crt                                         |
| Go Daddy Root Certificate Authority - G2                    | Dec 31 23:59:59 2037 GMT | Go_Daddy_Root_Certificate_Authority_-_G2.crt                    |
| Hellenic Academic and Research Institutions ECC RootCA 2015 | Jun 30 10:37:12 2040 GMT | Hellenic_Academic_and_Research_Institutions_ECC_RootCA_2015.crt |
| Hellenic Academic and Research Institutions RootCA 2011     | Dec 1 13:49:52 2031 GMT  | Hellenic_Academic_and_Research_Institutions_RootCA_2011.crt     |
| Hellenic Academic and Research Institutions RootCA 2015     | Jun 30 10:11:21 2040 GMT | Hellenic_Academic_and_Research_Institutions_RootCA_2015.crt     |
| Hongkong Post Root CA 1                                     | May 15 04:52:29 2023 GMT | Hongkong_Post_Root_CA_1.crt                                     |
| ISRG Root X1                                                | Jun 4 11:04:38 2035 GMT  | ISRG_Root_X1.crt                                                |
| IdenTrust Commercial Root CA 1                              | Jan 16 18:12:23 2034 GMT | IdenTrust_Commercial_Root_CA_1.crt                              |
| IdenTrust Public Sector Root CA 1                           | Jan 16 17:53:32 2034 GMT | IdenTrust_Public_Sector_Root_CA_1.crt                           |
| Imprivata Embedded Code Signing CA                          | Sep 7 16:20:00 2033 GMT  | Imprivata.crt                                                   |
| Izenpe.com <sup>426</sup>                                   | Dec 13 08:27:25 2037 GMT | Izenpe.com <sup>427</sup> .crt                                  |
| LuxTrust Global Root 2                                      | Mar 5 13:21:57 2035 GMT  | LuxTrust_Global_Root_2.crt                                      |

<sup>426</sup> <http://Izenpe.com><sup>427</sup> <http://Izenpe.com>



| Certificate name                                              | Expiry date              | File in /etc/ssl/certs                             |
|---------------------------------------------------------------|--------------------------|----------------------------------------------------|
| Microsec e-Szigno Root CA 2009                                | Dec 30 11:30:18 2029 GMT | Microsec_e-Szigno_Root_CA_2009.crt                 |
| NetLock Arany (Class Gold) FÅ‘tanÃºsÃ†vÃ¡ny                   | Dec 6 15:08:21 2028 GMT  | NetLock_Arany_=Class_Gold=_FÅ‘tanÃºsÃ†vÃ¡ny.crt    |
| Network Solutions Certificate Authority                       | Dec 31 23:59:59 2029 GMT | Network_Solutions_Certificate_Authority.crt        |
| OISTE WISeKey Global Root GA CA                               | Dec 11 16:09:51 2037 GMT | OISTE_WISeKey_Global_Root_GA_CA.crt                |
| OISTE WISeKey Global Root GB CA                               | Dec 1 15:10:31 2039 GMT  | OISTE_WISeKey_Global_Root_GB_CA.crt                |
| OISTE WISeKey Global Root GC CA                               | May 9 09:58:33 2042 GMT  | OISTE_WISeKey_Global_Root_GC_CA.crt                |
| QuoVadis Root Certification Authority                         | Mar 17 18:33:33 2021 GMT | QuoVadis_Root_CA.crt                               |
| QuoVadis Root CA 1 G3                                         | Jan 12 17:27:44 2042 GMT | QuoVadis_Root_CA_1_G3.crt                          |
| QuoVadis Root CA 2                                            | Nov 24 18:23:33 2031 GMT | QuoVadis_Root_CA_2.crt                             |
| QuoVadis Root CA 2 G3                                         | Jan 12 18:59:32 2042 GMT | QuoVadis_Root_CA_2_G3.crt                          |
| QuoVadis Root CA 3                                            | Nov 24 19:06:44 2031 GMT | QuoVadis_Root_CA_3.crt                             |
| QuoVadis Root CA 3 G3                                         | Jan 12 20:26:32 2042 GMT | QuoVadis_Root_CA_3_G3.crt                          |
| SSL.com <sup>428</sup> EV Root Certification Authority ECC    | Feb 12 18:15:23 2041 GMT | SSL.com_EV_Root_Certification_Authority_ECC.crt    |
| SSL.com <sup>429</sup> EV Root Certification Authority RSA R2 | May 30 18:14:37 2042 GMT | SSL.com_EV_Root_Certification_Authority_RSA_R2.crt |
| SSL.com <sup>430</sup> Root Certification Authority ECC       | Feb 12 18:14:03 2041 GMT | SSL.com_Root_Certification_Authority_ECC.crt       |
| SSL.com <sup>431</sup> Root Certification Authority RSA       | Feb 12 17:39:39 2041 GMT | SSL.com_Root_Certification_Authority_RSA.crt       |
| SZAFIR ROOT CA2                                               | Oct 19 07:43:30 2035 GMT | SZAFIR_ROOT_CA2.crt                                |
| SecureSign RootCA11                                           | Apr 8 04:56:47 2029 GMT  | SecureSign_RootCA11.crt                            |

<sup>428</sup> <http://SSL.com><sup>429</sup> <http://SSL.com><sup>430</sup> <http://SSL.com><sup>431</sup> <http://SSL.com>



| <b>Certificate name</b>                            | <b>Expiry date</b>          | <b>File in /etc/ssl/certs</b>                          |
|----------------------------------------------------|-----------------------------|--------------------------------------------------------|
| SecureTrust CA                                     | Dec 31 19:40:55<br>2029 GMT | SecureTrust_CA.crt                                     |
| Secure Global CA                                   | Dec 31 19:52:06<br>2029 GMT | Secure_Global_CA.crt                                   |
| Security Communication RootCA2                     | May 29 05:00:39<br>2029 GMT | Security_Communication_RootCA2.crt                     |
| Security Communication RootCA1                     | Sep 30 04:20:49<br>2023 GMT | Security_Communication_Root_CA.crt                     |
| Sonera Class2 CA                                   | Apr 6 07:29:40<br>2021 GMT  | Sonera_Class_2_Root_CA.crt                             |
| Staat der Nederlanden EV Root CA                   | Dec 8 11:10:28<br>2022 GMT  | Staat_der_Nederlanden_EV_Root_CA.crt                   |
| Staat der Nederlanden Root CA - G2                 | Mar 25 11:03:10<br>2020 GMT | Staat_der_Nederlanden_Root_CA--G2.crt                  |
| Staat der Nederlanden Root CA - G3                 | Nov 13 23:00:00<br>2028 GMT | Staat_der_Nederlanden_Root_CA--G3.crt                  |
| Starfield Class 2 Certification Authority          | Jun 29 17:39:16<br>2034 GMT | Starfield_Class_2_CA.crt                               |
| Starfield Root Certificate Authority - G2          | Dec 31 23:59:59<br>2037 GMT | Starfield_Root_Certificate_Authority_-_G2.crt          |
| Starfield Services Root Certificate Authority - G2 | Dec 31 23:59:59<br>2037 GMT | Starfield_Services_Root_Certificate_Authority_-_G2.crt |
| SwissSign Gold CA - G2                             | Oct 25 08:30:35<br>2036 GMT | SwissSign_Gold_CA_-_G2.crt                             |
| SwissSign Silver CA - G2                           | Oct 25 08:32:46<br>2036 GMT | SwissSign_Silver_CA_-_G2.crt                           |
| T-TeleSec GlobalRoot Class 2                       | Oct 1 23:59:59<br>2033 GMT  | T-TeleSec_GlobalRoot_Class_2.crt                       |
| T-TeleSec GlobalRoot Class 3                       | Oct 1 23:59:59<br>2033 GMT  | T-TeleSec_GlobalRoot_Class_3.crt                       |
| TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1      | Oct 25 08:25:55<br>2043 GMT | TUBITAK_Kamu_SM_SSL_Kok_Sertifikasi_-_Surum_1.crt      |
| TWCA Global Root CA                                | Dec 31 15:59:59<br>2030 GMT | TWCA_Global_Root_CA.crt                                |
| TWCA Root Certification Authority                  | Dec 31 15:59:59<br>2030 GMT | TWCA_Root_Certification_Authority.crt                  |
| Government Root Certification Authority            | Dec 5 13:23:33<br>2032 GMT  | Taiwan_GRCA.crt                                        |
| TeliaSonera Root CA v1                             | Oct 18 12:00:50<br>2032 GMT | TeliaSonera_Root_CA_v1.crt                             |



| <b>Certificate name</b>                                      | <b>Expiry date</b>          | <b>File in /etc/ssl/certs</b>                                    |
|--------------------------------------------------------------|-----------------------------|------------------------------------------------------------------|
| TrustCor ECA-1                                               | Dec 31 17:28:07<br>2029 GMT | TrustCor_ECA-1.crt                                               |
| TrustCor RootCert CA-1                                       | Dec 31 17:23:16<br>2029 GMT | TrustCor_RootCert_CA-1.crt                                       |
| TrustCor RootCert CA-2                                       | Dec 31 17:26:39<br>2034 GMT | TrustCor_RootCert_CA-2.crt                                       |
| Trustis FPS Root CA                                          | Jan 21 11:36:54<br>2024 GMT | Trustis_FPS_Root_CA.crt                                          |
| UCA Extended Validation Root                                 | Dec 31 00:00:00<br>2038 GMT | UCA_Extended_Validation_Root.crt                                 |
| UCA Global G2 Root                                           | Dec 31 00:00:00<br>2040 GMT | UCA_Global_G2_Root.crt                                           |
| USERTrust ECC Certification Authority                        | Jan 18 23:59:59<br>2038 GMT | USERTrust_ECC_Certification_Authority.crt                        |
| USERTrust RSA Certification Authority                        | Jan 18 23:59:59<br>2038 GMT | USERTrust_RSA_Certification_Authority.crt                        |
| VeriSign Class 3 Public Primary Certification Authority - G4 | Jan 18 23:59:59<br>2038 GMT | VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt |
| VeriSign Class 3 Public Primary Certification Authority - G5 | Jul 16 23:59:59<br>2036 GMT | VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt |
| VeriSign Universal Root Certification Authority              | Dec 1 23:59:59<br>2037 GMT  | VeriSign_Universal_Root_Certification_Authority.crt              |
| VeriSign Class 3 Public Primary Certification Authority - G3 | Jul 16 23:59:59<br>2036 GMT | VeriSign_Class_3_Public_Primary_Certification_Authority_-_G3.crt |
| XRamp Global Certification Authority                         | Jan 1 05:37:19<br>2035 GMT  | XRamp_Global_CA_Root.crt                                         |
| certSIGN ROOT CA                                             | Jul 4 17:20:04<br>2031 GMT  | certSIGN_ROOT_CA.crt                                             |
| ePKI Root Certification Authority                            | Dec 20 02:31:27<br>2034 GMT | ePKI_Root_Certification_Authority.crt                            |
| thawte Primary Root CA                                       | Jul 16 23:59:59<br>2036 GMT | thawte_Primary_Root_CA.crt                                       |
| thawte Primary Root CA - G2                                  | Jan 18 23:59:59<br>2038 GMT | thawte_Primary_Root_CA_-_G2.crt                                  |
| thawte Primary Root CA - G3                                  | Dec 1 23:59:59<br>2037 GMT  | thawte_Primary_Root_CA_-_G3.crt                                  |



## 7.11.2 IGEL OS Creator (OSC)

### Supported Devices

|         |                                     |
|---------|-------------------------------------|
| UD2-LX: | UD2-LX 51<br>UD2-LX 50<br>UD2-LX 40 |
| UD3-LX: | UD3-LX 60<br>UD3-LX 51<br>UD3-LX 50 |
| UD5-LX: | UD5-LX 50                           |
| UD6-LX: | UD6-LX 51                           |
| UD7-LX: | UD7-LX 11<br>UD7-LX 10              |
| UD9-LX: | UD9-LX Touch 41<br>UD9-LX 40        |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>432</sup>.

- [Component Versions 11.03.100](#)(see page 1741)
- [New Features 11.03.100](#)(see page 1743)

### Component Versions 11.03.100

- **Clients**

| Product  | Version   |
|----------|-----------|
| Zulu JRE | 8.42.0.23 |

---

<sup>432</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



- Smartcard**

|                             |               |
|-----------------------------|---------------|
| Reader Driver MUSCLE CCID   | 1.4.31-1igel6 |
| Resource Manager PC/SC Lite | 1.8.23-1igel8 |

- System Components**

|                                         |                              |
|-----------------------------------------|------------------------------|
| OpenSSL                                 | 1.0.2g-1ubuntu4.15           |
| Bluetooth Stack (bluez)                 | 5.50-0ubuntu1igel5           |
| MESA OpenGL stack                       | 19.2.5-1igel93               |
| VDPAU Library version                   | 1.2-1igel911                 |
| Graphics Driver INTEL                   | 2.99.917+git20191117-igel939 |
| Graphics Driver ATI/RADEON              | 19.0.1-3igel936              |
| Graphics Driver ATI/AMDGPU              | 19.0.1-5igel924              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867              |
| Graphics Driver Nvidia                  | 418.56-0ubuntu1              |
| Graphics Driver Vboxvideo               | 1.0.0-igel798                |
| Graphics Driver VMware                  | 13.3.0-2igel857              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build2-igel925        |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |
| Graphics Driver VESA                    | 2.4.0-1igel855               |
| Input Driver Evdev                      | 2.10.6-1igel888              |
| Input Driver Elographics                | 1.4.1-1build5igel633         |
| Input Driver Synaptics                  | 1.9.1-1ubuntu1igel866        |
| Input Driver VMMouse                    | 13.1.0-1ubuntu2igel635       |
| Input Driver Wacom                      | 0.36.1-0ubuntu2igel888       |
| Kernel                                  | 4.19.85 #mainline-lxos-r2872 |
| Xorg X11 Server                         | 1.20.5-1igel914              |
| Lightdm Graphical Login Manager         | 1.18.3-0ubuntu1.1            |



|                      |                         |
|----------------------|-------------------------|
| XFCE4 Window Manager | 4.12.3-1ubuntu2igel675  |
| ISC DHCP Client      | 4.3.3-5ubuntu12.10igel7 |
| WebKit2Gtk           | 2.26.2-1igel27          |
| Python2              | 2.7.12                  |
| Python3              | 3.5.2                   |

## New Features 11.03.100

### Hardware

- Added hardware support for **LG CL600N**.
- Added hardware support for **LG CL600W**.

## 7.12 Notes for Release 11.02.150

|                       |            |              |
|-----------------------|------------|--------------|
| <b>Software:</b>      | Version    | 11.02.150    |
| <b>Release Date:</b>  | 2019-09-09 |              |
| <b>Release Notes:</b> | Version    | RN-1102150-1 |
| <b>Last update:</b>   | 2019-09-09 |              |

- Supported Devices 11.02.150(see page 1743)
- Component Versions 11.02.150(see page 1744)
- General Information 11.02.150(see page 1748)
- Security Fixes 11.02.150(see page 1749)
- Known Issues 11.02.150(see page 1752)
- New Features 11.02.150(see page 1754)
- Resolved Issues 11.02.150(see page 1754)

### 7.12.1 Supported Devices 11.02.150

| <b>IGEL devices:</b> |           |
|----------------------|-----------|
| UD2-LX:              | UD2-LX 50 |
|                      | UD2-LX 40 |



|         |                              |
|---------|------------------------------|
| UD3-LX: | UD3-LX 51<br>UD3-LX 50       |
| UD5-LX: | UD5-LX 50                    |
| UD6-LX: | UD6-LX 51                    |
| UD7-LX: | UD7-LX 10                    |
| UD9-LX: | UD9-LX Touch 41<br>UD9-LX 40 |

For supported IGEL OS 11 third-party devices, see [Devices Supported by IGEL OS 11](#)<sup>433</sup>.

### 7.12.2 Component Versions 11.02.150

- **Clients**

| Product                           | Version                         |
|-----------------------------------|---------------------------------|
| Citrix HDX Realtime Media Engine  | 2.8.0-2235                      |
| Citrix Receiver                   | 13.10.0.20                      |
| Citrix Receiver                   | 13.5.0.10185126                 |
| Citrix Workspace App              | 19.6.0.60                       |
| deviceTRUST Citrix Channel        | 19.1.200.2                      |
| Ericom PowerTerm                  | 12.0.1.0.20170219.2-_dev_-34574 |
| Ericom PowerTerm                  | 12.5_x64_20190619_12.5.1.40008  |
| Evidian AuthMgr                   | 1.5.7116                        |
| Evince PDF Viewer                 | 3.18.2-1ubuntu4.6               |
| FabulaTech USB for Remote Desktop | 5.2.29                          |
| Firefox                           | 60.9.0                          |

<sup>433</sup> <https://kb.igel.com/os11-supported-hardware>



|                                        |                                           |
|----------------------------------------|-------------------------------------------|
| IBM iAccess Client Solutions           | 1.1.8.1                                   |
| IGEL RDP Client                        | 2.2                                       |
| Imprivata OneSign ProveID Embedded     | onesign-bootstrap-loader_1.0.523630_amd64 |
| deviceTRUST RDP Channel                | 19.1.200.2                                |
| NCP Secure Enterprise Client           | 5.10_rev40552                             |
| NX Client                              | 6.7.6                                     |
| Open VPN                               | 2.3.10-1ubuntu2.2                         |
| Zulu JRE                               | 8.40.0.25                                 |
| Parallels Client (64 bit)              | 17.0.21282                                |
| Spice GTK (Red Hat Virtualization)     | 0.36-1~git20190601igel61                  |
| Remote Viewer (Red Hat Virtualization) | 8.0-1igel49                               |
| Usbredir (Red Hat Virtualization)      | 0.8.0-1igel49                             |
| Teradici PCoIP Software Client         | 19.05.5-18.04                             |
| ThinLinc Client                        | 4.10.0-6068                               |
| ThinPrint Client                       | 7.5.88                                    |
| Totem Media Player                     | 2.30.2                                    |
| Parole Media Player                    | 1.0.1-0ubuntu1igel18                      |
| VNC Viewer                             | 1.9.0+dfsg-3igel8                         |
| VMware Horizon Client                  | 5.0.0-12557422                            |
| Voip Client Ekiga                      | 4.0.1                                     |

- **Dictation**

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20180621 |
| Philips Speech driver                     | 12.7.11  |



- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.8    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.3.2    |

- **Smartcard**

|                                           |                        |
|-------------------------------------------|------------------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101                |
| PKCS#11 Library Athena IDProtect          | 623.07                 |
| PKCS#11 Library cryptovision sc/interface | 7.1.20                 |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0              |
| PKCS#11 Library SecMaker NetID            | 6.7.2.36               |
| PKCS#11 Library 90meter                   | 20190522               |
| Reader Driver ACS CCID                    | 1.1.6-1igel1           |
| Reader Driver Gemalto eToken              | 10.0.37-0              |
| Reader Driver HID Global Omnikey          | 4.3.3                  |
| Reader Driver Identive CCID               | 5.0.35                 |
| Reader Driver Identive eHealth200         | 1.0.5                  |
| Reader Driver Identive SCRKBC             | 5.0.24                 |
| Reader Driver MUSCLE CCID                 | 1.4.30-1igel3          |
| Reader Driver REINER SCT cyberJack        | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite               | 1.8.23-1igel1          |
| Cherry USB2LAN Proxy                      | 3.2.0.3                |

- **System Components**

|         |                    |
|---------|--------------------|
| OpenSSL | 1.0.2g-1ubuntu4.15 |
|---------|--------------------|



|                                         |                              |
|-----------------------------------------|------------------------------|
| OpenSSH Client                          | 7.2p2-4ubuntu2.8             |
| OpenSSH Server                          | 7.2p2-4ubuntu2.8             |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5           |
| MESA OpenGL stack                       | 19.0.8-1igel73               |
| VAAPI ABI Version                       | 0.40                         |
| VDPAU Library version                   | 1.1.1-3ubuntu1               |
| Graphics Driver INTEL                   | 2.99.917+git20190724-igel907 |
| Graphics Driver ATI/RADEON              | 19.0.1-2igel890              |
| Graphics Driver ATI/AMDGPU              | 19.0.1-4igel894              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867              |
| Graphics Driver Nvidia                  | 418.56-0ubuntu1              |
| Graphics Driver Vboxvideo               | 1.0.0-igel798                |
| Graphics Driver VMware                  | 13.3.0-2igel857              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1igel775         |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |
| Graphics Driver VESA                    | 2.4.0-1igel855               |
| Input Driver Evdev                      | 2.10.6-1igel888              |
| Input Driver Elographics                | 1.4.1-1build5igel633         |
| Input Driver eGalax                     | 2.5.5814                     |
| Input Driver Synaptics                  | 1.9.1-1ubuntu1igel866        |
| Input Driver VMMouse                    | 13.1.0-1ubuntu2igel635       |
| Input Driver Wacom                      | 0.36.1-0ubuntu2igel888       |
| Kernel                                  | 4.19.65 #mainline-lxos-r2782 |
| Xorg X11 Server                         | 1.19.7-1igel913              |
| Xorg Xephyr                             | 1.19.7-1igel913              |



|                                 |                               |
|---------------------------------|-------------------------------|
| CUPS printing daemon            | 2.1.3-4ubuntu0.9igel27        |
| PrinterLogic                    | 18.2.1.128                    |
| Lightdm Graphical Login Manager | 1.18.3-0ubuntu1.1             |
| XFCE4 Window Manager            | 4.12.3-1ubuntu2igel675        |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7       |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.3igel74  |
| ModemManager                    | 1.10.0-1~ubuntu18.04.2igel3   |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.2            |
| GStreamer 1.x                   | 1.16.0-1igel214               |
| WebKit2Gtk                      | 2.24.2-0ubuntu0.19.04.1igel18 |
| Python2                         | 2.7.12                        |
| Python3                         | 3.5.2                         |

- **Features with Limited IGEL Support**

|                                    |                                  |
|------------------------------------|----------------------------------|
| Mobile Device Access USB (MTP)     | 1.1.16-2igel1                    |
| Mobile Device Access USB (imobile) | 1.2.1~git20181030.92c5462-1igel5 |
| Mobile Device Access USB (gphoto)  | 2.5.22-3igel1                    |
| VPN OpenConnect                    | 7.08-1                           |
| Scanner support / Sane             | 1.0.27-1                         |
| VirtualBox                         | 6.0.10-dfsg-4igel31              |

- **Features with Limited Functionality**

|                   |        |
|-------------------|--------|
| Cisco JVDI Client | 12.1.0 |
|-------------------|--------|

### 7.12.3 General Information 11.02.150

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download



- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

#### 7.12.4 Security Fixes 11.02.150

##### Firefox

- Updated **Firefox** browser to version **60.9.0 ESR**.  
Including Fixes from **Security Advisory 2019-27**:  
[More...](#)  
CVE-2019-11746, CVE-2019-11744, CVE-2019-11753, CVE-2019-11752, CVE-2019-9812, CVE-2019-11743, and CVE-2019-11740.
- Fixes for **mfsa2019-22**, also known as:  
[More...](#)  
CVE-2019-9811, CVE-2019-11711, CVE-2019-11712, CVE-2019-11713, CVE-2019-11729, CVE-2019-11715, CVE-2019-11717, CVE-2019-11719, CVE-2019-11730, and CVE-2019-11709.
- Fixes for **mfsa2019-19**, also known as: CVE-2019-11708.
- Fixes for **mfsa2019-18**, also known as: CVE-2019-11707.
- Fixes for **mfsa2019-08**, also known as:  
[More...](#)  
CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2018-18506, and CVE-2019-9788.
- Fixes for **mfsa2019-05**, also known as: CVE-2018-18356, CVE-2019-5785.
- Fixes for **mfsa2019-02**, also known as: CVE-2018-18500, CVE-2018-18505, and CVE-2018-18501.
- Added allowance for Firefox to access **Yubikey (FIDO/U2F)** if apparmor is active.

##### Base system

- Fixed security issue **CVE-2019-15902** in **4.19.x kernel**.
- Set default **umask to 0077** for all non-root users.
- Remote users home is now **/home/ruser**.
- Fixed **policykit-1** security issue CVE-2019-6133.
- Fixed **tiff** security issues:  
[More...](#)  
CVE-2019-7663, CVE-2019-6128, CVE-2018-19210, CVE-2018-17000, CVE-2018-12900, and CVE-2018-10779.
- Fixed **lcms2** security issue CVE-2018-16435.
- Fixed **libpng1.6** security issues CVE-2019-7317 and CVE-2018-13785.
- Fixed **nss** security issues CVE-2018-18508, CVE-2019-11729, and CVE-2019-11719.
- Fixed **procps** security issues:

**More...**

CVE-2018-1126, CVE-2018-1125, CVE-2018-1124,  
CVE-2018-1123 and CVE-2018-1122.

- Fixed **evince** security issues CVE-2019-11459 and CVE-2019-1010006.
- Fixed **gdk-pixbuf** security issue CVE-2017-12447.
- Fixed **gst-plugins-base0.10** security issue CVE-2019-9928.
- Fixed **bind9** security issues CVE-2019-6465, CVE-2018-5745 and CVE-2018-5743.
- Fixed **libgd2** security issues CVE-2019-6978 and CVE-2019-6977.
- Fixed **ghostscript** security issues CVE-2019-3839, CVE-2019-3838 and CVE-2019-3835.
- Fixed **ldb** security issue CVE-2019-3824.
- Fixed **file** security issues CVE-2019-8907 and CVE-2019-8905.
- Fixed **poppler** security issues:

**More...**

CVE-2019-9200, CVE-2019-9903, CVE-2019-9631, CVE-2019-12293,  
CVE-2019-10872, CVE-2019-10023, CVE-2019-10021, CVE-2019-10019,  
CVE-2019-10018, CVE-2018-20662, CVE-2018-18897, and CVE-2017-9865.

- Fixed **samba** security issues CVE-2019-3880 and CVE-2018-16860.
- Fixed **openssl** security issue CVE-2019-1559.
- Fixed **libxslt** security issue CVE-2019-11068.
- Fixed **openssh** security issue CVE-2019-6111.
- Fixed **wget** security issue CVE-2019-5953.
- Fixed **wpa** security issues:

**More...**

CVE-2019-9495, CVE-2019-9497, CVE-2019-9498,  
CVE-2019-9499, and CVE-2019-11555.

- Fixed **gtk+2.0** security issue CVE-2013-7447.
- Fixed **heimdal** security issues CVE-2019-12098 and CVE-2018-16860.
- Fixed **webkit2gtk** security issues CVE-2019-8615, CVE-2019-8607, and CVE-2019-8595.
- Fixed **gimp** security issues:

**More...**

CVE-2017-17786, CVE-2017-17789, CVE-2017-17784,  
CVE-2017-17787, CVE-2017-17785, and CVE-2017-17788.

- Fixed **libtomcrypt** security issue CVE-2018-12437.
- Fixed **unzip** security issues CVE-2019-13232, CVE-2018-1000035, CVE-2016-9844, and  
CVE-2014-9913.
- Fixed **curl** security issues:

**More...**

CVE-2018-16840, CVE-2018-16839, CVE-2019-3823,  
CVE-2019-3822, CVE-2018-16890, and CVE-2019-5346.

- Fixed **gnutls28** security issues CVE-2018-10846, CVE-2018-10845, CVE-2018-10844, and  
CVE-2018-1084.
- Fixed **db5.3** security issue CVE-2019-8457.



- Fixed **qtbase-opensource-src** security issues CVE-2018-19873, CVE-2018-19870, and CVE-2018-15518.

- Fixed **libssh2** security issues:

[More...](#)

CVE-2019-3863, CVE-2019-3862, CVE-2019-3861, CVE-2019-3860, CVE-2019-3859, CVE-2019-3858, CVE-2019-3857, CVE-2019-3856, and CVE-2019-3855.

- Fixed **network-manager** security issue CVE-2018-15688.

- Fixed **elfutils** security issues:

[More...](#)

CVE-2019-7665, CVE-2019-7150, CVE-2019-7149, CVE-2018-18521, CVE-2018-18520, CVE-2018-18310, CVE-2018-16403, CVE-2018-16402, and CVE-2018-16062.

- Fixed **libsndfile** security issues:

[More...](#)

CVE-2019-3832, CVE-2018-19758, CVE-2018-19662, CVE-2018-19661, CVE-2018-19432, CVE-2018-13139, CVE-2017-6892, CVE-2017-17457, CVE-2017-17456, CVE-2017-16942, CVE-2017-14634, CVE-2017-14246, and CVE-2017-14245.

- Fixed **dbus** security issue CVE-2019-12749.

- Fixed **vim** security issues CVE-2019-12735 and CVE-2017-5953.

- Fixed **glib2.0** security issue CVE-2019-12450.

- Fixed **openssl (1.1.x)** security issues:

[More...](#)

CVE-2019-1543, CVE-2018-0737, CVE-2018-0735, CVE-2018-0734, and CVE-2018-0732.

- Fixed **sqlite3** security issues:

[More...](#)

CVE-2019-9937, CVE-2019-9936, CVE-2019-8457, CVE-2018-20506, CVE-2018-20346, CVE-2017-2520, CVE-2017-2519, CVE-2017-2518, CVE-2017-13685, CVE-2017-10989, and CVE-2016-6153.

- Fixed **systemd** security issues:

[More...](#)

CVE-2019-6454, CVE-2019-6454, CVE-2018-1049, CVE-2018-15686, and CVE-2019-3842.

- Fixed **libseccomp** security issue CVE-2019-9893.

- Fixed **bzip2** security issues CVE-2019-12900 and CVE-2016-3189.

- Fixed **imagemagick** security issues:

[More...](#)

CVE-2019-9956, CVE-2019-7398, CVE-2019-7397, CVE-2019-7396, CVE-2019-7175, CVE-2019-11598, CVE-2019-11597, CVE-2019-11472, CVE-2019-11470, CVE-2019-10650, CVE-2019-10131, CVE-2018-20467, CVE-2018-18025, CVE-2018-18024, CVE-2018-18016, CVE-2018-17966,



CVE-2018-17965, CVE-2018-16413, CVE-2018-16412, CVE-2017-12806, and CVE-2017-12805.

- Fixed **expat** security issue CVE-2018-20843.
- Fixed **glib2.0** security issue CVE-2019-13012.
- Fixed **libvirt** security issues CVE-2019-10167 and CVE-2019-10161.
- Fixed **gvfs** security issue CVE-2019-12795.
- Fixed **libmspack** security issue CVE-2019-1010305.
- Fixed **bash** security issue CVE-2019-9924.
- Fixed **openldap** security issues CVE-2019-13565 and CVE-2019-13057.
- Updated **libwebkit2gtk-4.0-37** to version **2.24.2**.

Security fixes:

**More...**

CVE-2019-8595, CVE-2019-8607, CVE-2019-8615, CVE-2019-6251, CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378, CVE-2018-4382, CVE-2018-4392, CVE-2018-4416, CVE-2018-4345, CVE-2018-4386, and CVE-2018-4372.

- Fixed a vulnerability in the **custom environment variable framework**.
- Fixed possible malicious **owner change within TC setup configuration**.
- Fixed **kernel TCP** vulnerabilities CVE-2019-11477: **SACK Panic**, CVE-2019-11478: **SACK Slowness**, and CVE-2019-11479: **Excess resource consumption due to low MSS values**.
- Changed minimally allowed **MSS size** to **1000** to prevent possible Denial of Service attacks.
- Fixed a vulnerability in **Java configuration script**.

## 7.12.5 Known Issues 11.02.150

### Citrix

- With activated DRI3 and AMD GPU, Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H264, MPEG1 and MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.  
As a workaround, insert the smartcard before starting StoreFront login.
- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compressin" > "For the entire screen".
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264 acceleration plugin**, the following registry key must be enabled:  
**More...**

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |



|              |                           |
|--------------|---------------------------|
| <b>Value</b> | <u>enabled / disabled</u> |
|--------------|---------------------------|

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

#### VMware Horizon

- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off. In the IGEL Setup client, **drive mapping** can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping**. It is also recommended to disable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection entirely** or at least to **deny storage devices** by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Enable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection **do not appear in the remote desktop**. Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.

#### Wi-Fi

- **TP-Link Archer T2UH Wi-Fi adapters** do not work after system suspend/resume. Workaround: Disable system suspend under **IGEL Setup > System > Power Options > Shutdown**.

#### Parallels Client

- **Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** once with disabled FIPS support.

#### Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice**: spice-xpi firefox plugin is no longer supported. The "Console Invocation" has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

#### Multimedia

- Multimedia **redirection with GStreamer** could fail with the **Nouveau GPU driver**.

#### Audio

- IGEL **UD2 (D220)** fails to restore the **volume level of the speaker** when the device used firmware version **11.01.110** before.



## 7.12.6 New Features 11.02.150

### Hardware

- Improved support for **ADS-Tec VMT9000** devices:
  - Enable **rs-232 additional power supply** without restart.
  - Enable an **external Wi-Fi antenna** without restart.
  - Enable **shutdown by ignition off**.
- Added hardware support for **Dell WYSE 5020**.

## 7.12.7 Resolved Issues 11.02.150

### DP/IGEL RDP Client 2

- Fixed **RDP graphics** issues with **Windows 2008(R2) Server** (when **RemoteFX** is not enabled).
- Fixed some smaller **graphical RDP issues** with **Windows 2012 R2** if using **Clearcodec**.

### Network

- Changed **minimally allowed MSS size** to "**750**" to avoid problems with some VPN solutions.
- Added a new registry key to be able to configure the **minimally allowed TCP MSS size**.

A new registry key:

[More...](#)

|           |                                                                             |
|-----------|-----------------------------------------------------------------------------|
| Parameter | Minimal TCP send MSS size                                                   |
| Registry  | system.sysctl.tcp_min_snd_mss                                               |
| Type      | Integer                                                                     |
| Value     | <u>750</u>                                                                  |
| Tooltip   | Minimal TCP send MSS size (configurable value in the area from 200 to 1450) |

### Hardware

- Fixed **EFI freeze** problem **after bootcode update on** devices like the **HP t630** and probably others too.
- Added support for newer **Prolific PL2303 USB serial adapters** (used in UD3 LX60).

### Firefox

- Fixed: **Homepage cannot be set**.

### X11 system

- Fixed **Multi-GPU NVIDIA** setups **with Display Switch**.
- Prevent configuration of **Display Switch** utility **on unlicensed devices**.
- Added **new registry keys** to be able **to configure some modesetting options** if needed.

New registry keys:

[More...](#)

|           |                                     |
|-----------|-------------------------------------|
| Parameter | Use DRI3 PageFlip feature           |
| Registry  | x.drivers.modesetting.use_page_flip |



|           |                                                              |
|-----------|--------------------------------------------------------------|
| Range     | <u>[Default]</u> [False] [True]                              |
| Info      | "Default" (normally use page flip feature)                   |
| Parameter | Use shadow framebuffer layer                                 |
| Registry  | x.drivers.modesetting.use_shadow_fb                          |
| Range     | <u>[Default]</u> [False] [True]                              |
| Info      | "Default" (normally use shadow framebuffer)                  |
| Parameter | Use double shadow framebuffer to improve VNC performance     |
| Registry  | x.drivers.modesetting.use_double_shadow                      |
| Range     | <u>[False]</u> [True]                                        |
| Parameter | Use software cursor for modesetting driver                   |
| Registry  | x.drivers.modesetting.use_sw_cursor                          |
| Range     | <u>[Default]</u> [False] [True]                              |
| Info      | "Default" (normally false)                                   |
| Parameter | Choose acceleration method                                   |
| Registry  | x.drivers.modesetting.accel_method                           |
| Range     | <u>[Default]</u> [Glamor] [None]                             |
| Info      | "Default" (normally Glamor is used)                          |
| Parameter | Force usage of DRI3 regardless of x.drivers.use_dri3 setting |
| Registry  | x.drivers.modesetting.force_dri3                             |
| Type      | Bool                                                         |
| Value     | False                                                        |

## 7.13 Notes for Release 11.02.130

|                       |            |              |
|-----------------------|------------|--------------|
| <b>Software:</b>      | Version    | 11.02.130    |
| <b>Release Date:</b>  | 2019-08-23 |              |
| <b>Release Notes:</b> | Version    | RN-1102130-1 |
| <b>Last update:</b>   | 2019-08-23 |              |

- Supported Devices 11.02.130(see page 1756)
- Component Versions 11.02.130(see page 1756)
- General Information 11.02.130(see page 1761)
- Security Fixes 11.02.130(see page 1761)
- Known Issues 11.02.130(see page 1764)
- Resolved Issues 11.02.130(see page 1766)



### 7.13.1 Supported Devices 11.02.130

#### **IGEL devices:**

|         |                              |
|---------|------------------------------|
| UD2-LX: | UD2-LX 50<br>UD2-LX 40       |
| UD3-LX: | UD3-LX 51<br>UD3-LX 50       |
| UD5-LX: | UD5-LX 50                    |
| UD6-LX: | UD6-LX 51                    |
| UD7-LX: | UD7-LX 10                    |
| UD9-LX: | UD9-LX Touch 41<br>UD9-LX 40 |

For supported IGEL OS 11 third-party devices, see [Devices Supported by IGEL OS 11](#)<sup>434</sup>.

### 7.13.2 Component Versions 11.02.130

- **Clients**

| Product                          | Version                         |
|----------------------------------|---------------------------------|
| Citrix HDX Realtime Media Engine | 2.8.0-2235                      |
| Citrix Receiver                  | 13.10.0.20                      |
| Citrix Receiver                  | 13.5.0.10185126                 |
| Citrix Workspace App             | 19.6.0.60                       |
| deviceTRUST Citrix Channel       | 19.1.200.2                      |
| Ericom PowerTerm                 | 12.0.1.0.20170219.2-_dev_-34574 |

<sup>434</sup> <https://kb.igel.com/os11-supported-hardware>



|                                        |                                           |
|----------------------------------------|-------------------------------------------|
| Ericom PowerTerm                       | 12.5_x64_20190619_12.5.1.40008            |
| Evidian AuthMgr                        | 1.5.7116                                  |
| Evince PDF Viewer                      | 3.18.2-1ubuntu4.6                         |
| FabulaTech USB for Remote Desktop      | 5.2.29                                    |
| Firefox                                | 60.8.0                                    |
| IBM iAccess Client Solutions           | 1.1.8.1                                   |
| IGEL RDP Client                        | 2.2                                       |
| Imprivata OneSign ProveID Embedded     | onesign-bootstrap-loader_1.0.523630_amd64 |
| deviceTRUST RDP Channel                | 19.1.200.2                                |
| NCP Secure Enterprise Client           | 5.10_rev40552                             |
| NX Client                              | 6.7.6                                     |
| Open VPN                               | 2.3.10-1ubuntu2.2                         |
| Zulu JRE                               | 8.40.0.25                                 |
| Parallels Client (64 bit)              | 17.0.21282                                |
| Spice GTK (Red Hat Virtualization)     | 0.36-1~git20190601igel61                  |
| Remote Viewer (Red Hat Virtualization) | 8.0-1igel49                               |
| Usbredir (Red Hat Virtualization)      | 0.8.0-1igel49                             |
| Teradici PCoIP Software Client         | 19.05.5-18.04                             |
| ThinLinc Client                        | 4.10.0-6068                               |
| ThinPrint Client                       | 7.5.88                                    |
| Totem Media Player                     | 2.30.2                                    |
| Parole Media Player                    | 1.0.1-0ubuntu1igel18                      |
| VNC Viewer                             | 1.9.0+dfsg-3igel8                         |
| VMware Horizon Client                  | 5.0.0-12557422                            |
| Voip Client Ekiga                      | 4.0.1                                     |

- **Dictation**



|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20180621 |
| Philips Speech driver                     | 12.7.11  |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.8    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.3.2    |

- **Smartcard**

|                                           |              |
|-------------------------------------------|--------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101      |
| PKCS#11 Library Athena IDProtect          | 623.07       |
| PKCS#11 Library cryptovision sc/interface | 7.1.20       |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0    |
| PKCS#11 Library SecMaker NetID            | 6.7.2.36     |
| PKCS#11 Library 90meter                   | 20190522     |
| Reader Driver ACS CCID                    | 1.1.6-1igel1 |
| Reader Driver Gemalto eToken              | 10.0.37-0    |
| Reader Driver HID Global Omnikey          | 4.3.3        |
| Reader Driver Identive CCID               | 5.0.35       |
| Reader Driver Identive eHealth200         | 1.0.5        |
| Reader Driver Identive SCRKBC             | 5.0.24       |



|                                    |                        |
|------------------------------------|------------------------|
| Reader Driver MUSCLE CCID          | 1.4.30-1igel3          |
| Reader Driver REINER SCT cyberJack | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite        | 1.8.23-1igel1          |
| Cherry USB2LAN Proxy               | 3.2.0.3                |

- **System Components**

|                                         |                              |
|-----------------------------------------|------------------------------|
| OpenSSL                                 | 1.0.2g-1ubuntu4.15           |
| OpenSSH Client                          | 7.2p2-4ubuntu2.8             |
| OpenSSH Server                          | 7.2p2-4ubuntu2.8             |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5           |
| MESA OpenGL stack                       | 19.0.8-1igel73               |
| VAAPI ABI Version                       | 0.40                         |
| VDPAU Library version                   | 1.1.1-3ubuntu1               |
| Graphics Driver INTEL                   | 2.99.917+git20190724-igel907 |
| Graphics Driver ATI/Radeon              | 19.0.1-2igel890              |
| Graphics Driver ATI/AMDGPU              | 19.0.1-4igel894              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867              |
| Graphics Driver Nvidia                  | 418.56-0ubuntu1              |
| Graphics Driver Vboxvideo               | 1.0.0-igel798                |
| Graphics Driver VMware                  | 13.3.0-2igel857              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1igel775         |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |
| Graphics Driver VESA                    | 2.4.0-1igel855               |
| Input Driver Evdev                      | 2.10.6-1igel888              |
| Input Driver Elographics                | 1.4.1-1build5igel633         |
| Input Driver eGalax                     | 2.5.5814                     |
| Input Driver Synaptics                  | 1.9.1-1ubuntu1igel866        |



|                                 |                               |
|---------------------------------|-------------------------------|
| Input Driver VMMouse            | 13.1.0-1ubuntu2igel635        |
| Input Driver Wacom              | 0.36.1-0ubuntu2igel888        |
| Kernel                          | 4.19.65 #mainline-lxos-r2782  |
| Xorg X11 Server                 | 1.19.6-1ubuntu4.3igel910      |
| Xorg Xephyr                     | 1.19.6-1ubuntu4.3igel910      |
| CUPS printing daemon            | 2.1.3-4ubuntu0.9igel27        |
| PrinterLogic                    | 18.2.1.128                    |
| Lightdm Graphical Login Manager | 1.18.3-0ubuntu1.1             |
| XFCE4 Window Manager            | 4.12.3-1ubuntu2igel675        |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7       |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.3igel74  |
| ModemManager                    | 1.10.0-1~ubuntu18.04.2igel3   |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.2            |
| GStreamer 1.x                   | 1.16.0-1igel214               |
| WebKit2Gtk                      | 2.24.2-0ubuntu0.19.04.1igel18 |
| Python2                         | 2.7.12                        |
| Python3                         | 3.5.2                         |

- **Features with Limited IGEL Support**

|                                    |                                  |
|------------------------------------|----------------------------------|
| Mobile Device Access USB (MTP)     | 1.1.16-2igel1                    |
| Mobile Device Access USB (imobile) | 1.2.1~git20181030.92c5462-1igel5 |
| Mobile Device Access USB (gphoto)  | 2.5.22-3igel1                    |
| VPN OpenConnect                    | 7.08-1                           |
| Scanner support / Sane             | 1.0.27-1                         |
| VirtualBox                         | 6.0.10-dfsg-4igel31              |

- **Features with Limited Functionality**

|                   |        |
|-------------------|--------|
| Cisco JVDI Client | 12.1.0 |
|-------------------|--------|



### 7.13.3 General Information 11.02.130

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver.

### 7.13.4 Security Fixes 11.02.130

#### Firefox

- Updated **Firefox** browser to version **60.8.0 ESR**.

- Fixes for **mfsa2019-22**, also known as:

[More...](#)

CVE-2019-9811, CVE-2019-11711, CVE-2019-11712, CVE-2019-11713, CVE-2019-11729, CVE-2019-11715, CVE-2019-11717, CVE-2019-11719, CVE-2019-11730, and CVE-2019-11709.

- Fixes for **mfsa2019-19**, also known as: CVE-2019-11708.

- Fixes for **mfsa2019-18**, also known as: CVE-2019-11707.

- Fixes for **mfsa2019-08**, also known as:

[More...](#)

CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2018-18506, and CVE-2019-9788.

- Fixes for **mfsa2019-05**, also known as: CVE-2018-18356, CVE-2019-5785.

- Fixes for **mfsa2019-02**, also known as: CVE-2018-18500, CVE-2018-18505, and CVE-2018-18501.

- Added allowance for Firefox to access **Yubikey (FIDO/U2F)** if apparmor is active.

#### Base system

- Set default **umask to 0077** for all non-root users.

- Remote users home is now **/home/ruser**.

- Fixed **policykit-1** security issue CVE-2019-6133.

- Fixed **tiff** security issues:

[More...](#)

CVE-2019-7663, CVE-2019-6128, CVE-2018-19210, CVE-2018-17000, CVE-2018-12900, and CVE-2018-10779.



- Fixed **lcms2** security issue CVE-2018-16435.
- Fixed **libpng1.6** security issues CVE-2019-7317 and CVE-2018-13785.
- Fixed **nss** security issues CVE-2018-18508, CVE-2019-11729, and CVE-2019-11719.
- Fixed **procps** security issues:  
[More...](#)

CVE-2018-1126, CVE-2018-1125, CVE-2018-1124,  
CVE-2018-1123 and CVE-2018-1122.

- Fixed **evince** security issues CVE-2019-11459 and CVE-2019-1010006.
- Fixed **gdk-pixbuf** security issue CVE-2017-12447.
- Fixed **gst-plugins-base0.10** security issue CVE-2019-9928.
- Fixed **bind9** security issues CVE-2019-6465, CVE-2018-5745 and CVE-2018-5743.
- Fixed **libgd2** security issues CVE-2019-6978 and CVE-2019-6977.
- Fixed **ghostscript** security issues CVE-2019-3839, CVE-2019-3838 and CVE-2019-3835.
- Fixed **ldb** security issue CVE-2019-3824.
- Fixed **file** security issues CVE-2019-8907 and CVE-2019-8905.
- Fixed **poppler** security issues:  
[More...](#)

CVE-2019-9200, CVE-2019-9903, CVE-2019-9631, CVE-2019-12293,  
CVE-2019-10872, CVE-2019-10023, CVE-2019-10021, CVE-2019-10019,  
CVE-2019-10018, CVE-2018-20662, CVE-2018-18897, and CVE-2017-9865.

- Fixed **samba** security issues CVE-2019-3880 and CVE-2018-16860.
- Fixed **openssl** security issue CVE-2019-1559.
- Fixed **libxslt** security issue CVE-2019-11068.
- Fixed **openssh** security issue CVE-2019-6111.
- Fixed **wget** security issue CVE-2019-5953.
- Fixed **wpa** security issues:  
[More...](#)

CVE-2019-9495, CVE-2019-9497, CVE-2019-9498,  
CVE-2019-9499, and CVE-2019-11555.

- Fixed **gtk+2.0** security issue CVE-2013-7447.
- Fixed **heimdal** security issues CVE-2019-12098 and CVE-2018-16860.
- Fixed **webkit2gtk** security issues CVE-2019-8615, CVE-2019-8607, and CVE-2019-8595.
- Fixed **gimp** security issues:  
[More...](#)

CVE-2017-17786, CVE-2017-17789, CVE-2017-17784,  
CVE-2017-17787, CVE-2017-17785, and CVE-2017-17788.

- Fixed **libtomcrypt** security issue CVE-2018-12437.
- Fixed **unzip** security issues CVE-2019-13232, CVE-2018-1000035, CVE-2016-9844, and  
CVE-2014-9913.
- Fixed **curl** security issues:  
[More...](#)

CVE-2018-16840, CVE-2018-16839, CVE-2019-3823,  
CVE-2019-3822, CVE-2018-16890, and CVE-2019-5346.



- Fixed **gnutls28** security issues CVE-2018-10846, CVE-2018-10845, CVE-2018-10844, and CVE-2018-1084.
- Fixed **db5.3** security issue CVE-2019-8457.
- Fixed **qtbase-opensource-src** security issues CVE-2018-19873, CVE-2018-19870, and CVE-2018-15518.
- Fixed **libssh2** security issues:  
[More...](#)

CVE-2019-3863, CVE-2019-3862, CVE-2019-3861, CVE-2019-3860, CVE-2019-3859, CVE-2019-3858, CVE-2019-3857, CVE-2019-3856, and CVE-2019-3855.
- Fixed **network-manager** security issue CVE-2018-15688.
- Fixed **elfutils** security issues:  
[More...](#)

CVE-2019-7665, CVE-2019-7150, CVE-2019-7149, CVE-2018-18521, CVE-2018-18520, CVE-2018-18310, CVE-2018-16403, CVE-2018-16402, and CVE-2018-16062.
- Fixed **libsndfile** security issues:  
[More...](#)

CVE-2019-3832, CVE-2018-19758, CVE-2018-19662, CVE-2018-19661, CVE-2018-19432, CVE-2018-13139, CVE-2017-6892, CVE-2017-17457, CVE-2017-17456, CVE-2017-16942, CVE-2017-14634, CVE-2017-14246, and CVE-2017-14245.
- Fixed **dbus** security issue CVE-2019-12749.
- Fixed **vim** security issues CVE-2019-12735 and CVE-2017-5953.
- Fixed **glib2.0** security issue CVE-2019-12450.
- Fixed **openssl (1.1.x)** security issues:  
[More...](#)

CVE-2019-1543, CVE-2018-0737, CVE-2018-0735, CVE-2018-0734, and CVE-2018-0732.
- Fixed **sqlite3** security issues:  
[More...](#)

CVE-2019-9937, CVE-2019-9936, CVE-2019-8457, CVE-2018-20506, CVE-2018-20346, CVE-2017-2520, CVE-2017-2519, CVE-2017-2518, CVE-2017-13685, CVE-2017-10989, and CVE-2016-6153.
- Fixed **systemd** security issues:  
[More...](#)

CVE-2019-6454, CVE-2019-6454, CVE-2018-1049, CVE-2018-15686, and CVE-2019-3842.
- Fixed **libseccomp** security issue CVE-2019-9893.
- Fixed **bzip2** security issues CVE-2019-12900 and CVE-2016-3189.
- Fixed **imagemagick** security issues:  
[More...](#)



CVE-2019-9956, CVE-2019-7398, CVE-2019-7397, CVE-2019-7396, CVE-2019-7175, CVE-2019-11598, CVE-2019-11597, CVE-2019-11472, CVE-2019-11470, CVE-2019-10650, CVE-2019-10131, CVE-2018-20467, CVE-2018-18025, CVE-2018-18024, CVE-2018-18016, CVE-2018-17966, CVE-2018-17965, CVE-2018-16413, CVE-2018-16412, CVE-2017-12806, and CVE-2017-12805.

- Fixed **expat** security issue CVE-2018-20843.
- Fixed **glib2.0** security issue CVE-2019-13012.
- Fixed **libvirt** security issues CVE-2019-10167 and CVE-2019-10161.
- Fixed **gvfs** security issue CVE-2019-12795.
- Fixed **libmspack** security issue CVE-2019-1010305.
- Fixed **bash** security issue CVE-2019-9924.
- Fixed **openldap** security issues CVE-2019-13565 and CVE-2019-13057.
- Updated **libwebkit2gtk-4.0-37** to version **2.24.2**.

Security fixes:

[More...](#)

CVE-2019-8595, CVE-2019-8607, CVE-2019-8615, CVE-2019-6251, CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378, CVE-2018-4382, CVE-2018-4392, CVE-2018-4416, CVE-2018-4345, CVE-2018-4386, and CVE-2018-4372.

- Fixed a vulnerability in the **custom environment variable framework**.
- Fixed possible malicious **owner change within TC setup configuration**.
- Fixed **kernel TCP** vulnerabilities CVE-2019-11477: **SACK Panic**, CVE-2019-11478: **SACK Slowness**, and CVE-2019-11479: **Excess resource consumption due to low MSS values**.
- Changed minimally allowed **MSS size** to **1000** to prevent possible Denial of Service attacks.
- Fixed a vulnerability in **Java configuration script**.

### 7.13.5 Known Issues 11.02.130

#### Citrix

- With activated DRI3 and AMD GPU, Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H264, MPEG1 and MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.  
As a workaround, insert the smartcard before starting StoreFront login.
- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" > "For the entire screen".
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264 acceleration plugin**, the following registry key must be enabled:



### More...

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Value     | enabled / <u>disabled</u>                                        |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

### VMware Horizon

- **Sound redirection in PCoIP** is broken when the so-called lightweight-client is used, which has become the new default.  
Sound redirection can still be used by choosing the rollback-client instead. This can be done by setting the IGEL Registry key:

### More...

|           |                                         |
|-----------|-----------------------------------------|
| Parameter | Allow rollback to former client variant |
| Registry  | vmware.view.allow-client-rollback       |
| Value     | enabled / <u>disabled</u>               |

- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off.  
In the IGEL Setup client, **drive mapping** can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping**.  
It is also recommended to disable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection entirely** or at least to **deny storage devices** by adding a filter to the USB class rules.  
Furthermore, Horizon Client relies on the OS to mount the storage device itself. Enable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.

- **External drives** mounted already before connection **do not appear in the remote desktop**.  
Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.

### WiFi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.  
Workaround: Disable system suspend under **IGEL Setup > System > Power Options > Shutdown**.

### Parallels Client

- **Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** once with disabled FIPS support.

### Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign smartcards**.

### Appliance Mode



- Appliance mode **RHEV/Spice**: spice-xpi firefox plugin is no longer supported. The "Console Invocation" has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

#### Multimedia

- Multimedia **redirection with GStreamer** could fail with the **Nouveau GPU driver**.

#### Audio

- IGEL **UD2 (D220)** fails to restore the **volume level of the speaker** when the device used firmware version **11.01.110** before.

### 7.13.6 Resolved Issues 11.02.130

#### Base system

- Fixed **ActiveDirectory/Kerberos password change** with "Change Password" accessory for users who are members of many (~300+) AD groups.
- Fixed **IGEL license retrieval** via FTP protocol in IGEL Setup Assistant and integrated license browser.

#### Remote Management

- Fixed **automatic registering in the UMS** using DNS entry or DHCP tag.

### 7.14 Notes for Release 11.02.100

|                       |            |              |
|-----------------------|------------|--------------|
| <b>Software:</b>      | Version    | 11.02.100    |
| <b>Release Date:</b>  | 2019-08-14 |              |
| <b>Release Notes:</b> | Version    | RN-1102100-1 |
| <b>Last update:</b>   | 2019-08-14 |              |

- 
- [IGEL OS 11](#)(see page 1766)
  - [IGEL OS Creator \(OSC\)](#)(see page 1814)

### 7.14.1 IGEL OS 11

- [Supported Devices 11.02.100](#)(see page 1767)
- [Component Versions 11.02.100](#)(see page 1767)
- [General Information 11.02.100](#)(see page 1772)
- [Security Fixes 11.02.100](#)(see page 1772)
- [Known Issues 11.02.100](#)(see page 1775)
- [New Features 11.02.100](#)(see page 1777)



- Resolved Issues 11.02.100(see page 1801)
- CA Certificates Contained in IGEL OS 11.02.100(see page 1811)

## Supported Devices 11.02.100

|         |                              |
|---------|------------------------------|
| UD2-LX: | UD2-LX 40<br>UD2-LX 50       |
| UD3-LX: | UD3-LX 51<br>UD3-LX 50       |
| UD5-LX: | UD5-LX 50                    |
| UD6-LX: | UD6-LX 51                    |
| UD7-LX: | UD7-LX 10                    |
| UD9-LX: | UD9-LX Touch 41<br>UD9-LX 40 |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>435</sup>.

## Component Versions 11.02.100

- **Clients**

| Product                          | Version                         |
|----------------------------------|---------------------------------|
| Citrix HDX Realtime Media Engine | 2.8.0-2235                      |
| Citrix Receiver                  | 13.10.0.20                      |
| Citrix Receiver                  | 13.5.0.10185126                 |
| Citrix Workspace App             | 19.6.0.60                       |
| deviceTRUST Citrix Channel       | 19.1.200.2                      |
| Ericom PowerTerm                 | 12.0.1.0.20170219.2-_dev_-34574 |
| Ericom PowerTerm                 | 12.5_x64_20190619_12.5.1.40008  |

<sup>435</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



|                                        |                                           |
|----------------------------------------|-------------------------------------------|
| Evidian AuthMgr                        | 1.5.7116                                  |
| Evince PDF Viewer                      | 3.18.2-1ubuntu4.6                         |
| FabulaTech USB for Remote Desktop      | 5.2.29                                    |
| Firefox                                | 60.8.0                                    |
| IBM iAccess Client Solutions           | 1.1.8.1                                   |
| IGEL RDP Client                        | 2.2                                       |
| Imprivata OneSign ProveID Embedded     | onesign-bootstrap-loader_1.0.523630_amd64 |
| deviceTRUST RDP Channel                | 19.1.200.2                                |
| NCP Secure Enterprise Client           | 5.10_rev40552                             |
| NX Client                              | 6.7.6                                     |
| Open VPN                               | 2.3.10-1ubuntu2.2                         |
| Zulu JRE                               | 8.40.0.25                                 |
| Parallels Client (64 bit)              | 17.0.21282                                |
| Spice GTK (Red Hat Virtualization)     | 0.36-1~git20190601igel61                  |
| Remote Viewer (Red Hat Virtualization) | 8.0-1igel49                               |
| Usbredir (Red Hat Virtualization)      | 0.8.0-1igel49                             |
| Teradici PCoIP Software Client         | 19.05.5-18.04                             |
| ThinLinc Client                        | 4.10.0-6068                               |
| ThinPrint Client                       | 7.5.88                                    |
| Totem Media Player                     | 2.30.2                                    |
| Parole Media Player                    | 1.0.1-0ubuntu1igel18                      |
| VNC Viewer                             | 1.9.0+dfsg-3igel8                         |
| VMware Horizon Client                  | 5.0.0-12557422                            |
| Voip Client Ekiga                      | 4.0.1                                     |

- **Dictation**



|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20180621 |
| Philips Speech driver                     | 12.7.11  |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.8    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.3.2    |

- **Smartcard**

|                                           |              |
|-------------------------------------------|--------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101      |
| PKCS#11 Library Athena IDProtect          | 623.07       |
| PKCS#11 Library cryptovision sc/interface | 7.1.20       |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0    |
| PKCS#11 Library SecMaker NetID            | 6.7.2.36     |
| PKCS#11 Library 90meter                   | 20190522     |
| Reader Driver ACS CCID                    | 1.1.6-1igel1 |
| Reader Driver Gemalto eToken              | 10.0.37-0    |
| Reader Driver HID Global Omnikey          | 4.3.3        |
| Reader Driver Identive CCID               | 5.0.35       |
| Reader Driver Identive eHealth200         | 1.0.5        |
| Reader Driver Identive SCRKBC             | 5.0.24       |



|                                    |                        |
|------------------------------------|------------------------|
| Reader Driver MUSCLE CCID          | 1.4.30-1igel3          |
| Reader Driver REINER SCT cyberJack | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite        | 1.8.23-1igel1          |
| Cherry USB2LAN Proxy               | 3.2.0.3                |

- **System Components**

|                                         |                              |
|-----------------------------------------|------------------------------|
| OpenSSL                                 | 1.0.2g-1ubuntu4.15           |
| OpenSSH Client                          | 7.2p2-4ubuntu2.8             |
| OpenSSH Server                          | 7.2p2-4ubuntu2.8             |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5           |
| MESA OpenGL stack                       | 19.0.8-1igel73               |
| VAAPI ABI Version                       | 0.40                         |
| VDPAU Library version                   | 1.1.1-3ubuntu1               |
| Graphics Driver INTEL                   | 2.99.917+git20190724-igel907 |
| Graphics Driver ATI/Radeon              | 19.0.1-2igel890              |
| Graphics Driver ATI/AMDGPU              | 19.0.1-4igel894              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867              |
| Graphics Driver Nvidia                  | 418.56-0ubuntu1              |
| Graphics Driver Vboxvideo               | 1.0.0-igel798                |
| Graphics Driver VMware                  | 13.3.0-2igel857              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1igel775         |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |
| Graphics Driver VESA                    | 2.4.0-1igel855               |
| Input Driver Evdev                      | 2.10.6-1igel888              |
| Input Driver Elographics                | 1.4.1-1build5igel633         |
| Input Driver eGalax                     | 2.5.5814                     |
| Input Driver Synaptics                  | 1.9.1-1ubuntu1igel866        |



|                                 |                               |
|---------------------------------|-------------------------------|
| Input Driver VMMouse            | 13.1.0-1ubuntu2igel635        |
| Input Driver Wacom              | 0.36.1-0ubuntu2igel888        |
| Kernel                          | 4.19.65 #mainline-lxos-r2782  |
| Xorg X11 Server                 | 1.19.6-1ubuntu4.3igel910      |
| Xorg Xephyr                     | 1.19.6-1ubuntu4.3igel910      |
| CUPS printing daemon            | 2.1.3-4ubuntu0.9igel27        |
| PrinterLogic                    | 18.2.1.128                    |
| Lightdm Graphical Login Manager | 1.18.3-0ubuntu1.1             |
| XFCE4 Window Manager            | 4.12.3-1ubuntu2igel675        |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7       |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.3igel74  |
| ModemManager                    | 1.10.0-1~ubuntu18.04.2igel3   |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.2            |
| GStreamer 1.x                   | 1.16.0-1igel214               |
| WebKit2Gtk                      | 2.24.2-0ubuntu0.19.04.1igel18 |
| Python2                         | 2.7.12                        |
| Python3                         | 3.5.2                         |

- **Features with Limited IGEL Support**

|                                    |                                  |
|------------------------------------|----------------------------------|
| Mobile Device Access USB (MTP)     | 1.1.16-2igel1                    |
| Mobile Device Access USB (imobile) | 1.2.1~git20181030.92c5462-1igel5 |
| Mobile Device Access USB (gphoto)  | 2.5.22-3igel1                    |
| VPN OpenConnect                    | 7.08-1                           |
| Scanner support / Sane             | 1.0.27-1                         |
| VirtualBox                         | 6.0.10-dfsg-4igel31              |

- **Features with Limited Functionality**

|                   |        |
|-------------------|--------|
| Cisco JVDI Client | 12.1.0 |
|-------------------|--------|



## General Information 11.02.100

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver.

## Security Fixes 11.02.100

### Firefox

- Updated **Firefox** browser to version **60.8.0 ESR**.
- Fixes for **mfsa2019-22**, also known as:

[More...](#)

CVE-2019-9811, CVE-2019-11711, CVE-2019-11712, CVE-2019-11713, CVE-2019-11729, CVE-2019-11715, CVE-2019-11717, CVE-2019-11719, CVE-2019-11730, and CVE-2019-11709.

- Fixes for **mfsa2019-19**, also known as: CVE-2019-11708.
- Fixes for **mfsa2019-18**, also known as: CVE-2019-11707.
- Fixes for **mfsa2019-08**, also known as:

[More...](#)

CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2018-18506, and CVE-2019-9788.

- Fixes for **mfsa2019-05**, also known as: CVE-2018-18356, CVE-2019-5785.
- Fixes for **mfsa2019-02**, also known as: CVE-2018-18500, CVE-2018-18505, and CVE-2018-18501.
- Added allowance for Firefox to access **Yubikey (FIDO/U2F)** if apparmor is active.

### Base system

- Set default **umask to 0077** for all non-root users.
- Remote users home is now **/home/ruser**.
- Fixed **policykit-1** security issue CVE-2019-6133.
- Fixed **tiff** security issues:  
[More...](#)



CVE-2019-7663, CVE-2019-6128, CVE-2018-19210, CVE-2018-17000, CVE-2018-12900, and CVE-2018-10779.

- Fixed **lcms2** security issue CVE-2018-16435.
- Fixed **libpng1.6** security issues CVE-2019-7317 and CVE-2018-13785.
- Fixed **nss** security issues CVE-2018-18508, CVE-2019-11729, and CVE-2019-11719.
- Fixed **procps** security issues:  
[More...](#)

CVE-2018-1126, CVE-2018-1125, CVE-2018-1124, CVE-2018-1123 and CVE-2018-1122.

- Fixed **evince** security issues CVE-2019-11459 and CVE-2019-1010006.
- Fixed **gdk-pixbuf** security issue CVE-2017-12447.
- Fixed **gst-plugins-base0.10** security issue CVE-2019-9928.
- Fixed **bind9** security issues CVE-2019-6465, CVE-2018-5745 and CVE-2018-5743.
- Fixed **libgd2** security issues CVE-2019-6978 and CVE-2019-6977.
- Fixed **ghostscript** security issues CVE-2019-3839, CVE-2019-3838 and CVE-2019-3835.
- Fixed **ldb** security issue CVE-2019-3824.
- Fixed **file** security issues CVE-2019-8907 and CVE-2019-8905.
- Fixed **poppler** security issues:  
[More...](#)

CVE-2019-9200, CVE-2019-9903, CVE-2019-9631, CVE-2019-12293, CVE-2019-10872, CVE-2019-10023, CVE-2019-10021, CVE-2019-10019, CVE-2019-10018, CVE-2018-20662, CVE-2018-18897, and CVE-2017-9865.

- Fixed **samba** security issues CVE-2019-3880 and CVE-2018-16860.
- Fixed **openssl** security issue CVE-2019-1559.
- Fixed **libxslt** security issue CVE-2019-11068.
- Fixed **openssh** security issue CVE-2019-6111.
- Fixed **wget** security issue CVE-2019-5953.
- Fixed **wpa** security issues:  
[More...](#)

CVE-2019-9495, CVE-2019-9497, CVE-2019-9498, CVE-2019-9499, and CVE-2019-11555.

- Fixed **gtk+2.0** security issue CVE-2013-7447.
- Fixed **heimdal** security issues CVE-2019-12098 and CVE-2018-16860.
- Fixed **webkit2gtk** security issues CVE-2019-8615, CVE-2019-8607, and CVE-2019-8595.
- Fixed **gimp** security issues:  
[More...](#)

CVE-2017-17786, CVE-2017-17789, CVE-2017-17784, CVE-2017-17787, CVE-2017-17785, and CVE-2017-17788.

- Fixed **libtomcrypt** security issue CVE-2018-12437.
- Fixed **unzip** security issues CVE-2019-13232, CVE-2018-1000035, CVE-2016-9844, and CVE-2014-9913.
- Fixed **curl** security issues:  
[More...](#)



CVE-2018-16840, CVE-2018-16839, CVE-2019-3823,  
CVE-2019-3822, CVE-2018-16890, and CVE-2019-5346.

- Fixed **gnutls28** security issues CVE-2018-10846, CVE-2018-10845, CVE-2018-10844, and  
CVE-2018-1084.
- Fixed **db5.3** security issue CVE-2019-8457.
- Fixed **qtbase-opensource-src** security issues CVE-2018-19873, CVE-2018-19870, and  
CVE-2018-15518.
- Fixed **libssh2** security issues:  
**More...**

CVE-2019-3863, CVE-2019-3862, CVE-2019-3861,  
CVE-2019-3860, CVE-2019-3859, CVE-2019-3858,  
CVE-2019-3857, CVE-2019-3856, and CVE-2019-3855.
- Fixed **network-manager** security issue CVE-2018-15688.
- Fixed **elfutils** security issues:  
**More...**

CVE-2019-7665, CVE-2019-7150, CVE-2019-7149,  
CVE-2018-18521, CVE-2018-18520, CVE-2018-18310,  
CVE-2018-16403, CVE-2018-16402, and CVE-2018-16062.
- Fixed **libsndfile** security issues:  
**More...**

CVE-2019-3832, CVE-2018-19758, CVE-2018-19662, CVE-2018-19661,  
CVE-2018-19432, CVE-2018-13139, CVE-2017-6892, CVE-2017-17457,  
CVE-2017-17456, CVE-2017-16942, CVE-2017-14634, CVE-2017-14246,  
and CVE-2017-14245.
- Fixed **dbus** security issue CVE-2019-12749.
- Fixed **vim** security issues CVE-2019-12735 and CVE-2017-5953.
- Fixed **glib2.0** security issue CVE-2019-12450.
- Fixed **openssl (1.1.x)** security issues:  
**More...**

CVE-2019-1543, CVE-2018-0737, CVE-2018-0735,  
CVE-2018-0734, and CVE-2018-0732.
- Fixed **sqlite3** security issues:  
**More...**

CVE-2019-9937, CVE-2019-9936, CVE-2019-8457, CVE-2018-20506,  
CVE-2018-20346, CVE-2017-2520, CVE-2017-2519, CVE-2017-2518,  
CVE-2017-13685, CVE-2017-10989, and CVE-2016-6153.
- Fixed **systemd** security issues:  
**More...**

CVE-2019-6454, CVE-2019-6454, CVE-2018-1049,  
CVE-2018-15686, and CVE-2019-3842.
- Fixed **libseccomp** security issue CVE-2019-9893.
- Fixed **bzip2** security issues CVE-2019-12900 and CVE-2016-3189.



- Fixed **imagemagick** security issues:

[More...](#)

CVE-2019-9956, CVE-2019-7398, CVE-2019-7397, CVE-2019-7396, CVE-2019-7175, CVE-2019-11598, CVE-2019-11597, CVE-2019-11472, CVE-2019-11470, CVE-2019-10650, CVE-2019-10131, CVE-2018-20467, CVE-2018-18025, CVE-2018-18024, CVE-2018-18016, CVE-2018-17966, CVE-2018-17965, CVE-2018-16413, CVE-2018-16412, CVE-2017-12806, and CVE-2017-12805.

- Fixed **expat** security issue CVE-2018-20843.
- Fixed **glib2.0** security issue CVE-2019-13012.
- Fixed **libvirt** security issues CVE-2019-10167 and CVE-2019-10161.
- Fixed **gvfs** security issue CVE-2019-12795.
- Fixed **libmspack** security issue CVE-2019-1010305.
- Fixed **bash** security issue CVE-2019-9924.
- Fixed **openldap** security issues CVE-2019-13565 and CVE-2019-13057.
- Updated **libwebkit2gtk-4.0-37** to version **2.24.2**.

Security fixes:

[More...](#)

CVE-2019-8595, CVE-2019-8607, CVE-2019-8615, CVE-2019-6251, CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378, CVE-2018-4382, CVE-2018-4392, CVE-2018-4416, CVE-2018-4345, CVE-2018-4386, and CVE-2018-4372.

- Fixed a vulnerability in the **custom environment variable framework**.
- Fixed possible malicious **owner change within TC setup configuration**.
- Fixed **kernel TCP** vulnerabilities CVE-2019-11477: **SACK Panic**, CVE-2019-11478: **SACK Slowness**, and CVE-2019-11479: **Excess resource consumption due to low MSS values**.
- Changed minimally allowed **MSS size** to **1000** to prevent possible Denial of Service attacks.
- Fixed a vulnerability in **Java configuration script**.

## Known Issues 11.02.100

### Citrix

- With activated DRI3 and AMD GPU, Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H264, MPEG1 and MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.  
As a workaround, insert the smartcard before starting StoreFront login.
- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" > "For the entire screen".



- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264 acceleration plugin**, the following registry key must be enabled:

[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Range     | enabled / <u>disabled</u>                                        |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

#### VMware Horizon

- Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off. In the IGEL Setup client, **drive mapping** can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping**. It is also recommended to disable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection entirely** or at least to **deny storage devices** by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage device itself. Enable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.
- External drives** mounted already before connection **do not appear in the remote desktop**. Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.

#### WiFi

- TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume. Workaround: Disable system suspend under **IGEL Setup > System > Power Options > Shutdown**.

#### Parallels Client

- Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** once with disabled FIPS support.

#### Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice**: spice-xpi firefox plugin is no longer supported. The "Console Invocation" has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

#### Multimedia

- Multimedia **redirection with GStreamer** could fail with the **Nouveau GPU driver**.



## Audio

- IGEL **UD2 (D220)** fails to restore the **volume level of the speaker** when the device used firmware version **11.01.110** before.

## New Features 11.02.100

## Citrix

- Integrated **Citrix Workspace app 19.06**.

Available Citrix Workspace apps in this release: 19.06, 13.10 and 13.5.

- Added a new registry key to support **1536-bit RSA keys** for client authentication. Factory default for this release is "true".

**More...**

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Enables RSA 1536 cipher suite         |
| Registry  | ica.allregions.enable_rsa_1536        |
| Range     | <u>factory default</u> / false / true |

- Added a new **registry key** to enable **different cipher suites** for client authentication. Factory default for this release is "ALL".

**More...**

|           |                                                   |
|-----------|---------------------------------------------------|
| Parameter | Enables different cipher suite                    |
| Registry  | ica.allregions.sslciphers                         |
| Range     | <u>factory default</u> / ALL / GOV / COM          |
|           | > TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – GOV/ALL |
|           | > TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – GOV/ALL |
|           | > TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA – COM/ALL    |

- Added a new **registry key** to support **keyboard layout synchronization**.

**More...**

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Keyboard layout synchronization               |
| Registry  | ica.modules.virtualdriver.keyboardsync.enable |
| Value     | <u>false</u> / true                           |

- Updated **Citrix HDX RTME** used for optimization of Skype for Business to version **2.8.0-2235**.
- Added support for **Citrix Workspace Launcher** functionality as described at <https://support.citrix.com/article/CTX237727>.
- Added **Citrix Farm Selection**, a facility to manually select one of the configured services / farms for StoreFront login.

**More...**

|           |                                    |
|-----------|------------------------------------|
| Parameter | Citrix store selection             |
| Registry  | ica.pnlogin.farm_selection.enabled |
| Value     | <u>off</u> / on                    |

**Info:**

Off: All servers are used in parallel. If switched on, a user has to select the store via a dialog box before entering the login data.

- **Timeout** for the selection dialog:

[More...](#)

|           |                                    |
|-----------|------------------------------------|
| Parameter | Timeout                            |
| Registry  | ica.pnlogin.farm_selection.timeout |
| Value     | <u>0</u> (no timeout) seconds      |

- **Width** of the dialog window:

[More...](#)

|           |                                      |
|-----------|--------------------------------------|
| Parameter | Selection box window width           |
| Registry  | ica.pnlogin.farm_selection.win_width |
| Value     | <u>400</u> pixel                     |

- **Height** of the dialog window:

[More...](#)

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Selection box window height           |
| Registry  | ica.pnlogin.farm_selection.win_height |
| Value     | <u>400</u> pixel                      |

- **Changed the defaults** for following parameters:

[More...](#)

|            |                                                                                                                                                                   |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Window</b>                                                                                                        |
| Parameter  | Multimonitor full-screen mode                                                                                                                                     |
| Registry   | ica.wfclient.usexdgfullscreen<br>ica.wfclient.spanmonitorenable                                                                                                   |
| Range      | [Restrict full-screen session to one monitor]<br>[Expand full-screen session across all monitors]<br>[Expand the session over a self-selected number of monitors] |
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; HDX Multimedia</b>                                                                                                |
| Parameter  | Multimedia redirection                                                                                                                                            |
| Registry   | ica.module.virtualdriver.multimedia.enable                                                                                                                        |
| Value      | <u>enabled</u> / disabled                                                                                                                                         |
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; HDX Multimedia</b>                                                                                                |
|            | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; Skype for Business</b>                                                                |
| Parameter  | HDX Realtime Media Engine                                                                                                                                         |
| Registry   | ica.module.virtualdriver.hdxrtme.enable                                                                                                                           |



|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

- Updated the **Nuance virtual channel** for ICA to version **B301**.

#### RDP/IGEL RDP Client 2

- Added a field '**Collection**' to RDP session server page.  
[More...](#)

**IGEL Setup > Sessions > RDP > RDP Sessions > RDP Session > Server**

**IGEL Setup > Sessions > RDP > RDP Sessions > RDP Session > Options**

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | Collection                                       |
| Registry  | sessions.winconnect<NR>.option.load-balance-info |

#### VMware Horizon

- Added parameters to specify **webcam frame size** and **rate for RTAV**.

[More...](#)

|           |                               |
|-----------|-------------------------------|
| Parameter | Webcam frame width            |
| Registry  | vmware.view.rtav-frame-width  |
| Value     | <u>&lt;empty_string&gt;</u>   |
| Parameter | Webcam frame height           |
| Registry  | vmware.view.rtav-frame-height |
| Value     | <u>&lt;empty_string&gt;</u>   |
| Parameter | Webcam frame rate             |
| Registry  | vmware.view.rtav-frame-rate   |
| Value     | <u>&lt;empty_string&gt;</u>   |

- Updated **Horizon Client** to version **5.0.0-12557422**.
- Added a possibility to easily evaluate **Horizon Blast decoder states**. By default, sessions are evaluated after usage, and the result is written into the journal log. This can also be used with GUI notifications at runtime.
- Added **new USB classes** to **Horizon USB Redirection** class configuration: **Audio (input)**, **Audio (Output)**, **Imaging**, **Video (Input)**.

#### Parallels Client

- Updated **Parallels Client** to version **17.0**.
- Added a possibility to set apps to **autostart on Parallels RAS**.

#### PowerTerm

- Added **Ericom PowerTerm** terminal emulation. This feature requires an **additional license**.  
The following **versions** are available:  
**12.0.1.0\_20170219.2-dev-34574**  
**12.5\_x64\_20190619\_12.5.1.40008**

#### IBM\_525

- Improved startup time** of IBM iAccess Client.



- **Improved configuration** of IBM iAccess Client via **IGEL Setup**.

[More...](#)

|           |                                                                                         |
|-----------|-----------------------------------------------------------------------------------------|
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Connection > Advanced |
| Parameter | Bypass signon                                                                           |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.ssoenabled</code>                              |
| Value     | <code>enabled / <u>disabled</u></code>                                                  |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Font         |
| Parameter | Antialiasing                                                                            |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.textantialiasing</code>                        |
| Value     | <code>enabled / <u>disabled</u></code>                                                  |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor       |
| Parameter | Allow blinking cursor                                                                   |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.blinkcursor</code>                             |
| Value     | <code>enabled / <u>disabled</u></code>                                                  |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor       |
| Parameter | Show blinking text with                                                                 |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.blinkstate</code>                              |
| Value     | <code>[Blinking Text] [Host Color] [Mapped Color]</code>                                |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor       |
| Parameter | Blink Color                                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.blinkcolor_fg</code>                           |
| Value     | <code>#ffc800</code>                                                                    |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor       |
| Parameter | Blink Color Background                                                                  |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.blinkcolor_bg</code>                           |
| Value     | <code>#000000</code>                                                                    |



|           |                                                                                      |
|-----------|--------------------------------------------------------------------------------------|
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Rule Line |
| Parameter | Rule Line                                                                            |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.ruleline</code>                             |
| Value     | <u>enabled</u> / <u>disabled</u>                                                     |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Rule Line |
| Parameter | Follow Cursor                                                                        |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.rulelinefollows</code>                      |
| Value     | <u>enabled</u> / <u>disabled</u>                                                     |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Rule Line |
| Parameter | Style                                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.rulelinestyle</code>                        |
| Value     | <u>[Crosshair]</u> <u>[Vertical]</u> <u>[Horizontal]</u>                             |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color     |
| Parameter | Green                                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fgn_fg</code>                         |
| Value     | <u>#00ff00</u>                                                                       |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color     |
| Parameter | Green Background                                                                     |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fgn_bg</code>                         |
| Value     | <u>#000000</u>                                                                       |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color     |
| Parameter | White                                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fwt_fg</code>                         |
| Value     | <u>#ffffff</u>                                                                       |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color     |
| Parameter | White Background                                                                     |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fwt_bg</code>                         |



|           |                                                                                  |
|-----------|----------------------------------------------------------------------------------|
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Red                                                                              |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_frd_fg</code>                     |
| Value     | <u>#ff0000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Red Background                                                                   |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_frd_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Turquoise                                                                        |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_ftq_fg</code>                     |
| Value     | <u>#00ffff</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Turquoise Background                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_ftq_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Yellow                                                                           |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fyw_fg</code>                     |
| Value     | <u>#ffff00</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Yellow Background                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fyw_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Pink                                                                             |



|           |                                                                                  |
|-----------|----------------------------------------------------------------------------------|
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fpk_fg</code>                     |
| Value     | <u>#ff00ff</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Pink Background                                                                  |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fpk_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Blue                                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fbl_fg</code>                     |
| Value     | <u>#7890f0</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Blue Background                                                                  |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fbl_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Status Indicators                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_osi</code>                        |
| Value     | <u>#7890f0</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Information Indicators                                                           |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_oui</code>                        |
| Value     | <u>#ffffff</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Attention Indicators                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_oai</code>                        |
| Value     | <u>#ffff00</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |



| Parameter      | Error Indicators                                                                            |
|----------------|---------------------------------------------------------------------------------------------|
| Registry Value | <code>sessions.iaccess&lt;NR&gt;.options.color_oei</code><br><code>#ff0000</code>           |
| Setup          | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color            |
| Parameter      | OIA Background                                                                              |
| Registry Value | <code>sessions.iaccess&lt;NR&gt;.options.color_oob</code><br><code>#000000</code>           |
| Setup          | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color            |
| Parameter      | Screen Background                                                                           |
| Registry Value | <code>sessions.iaccess&lt;NR&gt;.options.color_sbg</code><br><code>#000000</code>           |
| Setup          | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color            |
| Parameter      | Highlight active field                                                                      |
| Registry Value | <code>sessions.iaccess&lt;NR&gt;.options.actfieldhilite</code><br><u>enabled / disabled</u> |
| Setup          | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color            |
| Parameter      | Active Field                                                                                |
| Registry Value | <code>sessions.iaccess&lt;NR&gt;.options.color_actf_fg</code><br><code>#000000</code>       |
| Setup          | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color            |
| Parameter      | Active Field Background                                                                     |
| Registry Value | <code>sessions.iaccess&lt;NR&gt;.options.color_actf_bg</code><br><code>#ffff00</code>       |
| Setup          | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color            |
| Parameter      | Crosshair Ruler Color                                                                       |
| Registry Value | <code>sessions.iaccess&lt;NR&gt;.options.color_crc</code><br><code>#00ff00</code>           |



|           |                                                                                              |
|-----------|----------------------------------------------------------------------------------------------|
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color             |
| Parameter | Column Separator                                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_ccs</code>                                    |
| Value     | <code>#ffffff</code>                                                                         |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences                |
| Parameter | Start window maximized                                                                       |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.ismaximized</code>                                  |
| Value     | <u>enabled / disabled</u>                                                                    |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences > Keyboard     |
| Parameter | Keyboard Remapping File                                                                      |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.keyremapfile</code>                                 |
| Value     | <u>IBMi.kmp</u>                                                                              |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences > Popup Keypad |
| Parameter | Popup Keypad File                                                                            |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.poppadfile</code>                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences > Toolbar      |
| Parameter | Toolbar File                                                                                 |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.toolbarfile</code>                                  |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup                                   |
| Parameter | Open new sessions in a new tab                                                               |
| Registry  | <code>ibm.iaccess.acssm.opensessionintab</code>                                              |
| Value     | <u>enabled / disabled</u>                                                                    |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup                                   |
| Parameter | Always display the tab bar                                                                   |
| Registry  | <code>ibm.iaccess.acssm.alwaysshownowtabbar</code>                                           |
| Value     | <u>enabled / disabled</u>                                                                    |



|           |                                                            |
|-----------|------------------------------------------------------------|
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup |
| Parameter | Switch to new tab when created                             |
| Registry  | <code>ibm.iaccess.acssm.switchtonewtab</code>              |
| Value     | <u>enabled</u> / disabled                                  |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup |
| Parameter | Send a warning when closing multiple tabs                  |
| Registry  | <code>ibm.iaccess.acssm.closemultipletabwarning</code>     |
| Value     | <u>enabled</u> / disabled                                  |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup |
| Parameter | Do not start tabbed sessions until the tab is selected     |
| Registry  | <code>ibm.iaccess.acssm.tabdelayedstart</code>             |
| Value     | <u>enabled</u> / <u>disabled</u>                           |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup |
| Parameter | New Tab Action                                             |
| Registry  | <code>ibm.iaccess.acssm.newtabaction</code>                |
| Value     | [Disable and Hide] [Run the Same] [Run Other...]           |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup |
| Parameter | Tab Placement                                              |
| Registry  | <code>ibm.iaccess.acssm.tabplacement</code>                |
| Value     | [Top] [Bottom] [Left] [Right]                              |

## NX client

- Updated **NoMachine Client** to version **6.7.6**.

## ThinLinc

- Updated **Cendio ThinLinc** to version **4.10**.
  - Added support for all of **ThinLinc's login methods: password, public key, smartcard and Kerberos**. Additional parameters can be set when smartcard is chosen.
- [More...](#)

|            |                                                                                       |
|------------|---------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; ThinLinc &gt; ThinLinc Sessions &gt; ThinLinc Session &gt; Login</b> |
| Parameter  | Method of authentication                                                              |



|                      |                                                                                       |
|----------------------|---------------------------------------------------------------------------------------|
| Registry             | sessions.thinlinc%.login.authentication_method                                        |
| Value                | <u>password</u> / publickey / scppublickey / kerberos                                 |
| IGEL Setup Parameter | <b>Sessions &gt; ThinLinc &gt; ThinLinc Sessions &gt; ThinLinc Session &gt; Login</b> |
| Registry             | sessions.thinlinc%.options.user                                                       |
| Value                |                                                                                       |
| IGEL Setup Parameter | <b>Sessions &gt; ThinLinc &gt; ThinLinc Sessions &gt; ThinLinc Session &gt; Login</b> |
| Registry             | sessions.thinlinc%.option.crypt_password                                              |
| Value                |                                                                                       |
| IGEL Setup Parameter | <b>Sessions &gt; ThinLinc &gt; ThinLinc Sessions &gt; ThinLinc Session &gt; Login</b> |
| Registry             | sessions.thinlinc%.login.smartcard_subject_as_name                                    |
| Value                | <u>enabled</u> / disabled                                                             |
| IGEL Setup Parameter | <b>Sessions &gt; ThinLinc &gt; ThinLinc Sessions &gt; ThinLinc Session &gt; Login</b> |
| Registry             | Connect the client automatically when a smartcard is found                            |
| Value                | sessions.thinlinc%.login.smartcard_autoconnect                                        |
| IGEL Setup Parameter | <u>enabled</u> / disabled                                                             |
| IGEL Setup Parameter | <b>Sessions &gt; ThinLinc &gt; ThinLinc Sessions &gt; ThinLinc Session &gt; Login</b> |
| Registry             | Disconnect the client automatically when the smartcard is removed                     |
| Value                | sessions.thinlinc%.login.smartcard_disconnect                                         |
| IGEL Setup Parameter | <u>enabled</u> / disabled                                                             |
| IGEL Setup Parameter | <b>Sessions &gt; ThinLinc &gt; ThinLinc Sessions &gt; ThinLinc Session &gt; Login</b> |
| Registry             | Allow transmission of the smartcard's passphrase for logging in                       |
| Value                | sessions.thinlinc%.login.smartcard_passphrase_sso                                     |
| IGEL Setup Parameter | <u>enabled</u> / <u>disabled</u>                                                      |
| IGEL Setup Parameter | <b>Sessions &gt; ThinLinc &gt; ThinLinc Sessions &gt; ThinLinc Session &gt; Login</b> |
| Registry             | Smartcard filter                                                                      |
| Value                | sessions.thinlinc%.login.smartcard_filter_1                                           |
| IGEL Setup Parameter | <b>Sessions &gt; ThinLinc &gt; ThinLinc Sessions &gt; ThinLinc Session &gt; Login</b> |
| Registry             | Smartcard filter                                                                      |
| Value                | sessions.thinlinc%.login.smartcard_filter_2                                           |
| IGEL Setup Parameter | <b>Sessions &gt; ThinLinc &gt; ThinLinc Sessions &gt; ThinLinc Session &gt; Login</b> |
| Registry             | Smartcard filter                                                                      |
| Value                | sessions.thinlinc%.login.smartcard_filter_3                                           |



- Added **Teradici PCoIP Client** version **19.05.5**. This feature requires an **additional license**.

The following parameters are available:

[More...](#)

|            |                                                                                                                                                                  |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>System &gt; Firmware Customization &gt; Features</b>                                                                                                          |
| Parameter  | Teradici PCoIP Client                                                                                                                                            |
| Registry   | services.addition_teradici_pcoip_client.enabled                                                                                                                  |
| Value      | <u>enabled</u> / disabled                                                                                                                                        |
| IGEL Setup | <b>Sessions &gt; Teradici PCoIP Client &gt; PCoIP Sessions &gt; PCoIP Session &gt; Connection settings</b>                                                       |
| Parameter  | Use IGEL Setup for configuration                                                                                                                                 |
| Registry   | sessions.pcoip<NR>.options.igel-connection                                                                                                                       |
| Value      | <u>disabled</u> / enabled                                                                                                                                        |
| IGEL Setup | <b>Sessions &gt; Teradici PCoIP Client &gt; PCoIP Sessions &gt; PCoIP Session &gt; Connection settings</b>                                                       |
| Parameter  | Server                                                                                                                                                           |
| Registry   | sessions.pcoip<NR>.options.address                                                                                                                               |
| IGEL Setup | <b>Sessions &gt; Teradici PCoIP Client &gt; PCoIP Sessions &gt; PCoIP Session &gt; Connection settings</b>                                                       |
| Parameter  | Server certificate verification mode                                                                                                                             |
| Registry   | sessions.pcoip<NR>.options.security-mode                                                                                                                         |
| Range      | [Not required] [Warn but allow] [Full verification]                                                                                                              |
| IGEL Setup | <b>Sessions &gt; Teradici PCoIP Client &gt; PCoIP Sessions &gt; PCoIP Session &gt; Login</b>                                                                     |
| Parameter  | Authentication type                                                                                                                                              |
| Registry   | sessions.pcoip<NR>.options.auth-type                                                                                                                             |
| Range      | [Password authentication] [Smartcard authentication]                                                                                                             |
| IGEL Setup | <b>Sessions &gt; Teradici PCoIP Client &gt; PCoIP Sessions &gt; PCoIP Session &gt; Window</b>                                                                    |
| Parameter  | Window mode                                                                                                                                                      |
| Registry   | sessions.pcoip<NR>.options.window-mode                                                                                                                           |
| Range      | [User defined] [Fullscreen One Monitor] [Fullscreen All Monitors] [Window]                                                                                       |
| IGEL Setup | <b>Sessions &gt; Teradici PCoIP Client &gt; PCoIP Sessions &gt; PCoIP Session &gt; Window</b>                                                                    |
| Parameter  | User interface translation                                                                                                                                       |
| Registry   | sessions.pcoip<NR>.options.language                                                                                                                              |
| Range      | [System setting] [English] [German] [French] [Spanish] [Portuguese (EU)] [Portuguese (Brazil)] [Italian] [Japanese] [Chinese(Simplified)] [Chinese(Traditional)] |



|           |                                                    |
|-----------|----------------------------------------------------|
| Parameter | Log level                                          |
| Registry  | sessions.pcoip<NR>.options.log-level               |
| Range     | [Global setting] [Critical] [Error] [Info] [Debug] |

- Added support for **global settings**:

[More...](#)

|           |                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter | Log level                                                                                                                                                                                                            |
| Registry  | pcoip.log-level                                                                                                                                                                                                      |
| Range     | [Critical] [Error] [ <a href="#">Info</a> ] [Debug]                                                                                                                                                                  |
| Parameter | Show codec indicator                                                                                                                                                                                                 |
| Registry  | pcoip.codec_indicator                                                                                                                                                                                                |
| Value     | <u>disabled</u> / enabled                                                                                                                                                                                            |
| Info:     | <p>Added small dot in the bottom left corner during the session to indicate which codec is being used. Green indicates simple codec; blue indicates tic2 codec.</p> <p>This is only available as global setting.</p> |

- UMS option "**Save device files for support**" now includes Teradici PCoIP client's data.

## Firefox

- Added new parameters: **Allow a custom command before and after browser session**.

[More...](#)

|           |                                |
|-----------|--------------------------------|
| Parameter | init_action                    |
| Registry  | sessions.browser%.init_action  |
| Value     | <u>&lt;empty string&gt;</u>    |
| Parameter | final_action                   |
| Registry  | sessions.browser%.final_action |
| Value     | <u>&lt;empty string&gt;</u>    |

## Network

- New feature regarding **lock** and **logon screen**: Network icons are shown on the panel and appear under the same conditions as during normal operation. None of them has a context menu though. Clicking on the Wi-Fi icon directly invokes the Wireless Manager when it is enabled. If blocking/unblocking Wi-Fi by the user is enabled, there is an additional button on the Wireless Manager for blocking and a preceding dialog for unblocking.
- SCEP**: Added a registry key for specifying a **suffix for CommonName/SubjectAltName** when the type is "**DNS Name (auto)**" or "**DNS Name as UPN (auto)**".

[More...](#)



|                                                                                                                   |                                               |
|-------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| Parameter                                                                                                         | CommonName/SubjectAltName Suffix              |
| Registry                                                                                                          | network.scepclient.cert%.subjectaltnamesuffix |
| Value                                                                                                             | <u>&lt;empty&gt;</u>                          |
| <b>Info:</b>                                                                                                      |                                               |
| Automatic replacements in the value:                                                                              |                                               |
| %D -> the system's DNS domain name at the time the CSR is created<br>%% -> %<br>Other %X are currently discarded. |                                               |

- Added a mechanism for **retrieving the SCEP challenge password with a custom script**. Setting the following registry key to "true" enables the use of the script. The registry key network.scepclient.cert%.crypt\_password will be ignored. (The script may use it for its own purpose though.)

[More...](#)

|           |                                                         |
|-----------|---------------------------------------------------------|
| Parameter | Use Challenge Password Command                          |
| Registry  | network.scepclient.cert%.use_challenge_password_command |
| Value     | <u>enabled / disabled</u>                               |

If the above key is enabled, the value of this key will be passed to bash for execution. It happens when the SCEP challenge password is needed for creating a certificate signing request. The script is supposed to output the challenge password on its standard output. For convenience, any Carriage-Return characters are stripped off the script before execution by bash.

[More...](#)

|           |                                                     |
|-----------|-----------------------------------------------------|
| Parameter | Challenge Password Command                          |
| Registry  | network.scepclient.cert%.challenge_password_command |
| Value     | <u>&lt;empty_string&gt;</u>                         |

- Added **NCP Secure Enterprise VPN Client** version **5.10\_rev40552** (configurable under **IGEL Setup > Network > VPN > NCP VPN Client**).

## Wi-Fi

- Added: **Wi-Fi adapters can be turned off** and **on** by the tray icon context menu when the following registry key is enabled:

[More...](#)

|           |                                            |
|-----------|--------------------------------------------|
| Parameter | Enable Wi-Fi switch                        |
| Registry  | network.applet.wireless.enable_wifi_switch |
| Value     | <u>enabled / disabled</u>                  |

- Added support for **Realtek 8821CE wireless cards**.

## Imprivata



- **Imprivata Appliance 6.3** or higher is needed now.  
Please see the Imprivata Supported Components guide (<http://documentation.imprivata.com/01RefArch/Content/Topics/OSSupportedComponents.htm#ProvID>) for support and upgrade considerations.
- Added a new parameter to Imprivata.conf: "**Redirection of Smartcards**".  
**More...**

#### **IGEL Setup > Sessions > Appliance Mode > Imprivata**

|           |                                        |
|-----------|----------------------------------------|
| Parameter | Redirection of Smartcards              |
| Registry  | imprivata.native_smartcard_redirection |
| Value     | <u>enabled</u> / <u>disabled</u>       |

- Added a new parameter: "**Path to Certificate**".  
**More...**

#### **IGEL Setup > Sessions > Appliance Mode > Imprivata**

|           |                               |
|-----------|-------------------------------|
| Parameter | Path to Certificate           |
| Registry  | imprivata.path_to_certificate |

#### Smartcard

- Added **90meter** smartcard library. This feature requires an **additional license**.  
Use the following parameters to activate:  
**More...**

|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| IGEL Setup | <b>System &gt; Firmware Customization &gt; Features</b>                       |
| Parameter  | 90meter Smart Card Support                                                    |
| Registry   | services.addition_smartcard_90meter.enabled                                   |
| Value      | <u>enabled</u> / <u>disabled</u>                                              |
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Smartcard</b> |
| Parameter  | Horizon logon with smartcards supported by 90meter library                    |
| Registry   | vmware.view.pkcs11.use_90meter                                                |
| Value      | <u>enabled</u> / <u>disabled</u>                                              |
| IGEL Setup | <b>Sessions &gt; Browser &gt; Browser Global &gt; Smartcard Middleware</b>    |
| Parameter  | 90meter Security Device                                                       |
| Registry   | browserglobal.security_device.90meter                                         |
| Value      | <u>enabled</u> / <u>disabled</u>                                              |
| IGEL Setup | <b>Security &gt; Smartcard &gt; Middleware</b>                                |
| Parameter  | 90meter                                                                       |
| Registry   | scard.pkcs11.use_90meter                                                      |
| Value      | <u>enabled</u> / <u>disabled</u>                                              |

- New **IGEL Smartcard** mode **without Locking Desktop** (reintroduced feature of Linux 5.x firmware).  
**More...**



### **IGEL Setup > Security > Logon > IGEL Smartcard**

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Enable IGEL Smartcard without Locking Desktop |
| Registry  | scard.scardd.enable_nolock                    |
| Value     | <u>enabled</u> / <u>disabled</u>              |

### **IGEL Setup > Security > Logon > IGEL Smartcard**

|           |                                  |
|-----------|----------------------------------|
| Parameter | On Smartcard Removal, terminate  |
| Registry  | scard.scardd.session_termination |
| Value     | <u>all</u> / <u>smartcard</u>    |

- Updated **SecMaker NetID** to version **6.7.2.36**: now **YubiKey 5** is supported.
- Updated **CHERRY USB-LAN Proxy** to version **3.2.0.3**. This version provides enhanced configuration.

[More...](#)

### **IGEL Setup > Security > Smartcard > Services**

|           |                                    |
|-----------|------------------------------------|
| Parameter | Bind IP                            |
| Registry  | devices.cherry.usblanproxy.bind-ip |
| Value     | <u>auto</u>                        |

### **IGEL Setup > Security > Smartcard > Services**

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Https Server Port                     |
| Registry  | devices.cherry.usblanproxy.https-port |
| Value     | <u>443</u>                            |

### **IGEL Setup > Security > Smartcard > Services**

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | SICCT Announce IP                            |
| Registry  | devices.cherry.usblanproxy.sicct-announce-ip |
| Value     | <u>broadcast</u>                             |

### **IGEL Setup > Security > Smartcard > Services**

|           |                                                |
|-----------|------------------------------------------------|
| Parameter | SICCT Announce Port                            |
| Registry  | devices.cherry.usblanproxy.sicct-announce-port |
| Value     | <u>4742</u>                                    |

### **IGEL Setup > Security > Smartcard > Services**

|           |                                                    |
|-----------|----------------------------------------------------|
| Parameter | SICCT Announce Interval                            |
| Registry  | devices.cherry.usblanproxy.sicct-announce-interval |
| Value     | <u>30</u>                                          |

### **IGEL Setup > Security > Smartcard > Services**

|           |                                          |
|-----------|------------------------------------------|
| Parameter | USB Fast Mode                            |
| Registry  | devices.cherry.usblanproxy.usb-fast-mode |
| Value     | <u>enabled</u> / <u>disabled</u>         |

### **IGEL Setup > Security > Smartcard > Services**



|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Alternate Initialization Method for G87-1505  |
| Registry  | devices.cherry.usblanproxy.usb-1505-alt-setup |
| Value     | <u>enabled</u> / <u>disabled</u>              |

- Added a command line tool **pcsc\_scan** for smartcard debugging.
  - Added configuration parameters for some settings of **smartcard library OpenSC**.
- More...**

|           |                                                                    |
|-----------|--------------------------------------------------------------------|
| Parameter | Debug level                                                        |
| Registry  | scard.pkcs11.opensc.default.debug                                  |
| Value     | <u>0</u>                                                           |
| Parameter | Debug file                                                         |
| Registry  | scard.pkcs11.opensc.default.debug_file                             |
| Value     | <u>stderr</u>                                                      |
| Parameter | Max. send size                                                     |
| Registry  | scard.pkcs11.opensc.default.pcsc.max_send_size                     |
| Value     | <u>255</u>                                                         |
| Parameter | Max. receive size                                                  |
| Registry  | scard.pkcs11.opensc.default.pcsc.max_recv_size                     |
| Value     | <u>256</u>                                                         |
| Parameter | Connect exclusive                                                  |
| Registry  | scard.pkcs11.opensc.default.pcsc.connect_exclusive                 |
| Value     | <u>enabled</u> / <u>disabled</u>                                   |
| Parameter | Disconnect action                                                  |
| Registry  | scard.pkcs11.opensc.default.pcsc.disconnect_action                 |
| Value     | <u>leave</u> / <u>reset</u> / <u>unpower</u>                       |
| Parameter | Transaction end action                                             |
| Registry  | scard.pkcs11.opensc.default.pcsc.transaction_end_action            |
| Value     | <u>leave</u> / <u>reset</u> / <u>unpower</u>                       |
| Parameter | Reconnect action                                                   |
| Registry  | scard.pkcs11.opensc.default.pcsc.reconnect_action                  |
| Value     | <u>leave</u> / <u>reset</u> / <u>unpower</u>                       |
| Parameter | Enable pinpad                                                      |
| Registry  | scard.pkcs11.opensc.default.pcsc.enable_pinpad                     |
| Value     | <u>enabled</u> / <u>disabled</u>                                   |
| Parameter | Use PIN caching                                                    |
| Registry  | scard.pkcs11.opensc.default.pkcs15.use_pin_caching                 |
| Value     | <u>enabled</u> / <u>disabled</u>                                   |
| Parameter | How many times to use a PIN from cache before re-authenticating it |
| Registry  | scard.pkcs11.opensc.default.pkcs15.pin_cache_counter               |
| Value     | <u>10</u>                                                          |



|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | PIN caching ignores user consent                                 |
| Registry  | scard.pkcs11.opensc.default.pkcs15.pin_cache_ignore_user_consent |
| Value     | enabled / <u>disabled</u>                                        |

- Updated **cryptovision sc/interface PKCS#11** smartcard library to version **7.1.20**.

Changes in this revision:

- Fixed a possible **deadlock** in the PKCS#11 module on Linux, if **C\_Finalize** is called during a PCSC event, for example **C\_WaitForSlotEvent**.
- ROCA check** in the Smartcard Manager, based on the "ROCA detection tool", see <https://github.com/crocs-muni/roca>.
- Renaming** of the container label in Smartcard Manager **with F2** is now possible.

#### CUPS Printing

- Added **SMB Network Print** client function.

[More...](#)

#### **IGEL Setup > Devices > Printer > CUPS > Printers > Dialog**

|           |                                |
|-----------|--------------------------------|
| Parameter | Printer Port                   |
| Registry  | print.cups.printer<NR>.backend |
| Value     | smb                            |

#### **IGEL Setup > Devices > Printer > CUPS > Printers > Dialog**

|           |                                   |
|-----------|-----------------------------------|
| Parameter | SMB Server                        |
| Registry  | print.cups.printer<NR>.smb_server |

#### **IGEL Setup > Devices > Printer > CUPS > Printers > Dialog**

|           |                                      |
|-----------|--------------------------------------|
| Parameter | SMB Workgroup                        |
| Registry  | print.cups.printer<NR>.smb_workgroup |

#### **IGEL Setup > Devices > Printer > CUPS > Printers > Dialog**

|           |                                    |
|-----------|------------------------------------|
| Parameter | SMB Printer                        |
| Registry  | print.cups.printer<NR>.smb_printer |

#### **IGEL Setup > Devices > Printer > CUPS > Printers > Dialog**

|           |                                 |
|-----------|---------------------------------|
| Parameter | SMB Port                        |
| Registry  | print.cups.printer<NR>.smb_port |
| Value     | enabled / <u>disabled</u>       |

#### **IGEL Setup > Devices > Printer > CUPS > Printers > Dialog**

|           |                                     |
|-----------|-------------------------------------|
| Parameter | Use Kerberos Authentication         |
| Registry  | print.cups.printer<NR>.smb_kerberos |
| Value     | enabled / <u>disabled</u>           |

#### **IGEL Setup > Devices > Printer > CUPS > Printers > Dialog**

|           |                                        |
|-----------|----------------------------------------|
| Parameter | Use Passthrough Authentication         |
| Registry  | print.cups.printer<NR>.smb_passthrough |
| Value     | enabled / <u>disabled</u>              |

**IGEL Setup > Devices > Printer > CUPS > Printers > Dialog**

|                                                                                 |                                       |
|---------------------------------------------------------------------------------|---------------------------------------|
| Parameter                                                                       | SMB User                              |
| Registry                                                                        | print.cups.printer<NR>.smb_user       |
| <b>IGEL Setup &gt; Devices &gt; Printer &gt; CUPS &gt; Printers &gt; Dialog</b> |                                       |
| Parameter                                                                       | SMB Password                          |
| Registry                                                                        | print.cups.printer<NR>.crypt_password |

Base system

- Added a possibility to configure **scheduled commands**. Registry keys: system.cron.\*\*
- Buddy update** enhancements:

- Automatic load balancing:**

A client collects up to eight server candidates from which one is selected randomly. Collection stops when the number specified in the following registry key is reached. Otherwise collection stops after a timeout.

[More...](#)

|           |                                    |
|-----------|------------------------------------|
| Parameter | Buddy Update Server Candidates     |
| Registry  | update.ftp.buddy_server_candidates |
| Value     | 1                                  |

- Grouping:**

Buddy update servers and clients only interact with each other when they are in the same group determined by the following registry key (a non-negative integer number). This feature is mainly useful when different firmware versions shall be used in parallel.

[More...](#)

|           |                           |
|-----------|---------------------------|
| Parameter | Buddy Group ID            |
| Registry  | update.ftp.buddy_group_id |
| Value     | 0                         |

- Added: **Firmware update** scheduled **on shutdown** is now **invoked on reboot** too.
- Added package **ldap-utils** which can be used by custom scripts.
- Updated **Kernel** to mainline version **4.19.65**.
- Moved the **EULA** page in IGEL Setup Assistant into the **demo activation workflow**.
- Updated EULA** displayed in OSC and IGEL Setup Assistant.
- Added: When IGEL Setup Assistant is used to download a **demo license via Wi-Fi**, the **local Wi-Fi manager** will be **enabled by default**.
- Updated **Fluendo multimedia codecs** to the following versions:

[More...](#)

|                        |            |          |
|------------------------|------------|----------|
| gst-fluendo-aacdec     | 21/03/2019 | 0.10.39  |
| gst-fluendo-asfdemux   | 21/03/2019 | 0.10.89  |
| gst-fluendo-h264dec    | 21/03/2019 | 0.10.53  |
| gst-fluendo-mp3        | 21/03/2019 | 0.10.39  |
| gst-fluendo-mpeg4video | 21/03/2019 | 0.10.43  |
| gst-fluendo-vadec      | 21/03/2019 | 0.10.208 |
| gst-fluendo-wmadec     | 21/03/2019 | 0.10.68  |



|                    |            |         |
|--------------------|------------|---------|
| gst-fluendo-wmvdec | 20/03/2019 | 0.10.65 |
|--------------------|------------|---------|

- Replaced **timesyncd** with **chrony NTP**. Added a new registry key:  
[More...](#)

|           |                                        |
|-----------|----------------------------------------|
| Parameter | Use NTP Servers from DNS SRV record    |
| Registry  | system.time.ntp_use_dnssrv_timeservers |
| Value     | <u>enabled</u> / disabled              |

- Updated **CA Certificates** to version **20190122** (Mozilla authority bundle version 2.30).  
 The following authorities were added:

[More...](#)

- "Certigna Root CA"
- "GTS Root R1"
- "GTS Root R2"
- "GTS Root R3"
- "GTS Root R4"
- "UCA Extended Validation Root"
- "UCA Global G2 Root"
- "GlobalSign Root CA - R6"
- "OISTE WISEKey Global Root GC CA"
- "GDCA TrustAUTH R5 ROOT"
- "SSL.com EV Root Certification Authority ECC"
- "SSL.com EV Root Certification Authority RSA R2"
- "SSL.com Root Certification Authority ECC"
- "SSL.com Root Certification Authority RSA"
- "TrustCor ECA-1"
- "TrustCor RootCert CA-1"
- "TrustCor RootCert CA-2"

The following authorities were removed:

[More...](#)

- "Certplus Root CA G1"
- "Certplus Root CA G2"
- "OpenTrust Root CA G1"
- "OpenTrust Root CA G2"
- "OpenTrust Root CA G3"
- "TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı H5"
- "Visa eCommerce Root"
- "ACEDICOM Root"
- "AddTrust Low-Value Services Root"
- "AddTrust Public Services Root"
- "AddTrust Qualified Certificates Root"
- "CA Disig Root R1"
- "CNNIC ROOT"
- "Camerfirma Chambers of Commerce Root"
- "Camerfirma Global Chambersign Root"



- "Certinomis - Autorité Racine"
- "Certum Root CA"
- "China Internet Network Information Center EV Certificates Root"
- "Comodo Secure Services root"
- "Comodo Trusted Services root"
- "DST ACES CA X6"
- "GeoTrust Global CA 2"
- "PSCPProcert"
- "Security Communication EV RootCA1"
- "Swisscom Root CA 1"
- "Swisscom Root CA 2"
- "Swisscom Root EV CA 2"
- "TURKTRUST Certificate Services Provider Root 2007"
- "TUBITAK UEKAE Kok Sertifika Hizmet Saglayicisi - Surum 3"
- "UTN USERFirst Hardware Root CA"

## Driver

- Added registry keys to modify the Intel graphic driver usage of **framebuffer compression** and **power management**.

New registry keys:

[More...](#)

|           |                                                             |
|-----------|-------------------------------------------------------------|
| Parameter | Power saving display C-States to use                        |
| Registry  | x.drivers.intel.dc_setting                                  |
| Range     | <a href="#">[Default]</a> [Disable] [Up to DC5] [Up to DC6] |
| Info:     | "Default" - driver default                                  |
| Parameter | Use framebuffer compression                                 |
| Registry  | x.drivers.intel.fbc_setting                                 |
| Range     | <a href="#">[Default]</a> [Disable]                         |
| Info:     | "Default" - driver default                                  |

- Updated **Philips Speech Driver** to version **12.7.11**.
- Updated **signotec Citrix Virtual Channel** driver to version **8.0.8**.
- Updated **StepOver TCP Client** to version **2.3.2**.
- Updated **deviceTRUST Client** to version **19.1.200**. These are the release notes:  
Welcome to the release of the deviceTRUST 19.1.200 IGEL client, providing the context of IGEL thin client and UD Pocket devices into your virtual sessions. This release includes support for logical disks attached to the IGEL endpoint, plus bug fixes and stability improvements over the previous 19.1.100 release.

## Logical Disks



We've added support for real-time properties representing the LOGICAL DISKS attached to the IGEL endpoint. This includes:

**More...**

DEVICE\_LOGICALDISK\_X\_TYPE – Either Fixed or Removable.  
 DEVICE\_LOGICALDISK\_X\_LABEL – The volume label.  
 DEVICE\_LOGICALDISK\_X\_FILESYSTEM – The type of file system.  
 DEVICE\_LOGICALDISK\_X\_PATHS – The paths that the disk is mounted.  
 DEVICE\_LOGICALDISK\_X\_TOTALMB – The total space available on the disk. This property is only available for mounted disks.  
 DEVICE\_LOGICALDISK\_X\_FREEMB – The free space available on the disk. This property is only available for mounted disks.  
 DEVICE\_LOGICALDISK\_X\_NAME – The name of the underlying physical disk.  
 DEVICE\_LOGICALDISK\_X\_VENDORID – The vendor identifier uniquely identifying the manufacturer. This property is only available for USB or PCI connected devices.  
 DEVICE\_LOGICALDISK\_X\_PRODUCTID – The product identifier uniquely identifying the product. This property is only available for USB or PCI connected devices.  
 DEVICE\_LOGICALDISK\_X\_SERIALNUMBER – The serial number of the physical disk.  
 DEVICE\_LOGICALDISK\_X\_BUSTYPE – The storage bus type linked to the physical disk.  
 DEVICE\_LOGICALDISK\_COUNT – The number of logical disks.

#### X11 system

- Added a new parameter to allow configuration of '**Display Switch**' confirmation dialog timeout.

**More...**

| IGEL Setup | <b>Accessories &gt; Display Switch &gt; Options</b> |
|------------|-----------------------------------------------------|
| Parameter  | Timeout for confirmation dialog                     |
| Registry   | sessions.user_display0.options.confirm_timeout      |
| Value      | 10                                                  |

- Re-Enable 'Display Switch' session start script to cycle simple modes.
- Added new options for **lid handling**.

**More...**

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Lid close action while plugged in     |
| Registry  | system.actions.lid.ac                 |
| Range     | [Turn off display] [Suspend]          |
| Parameter | Lid close action while not plugged in |
| Registry  | system.actions.lid.battery            |
| Range     | [Turn off display] [Suspend]          |

- Added new registry keys to change the xorg input driver for an input device class.  
 New registry keys:

For keyboards:

**More...**

|           |                               |
|-----------|-------------------------------|
| Parameter | Xorg driver to use            |
| Registry  | userinterface.keyboard.driver |
| Range     | [Evdev] [Libinput]            |

For touchpads:

**More...**

|           |                                |
|-----------|--------------------------------|
| Parameter | Xorg driver to use             |
| Registry  | userinterface.touchpad.driver  |
| Range     | [Evdev] [Synaptics] [Libinput] |

For touchscreens:

**More...**

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Xorg driver to use                    |
| Registry  | userinterface.touchscreen.xorg_driver |
| Range     | [Evdev] [Libinput]                    |

For mouse:

**More...**

|           |                            |
|-----------|----------------------------|
| Parameter | Xorg driver to use         |
| Registry  | userinterface.mouse.driver |
| Range     | [Evdev] [Libinput]         |

- Added some registry keys to disable loading of **DRM kernel modules** (graphic).

**More...**

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Disable the loading of the RADEON DRM driver |
| Registry  | x.drivers.ati.disable                        |
| Value     | 0                                            |
| Parameter | Disable the loading of the AMDGPU DRM driver |
| Registry  | x.drivers.amdgpu.disable                     |
| Value     | 0                                            |
| Parameter | Disable the loading of the i915 DRM driver   |
| Registry  | x.drivers.intel.disable                      |



|           |                                                 |
|-----------|-------------------------------------------------|
| Value     | <u>0</u>                                        |
| Parameter | Disable the loading of the NVIDIA kernel driver |
| Registry  | x.drivers.nvidia.disable                        |
| Value     | <u>0</u>                                        |
| Parameter | Disable the loading of the NOUVEAU DRM driver   |
| Registry  | x.drivers.nouveau.disable                       |
| Value     | <u>0</u>                                        |
| Parameter | Disable the loading of the QXL DRM driver       |
| Registry  | x.drivers.qxl.disable                           |
| Value     | <u>0</u>                                        |
| Parameter | Disable the loading of the VMGFX DRM driver     |
| Registry  | x.drivers.vmware.disable                        |
| Value     | <u>0</u>                                        |
| Parameter | Disable the loading of the VBOXVIDEO DRM driver |
| Registry  | x.drivers.vboxvideo.disable                     |
| Value     | <u>0</u>                                        |

- Updated **DisplayLink** driver to version **5.1.26** to solve some startup issues.

#### Evidian

- Updated **Evidian rsUserAuth** to version **1.5.7116**.

#### Hardware

- Added hardware support for **Rein Medical Silenio 122CT and 124CT**.
- Added hardware support for **Advantech POC-W213L** and **POC-W243L**.
- Added hardware support for **ADS-TEC VMT 9000 Serie**.
- Added hardware support for **Fujitsu Esprimo Q957**.
- Added hardware support for **ADS-TEC VMT 9000 Serie**.
- Added hardware support for **LG AiO Cloud Device 38"**
- Added hardware support for the following **headsets**:  
**More...**
  - Jabra Engage 50
  - Jabra Engage 65



- Jabra Engage 75
- Jabra Evolve 30 II (Ver. B)
- Jabra Evolve 30 II (Ver. C)
- Jabra Evolve 40 (Ver. B) - USB-C
- Jabra Evolve 40 (Ver. D)
- Jabra Evolve 65
- Jabra Evolve 75
- Plantronics Voyager 5200 UC
- Plantronics Voyager 6200 UC
- Plantronics Voyager 8200 UC
- Plantronics ENCOREPRO 720 + DA70
- Plantronics ENCOREPRO 720 + DA80
- Plantronics ENCOREPRO 520D + DA90
- Sennheiser SC70
- Added hardware support for **HP t430**.
- Added hardware support for **HP t420**.

#### Java

- Replaced Oracle JRE by **AZUL's Zulu JRE**.
- Updated **Zulu JRE** to version **8.40.0.25**.

#### Remote Management

- **Connection order between UMS and ICG** can now be configured.  
[More...](#)

|          |                                                       |
|----------|-------------------------------------------------------|
| Registry | <code>system.remotemanager.icg_try_ums_connect</code> |
| Value    | <u>enabled</u> / <u>disabled</u>                      |

When an ICG connection is configured and the parameter is enabled, the device tries to connect directly to UMS. If the connection was established successfully, the device is managed by UMS and not over ICG until new start of the device or network.

#### IGEL Cloud Gateway

- Added **VNC Shadowing** support **over ICG**. To use this feature, **UMS 6.02.110 or later** and **ICG 2.01.100 or later** are required.

#### Resolved Issues 11.02.100

##### Citrix

- Improved **USB handling of SpaceMouse**.
- Improved **USB redirection** handling with **Citrix Workspace App 19.06**.
- Fixed **stability issues** with **Citrix Browser Content Redirection**.

##### OSC Installer

- Fixed: OSC Installer does not disable **EFI** when **MSDOS partitioning** was chosen.



## Citrix Receiver 13

- Added a **switch** to enable the possibility to **launch multiple desktop sessions with RTME and h.264 acceleration**. This switch should not be used when "**Enable Secure ICA**" is active for specific delivery group.

[More...](#)

|          |                           |
|----------|---------------------------|
| Registry | ica.workaround-dual-rtme  |
| Value    | <u>enabled / disabled</u> |

## RDP/IGEL RDP Client 2

- Added a registry key to use **rdpglobal window settings for remote apps**.

[More...](#)

|           |                                                             |
|-----------|-------------------------------------------------------------|
| Parameter | Enable global windwos settings for remote app               |
| Registry  | rdp.winconnect.enable-global-window-settings-for-remote-app |
| Value     | <u>enabled / disabled</u>                                   |

- Added negotiation: **Kerberos as fallback for disabled NTLM authentication**. This only works when **Active Directory/Kerberos Logon** is enabled.
- Fixed **RD Web Access** not working with special characters in name or password. This only works when **Active Directory/Kerberos Logon** is enabled.
- Fixed **smartcard redirection in RDP: SCardGetAttrib** was failing if **pbAttr** was NULL. The fix should help running Dutch Zorg-ID applications.

## RD Web Access

- Fixed **not starting RDP Remote Applications**.

## VMware Horizon

- Added **recognition for password change** and **password expired** dialog in Horizon local logon sessions or appliance mode.
- Fixed configuration choice for usage of **relative mouse feature**.
- Added possibility to use the **rollback variant of the Horizon Client**.

[More...](#)

|           |                                         |
|-----------|-----------------------------------------|
| Parameter | Allow rollback to former client variant |
| Registry  | vmware.view.allow-client-rollback       |
| Value     | <u>enabled / disabled</u>               |

- Fixed a problem with the client where connection to the **remote desktop using PCoIP protocol failed** occasionally.

## Teradici PCoIP Client

- Fixed unwanted **restart of login window** after session logoff or disconnect.

## Firefox

- Fixed Firefox **not accepting proxy credentials** from setup.
- Fixed **print hotkey** disable option not working with Firefox 60.
- Fixed **browserglobal.app.local\_subdirs\_whitelist** not working.



## Network

- Fixed: **Failure to reach SCEP server** in the client certificate renewal phase resulted in loss of SCEP server and client certificates.
- Changed **e1000e driver** to out of tree version **3.4.2.3** directly from Intel.
- Changed **igb driver** to out of tree version **5.3.5.22** directly from Intel.
- Added possibility to **switch between third-party** and **kernel Intel IGB network driver**.

New registry key:

**More...**

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Use thirdparty igb kernel module      |
| Registry  | network.drivers.igb.prefer_thirdparty |
| Range     | [Auto] [Yes] [No]                     |

**Info:** "Auto" (use thirdparty in most cases)

- Added possibility to **switch between third-party** and **kernel intel E1000E network driver**.

New registry key:

**More...**

|           |                                          |
|-----------|------------------------------------------|
| Parameter | Use thirdparty e1000e kernel module      |
| Registry  | network.drivers.e1000e.prefer_thirdparty |
| Range     | [Auto] [Yes] [No]                        |

**Info:** "Auto" (use thirdparty in most cases)

- Fixed **instability of netmounts** with static IP configuration.
- Added possibility to **switch between third-party r8168** and **kernel r8169 realtek network driver**.

New registry key:

**More...**

|           |                                    |
|-----------|------------------------------------|
| Parameter | Use thirdparty r8168 kernel module |
| Registry  | network.drivers.r8169.prefer_r8168 |
| Range     | [Auto] [Yes] [No]                  |

**Info:** "Auto" (use r8168 in most cases)

- Added a possibility to choose the **variant of the realtek r8168 driver**.

A new registry key:

**More...**

|           |                                                                 |
|-----------|-----------------------------------------------------------------|
| Parameter | Choose realtek r8168 variant (only if "prefer r8168" is chosen) |
| Registry  | network.drivers.r8169.r8168_variant                             |
| Range     | [Default] [No NAPI] [NAPI]                                      |

**Info:** "Default" (use NAPI in most cases)

- Fixed: **Second Ethernet** interface **did not get configured** when the first one was disabled.
- Fixed: **802.1X Ethernet** configuration **with user interaction** was broken.

## Wi-Fi

- Fixed not working **TP Link Archer T2UH**.
- Fixed not working **Broadcom SDIO WLAN cards** as present in Advantech AIM8IAC device for example.



## Smartcard

- Updated **cryptovision sc/interface PKCS#11 smartcard library** to version **7.1.20**.
- Fixed a possible **deadlock** in the **PKCS#11 module** on Linux if **C\_Finalize** is called during a PCSC event, for example C\_WaitForSlotEvent.
- Fixed **OpenSC** setting **max\_send\_size** for reader driver pcsc in **/etc/opensc/opensc.conf**.
- Fixed **Dell KB813 Smartcard Keyboard** in combination with certain smartcards driven by OpenSC PKCS#11 module. Before this fix, **authentication to Citrix StoreFront and VMWare Horizon failed**.

## Base system

- Improved: Ensured that the **Unit ID for IGEL devices is the MAC address of the onboard network card**.
- Fixed **license expiry warning at boot**. Before this fix, in some cases the warning wrongly appeared at every boot.
- Fixed **unmounting storage devices via In-session control bar**.
- Fixed **server-dependent crash** when installing license via FTP.
- Fixed retrieving of **serial number of a connected screen**.
- Fixed random **90 seconds shutdown delay** (systemd).
- Fixed wrong behavior with **expired evaluation licenses** in some cases.
- Added message in **bootsplash** when a custom partition will get created.
- Fixed **bug in the screenlock countdown** that occurred, when display of remaining seconds was not desired.
- Fixed **shortcut configuration for shutdown, restart and icon** sort to be applied without reboot.
- Added **apparmor** rule to allow **tcpdump** to write to /debuglog.
- Fixed **hotkey configuration to be applied without reboot**.
- Fixed: **UD2 screen goes black** with certain multimonitor configurations.
- Improved new **license detection** in **IGEL Setup Assistant**.
- Fixed **AD/Kerberos logon** in case parameter **auth.login.krb5\_enterprise** is set to false.
- Fixed: **System logoff waits for Citrix logoff** now.
- Fixed **NTP synchronization** problems **when changing the NTP client** from **timesyncd** to **chrony**.
- Added **switch** to enable **DNS hostname lookup for SSH server**:

[More...](#)

|           |                                     |
|-----------|-------------------------------------|
| Parameter | Use DNS to resolve client hostnames |
| Registry  | network.ssh_server.use_dns          |
| Value     | <u>enabled</u> / <u>disabled</u>    |

- Fixed **USB printer aliases**.
- Fixed **gtk-3 icon sizes for High DPI** configurations.
- Enhanced **bootloader** to allow the setting of some kernel command line parameters with registry keys.

New registry keys:

[More...](#)

|           |                                 |
|-----------|---------------------------------|
| Parameter | Disable use of APIC controller. |
|-----------|---------------------------------|



|                                             |                                               |
|---------------------------------------------|-----------------------------------------------|
| Registry                                    | system.kernel.bootparams.noapic               |
| Value                                       | <u>enabled / disabled</u>                     |
| Parameter                                   | Disable use of ACPI.                          |
| Registry                                    | system.kernel.bootparams.noacpi               |
| Value                                       | <u>enabled / disabled</u>                     |
| Parameter                                   | Use only one CPU core and disable all others. |
| Registry                                    | system.kernel.bootparams.nosmp                |
| Value                                       | <u>enabled / disabled</u>                     |
| Parameter                                   | Enable debug console on serial port 1.        |
| Registry                                    | system.kernel.bootparams.serial_console_debug |
| Value                                       | <u>enabled / disabled</u>                     |
| Parameter                                   | Limit CPU core usage (0 means no limit).      |
| Registry                                    | system.kernel.bootparams.maxcpus              |
| Value                                       | "0"                                           |
| Parameter                                   | Set maximum allowed cstate on intel cpus.     |
| Registry                                    | system.kernel.bootparams.max_cstate           |
| Range                                       | [No limit] [1] [2] [3] [4] [5] [6]            |
| <i>Info: do not limit intel cstate</i>      |                                               |
| Parameter                                   | IOMMU usage setting.                          |
| Registry                                    | system.kernel.bootparams.iommu                |
| Range                                       | [On] [Off] [ <u>Passthrough</u> ] [Force]     |
| <i>Info: Use IOMMU passthrough possible</i> |                                               |
| Parameter                                   | IOMMU usage setting for AMD systems.          |
| Registry                                    | system.kernel.bootparams.amd_iommu            |
| Range                                       | [ <u>On</u> ] [Off]                           |
| <i>Info: Use IOMMU if possible</i>          |                                               |



|                                    |                                        |
|------------------------------------|----------------------------------------|
| Parameter                          | IOMMU usage setting for Intel systems. |
| Registry                           | system.kernel.bootparams.intel_iommu   |
| Range                              | [On] [Off]                             |
| <b>Info:</b> Use IOMMU if possible |                                        |

- Added a new registry key to set **USB quirks**:

[More...](#)

|           |                                                                                              |
|-----------|----------------------------------------------------------------------------------------------|
| Parameter | Set XHCI USB quirks to fix some hardware issues                                              |
| Registry  | system.kernel.bootparams.xhci-hcd_quirks                                                     |
| Range     | [No quirk] [Spurious Reboot quirk] [Spurious Wakeup quirk]<br>[Spurious Reboot Wakeup quirk] |

- Lenovo ThinkCentre M73 needs the **system.kernel.bootparams.xhci-hcd\_quirks** registry key set to `Spurious Reboot quirk` to fix reboot after shutdown problem.
- Added column "**Syslog style template**" to **Remote Syslog setup page**. This allows to change rsyslog output style e.g. to newer SyslogProtocol23Format which is supported by graylog.
- Disable **martian packet logging**.

## Driver

- Updated **deviceTRUST Client** to version **19.1.200**.
  - Fixed an issue reading the **DEVICE\_IGEL\_ICG\_SERVER** property.
  - Fixed an issue where the **NETWORK** and **LOCATION** property providers **could cause the client to freeze** if a disconnection occurred whilst these property providers were checking for changes.
  - Fixed an **open file handle leak** which led to the client process reaching its file handle limits when left running for a long period of time.
- Fixed not working **WACOM** device **DTU-1141B**.

## Custom Partition

- Added **message in bootsplash** when a **custom partition** will get **created**.
- Fixed **ownership of extracted data**: don't preserve original owner while extracting data into custom partition.

## Storage Devices

- Fixed **automounting of storage devices** inside of **Olympus DS-9500 Digital Voice Recorder**.

## Appliance Mode

- Fixed: **In-session control bar** could not be deactivated in **Citrix SelfService appliance mode**.

## X11 system

- There is now a **registry key to ignore a 3Dconnexion SpaceMouse** for IGEL graphical use (X11). If activated, the SpaceMouse is only passed through to the desktop session. If disabled, it acts like a standard mouse.

[More...](#)



|            |                                                          |
|------------|----------------------------------------------------------|
| IGEL Setup | <b>System &gt; Registry</b>                              |
| Parameter  | Deactivates a 3Dconnexion SpaceMouse as a standard mouse |
| Registry   | userinterface.mouse.spacemouse.x11_ignore                |
| Value      | <u>enabled</u> / disabled                                |

- The following **SpaceMouse** products are included:

[More...](#)

| VID    | PID    | Vendor         | Product                                  |
|--------|--------|----------------|------------------------------------------|
| 0x046D | 0xC603 | Logitech, Inc. | 3Dconnexion SpaceMouse Plus XT           |
| 0x046D | 0xC605 | Logitech, Inc. | 3Dconnexion CADman                       |
| 0x046D | 0xC606 | Logitech, Inc. | 3Dconnexion SpaceMouse Classic           |
| 0x046D | 0xC621 | Logitech, Inc. | 3Dconnexion SpaceBall 5000               |
| 0x046D | 0xC623 | Logitech, Inc. | 3Dconnexion SpaceTraveller 3D Mouse      |
| 0x046D | 0xC625 | Logitech, Inc. | 3Dconnexion SpacePilot 3D Mouse          |
| 0x046D | 0xC626 | Logitech, Inc. | 3Dconnexion SpaceNavigator 3D Mouse      |
| 0x046D | 0xC627 | Logitech, Inc. | 3Dconnexion SpaceExplorer 3D Mouse       |
| 0x046D | 0xC628 | Logitech, Inc. | 3Dconnexion SpaceNavigator for Notebooks |
| 0x046D | 0xC629 | Logitech, Inc. | 3Dconnexion SpacePilot Pro 3D Mouse      |
| 0x046D | 0xC62B | Logitech, Inc. | 3Dconnexion SpaceMouse Pro               |
| 0x256F | **     | 3Dconnexion    | SpaceMouse                               |

- USB device reset** via USB powercycle is now available on **UD6/UD7**.
- Fixed: Problems with **internal graphic cards** and **Nvidia graphic cards**.
- Display Switch** application will now use some settings from 'Advanced' dialog in 'Simple' mode.
- Fixed **display hotplug failing** on initial lock screen with Active Directory logon.
- Fixed **screen corruption** with DPMS and enabled composite manager.
- Fixed **screen flickering** in some cases when "**Force NumLock On**" (x.global.forcenumlock) is active.
- Fixed **Display Switch** utility not starting with some translations.
- Fixed an issue with the **noDDC mode** which was not always working as expected.
- Fixed **wrongly detected embedded DisplayPort** on **Dell Wyse 5070** Extended hardware.
- Added the possibility to change an **embedded DisplayPort** to a normal **DisplayPort**.

[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Use embedded displayport as normal displayport (reboot required) |
| Registry  | x.drivers.intel.edp_is_dp                                        |
| Range     | <u>[default]</u> [enable] [disable]                              |



- Fixed some **multimonitor** (>4) issues with **Nvidia graphic cards**.
- Fixed **monitor screen ID** shown with **Nvidia nvs810 GPU**.
- Added consideration of **hardware limits for choosing automatic resolution** in **Xorg config** (currently only for IGEL hardware).
- Fixed problem with **modesetting driver** and **two 2160x1440 monitors** in extended configuration.
- Added a new registry key to enable use of **linear framebuffer for modesetting driver**.  
New registry key:  
[More...](#)

|                                               |                                              |
|-----------------------------------------------|----------------------------------------------|
| Parameter                                     | Use linear instead of tiled framebuffer      |
| Registry                                      | x.drivers.modesetting.use_linear_framebuffer |
| Range                                         | <u>[Default]</u> [False] [True]              |
| Info:                                         |                                              |
| Use linear framebuffer only in special cases. |                                              |

- Fixed configuration where old **Display Switch** took precedence over configuration from new Display Switch and preventing changes.

## X Server

- Fixed issue with **primary / secondary screens** were switched in some cases.

## Audio

- Fixed **bad quality sound over DisplayPort** in a Citrix ICA session or other applications using ALSA API.
- Fixed **jack detection of the headphone port in Dell Wyse 3040**.
- Fixed **configuration of default audio output and input**.

## Media Player (Parole)

- Fixed a problem where **parole media player** would **hang** instead of playing audio **while audio-visualization** is enabled.
- Fixed parole media player **not handling audio hotkeys in fullscreen mode**.

## Misc

- **Monitoring Agent** uses now **only the half size of the debuglog partition**.  
When the setup option **log\_max\_size** with the option **log\_rotation** creates an overall consumption that is bigger than 50% of the debuglog partition size, the size for each log automatically will be decreased to a value that allows a full rotation which occupies exactly 50% of the partition size.

## Hardware

- Fixed not working **network** on **Beckhoff CB3163, CB6263** and **CB6363** systems.
- Fixed not working network on **Lex 3I380D**.
- Fixed **shutdown** issue of **Lenovo ThinkCentre M73** (rebooted 2 - 3 seconds after power off).



- Added a **possibility to change** some **DRM settings** and **limit the DisplayPort lane bandwidth** on Intel devices.

Added new registry keys:

[More...](#)

|                                                           |                                                                                                   |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Parameter                                                 | Use best graphic mode for all screens on console.                                                 |
| Registry                                                  | x.drivers.kms.best_console_mode                                                                   |
| Range                                                     | [Default] [Enabled] [Disabled]                                                                    |
| Info: "Default" is enabled in most cases.                 |                                                                                                   |
| Parameter                                                 | Limit the maximum console resolution width to this value.                                         |
| Registry                                                  | x.drivers.kms.max_console_width                                                                   |
| Type                                                      | Integer                                                                                           |
| Value                                                     | "0"                                                                                               |
| Info: "0" means default setting. Use the default setting. |                                                                                                   |
| Parameter                                                 | Limit the maximum console resolution height to this value.                                        |
| Registry                                                  | x.drivers.kms.max_console_height                                                                  |
| Type                                                      | Integer                                                                                           |
| Value                                                     | "0"                                                                                               |
| Info: "0" means default setting. Use the default setting. |                                                                                                   |
| Parameter                                                 | Set graphic kernel driver debug level.                                                            |
| Registry                                                  | x.drivers.kms.debug_level                                                                         |
| Range                                                     | [No debug] [Basic] [Basic + core] [Basic + core + atomic] [Full]                                  |
| Info: Warning log will grow very fast.                    |                                                                                                   |
| Only for Intel i915 driver:                               |                                                                                                   |
| Parameter                                                 | Limit the maximum DisplayPort lane link rate.                                                     |
| Registry                                                  | x.drivers.intel.max_dp_link_rate                                                                  |
| Range                                                     | [default] [1.62Gbps] [2.16Gbps] [2.7Gbps] [3.24Gbps]<br>[4.32Gbps] [5.4Gbps] [6.48Gbps] [8.1Gbps] |
| Info: "Default" means hardware default limit.             |                                                                                                   |



|                                       |                                                        |
|---------------------------------------|--------------------------------------------------------|
| Parameter                             | Disable the DP audio support in the i915 DRM driver.   |
| Registry                              | x.drivers.intel.disable_dp_audio                       |
| Range                                 | <u>[Default]</u> [No][Yes]                             |
| Info: "Default" - support is enabled. |                                                        |
| Parameter                             | Disable the HDMI audio support in the i915 DRM driver. |
| Registry                              | x.drivers.intel.disable_hdmi_audio                     |
| Range                                 | <u>[Default]</u> [No][Yes]                             |
| Info: "Default" - support is enabled. |                                                        |

- Fixed **black screen** issue with some monitors and 2560x1440 resolution - occurred on **UD2 LX50** and **other Intel GPUs**.
- Fixed detection of **Dell Wyse 5070** for the non-extended version.
- Fixed issues with **not working Touchpad** and **Trackpoint** on Lenovo laptops.
- Fixed **vanishing mouse cursor on Ryzen 3** devices.
- Fixed problems with **2 or more monitors** on a **DisplayLink** adapter.
- Added possibility to use **AMDGPU PRO** driver instead of the kernel integrated driver.
- **Ryzen 3** devices (1200, 1300X, 2200G, 2200U and 2300U) **will use the AMDGPU PRO driver** if registry key x.drivers.amdgpu.use\_amdgpu\_pro is set to auto (default).
- A new registry key (settings to this key will only work after reboot):
   
**More...**

|           |                                 |
|-----------|---------------------------------|
| Parameter | Use AMDGPU PRO driver           |
| Registry  | x.drivers.amdgpu.use_amdgpu_pro |
| Range     | <u>[Auto]</u> [True] [False]    |

## Remote Management

- When **TC is managed over ICG**, settings received in the connection stage does not apply immediately. The settings must be applied after user prompt dialog.
- Fixed **UMS synchronization** of configuration changes made in "Emergency mode". Fixed sporadically failures while sending data over ICG.
- Fixed **wallpaper configuration** if ICG protocol is used.
- Fixed **releasing from UMS** when the device was offline during removal from UMS.
- Added: The **endpoint can now report up to 8 monitors** in UMS information.
- Fixed **UMS jobs** have not been executed when delivered at the next system boot.



## CA Certificates Contained in IGEL OS 11.02.100

Contained CA certificates:

- ACCVRAIZ1, expires Dec 31 09:37:37 2030 GMT (ACCVRAIZ1.crt)
- AC RAIZ FNMT-RCM, expires Jan 1 00:00:00 2030 GMT (AC\_RAIZ\_FNMT-RCM.crt)
- Actalis Authentication Root CA, expires Sep 22 11:22:02 2030 GMT (Actalis\_Authentication\_Root\_CA.crt)
- AddTrust External CA Root, expires May 30 10:48:38 2020 GMT (AddTrust\_External\_Root.crt)
- AffirmTrust Commercial, expires Dec 31 14:06:06 2030 GMT (AffirmTrust\_Commercial.crt)
- AffirmTrust Networking, expires Dec 31 14:08:24 2030 GMT (AffirmTrust\_Networking.crt)
- AffirmTrust Premium, expires Dec 31 14:10:36 2040 GMT (AffirmTrust\_Premium.crt)
- AffirmTrust Premium ECC, expires Dec 31 14:20:24 2040 GMT (AffirmTrust\_Premium\_ECC.crt)
- Amazon Root CA 1, expires Jan 17 00:00:00 2038 GMT (Amazon\_Root\_CA\_1.crt)
- Amazon Root CA 2, expires May 26 00:00:00 2040 GMT (Amazon\_Root\_CA\_2.crt)
- Amazon Root CA 3, expires May 26 00:00:00 2040 GMT (Amazon\_Root\_CA\_3.crt)
- Amazon Root CA 4, expires May 26 00:00:00 2040 GMT (Amazon\_Root\_CA\_4.crt)
- Atos TrustedRoot 2011, expires Dec 31 23:59:59 2030 GMT (Atos\_TrustedRoot\_2011.crt)
- Autoridad de Certificacion Firmaprofesional CIF A62634068, expires Dec 31 08:38:15 2030 GMT (Autoridad\_de\_Certificacion\_Firmaprofesional\_CIF\_A62634068.crt)
- Baltimore CyberTrust Root, expires May 12 23:59:00 2025 GMT (Baltimore\_CyberTrust\_Root.crt)
- Buypass Class 2 Root CA, expires Oct 26 08:38:03 2040 GMT (Buypass\_Class\_2\_Root\_CA.crt)
- Buypass Class 3 Root CA, expires Oct 26 08:28:58 2040 GMT (Buypass\_Class\_3\_Root\_CA.crt)
- CA Disig Root R2, expires Jul 19 09:15:30 2042 GMT (CA\_Disig\_Root\_R2.crt)
- CFCA EV ROOT, expires Dec 31 03:07:01 2029 GMT (CFCA\_EV\_ROOT.crt)
- COMODO Certification Authority, expires Dec 31 23:59:59 2029 GMT (COMODO\_Certification\_Authority.crt)
- COMODO ECC Certification Authority, expires Jan 18 23:59:59 2038 GMT (COMODO\_ECC\_Certification\_Authority.crt)
- COMODO RSA Certification Authority, expires Jan 18 23:59:59 2038 GMT (COMODO\_RSA\_Certification\_Authority.crt)
- Certigna, expires Jun 29 15:13:05 2027 GMT (Certigna.crt)
- Certigna Root CA, expires Oct 1 08:32:27 2033 GMT (Certigna\_Root\_CA.crt)
- Certinomis - Root CA, expires Oct 21 09:17:18 2033 GMT (Certinomis\_-\_Root\_CA.crt)
- Class 2 Primary CA, expires Jul 6 23:59:59 2019 GMT (Certplus\_Class\_2\_Primary\_CA.crt)
- Certum Trusted Network CA, expires Dec 31 12:07:37 2029 GMT (Certum\_Trusted\_Network\_CA.crt)
- Certum Trusted Network CA 2, expires Oct 6 08:39:56 2046 GMT (Certum\_Trusted\_Network\_CA\_2.crt)
- Chambers of Commerce Root - 2008, expires Jul 31 12:29:50 2038 GMT (Chambers\_of\_Commerce\_Root\_-\_2008.crt)
- AAA Certificate Services, expires Dec 31 23:59:59 2028 GMT (Comodo\_AAA\_Services\_root.crt)
- Cybertrust Global Root, expires Dec 15 08:00:00 2021 GMT (Cybertrust\_Global\_Root.crt)
- D-TRUST Root Class 3 CA 2 2009, expires Nov 5 08:35:58 2029 GMT (D-TRUST\_Root\_Class\_3\_CA\_2\_2009.crt)
- D-TRUST Root Class 3 CA 2 EV 2009, expires Nov 5 08:50:46 2029 GMT (D-TRUST\_Root\_Class\_3\_CA\_2\_EV\_2009.crt)
- DST Root CA X3, expires Sep 30 14:01:15 2021 GMT (DST\_Root\_CA\_X3.crt)
- Deutsche Telekom Root CA 2, expires Jul 9 23:59:00 2019 GMT (Deutsche\_Telekom\_Root\_CA\_2.crt)
- DigiCert Global Root CA, expires Nov 10 00:00:00 2031 GMT (DigiCertGlobalRootCA.pem)
- DigiCert Assured ID Root CA, expires Nov 10 00:00:00 2031 GMT (DigiCert\_Assured\_ID\_Root\_CA.crt)



- DigiCert Assured ID Root G2, expires Jan 15 12:00:00 2038 GMT (DigiCert\_Assured\_ID\_Root\_G2.crt)
- DigiCert Assured ID Root G3, expires Jan 15 12:00:00 2038 GMT (DigiCert\_Assured\_ID\_Root\_G3.crt)
- DigiCert Global Root CA, expires Nov 10 00:00:00 2031 GMT (DigiCert\_Global\_Root\_CA.crt)
- DigiCert Global Root G2, expires Jan 15 12:00:00 2038 GMT (DigiCert\_Global\_Root\_G2.crt)
- DigiCert Global Root G3, expires Jan 15 12:00:00 2038 GMT (DigiCert\_Global\_Root\_G3.crt)
- DigiCert High Assurance EV Root CA, expires Nov 10 00:00:00 2031 GMT (DigiCert\_High\_Assurance\_EV\_Root\_CA.crt)
- DigiCert Trusted Root G4, expires Jan 15 12:00:00 2038 GMT (DigiCert\_Trusted\_Root\_G4.crt)
- E-Tugra Certification Authority, expires Mar 3 12:09:48 2023 GMT (E-Tugra\_Certification\_Authority.crt)
- EC-ACC, expires Jan 7 22:59:59 2031 GMT (EC-ACC.crt)
- EE Certification Centre Root CA, expires Dec 17 23:59:59 2030 GMT (EE\_Certification\_Centre\_Root\_CA.crt)
- [Entrust.net](#)<sup>436</sup> Certification Authority (2048), expires Jul 24 14:15:12 2029 GMT  
(Entrust.net\_Premium\_2048\_Secure\_Server\_CA.crt)
- Entrust Root Certification Authority, expires Nov 27 20:53:42 2026 GMT (Entrust\_Root\_Certification\_Authority.crt)
- Entrust Root Certification Authority - EC1, expires Dec 18 15:55:36 2037 GMT  
(Entrust\_Root\_Certification\_Authority\_-\_EC1.crt)
- Entrust Root Certification Authority - G2, expires Dec 7 17:55:54 2030 GMT (Entrust\_Root\_Certification\_Authority\_-\_G2.crt)
- GDCA TrustAUTH R5 ROOT, expires Dec 31 15:59:59 2040 GMT (GDCA\_TrustAUTH\_R5\_ROOT.crt)
- GTS Root R1, expires Jun 22 00:00:00 2036 GMT (GTS\_Root\_R1.crt)
- GTS Root R2, expires Jun 22 00:00:00 2036 GMT (GTS\_Root\_R2.crt)
- GTS Root R3, expires Jun 22 00:00:00 2036 GMT (GTS\_Root\_R3.crt)
- GTS Root R4, expires Jun 22 00:00:00 2036 GMT (GTS\_Root\_R4.crt)
- GeoTrust Global CA, expires May 21 04:00:00 2022 GMT (GeoTrust\_Global\_CA.crt)
- GeoTrust Primary Certification Authority, expires Jul 16 23:59:59 2036 GMT  
(GeoTrust\_Primary\_Certification\_Authority.crt)
- GeoTrust Primary Certification Authority - G2, expires Jan 18 23:59:59 2038 GMT  
(GeoTrust\_Primary\_Certification\_Authority\_-\_G2.crt)
- GeoTrust Primary Certification Authority - G3, expires Dec 1 23:59:59 2037 GMT  
(GeoTrust\_Primary\_Certification\_Authority\_-\_G3.crt)
- GeoTrust Universal CA, expires Mar 4 05:00:00 2029 GMT (GeoTrust\_Universal\_CA.crt)
- GeoTrust Universal CA 2, expires Mar 4 05:00:00 2029 GMT (GeoTrust\_Universal\_CA\_2.crt)
- GlobalSign, expires Jan 19 03:14:07 2038 GMT (GlobalSign\_ECC\_Root\_CA\_-\_R4.crt)
- GlobalSign, expires Jan 19 03:14:07 2038 GMT (GlobalSign\_ECC\_Root\_CA\_-\_R5.crt)
- GlobalSign Root CA, expires Jan 28 12:00:00 2028 GMT (GlobalSign\_Root\_CA.crt)
- GlobalSign, expires Dec 15 08:00:00 2021 GMT (GlobalSign\_Root\_CA\_-\_R2.crt)
- GlobalSign, expires Mar 18 10:00:00 2029 GMT (GlobalSign\_Root\_CA\_-\_R3.crt)
- GlobalSign, expires Dec 10 00:00:00 2034 GMT (GlobalSign\_Root\_CA\_-\_R6.crt)
- Global Chambersign Root - 2008, expires Jul 31 12:31:40 2038 GMT (Global\_Chambersign\_Root\_-\_2008.crt)
- Go Daddy Class 2 Certification Authority, expires Jun 29 17:06:20 2034 GMT (Go\_Daddy\_Class\_2\_CA.crt)
- Go Daddy Root Certificate Authority - G2, expires Dec 31 23:59:59 2037 GMT  
(Go\_Daddy\_Root\_Certificate\_Authority\_-\_G2.crt)
- Hellenic Academic and Research Institutions ECC RootCA 2015, expires Jun 30 10:37:12 2040 GMT  
(Hellenic\_Academic\_and\_Research\_Institutions\_ECC\_RootCA\_2015.crt)
- Hellenic Academic and Research Institutions RootCA 2011, expires Dec 1 13:49:52 2031 GMT

---

<sup>436</sup> <http://Entrust.net>



(Hellenic\_Academic\_and\_Research\_Institutions\_RootCA\_2011.crt)

- Hellenic Academic and Research Institutions RootCA 2015, expires Jun 30 10:11:21 2040 GMT

(Hellenic\_Academic\_and\_Research\_Institutions\_RootCA\_2015.crt)

- Hongkong Post Root CA 1, expires May 15 04:52:29 2023 GMT (Hongkong\_Post\_Root\_CA\_1.crt)

- ISRG Root X1, expires Jun 4 11:04:38 2035 GMT (ISRG\_Root\_X1.crt)

- IdenTrust Commercial Root CA 1, expires Jan 16 18:12:23 2034 GMT (IdenTrust\_Commercial\_Root\_CA\_1.crt)

- IdenTrust Public Sector Root CA 1, expires Jan 16 17:53:32 2034 GMT (IdenTrust\_Public\_Sector\_Root\_CA\_1.crt)

- Imprivata Embedded Code Signing CA, expires Sep 7 16:20:00 2033 GMT (Imprivata.crt)

- [Izenpe.com](http://Izenpe.com)<sup>437</sup>, expires Dec 13 08:27:25 2037 GMT ([Izenpe.com](http://Izenpe.com)<sup>438</sup>.crt)

- LuxTrust Global Root 2, expires Mar 5 13:21:57 2035 GMT (LuxTrust\_Global\_Root\_2.crt)

- Microsec e-Szigno Root CA 2009, expires Dec 30 11:30:18 2029 GMT (Microsec\_e-Szigno\_Root\_CA\_2009.crt)

- NetLock Arany (Class Gold) Főtanúsítvány, expires Dec 6 15:08:21 2028 GMT

(NetLock\_Arany\_=Class\_Gold=\_Főtanúsítvány.crt)

- Network Solutions Certificate Authority, expires Dec 31 23:59:59 2029 GMT

(Network\_Solutions\_Certificate\_Authority.crt)

- OISTE WISEKey Global Root GA CA, expires Dec 11 16:09:51 2037 GMT (OISTE\_WISEKey\_Global\_Root\_GA\_CA.crt)

- OISTE WISEKey Global Root GB CA, expires Dec 1 15:10:31 2039 GMT (OISTE\_WISEKey\_Global\_Root\_GB\_CA.crt)

- OISTE WISEKey Global Root GC CA, expires May 9 09:58:33 2042 GMT (OISTE\_WISEKey\_Global\_Root\_GC\_CA.crt)

- QuoVadis Root Certification Authority, expires Mar 17 18:33:33 2021 GMT (QuoVadis\_Root\_CA.crt)

- QuoVadis Root CA 1 G3, expires Jan 12 17:27:44 2042 GMT (QuoVadis\_Root\_CA\_1\_G3.crt)

- QuoVadis Root CA 2, expires Nov 24 18:23:33 2031 GMT (QuoVadis\_Root\_CA\_2.crt)

- QuoVadis Root CA 2 G3, expires Jan 12 18:59:32 2042 GMT (QuoVadis\_Root\_CA\_2\_G3.crt)

- QuoVadis Root CA 3, expires Nov 24 19:06:44 2031 GMT (QuoVadis\_Root\_CA\_3.crt)

- QuoVadis Root CA 3 G3, expires Jan 12 20:26:32 2042 GMT (QuoVadis\_Root\_CA\_3\_G3.crt)

- [SSL.com](http://SSL.com)<sup>439</sup> EV Root Certification Authority ECC, expires Feb 12 18:15:23 2041 GMT

(SSL.com\_EV\_Root\_Certification\_Authority\_ECC.crt)

- [SSL.com](http://SSL.com)<sup>440</sup> EV Root Certification Authority RSA R2, expires May 30 18:14:37 2042 GMT

(SSL.com\_EV\_Root\_Certification\_Authority\_RSA\_R2.crt)

- [SSL.com](http://SSL.com)<sup>441</sup> Root Certification Authority ECC, expires Feb 12 18:14:03 2041 GMT

(SSL.com\_Root\_Certification\_Authority\_ECC.crt)

- [SSL.com](http://SSL.com)<sup>442</sup> Root Certification Authority RSA, expires Feb 12 17:39:39 2041 GMT

(SSL.com\_Root\_Certification\_Authority\_RSA.crt)

- SZAFIR ROOT CA2, expires Oct 19 07:43:30 2035 GMT (SZAFIR\_ROOT\_CA2.crt)

- SecureSign RootCA11, expires Apr 8 04:56:47 2029 GMT (SecureSign\_RootCA11.crt)

- SecureTrust CA, expires Dec 31 19:40:55 2029 GMT (SecureTrust\_CA.crt)

- Secure Global CA, expires Dec 31 19:52:06 2029 GMT (Secure\_Global\_CA.crt)

- Security Communication RootCA2, expires May 29 05:00:39 2029 GMT (Security\_Communication\_RootCA2.crt)

- Security Communication RootCA1, expires Sep 30 04:20:49 2023 GMT (Security\_Communication\_Root\_CA.crt)

- Sonera Class2 CA, expires Apr 6 07:29:40 2021 GMT (Sonera\_Class\_2\_Root\_CA.crt)

- Staat der Nederlanden EV Root CA, expires Dec 8 11:10:28 2022 GMT (Staat\_der\_Nederlanden\_EV\_Root\_CA.crt)

- Staat der Nederlanden Root CA - G2, expires Mar 25 11:03:10 2020 GMT (Staat\_der\_Nederlanden\_Root\_CA\_-G2.crt)

- Staat der Nederlanden Root CA - G3, expires Nov 13 23:00:00 2028 GMT (Staat\_der\_Nederlanden\_Root\_CA\_-G3.crt)

- Starfield Class 2 Certification Authority, expires Jun 29 17:39:16 2034 GMT (Starfield\_Class\_2\_CA.crt)

---

<sup>437</sup> <http://Izenpe.com>

<sup>438</sup> <http://Izenpe.com>

<sup>439</sup> <http://SSL.com>

<sup>440</sup> <http://SSL.com>

<sup>441</sup> <http://SSL.com>

<sup>442</sup> <http://SSL.com>



- Starfield Root Certificate Authority - G2, expires Dec 31 23:59:59 2037 GMT (Starfield\_Root\_Certificate\_Authority\_-\_G2.crt)
- Starfield Services Root Certificate Authority - G2, expires Dec 31 23:59:59 2037 GMT (Starfield\_Services\_Root\_Certificate\_Authority\_-\_G2.crt)
- SwissSign Gold CA - G2, expires Oct 25 08:30:35 2036 GMT (SwissSign\_Gold\_CA\_-\_G2.crt)
- SwissSign Silver CA - G2, expires Oct 25 08:32:46 2036 GMT (SwissSign\_Silver\_CA\_-\_G2.crt)
- T-TelSec GlobalRoot Class 2, expires Oct 1 23:59:59 2033 GMT (T-TelSec\_GlobalRoot\_Class\_2.crt)
- T-TelSec GlobalRoot Class 3, expires Oct 1 23:59:59 2033 GMT (T-TelSec\_GlobalRoot\_Class\_3.crt)
- TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1, expires Oct 25 08:25:55 2043 GMT (TUBITAK\_Kamu\_SM\_SSL\_Kok\_Sertifikasi\_-\_Surum\_1.crt)
- TWCA Global Root CA, expires Dec 31 15:59:59 2030 GMT (TWCA\_Global\_Root\_CA.crt)
- TWCA Root Certification Authority, expires Dec 31 15:59:59 2030 GMT (TWCA\_Root\_Certification\_Authority.crt)
- Government Root Certification Authority, expires Dec 5 13:23:33 2032 GMT (Taiwan\_GRCA.crt)
- TeliaSonera Root CA v1, expires Oct 18 12:00:50 2032 GMT (TeliaSonera\_Root\_CA\_v1.crt)
- TrustCor ECA-1, expires Dec 31 17:28:07 2029 GMT (TrustCor\_ECA-1.crt)
- TrustCor RootCert CA-1, expires Dec 31 17:23:16 2029 GMT (TrustCor\_RootCert\_CA-1.crt)
- TrustCor RootCert CA-2, expires Dec 31 17:26:39 2034 GMT (TrustCor\_RootCert\_CA-2.crt)
- Trustis FPS Root CA, expires Jan 21 11:36:54 2024 GMT (Trustis\_FPS\_Root\_CA.crt)
- UCA Extended Validation Root, expires Dec 31 00:00:00 2038 GMT (UCA\_Extended\_Validation\_Root.crt)
- UCA Global G2 Root, expires Dec 31 00:00:00 2040 GMT (UCA\_Global\_G2\_Root.crt)
- USERTrust ECC Certification Authority, expires Jan 18 23:59:59 2038 GMT (USERTrust\_ECC\_Certification\_Authority.crt)
- USERTrust RSA Certification Authority, expires Jan 18 23:59:59 2038 GMT (USERTrust\_RSA\_Certification\_Authority.crt)
- VeriSign Class 3 Public Primary Certification Authority - G4, expires Jan 18 23:59:59 2038 GMT (VeriSign\_Class\_3\_Public\_Primary\_Certification\_Authority\_-\_G4.crt)
- VeriSign Class 3 Public Primary Certification Authority - G5, expires Jul 16 23:59:59 2036 GMT (VeriSign\_Class\_3\_Public\_Primary\_Certification\_Authority\_-\_G5.crt)
- VeriSign Universal Root Certification Authority, expires Dec 1 23:59:59 2037 GMT (VeriSign\_Universal\_Root\_Certification\_Authority.crt)
- VeriSign Class 3 Public Primary Certification Authority - G3, expires Jul 16 23:59:59 2036 GMT (Verisign\_Class\_3\_Public\_Primary\_Certification\_Authority\_-\_G3.crt)
- XRamp Global Certification Authority, expires Jan 1 05:37:19 2035 GMT (XRamp\_Global\_CA\_Root.crt)
- certSIGN ROOT CA, expires Jul 4 17:20:04 2031 GMT (certSIGN\_ROOT\_CA.crt)
- ePKI Root Certification Authority, expires Dec 20 02:31:27 2034 GMT (ePKI\_Root\_Certification\_Authority.crt)
- thawte Primary Root CA, expires Jul 16 23:59:59 2036 GMT (thawte\_Primary\_Root\_CA.crt)
- thawte Primary Root CA - G2, expires Jan 18 23:59:59 2038 GMT (thawte\_Primary\_Root\_CA\_-\_G2.crt)
- thawte Primary Root CA - G3, expires Dec 1 23:59:59 2037 GMT (thawte\_Primary\_Root\_CA\_-\_G3.crt)

## 7.14.2 IGEL OS Creator (OSC)

### Supported Devices

|         |           |
|---------|-----------|
| UD2-LX: | UD2-LX 40 |
|         | UD2-LX 50 |



|         |                              |
|---------|------------------------------|
| UD3-LX: | UD3-LX 51<br>UD3-LX 50       |
| UD5-LX: | UD5-LX 50                    |
| UD6-LX: | UD6-LX 51                    |
| UD7-LX: | UD7-LX 10                    |
| UD9-LX: | UD9-LX Touch 41<br>UD9-LX 40 |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>443</sup>.

- [Component Versions 11.02.100](#)(see page 1815)
- [New Features 11.02.100](#)(see page 1816)

## Component Versions 11.02.100

- **Clients**

| Product  | Version   |
|----------|-----------|
| Zulu JRE | 8.40.0.25 |

- **Smartcard**

|                             |               |
|-----------------------------|---------------|
| Reader Driver MUSCLE CCID   | 1.4.30-1igel3 |
| Resource Manager PC/SC Lite | 1.8.23-1igel1 |

- **System Components**

|                         |                    |
|-------------------------|--------------------|
| OpenSSL                 | 1.0.2g-1ubuntu4.15 |
| Bluetooth stack (bluez) | 5.50-0ubuntu1igel5 |
| MESA OpenGL stack       | 19.0.8-1igel73     |
| VDPAU Library version   | 1.1.1-3ubuntu1     |

<sup>443</sup> <https://kb.igel.com/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html>



|                                         |                               |
|-----------------------------------------|-------------------------------|
| Graphics Driver INTEL                   | 2.99.917+git20190724-igel907  |
| Graphics Driver ATI/RADEON              | 19.0.1-2igel890               |
| Graphics Driver ATI/AMDGPU              | 19.0.1-4igel894               |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867               |
| Graphics Driver Nvidia                  | 418.56-0ubuntu1               |
| Graphics Driver Vboxvideo               | 1.0.0-igel798                 |
| Graphics Driver VMware                  | 13.3.0-2igel857               |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1igel775          |
| Graphics Driver FBDEV                   | 0.5.0-1igel819                |
| Graphics Driver VESA                    | 2.4.0-1igel855                |
| Input Driver Evdev                      | 2.10.6-1igel888               |
| Input Driver Elographics                | 1.4.1-1build5igel633          |
| Input Driver Synaptics                  | 1.9.1-1ubuntu1igel866         |
| Input Driver VMMouse                    | 13.1.0-1ubuntu2igel635        |
| Input Driver Wacom                      | 0.36.1-0ubuntu2igel888        |
| Kernel                                  | 4.19.65 #mainline-lxos-r2782  |
| Xorg X11 Server                         | 1.19.6-1ubuntu4.3igel910      |
| Lightdm Graphical Login Manager         | 1.18.3-0ubuntu1.1             |
| XFCE4 Window Manager                    | 4.12.3-1ubuntu2igel675        |
| ISC DHCP Client                         | 4.3.3-5ubuntu12.10igel7       |
| WebKit2Gtk                              | 2.24.2-0ubuntu0.19.04.1igel18 |
| Python2                                 | 2.7.12                        |
| Python3                                 | 3.5.2                         |

## New Features 11.02.100

### Hardware

- Added hardware support for **Rein Medical Silenio 122CT** and **124CT**.
- Added hardware support for **Advantech POC-W213L** and **POC-W243L**.



- Added hardware support for **ADS-TEC VMT 9000 Serie**.
- Added hardware support for **Fujitsu Esprimo Q957**.
- Added hardware support for **ADS-TEC VMT 9000 Serie**.
- Added hardware support for **LG AiO Cloud Device 38"**.
- Added hardware support for **HP t430**.
- Added hardware support for **HP t420**.

## 7.15 Notes for Release 11.01.130

|                       |            |              |
|-----------------------|------------|--------------|
| <b>Software:</b>      | Version    | 11.01.130    |
| <b>Release Date:</b>  | 2019-07-24 |              |
| <b>Release Notes:</b> | Version    | RN-1101130-1 |
| <b>Last update:</b>   | 2019-07-23 |              |

- Supported Devices 11.01.130(see page 1817)
- Component Versions 11.01.130(see page 1818)
- General Information 11.01.130(see page 1822)
- Known Issues 11.01.130(see page 1822)
- Security Fixes 11.01.130(see page 1823)
- New Features 11.01.130(see page 1824)
- Resolved Issues 11.01.130(see page 1824)

### 7.15.1 Supported Devices 11.01.130

| <b>IGEL devices:</b> |                        |
|----------------------|------------------------|
| UD2-LX:              | UD2-LX 50<br>UD2-LX 40 |
| UD3-LX:              | UD3-LX 51<br>UD3-LX 50 |
| UD5-LX:              | UD5-LX 50              |
| UD6-LX:              | UD6-LX 51              |
| UD7-LX:              | UD7-LX 10              |



|         |                 |
|---------|-----------------|
| UD9-LX: | UD9-LX Touch 41 |
|         | UD9-LX 40       |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>444</sup>.

## 7.15.2 Component Versions 11.01.130

- **Clients**

| Product                                 | Version                 |
|-----------------------------------------|-------------------------|
| Citrix HDX Realtime Media Engine        | 2.8.0-2235              |
| Citrix Receiver                         | 13.10.0.20              |
| Citrix Receiver                         | 13.5.0.10185126         |
| Citrix Workspace App                    | 19.3.0.5                |
| deviceTRUST Citrix Channel              | 19.1.200.2              |
| Evidian AuthMgr                         | 1.5.7116                |
| Evince PDF Viewer                       | 3.18.2-1ubuntu4.3       |
| FabulaTech USB for Remote Desktop       | 5.2.29                  |
| Firefox                                 | 60.8.0                  |
| IBM iAccess Client Solutions            | 1.1.8.1                 |
| IGEL RDP Client                         | 2.2                     |
| Imprivata OneSign ProveID Embedded      |                         |
| deviceTRUST RDP Channel                 | 19.1.200.2              |
| NCP Secure Enterprise Client            | 5.10_rev40552           |
| NX Client                               | 5.3.12                  |
| Open VPN                                | 2.3.10-1ubuntu2.1       |
| Zulu JRE                                | 8.38.0.13               |
| Parallels Client (64 bit)               | 16.5.2.20595            |
| Remote Viewer (Red Hat Virtualization)  | 7.0-igel47              |
| Spice GTK (Red Hat Virtualization)      | 0.35                    |
| Spice Protocol (Red Hat Virtualization) | 0.12.14                 |
| Usbredir (Red Hat Virtualization)       | 0.8.0                   |
| Teradici PCoIP Software Client          | 19.05.4-18.04           |
| ThinLinc Client                         | 4.9.0-5775              |
| ThinPrint Client                        | 7.5.88                  |
| Totem Media Player                      | 2.30.2                  |
| Parole Media Player                     | 1.0.1-0ubuntu1igel16    |
| VNC Viewer                              | 1.8.0+git20180123-igel1 |

<sup>444</sup> <https://kb.igel.com/display/hardware/Third-Party+Devices+Supported+by+IGEL+OS+11>



|                       |                |
|-----------------------|----------------|
| VMware Horizon Client | 5.0.0-12557422 |
| Voip Client Ekiga     | 4.0.1          |

- **Dictation**

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B048     |
| Olympus driver for dictation              | 20180621 |
| Philips Speech Driver                     | 12.6.36  |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.6    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.1.0    |

- **Smartcard**

|                                           |              |
|-------------------------------------------|--------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101      |
| PKCS#11 Library Athena IDProtect          | 623.07       |
| PKCS#11 Library cryptovision sc/interface | 7.1.9.620    |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0    |
| PKCS#11 Library SecMaker NetID            | 6.7.0.23     |
| PKCS#11 Library 90meter                   | 20190522     |
| Reader Driver ACS CCID                    | 1.1.6-1igel1 |
| Reader Driver Gemalto eToken              | 10.0.37-0    |
| Reader Driver HID Global Omnikey          | 4.3.3        |
| Reader Driver Identive CCID               | 5.0.35       |
| Reader Driver Identive eHealth200         | 1.0.5        |



|                                    |                        |
|------------------------------------|------------------------|
| Reader Driver Identive SCRKBC      | 5.0.24                 |
| Reader Driver MUSCLE CCID          | 1.4.30-1igel3          |
| Reader Driver REINER SCT cyberJack | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite        | 1.8.23-1igel1          |
| Cherry USB2LAN Proxy               | 3.0.0.6                |

- **System Components**

|                                         |                              |
|-----------------------------------------|------------------------------|
| OpenSSL                                 | 1.0.2g-1ubuntu4.14           |
| OpenSSH Client                          | 7.2p2-4ubuntu2.7             |
| OpenSSH Server                          | 7.2p2-4ubuntu2.7             |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5           |
| MESA OpenGL stack                       | 18.3.3-1igel57               |
| VAAPI ABI Version                       | 0.40                         |
| VDPAU Library version                   | 1.1.1-3ubuntu1               |
| Graphics Driver INTEL                   | 2.99.917+git20190301-igel870 |
| Graphics Driver ATI/RADEON              | 18.1.0-1igel854              |
| Graphics Driver ATI/AMDGPU              | 18.1.0-1igel853              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.15-2igel775              |
| Graphics Driver Nvidia                  | 410.93-0ubuntu1              |
| Graphics Driver Vboxvideo               | 5.2.18-dfsg-2igel17          |
| Graphics Driver VMware                  | 13.3.0-2igel857              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1igel775         |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |
| Graphics Driver VESA                    | 2.4.0-1igel855               |
| Input Driver Evdev                      | 2.10.5-1ubuntu1igel750       |
| Input Driver Elographics                | 1.4.1-1build5igel633         |



|                                 |                              |
|---------------------------------|------------------------------|
| Input Driver eGalax             | 2.5.5814                     |
| Input Driver Synaptics          | 1.9.0-1ubuntu1igel748        |
| Input Driver VMMouse            | 13.1.0-1ubuntu2igel635       |
| Input Driver Wacom              | 0.36.1-0ubuntu1igel813       |
| Kernel                          | 4.18.20 #mainline-udos-r2755 |
| Xorg X11 Server                 | 1.19.6-1ubuntu4.2igel842     |
| Xorg Xephyr                     | 1.19.6-1ubuntu4.2igel842     |
| CUPS Printing Daemon            | 2.1.3-4ubuntu0.7igel23       |
| PrinterLogic                    | 18.2.1.128                   |
| Lightdm Graphical Login Manager | 1.18.3-0ubuntu1.1            |
| XFCE4 Window Manager            | 4.12.3-1ubuntu2igel675       |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7      |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.2igel58 |
| ModemManager                    | 1.6.8-2ubuntu1igel2          |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.1           |
| GStreamer 1.x                   | 1.14.4-1ubuntu1igel203       |
| Python2                         | 2.7.12                       |
| Python3                         | 3.5.2                        |

- **Features with Limited IGEL Support**

Mobile Device Access USB

VPN OpenConnect

Scanner support

VirtualBox

- **Features with Limited Functionality**

Cisco JVDI Client



### 7.15.3 General Information 11.01.130

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- Ericom PowerTerm
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver.

### 7.15.4 Known Issues 11.01.130

#### Citrix

- With activated DRI3 and AMD GPU, Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H264, MPEG1 and MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.  
As a workaround, insert the smartcard before starting StoreFront login.
- When using **Citrix Workspace App 19.03** in combination with **Philips Speech** driver, the session occasionally terminates improperly at logout and hangs.  
As a workaround, the usage of Citrix Receiver 13.10 is recommended when Philips Speech driver is needed.
- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" > "For the entire screen".
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264 acceleration plugin**, the following registry key must be enabled:  
**More...**

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Range     | enabled / <u>disabled</u>                                        |



This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

#### VMware Horizon

- **External drives** mounted already before connection **do not appear in the remote desktop**.  
Workaround: mapping the directory / media as a drive on desktop. The external devices will show up within the media drive then.
- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off.  
In the IGEL Setup client, **drive mapping** can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping**.  
It is also recommended to disable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection entirely** or at least to **deny storage devices** by adding a filter to the USB class rules.  
Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Enable **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**. The **Number of storage hotplug devices** has to be set to at least 1.

#### Parallels Client

- **Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** once with disabled FIPS support.

#### Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign smartcards**.

#### Multimedia

- Multimedia **redirection with GStreamer** could fail with the **Nouveau GPU driver**.

#### Base system

- On **NVIDIA GPU drivers**, the reported **resolutions of a display** may contain unsupported resolutions. When any of those are configured, there are visual bugs (e.g. the desktop does not render properly).

## 7.15.5 Security Fixes 11.01.130

#### Firefox

- Updated **Firefox** browser to version **60.8.0 ESR**.
- Fixed **mfsa2019-22** security issues:  
[More...](#)



CVE-2019-9811, CVE-2019-11711, CVE-2019-11712, CVE-2019-11713, CVE-2019-11729, CVE-2019-11715, CVE-2019-11717, CVE-2019-11719, CVE-2019-11730 and CVE-2019-11709.

- Fixed **mfsa2019-19** security issue CVE-2019-11708.
- Fixed **mfsa2019-18** security issue CVE-2019-11707.
- Fixed **mfsa2019-08** security issues:  
[More...](#)

CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2018-18506 and CVE-2019-9788.

- Fixed **mfsa2019-05** security issues CVE-2018-18356 and CVE-2019-5785.
- Fixed **mfsa2019-02** security issues CVE-2018-18500, CVE-2018-18505 and CVE-2018-18501.

## 7.15.6 New Features 11.01.130

Citrix

- Added support for **Citrix Workspace Launcher** functionality as described at <https://support.citrix.com/article/CTX237727>.

Base system

- Replaced **timesyncd** with **chrony NTP**.  
A new registry key:  
[More...](#)

|           |                                        |
|-----------|----------------------------------------|
| Parameter | Use NTP Servers from DNS SRV record    |
| Registry  | system.time.ntp_use_dnssrv_timeservers |
| Value     | <u>enabled</u> / <u>disabled</u>       |

Evidian

- Integrated **Evidian AuthMgr** version **1.5.7116**.

## 7.15.7 Resolved Issues 11.01.130

VMware Horizon

- Added a possibility to use the **rollback variant of the Horizon Client**.  
[More...](#)

|           |                                         |
|-----------|-----------------------------------------|
| Parameter | Allow rollback to former client variant |
| Registry  | vmware.view.allow-client-rollback       |
| Value     | <u>enabled</u> / <u>disabled</u>        |

Base system

- Fixed **NTP synchronization problems** with changing the NTP client from **timesyncd** to **chrony**.
- Fixed **USB printer aliases**.



## X11 system

- Fixed **screen corruption with DPMS** and enabled **composite manager**.
- Added consideration of **hardware limits** for choosing **automatic resolution in Xorg config** (currently only for IGEL hardware).

## Hardware

- Fixed **black screen** issue with some monitors and 2560x1440 resolution (occurred on **UD2 LX50** and **other Intel GPUs**).

## 7.16 Notes for Release 11.01.120

|                       |            |              |
|-----------------------|------------|--------------|
| <b>Software:</b>      | Version    | 11.01.120    |
| <b>Release Date:</b>  | 2019-07-05 |              |
| <b>Release Notes:</b> | Version    | RN-1101120-1 |
| <b>Last update:</b>   | 2019-07-05 |              |

- Supported Devices 11.01.120(see page 1825)
- Component Versions 11.01.120(see page 1826)
- General Information 11.01.120(see page 1830)
- Security Fixes 11.01.120(see page 1830)
- New Features 11.01.120(see page 1830)
- Resolved Issues 11.01.120(see page 1831)

## 7.16.1 Supported Devices 11.01.120

| <b>IGEL devices:</b> |                        |
|----------------------|------------------------|
| UD2-LX:              | UD2-LX 50<br>UD2-LX 40 |
| UD3-LX:              | UD3-LX 51<br>UD3-LX 50 |
| UD5-LX:              | UD5-LX 50              |
| UD6-LX:              | UD6-LX 51              |



|         |                 |
|---------|-----------------|
| UD7-LX: | UD7-LX 10       |
| UD9-LX: | UD9-LX Touch 41 |
|         | UD9-LX 40       |

See also [Third-Party Devices Supported by IGEL OS 11](#)<sup>445</sup>.

## 7.16.2 Component Versions 11.01.120

- **Clients**

| Product                                 | Version           |
|-----------------------------------------|-------------------|
| Citrix HDX Realtime Media Engine        | 2.8.0-2235        |
| Citrix Receiver                         | 13.10.0.20        |
| Citrix Receiver                         | 13.5.0.10185126   |
| Citrix Workspace App                    | 19.3.0.5          |
| deviceTRUST Citrix Channel              | 19.1.200.2        |
| Evidian AuthMgr                         | 1.5.6840          |
| Evince PDF Viewer                       | 3.18.2-1ubuntu4.3 |
| FabulaTech USB for Remote Desktop       | 5.2.29            |
| Firefox                                 | 60.7.2            |
| IBM iAccess Client Solutions            | 1.1.8.1           |
| IGEL RDP Client                         | 2.2               |
| Imprivata OneSign ProveID Embedded      |                   |
| deviceTRUST RDP Channel                 | 19.1.200.2        |
| NCP Secure Enterprise Client            | 5.10_rev40552     |
| NX Client                               | 5.3.12            |
| Open VPN                                | 2.3.10-1ubuntu2.1 |
| Zulu JRE                                | 8.38.0.13         |
| Parallels Client (64 bit)               | 16.5.2.20595      |
| Remote Viewer (Red Hat Virtualization)  | 7.0-igel47        |
| Spice GTK (Red Hat Virtualization)      | 0.35              |
| Spice Protocol (Red Hat Virtualization) | 0.12.14           |
| Usbredir (Red Hat Virtualization)       | 0.8.0             |
| Teradici PCoIP Software Client          | 19.05.4-18.04     |
| ThinLinc Client                         | 4.9.0-5775        |
| ThinPrint Client                        | 7.5.88            |
| Totem Media Player                      | 2.30.2            |

<sup>445</sup> <https://kb.igel.com/display/hardware/Third-Party+Devices+Supported+by+IGEL+OS+11>



|                       |                         |
|-----------------------|-------------------------|
| Parole Media Player   | 1.0.1-0ubuntu1igel16    |
| VNC Viewer            | 1.8.0+git20180123-igel1 |
| VMware Horizon Client | 5.0.0-12557422          |
| Voip Client Ekiga     | 4.0.1                   |

- **Dictation**

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B048     |
| Olympus driver for dictation              | 20180621 |
| Philips Speech Driver                     | 12.6.36  |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.6    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.1.0    |

- **Smartcard**

|                                           |              |
|-------------------------------------------|--------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101      |
| PKCS#11 Library Athena IDProtect          | 623.07       |
| PKCS#11 Library cryptovision sc/interface | 7.1.9.620    |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0    |
| PKCS#11 Library SecMaker NetID            | 6.7.0.23     |
| PKCS#11 Library 90meter                   | 20190522     |
| Reader Driver ACS CCID                    | 1.1.6-1igel1 |
| Reader Driver Gemalto eToken              | 10.0.37-0    |
| Reader Driver HID Global Omnikey          | 4.3.3        |



|                                    |                        |
|------------------------------------|------------------------|
| Reader Driver Identive CCID        | 5.0.35                 |
| Reader Driver Identive eHealth200  | 1.0.5                  |
| Reader Driver Identive SCRKBC      | 5.0.24                 |
| Reader Driver MUSCLE CCID          | 1.4.30-1igel3          |
| Reader Driver REINER SCT cyberJack | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite        | 1.8.23-1igel1          |
| Cherry USB2LAN Proxy               | 3.0.0.6                |

- **System Components**

|                                         |                              |
|-----------------------------------------|------------------------------|
| OpenSSL                                 | 1.0.2g-1ubuntu4.14           |
| OpenSSH Client                          | 7.2p2-4ubuntu2.7             |
| OpenSSH Server                          | 7.2p2-4ubuntu2.7             |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5           |
| MESA OpenGL stack                       | 18.3.3-1igel57               |
| VAAPI ABI Version                       | 0.40                         |
| VDPAU Library version                   | 1.1.1-3ubuntu1               |
| Graphics Driver INTEL                   | 2.99.917+git20190301-igel870 |
| Graphics Driver ATI/RADEON              | 18.1.0-1igel854              |
| Graphics Driver ATI/AMDGPU              | 18.1.0-1igel853              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.15-2igel775              |
| Graphics Driver Nvidia                  | 410.93-0ubuntu1              |
| Graphics Driver Vboxvideo               | 5.2.18-dfsg-2igel17          |
| Graphics Driver VMware                  | 13.3.0-2igel857              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1igel775         |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |
| Graphics Driver VESA                    | 2.4.0-1igel855               |



|                                 |                              |
|---------------------------------|------------------------------|
| Input Driver Evdev              | 2.10.5-1ubuntu1igel750       |
| Input Driver Elographics        | 1.4.1-1build5igel633         |
| Input Driver eGalax             | 2.5.5814                     |
| Input Driver Synaptics          | 1.9.0-1ubuntu1igel748        |
| Input Driver VMMouse            | 13.1.0-1ubuntu2igel635       |
| Input Driver Wacom              | 0.36.1-0ubuntu1igel813       |
| Kernel                          | 4.18.20 #mainline-udos-r2755 |
| Xorg X11 Server                 | 1.19.6-1ubuntu4.2igel842     |
| Xorg Xephyr                     | 1.19.6-1ubuntu4.2igel842     |
| CUPS Printing Daemon            | 2.1.3-4ubuntu0.7igel23       |
| PrinterLogic                    | 18.2.1.128                   |
| Lightdm Graphical Login Manager | 1.18.3-0ubuntu1.1            |
| XFCE4 Window Manager            | 4.12.3-1ubuntu2igel675       |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7      |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.2igel58 |
| ModemManager                    | 1.6.8-2ubuntu1igel2          |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.1           |
| GStreamer 1.x                   | 1.14.4-1ubuntu1igel203       |
| Python2                         | 2.7.12                       |
| Python3                         | 3.5.2                        |

- **Features with Limited IGEL Support**

|                          |
|--------------------------|
| Mobile Device Access USB |
| VPN OpenConnect          |
| Scanner support          |
| VirtualBox               |



- **Features with Limited Functionality**

|                   |      |
|-------------------|------|
| Cisco JVDI Client | 12.1 |
|-------------------|------|

### 7.16.3 General Information 11.01.120

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- Ericom PowerTerm
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

### 7.16.4 Security Fixes 11.01.120

Firefox

- Updated Firefox browser to version **60.7.2 ESR**.
- Fixed **mfsa2019-19** security issue CVE-2019-11708.
- Fixed **mfsa2019-18** security issue CVE-2019-11707.
- Fixed **mfsa2019-08** security issues.

[More...](#)

CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793,  
CVE-2019-9795, CVE-2019-9796, CVE-2018-18506, CVE-2019-9788.

- Fixed **mfsa2019-05** security issues CVE-2018-18356 and CVE-2019-5785.
- Fixed **mfsa2019-02** security issues CVE-2018-18500, CVE-2018-18505 and CVE-2018-18501.

Base system

- Fixed kernel TCP vulnerabilities **CVE-2019-11477**: SACK Panic, **CVE-2019-11478**: SACK Slowness and **CVE-2019-11479**: Excess Resource Consumption Due to Low MSS Values.
- Changed **minimally allowed MSS size** to '**1000**' to prevent possible Denial-of-Service attacks.

### 7.16.5 New Features 11.01.120

Citrix

- Added support for **Citrix Workspace Launcher** functionality as described at <https://support.citrix.com/article/CTX237727>.



## Teradici PCoIP Client

- Updated **Teradici PCoIP Client** to version **19.05.4**.

## 7.16.6 Resolved Issues 11.01.120

## Citrix

- SpaceMouse: Improved **USB handling**.
- Citrix Workspace App 19.03: Improved **USB redirection handling**.

## Network

- Fixed: The **second Ethernet interface** did not get configured when the first one was disabled.

## Base system

- Fixed **license expiry warning** at boot. Before this fix, in some cases the warning wrongly appeared at every boot.
- Fixed: **System logout** waits for Citrix logout now.

## Appliance Mode

- Fixed: **In-session control bar** could not be deactivated in **Citrix Self-Service appliance mode**.

## X11 system

- Fixed: Problems with **internal graphic cards** and **Nvidia graphic cards**.

## RD Web Access

- Fixed not starting **RDP Remote Applications**.

## Hardware

- Fixed **not working network** on Beckhoff CB3163, CB6263 and CB6363 systems.
- Fixed **not working network** on Lex 3I380D.
- Fixed **black screen** issue with some monitors and 2560x1440 resolution (occurred on UD2 LX50).
- Added possibility to **change** some **DRM settings** and limit the **DisplayPort lane bandwidth** on Intel devices.
- Added **new registry keys**:

[More...](#)

|           |                                                   |
|-----------|---------------------------------------------------|
| Parameter | Use best graphic mode for all screens on console. |
| Registry  | x.drivers.kms.best_console_mode                   |
| Range     | [Default] [Enabled] [Disabled]                    |

[Info: "Default" is enabled in most cases.](#)

|           |                                                           |
|-----------|-----------------------------------------------------------|
| Parameter | Limit the maximum console resolution width to this value. |
| Registry  | x.drivers.kms.max_console_width                           |
| Type      | Integer                                                   |



|                                                           |                                                                  |
|-----------------------------------------------------------|------------------------------------------------------------------|
| Value                                                     | "0"                                                              |
| Info: "0" means default setting. Use the default setting. |                                                                  |
| Parameter                                                 | Limit the maximum console resolution height to this value.       |
| Registry                                                  | x.drivers.kms.max_console_height                                 |
| Type                                                      | Integer                                                          |
| Value                                                     | "0"                                                              |
| Info: "0" means default setting. Use the default setting. |                                                                  |
| Parameter                                                 | Set graphic kernel driver debug level.                           |
| Registry                                                  | x.drivers.kms.debug_level                                        |
| Range                                                     | [No debug] [Basic] [Basic + core] [Basic + core + atomic] [Full] |
| Info: Warning log will grow very fast.                    |                                                                  |

Only for Intel i915 driver:

|                                               |                                                                                                   |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------|
| Parameter                                     | Limit the maximum DisplayPort lane link rate.                                                     |
| Registry                                      | x.drivers.intel.max_dp_link_rate                                                                  |
| Range                                         | [default] [1.62Gbps] [2.16Gbps] [2.7Gbps] [3.24Gbps]<br>[4.32Gbps] [5.4Gbps] [6.48Gbps] [8.1Gbps] |
| Info: "Default" means hardware default limit. |                                                                                                   |

## 7.17 Notes for Release 11.01.110

|                       |            |              |
|-----------------------|------------|--------------|
| <b>Software:</b>      | Version    | 11.01.110    |
| <b>Release Date:</b>  | 2019-06-06 |              |
| <b>Release Notes:</b> | Version    | RN-1101110-1 |
| <b>Last update:</b>   | 2019-06-06 |              |

- Supported Devices 11.01.110(see page 1833)
- Component Versions 11.01.110(see page 1833)
- General Information 11.01.110(see page 1837)
- Security Fixes 11.01.110(see page 1837)



- Known Issues 11.01.110(see page 1838)
- New Features 11.01.110(see page 1839)
- Resolved Issues 11.01.110(see page 1847)

### 7.17.1 Supported Devices 11.01.110

#### **IGEL devices:**

|         |                              |
|---------|------------------------------|
| UD2-LX: | UD2-LX 50<br>UD2-LX 40       |
| UD3-LX: | UD3-LX 51<br>UD3-LX 50       |
| UD5-LX: | UD5-LX 50                    |
| UD6-LX: | UD6-LX 51                    |
| UD7-LX: | UD7-LX 10                    |
| UD9-LX: | UD9-LX Touch 41<br>UD9-LX 40 |

For supported IGEL OS 11 third-party devices, see [Devices Supported by IGEL OS 11](#).<sup>446</sup>

### 7.17.2 Component Versions 11.01.110

#### • Clients

| Product                           | Version           |
|-----------------------------------|-------------------|
| Citrix HDX Realtime Media Engine  | 2.8.0-2235        |
| Citrix Receiver                   | 13.10.0.20        |
| Citrix Receiver                   | 13.5.0.10185126   |
| Citrix Workspace App              | 19.3.0.5          |
| deviceTRUST Citrix Channel        | 19.1.200.2        |
| Evidian AuthMgr                   | 1.5.6840          |
| Evince PDF Viewer                 | 3.18.2-1ubuntu4.3 |
| FabulaTech USB for Remote Desktop | 5.2.29            |

<sup>446</sup> <https://kb.igel.com/os11-supported-hardware>



|                                         |                         |
|-----------------------------------------|-------------------------|
| Firefox                                 | 60.7.0                  |
| IBM iAccess Client Solutions            | 1.1.8.1                 |
| IGEL RDP Client                         | 2.2                     |
| Imprivata OneSign ProvID Embedded       |                         |
| deviceTRUST RDP Channel                 | 19.1.200.2              |
| NCP Secure Enterprise Client            | 5.10_rev40552           |
| NX Client                               | 5.3.12                  |
| Open VPN                                | 2.3.10-1ubuntu2.1       |
| Zulu JRE                                | 8.36.0.1                |
| Parallels Client (64 bit)               | 16.5.2.20595            |
| Remote Viewer (Red Hat Virtualization)  | 7.0-igel47              |
| Spice GTK (Red Hat Virtualization)      | 0.35                    |
| Spice Protocol (Red Hat Virtualization) | 0.12.14                 |
| Usbredir (Red Hat Virtualization)       | 0.8.0                   |
| Teradici PCoIP Software Client          | 19.05.1-18.04           |
| ThinLinc Client                         | 4.9.0-5775              |
| ThinPrint Client                        | 7.5.88                  |
| Totem Media Player                      | 2.30.2                  |
| Parole Media Player                     | 1.0.1-0ubuntu1igel16    |
| VNC Viewer                              | 1.8.0+git20180123-igel1 |
| VMware Horizon Client                   | 5.0.0-12557422          |
| Voip Client Ekiga                       | 4.0.1                   |

- **Dictation**

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B048     |
| Olympus driver for dictation              | 20180621 |
| Philips Speech Driver                     | 12.6.36  |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.6    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.1.0    |



- **Smartcard**

|                                           |                        |
|-------------------------------------------|------------------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101                |
| PKCS#11 Library Athena IDProtect          | 623.07                 |
| PKCS#11 Library cryptovision sc/interface | 7.1.9.620              |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0              |
| PKCS#11 Library SecMaker NetID            | 6.7.0.23               |
| PKCS#11 Library 90meter                   | 20190522               |
| Reader Driver ACS CCID                    | 1.1.6-1igel1           |
| Reader Driver Gemalto eToken              | 10.0.37-0              |
| Reader Driver HID Global Omnikey          | 4.3.3                  |
| Reader Driver Identive CCID               | 5.0.35                 |
| Reader Driver Identive eHealth200         | 1.0.5                  |
| Reader Driver Identive SCRKBC             | 5.0.24                 |
| Reader Driver MUSCLE CCID                 | 1.4.30-1igel3          |
| Reader Driver REINER SCT cyberJack        | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite               | 1.8.23-1igel1          |
| Cherry USB2LAN Proxy                      | 3.0.0.6                |

- **System Components**

|                         |                    |
|-------------------------|--------------------|
| OpenSSL                 | 1.0.2g-1ubuntu4.14 |
| OpenSSH Client          | 7.2p2-4ubuntu2.7   |
| OpenSSH Server          | 7.2p2-4ubuntu2.7   |
| Bluetooth stack (bluez) | 5.50-0ubuntu1igel5 |
| MESA OpenGL stack       | 18.3.3-1igel57     |
| VAAPI ABI Version       | 0.40               |



|                                         |                              |
|-----------------------------------------|------------------------------|
| VDPAU Library version                   | 1.1.1-3ubuntu1               |
| Graphics Driver INTEL                   | 2.99.917+git20190301-igel870 |
| Graphics Driver ATI/RADEON              | 18.1.0-1igel854              |
| Graphics Driver ATI/AMDGPU              | 18.1.0-1igel853              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.15-2igel775              |
| Graphics Driver Nvidia                  | 410.93-0ubuntu1              |
| Graphics Driver Vboxvideo               | 5.2.18-dfsg-2igel17          |
| Graphics Driver VMware                  | 13.3.0-2igel857              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1igel775         |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |
| Graphics Driver VESA                    | 2.4.0-1igel855               |
| Input Driver Evdev                      | 2.10.5-1ubuntu1igel750       |
| Input Driver Elographics                | 1.4.1-1build5igel633         |
| Input Driver eGalax                     | 2.5.5814                     |
| Input Driver Synaptics                  | 1.9.0-1ubuntu1igel748        |
| Input Driver VMMouse                    | 13.1.0-1ubuntu2igel635       |
| Input Driver Wacom                      | 0.36.1-0ubuntu1igel813       |
| Kernel                                  | 4.18.20 #mainline-udos-r2519 |
| Xorg X11 Server                         | 1.19.6-1ubuntu4.2igel842     |
| Xorg Xephyr                             | 1.19.6-1ubuntu4.2igel842     |
| CUPS Printing Daemon                    | 2.1.3-4ubuntu0.7igel23       |
| PrinterLogic                            | 18.2.1.128                   |
| Lightdm Graphical Login Manager         | 1.18.3-0ubuntu1.1            |
| XFCE4 Window Manager                    | 4.12.3-1ubuntu2igel675       |



|                 |                              |
|-----------------|------------------------------|
| ISC DHCP Client | 4.3.3-5ubuntu12.10igel7      |
| NetworkManager  | 1.2.6-0ubuntu0.16.04.2igel58 |
| ModemManager    | 1.6.8-2ubuntu1igel2          |
| GStreamer 0.10  | 0.10.36-2ubuntu0.1           |
| GStreamer 1.x   | 1.14.4-1ubuntu1igel203       |
| Python2         | 2.7.12                       |
| Python3         | 3.5.2                        |

- **Features with Limited IGEL Support**

Mobile Device Access USB

VPN OpenConnect

Scanner support

VirtualBox

- **Features with Limited Functionality**

|                   |      |
|-------------------|------|
| Cisco JVDI Client | 12.1 |
|-------------------|------|

### 7.17.3 General Information 11.01.110

The following clients and features are not supported anymore

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- Ericom PowerTerm
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

### 7.17.4 Security Fixes 11.01.110

Firefox

- Updated Mozilla Firefox to version **60.7.0esr**.
- Fixed **mfsa2019-08** security issues.



[More...](#)

CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793,  
CVE-2019-9795, CVE-2019-9796, CVE-2018-18506, CVE-2019-9788.

- Fixed **mfsa2019-05** security issues CVE-2018-18356 and CVE-2019-5785.
- Fixed **mfsa2019-02** security issues CVE-2018-18500, CVE-2018-18505 and CVE-2018-18501.
- Firefox is now allowed to access **YubiKey** (FIDO/U2F) if **AppArmor** is active.

Base system

- Updated **libwebkit2gtk-4.0-37** to version **1.24.2**.

[More...](#)

CVE-2019-8595, CVE-2019-8607, CVE-2019-8615, CVE-2019-6251,  
CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378,  
CVE-2018-4382, CVE-2018-4392, CVE-2018-4416, CVE-2018-4345,  
CVE-2018-4386 and CVE-2018-4372.

## 7.17.5 Known Issues 11.01.110

Citrix

- With an **activated DRI3** and an **AMD GPU**, **Citrix H.264 acceleration plugin** could freeze. A selective H.264 mode (API v2) is not affected by this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection** of H.264, MPEG1 and MPEG2. GStreamer1.0 is used if **browser content redirection** is active.
- **Browser content redirection** does not work with **activated DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix StoreFront Login** with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is inserted after the start of Login.  
As a workaround, insert the smartcard before starting StoreFront Login.
- When using **Citrix Workspace App 18.10** in combination with **Philips Speech driver**, the session occasionally does not properly terminate at logoff and hangs.  
As a workaround, the usage of Citrix Receiver 13.10 is recommended when Philips Speech driver is needed.
- **Citrix H.264 acceleration plugin** does not work with the **enabled** server policy **Optimize for 3D graphics workload** in combination with the server policy **Use video codec compression > For the entire screen**.

VMware Horizon

- **External drives** are mounted already before connection, do not appear in the **remote desktop**.  
Workaround: Mapping the directory/media as a drive on desktop. The external devices will show up within the media drive then.
- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.



- On the one hand, when using **USB redirection for storage devices**: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
- On the other hand, when using **drive mapping** instead, it is recommended either to switch off USB redirection entirely or at least to deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug** has to be enabled and the **Number of storage hotplug devices** has to be set to at least 1.

#### Parallels Client

- Native USB redirection** does not work with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** once with **disabled FIPS support**.

#### Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign** smartcards.

#### Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.

#### Base system

- On **NVIDIA GPU** drivers, the **reported resolutions** of a display may contain unsupported resolutions. When any of those are configured, there are visual bugs (e.g. the desktop does not render properly).

### 7.17.6 New Features 11.01.110

#### Citrix

- Integrated **Citrix Workspace app 19.03**.  
Added new registry key to support **1536-bit RSA** keys for client authentication.  
[More...](#)

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Enable RSA 1536 cipher suit           |
| Registry  | ica.allregions.enabl_rsa_1536         |
| Range     | <u>factory default</u> / false / true |

- Added new registry key to enable **different cipher suites** for client authentication.  
[More...](#)

|           |                                 |
|-----------|---------------------------------|
| Parameter | Enables different cipher suites |
|-----------|---------------------------------|



|          |                                          |
|----------|------------------------------------------|
| Registry | <code>ica.allregions.sslciphers</code>   |
| Range    | <u>factory default</u> / ALL / GOV / COM |

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 – GOV/ALL
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 – GOV/ALL
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA – COM/ALL
- Added new registry key to support **keyboard layout synchronization**.

**More...**

|           |                                                            |
|-----------|------------------------------------------------------------|
| Parameter | Keyboard layout synchronization                            |
| Registry  | <code>ica.modules.virtualdriver.keyboardsync.enable</code> |
| Value     | <u>enabled</u> / <u>disabled</u>                           |

- Updated **Citrix HDX RTME**, used for optimization of Skype for Business, to version **2.8.0-2235**

## RDP/IGEL RDP Client 2

- Added **Field Collection to RDP** session server page

## VMware Horizon

- Added parameters to **specify webcam frame size** and **rate for RTAV**.

**More...**

|           |                                            |
|-----------|--------------------------------------------|
| Parameter | Webcam frame width                         |
| Registry  | <code>vmware.view.rtav-frame-width</code>  |
| Value     | <code>&lt;empty_string&gt;</code>          |
| Parameter | Webcam frame height                        |
| Registry  | <code>vmware.view.rtav-frame-height</code> |
| Value     | <code>&lt;empty_string&gt;</code>          |
| Parameter | Webcam frame rate                          |
| Registry  | <code>vmware.view.rtav-frame-rate</code>   |
| Value     | <code>&lt;empty_string&gt;</code>          |

- Updated **Horizon Client** to version **5.0.0-12557422**



- Added possibility to easily evaluate **Horizon Blast decoder states**. By default sessions are evaluated after usage and the result is written into the journal log.  
This can also be used with GUI notifications at runtime.

## Teradici PCoIP Client

- Added **Teradici PCoIP** Client version **19.05.1**. This feature requires an additional license.  
[More...](#)

|                      |                                                                                                                                                    |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| IGEL Setup Parameter | <b>System &gt; Firmware Customization &gt; Features</b><br>Teradici PCoIP Client                                                                   |
| Registry             | services.addition_teradici_pcoip_client.enabled                                                                                                    |
| Value                | <u>enabled</u> / disabled                                                                                                                          |
| IGEL Setup Parameter | <b>Sessions &gt; Teradici PCoIP Client &gt; PCoIP Sessions &gt; PCoIP Session &gt; Connection settings</b><br>Use IGEL Setup for configuration     |
| Registry             | sessions.pcoip<NR>.options.igel-connection                                                                                                         |
| Value                | enabled / <u>disabled</u>                                                                                                                          |
| IGEL Setup Parameter | <b>Sessions &gt; Teradici PCoIP Client &gt; PCoIP Sessions &gt; PCoIP Session &gt; Connection settings</b><br>Server                               |
| Registry             | sessions.pcoip<NR>.options.address                                                                                                                 |
| Value                | <empty_string>                                                                                                                                     |
| IGEL Setup Parameter | <b>Sessions &gt; Teradici PCoIP Client &gt; PCoIP Sessions &gt; PCoIP Session &gt; Connection settings</b><br>Server certificate verification mode |
| Registry             | sessions.pcoip<NR>.options.security-mode                                                                                                           |
| Range                | [Not required][ <u>Warn but allow</u> ][Full verification]                                                                                         |
| IGEL Setup Parameter | <b>Sessions &gt; Teradici PCoIP Client &gt; PCoIP Sessions &gt; PCoIP Session &gt; Login</b><br>Authentication type                                |



|            |                                                                                                                                                                     |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Registry   | <code>sessions.pcoip&lt;NR&gt;.options.auth-type</code>                                                                                                             |
| Range      | [Password authentication][Smartcard authentication]                                                                                                                 |
| IGEL Setup | <b>Sessions &gt; Teradici PCoIP Client &gt; PCoIP Sessions &gt; PCoIP Session &gt; Window</b>                                                                       |
| Parameter  | Window mode                                                                                                                                                         |
| Registry   | <code>sessions.pcoip&lt;NR&gt;.options.window-mode</code>                                                                                                           |
| Range      | [User defined][Fullscreen One Monitor][Fullscreen All Monitors]<br>[Window]                                                                                         |
| IGEL Setup | <b>Sessions &gt; Teradici PCoIP Client &gt; PCoIP Sessions &gt; PCoIP Session &gt; Window</b>                                                                       |
| Parameter  | User interface translation                                                                                                                                          |
| Registry   | <code>sessions.pcoip&lt;NR&gt;.options.language</code>                                                                                                              |
| Range      | [System setting][English] [German] [French][Spanish] [Portuguese (EU)]<br>[Portuguese (Brazil)] [Italian][Japanese] [Chinese(Simplified)]<br>[Chinese(Traditional)] |
| IGEL Setup | <b>Sessions &gt; Teradici PCoIP Client &gt; PCoIP Sessions &gt; PCoIP Session &gt; Window</b>                                                                       |
| Parameter  | Log level                                                                                                                                                           |
| Registry   | <code>sessions.pcoip&lt;NR&gt;.options.log-level</code>                                                                                                             |
| Range      | [Critical][Error][Info][Debug]                                                                                                                                      |

## Network

- Added a mechanism for retrieving the **SCEP challenge password** with a **custom script**. Setting the following registry key to true enables the use of the script. The registry key `network.scepclient.cert%.crypt_password` will be ignored. (The script may use it for its own purpose though.)

**More...**

|           |                                                                      |
|-----------|----------------------------------------------------------------------|
| Parameter | Use Challenge Password Command                                       |
| Registry  | <code>network.scepclient.cert%.use_challenge_password_command</code> |



|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

- If the above key is **true**, the value of this key will be passed to **bash for execution**. It happens when the SCEP challenge password is needed for creating a **certificate signing request**. The script is supposed to output the challenge password on its standard output. For convenience any carriage return characters are stripped off the script before execution by bash.

[More...](#)

|           |                                                     |
|-----------|-----------------------------------------------------|
| Parameter | Challenge Password Command                          |
| Registry  | network.scepclient.cert%.challenge_password_command |
| Value     | <empty_string>                                      |

#### Wi-Fi

- Added support for **Realtek 8821CE wireless cards**.

#### Smartcard

- Added **90meter** smart card library. This feature requires an additional license.

[More...](#)

|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| IGEL Setup | <b>System &gt; Firmware Customization &gt; Features</b>                       |
| Parameter  | 90meter Smart Card Support                                                    |
| Registry   | services.addition_smartcard_90meter.enabled                                   |
| Value      | <u>enabled / disabled</u>                                                     |
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Smartcard</b> |
| Parameter  | Horizon logon with smartcards supported by 90meter library                    |
| Registry   | vmware.view.pkcs11.use_90meter                                                |
| Value      | <u>enabled / disabled</u>                                                     |
| IGEL Setup | <b>Sessions &gt; Browser &gt; Browser Global &gt; Smartcard Middleware</b>    |
| Parameter  | 90meter Security Device                                                       |
| Registry   | browserglobal.security_device.90meter                                         |
| Value      | <u>enabled / disabled</u>                                                     |
| IGEL Setup | <b>Security &gt; Smartcard &gt; Middleware</b>                                |



|           |                           |
|-----------|---------------------------|
| Parameter | 90meter                   |
| Registry  | scard.pkcs11.use_90meter  |
| Value     | enabled / <u>disabled</u> |

## Base System

- Added package **ldap-utils** which can be used by **custom scripts**.

- Updated **libwebkit2gtk-4.0-37** to version **1.24.2**.

### More...

CVE-2019-8595, CVE-2019-8607, CVE-2019-8615, CVE-2019-6251,

CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378,

CVE-2018-4382, CVE-2018-4392, CVE-2018-4416, CVE-2018-4345,

CVE-2018-4386, CVE-2018-4372

- Updated **EULA** displayed in **OSC** and **IGEL Setup Assistant**.

- When the **IGEL Setup Assistant** is used to download a demo license via WiFi, the **local WiFi manager** will be enabled by default.

- Added possibility to **configure scheduled commands**. Registry keys: system.cron.\*

## Driver

- Updated **deviceTRUST Client** to version **19.1.200**. This release includes support for logical disks attached to the IGEL endpoint, plus bug fixes and stability improvements over the previous 19.1.100 release.

### Logical Disks

Added support for real-time properties representing the LOGICAL DISKS attached to the IGEL endpoint.

#### This includes...

- DEVICE\_LOGICALDISK\_X\_TYPE – Either Fixed or Removable.
- DEVICE\_LOGICALDISK\_X\_LABEL – The volume label.
- DEVICE\_LOGICALDISK\_X\_FILESYSTEM – The type of file system.
- DEVICE\_LOGICALDISK\_X\_PATHS – The paths that the disk is mounted.
- DEVICE\_LOGICALDISK\_X\_TOTALMB – The total space available on the disk. This property is only available for mounted disks.
- DEVICE\_LOGICALDISK\_X\_FREEMB – The free space available on the disk. This property is only available for mounted disks.
- DEVICE\_LOGICALDISK\_X\_NAME – The name of the underlying physical disk.
- DEVICE\_LOGICALDISK\_X\_VENDORID – The vendor identifier uniquely identifying the manufacturer. This property is only available for USB or PCI connected devices.
- DEVICE\_LOGICALDISK\_X\_PRODUCTID – The product identifier uniquely identifying the product. This property is only available for USB or PCI connected devices.
- DEVICE\_LOGICALDISK\_X\_SERIALNUMBER – The serial number of the physical disk.
- DEVICE\_LOGICALDISK\_X\_BUSTYPE – The storage bus type linked to the physical disk.
- DEVICE\_LOGICALDISK\_COUNT – The number of logical disks.



- Added registry keys to **modify the intel graphic driver usage** of framebuffer compression and power management.

[More...](#)

|           |                                          |
|-----------|------------------------------------------|
| Parameter | Power saving display C-States to use.    |
| Registry  | x.drivers.intel.dc_setting               |
| Range     | [Default][Disable][Up to DC5][Up to DC6] |
| Parameter | Use framebuffer compression.             |
| Registry  | x.drivers.intel.fbc_setting              |
| Range     | [Default][Disable]                       |

## X11 System

- Added new registry keys to **change the xorg input driver** for a input device class.

[More...](#)

For keyboards:

|           |                               |
|-----------|-------------------------------|
| Parameter | Xorg driver to use            |
| Registry  | userinterface.keyboard.driver |
| Range     | [Evdev] [Libinput]            |

For touchpads:

|           |                                |
|-----------|--------------------------------|
| Parameter | Xorg driver to use             |
| Registry  | userinterface.touchpad.driver  |
| Range     | [Evdev] [Synaptics] [Libinput] |

For touchscreens:

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Xorg driver to use                    |
| Registry  | userinterface.touchscreen.xorg_driver |
| Range     | [Evdev][Libinput]                     |

For mouse:



|           |                                         |
|-----------|-----------------------------------------|
| Parameter | Xorg driver to use                      |
| Registry  | <code>userinterface.mouse.driver</code> |
| Range     | [ <u>Evdev</u> ][Libinput]              |

- Added some registry keys to **disable loading of DRM kernel modules** (graphic).  
[More...](#)

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | Disable the loading of the RADEON DRM driver.    |
| Registry  | <code>x.drivers.ati.disable</code>               |
| Value     | enabled / <u>disabled</u>                        |
| Parameter | Disable the loading of the AMDGPU DRM driver.    |
| Registry  | <code>x.drivers.amdgpu.disable</code>            |
| Value     | enabled / <u>disabled</u>                        |
| Parameter | Disable the loading of the i915 DRM driver.      |
| Registry  | <code>x.drivers.intel.disable</code>             |
| Value     | enabled / <u>disabled</u>                        |
| Parameter | Disable the loading of the NVIDIA kernel driver. |
| Registry  | <code>x.drivers.nvidia.disable</code>            |
| Value     | enabled / <u>disabled</u>                        |
| Parameter | Disable the loading of the NOUVEAU DRM driver.   |
| Registry  | <code>x.drivers.nouveau.disable</code>           |
| Value     | enabled / <u>disabled</u>                        |
| Parameter | Disable the loading of the QXL DRM driver.       |
| Registry  | <code>x.drivers.qxl.disable</code>               |



|           |                                                  |
|-----------|--------------------------------------------------|
| Value     | <u>enabled / disabled</u>                        |
| Parameter | Disable the loading of the VMGFX DRM driver.     |
| Registry  | x.drivers.vmware.disable                         |
| Value     | <u>enabled / disabled</u>                        |
| Parameter | Disable the loading of the VBOXVIDEO DRM driver. |
| Registry  | x.drivers.vboxvideo.disable                      |
| Value     | <u>enabled / disabled</u>                        |

## Java

- Replaced **Oracle JRE** by **AZUL's Zulu JRE** version **8.36.0.1**.

## 7.17.7 Resolved Issues 11.01.110

## OSC Installer

- Fixed OSC Installer to **not disable EFI**, if MSDOS partitioning was chosen.

## Citrix

- Fixed stability issues with **Citrix Browser Content Redirection**.
- Fixed crash when **H264 acceleration** and **RTME** will be used on two or more concurrent **VDI sessions**.

## RDP/IGEL RDP Client 2

- Added registry key to use **rdpglobal window settings** for remote apps.  
[More...](#)

|           |                                                             |
|-----------|-------------------------------------------------------------|
| Parameter | Enable global windows settings for remote app               |
| Registry  | rdp.winconnect.enable-global-window-settings-for-remote-app |
| Value     | <u>enabled / disabled</u>                                   |

## VMware Horizon

- Added recognition for **password change** and **password expired dialog** in **Horizon local logon sessions** or **appliance mode**
- Fixed the configuration choice to use the **relative mouse feature**

## Firefox



- Fixed firefox not accepting **proxy credentials** from setup.
- Fixed **print hotkey disable option** not working with Firefox 60.
- Fixed browserglobal.app.local\_subdirs\_whitelist not working.
- Updated **Firefox** browser to version **60.7.0esr**.
- Fixes for **mfsa2019-08**.

**More...**

- CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793,
  - CVE-2019-9795, CVE-2019-9796, CVE-2018-18506, CVE-2019-9788.
- Fixes for **mfsa2019-05**, also known as: CVE-2018-18356, CVE-2019-5785.
- Fixes for **mfsa2019-02**, also known as: CVE-2018-18500, CVE-2018-18505, CVE-2018-18501.

## Network

- Fixed: Failure to reach **SCEP server** in the client certificate renewal phase resulted in loss of SCEP server and client certificates.
- Changed **e1000e driver** to out of tree version **3.4.2.3** - directly from Intel.
- Changed **igb driver** to out of tree version **5.3.5.22** - directly from Intel.
- Added possibility to switch between **thirdparty** and **kernel intel IGB network driver**.

**More...**

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Use thirdparty igb kernel module.     |
| Registry  | network.drivers.igb.prefer_thirdparty |
| Value     | [Auto] [Yes] [No]                     |

Info: "Auto" uses thirdparty in most cases

- Added possibility to switch between **thirdparty** and **kernel intel E1000E network driver**.

**More...**

|           |                                          |
|-----------|------------------------------------------|
| Parameter | Use thirdparty e1000e kernel module.     |
| Registry  | network.drivers.e1000e.prefer_thirdparty |
| Value     | [Auto] [Yes] [No]                        |

Info: "Auto" uses thirdparty in most cases

- Fixed instability with **netmounts with static ip configuration**.
- Added possibility to switch between **thirdparty r8168** and **kernel r8169 realtek network driver**.

**More...**

|           |                                     |
|-----------|-------------------------------------|
| Parameter | Use thirdparty r8168 kernel module. |
| Registry  | network.drivers.r8169.prefer_r8168  |
| Value     | [Auto] [Yes] [No]                   |



**Info:** "Auto" uses r8169 in most cases

- Added possibility to choose the variant of the **realtek r8168 driver**.

**More...**

|           |                                                                |
|-----------|----------------------------------------------------------------|
| Parameter | Choose realtek r8168 variant (only if prefer r8168 is chosen). |
| Registry  | network.drivers.r8169.r8168_variant                            |
| Value     | [Default][No NAPI][NAPI]                                       |

**Info:** "Auto" uses NAPI in most cases

## Wi-Fi

- Fixed non working **TP Link Archer T2UH**.

## Imprivata

- Fixed **Fast User Switching** with **Citrix** connections.

## Smartcard

- Fixed **OpenSC** setting `max_send_size` for reader driver pcsc in `/etc/opensc/opensc.conf`.
- Fixed **Dell KB813 smartcard keyboard** in combination with certain smartcards driven by **OpenSC PKCS#11** module. Before this fix authentication to **Citrix StoreFront** and **VMWare Horizon** failed.

## Base system

- Fixed retrieving of **serial number** from display.
- Fixed **random 90 seconds shutdown delay** (systemd).
- Fixed wrong behavior with **expired evaluation licenses** in some cases.
- Fixed a bug in the **screenlock countdown** that occurred when display of remaining seconds was not desired.
- Added **apparmor rule** to allow tcpdump to write to `/debuglog`.
- Bugfix **hotkey setting need reboot**.
- Fixed **UD2 screen goes black** problem with certain multimonitor configurations.
- Fixed **gtk-3 icon sizes** for **High-DPI** configurations.
- Enhanced **bootloader** to allow the setting of some kernel commandline parameters with registry keys.

**More...**

|           |                                 |
|-----------|---------------------------------|
| Parameter | Disable use of APIC controller. |
| Registry  | system.kernel.bootparams.noapic |
| Value     | enabled / <u>disabled</u>       |
| Parameter | Disable use of ACPI.            |



|                                        |                                                            |
|----------------------------------------|------------------------------------------------------------|
| Registry                               | <code>system.kernel.bootparams.noacpi</code>               |
| Value                                  | <u>enabled</u> / <u>disabled</u>                           |
| Parameter                              | Use only one CPU core and disable all others.              |
| Registry                               | <code>system.kernel.bootparams.nosmp</code>                |
| Value                                  | <u>enabled</u> / <u>disabled</u>                           |
| Parameter                              | Enable debug console on serial port 1.                     |
| Registry                               | <code>system.kernel.bootparams.serial_console_debug</code> |
| Value                                  | <u>enabled</u> / <u>disabled</u>                           |
| Parameter                              | Limit CPU core usage (0 means no limit).                   |
| Registry                               | <code>system.kernel.bootparams.maxcpus</code>              |
| Value                                  | "0"                                                        |
| Parameter                              | Set maximum allowed cstate on intel cpus.                  |
| Registry                               | <code>system.kernel.bootparams.max_cstate</code>           |
| Range                                  | [No limit] [1] [2] [3] [4] [5] [6]                         |
| <b>Info:</b> Do not limit intel cstate |                                                            |
| Parameter                              | IOMMU usage setting.                                       |
| Registry                               | <code>system.kernel.bootparams.iommu</code>                |
| Range                                  | [On] [Off] [Passthrough] [Force]                           |
| <b>Info:</b> Use IOMMU if possible     |                                                            |
| Parameter                              | IOMMU usage setting for AMD systems.                       |
| Registry                               | <code>system.kernel.bootparams.amd_iommu</code>            |
| Range                                  | [On] [Off]                                                 |


**Info: Use IOMMU if possible**

Parameter      IOMMU usage setting for Intel systems.

Registry      system.kernel.bootparams.intel\_iommu

Range      [On] [Off]

**Info: Use IOMMU if possible**

- Moved the **EULA** page in **IGEL Setup Assistant** into the **demo activation workflow**.
- Added new registry key to set **USB quirks**.

[More...](#)

Parameter      Set XHCI USB quirks to fix some hardware issues.

Registry      system.kernel.bootparams.xhci-hcd\_quirks

Range      [No quirk] [Spurious Reboot quirk] [Spurious Wakeup quirk][Spurious Reboot Wakeup quirk]

- Lenovo **ThinkCentre M73** needs the system.kernel.bootparams.xhci-hcd\_quirks registry key set to **Spurious Reboot quirk** to fix reboot after shutdown problem.

#### Driver

- Updated **deviceTRUST** Client to version **19.1.200**.

##### Bug Fixes:

- Fixed an issue reading the **DEVICE\_IGEL\_ICG\_SERVER** property.
- Fixed an issue where the **NETWORK** and **LOCATION** property providers could cause the client to freeze if a disconnection occurred whilst these property providers were checking for changes.
- Fixed an **open file handle leak** which lead to the client process reaching its file handle limits when left running for a long period of time.
- Fixed non working **WACOM device DTU-1141B**.

#### Custom Partition

- Fixed **ownership of extracted data**: don't preserve original owner while extracting data into custom partition.

#### Storage Devices

- Fixed **auto mounting** of storage devices inside of **Olympus DS-9500 Digital Voice Recorder**.

#### X11 system

- There is now a registry key to ignore a **3Dconnexion SpaceMouse** for IGEL graphical use (X11). If activated, the **SpaceMouse** is only passed through to the desktop session. If false, it acts also as the standard mouse.

[More...](#)



|           |                                                           |
|-----------|-----------------------------------------------------------|
| Parameter | Deactivates a 3Dconnexion SpaceMouse as a standard mouse. |
| Registry  | <code>userinterface.mouse.spacemouse.x11_ignore</code>    |
| Value     | <code>enabled</code> / <u><a href="#">disabled</a></u>    |

- The following SpaceMouse products are included (VID, PID, Vendor, Product).

**[More...](#)**

0x046D; 0xC603; Logitech, Inc.; 3Dconnexion Spacemouse Plus XT  
 0x046D; 0xC605; Logitech, Inc.; 3Dconnexion CADman  
 0x046D; 0xC606; Logitech, Inc.; 3Dconnexion Spacemouse Classic  
 0x046D; 0xC621; Logitech, Inc.; 3Dconnexion Spaceball 5000  
 0x046D; 0xC623; Logitech, Inc.; 3Dconnexion Space Traveller 3D Mouse  
 0x046D; 0xC625; Logitech, Inc.; 3Dconnexion Space Pilot 3D Mouse  
 0x046D; 0xC626; Logitech, Inc.; 3Dconnexion Space Navigator 3D Mouse  
 0x046D; 0xC627; Logitech, Inc.; 3Dconnexion Space Explorer 3D Mouse  
 0x046D; 0xC628; Logitech, Inc.; 3Dconnexion Space Navigator for Notebooks  
 0x046D; 0xC629; Logitech, Inc.; 3Dconnexion SpacePilot Pro 3D Mouse  
 0x046D; 0xC62B; Logitech, Inc.; 3Dconnexion Space Mouse Pro  
 0x256F; \*\*; 3Dconnexion; SpaceMouse

- USB device reset via USB powercycle on UD6/UD7 available.
- Fixed screen flicker in some cases if "Force NumLock On" (`x.global.forcenumlock`) is active.
- Fixed Display Switch utility not starting with some translations.
- Fixed an issue with the noDDC mode not always working as expected.
- Fixed wrongly detected embedded DisplayPort on Dell Wyse 5070 Extended hardware.
- Added the possibility to change an embedded DisplayPort to a normal DisplayPort.

**[More...](#)**

|           |                                                                                                   |
|-----------|---------------------------------------------------------------------------------------------------|
| Parameter | Use embedded displayport as normal displayport (reboot required).                                 |
| Registry  | <code>x.drivers.intel.edp_is_dp</code>                                                            |
| Range     | <u><a href="#">[default]</a></u> <u><a href="#">[enable]</a></u> <u><a href="#">[disable]</a></u> |

- Fixed some multimonitor (>4) issues with Nvidia graphic cards.
- Updated DisplayLink driver to version 5.1.26 to solve some startup issues.
- Fixed configuration from the old Display Switch taking precedence over configuration from new Display Switch and preventing changes.

## Audio



- Fixed bad quality sound over DisplayPort in a Citrix ICA session or other applications using ALSA API.
- Fixed jack detection of the headphone port in Dell Wyse 3040.
- Fixed configuration of default audio output and input.

#### Media Player (Parole)

- Fixed a problem where parole media player would hang instead of playing audio while audio-visualization is enabled.

#### Hardware

- Fixed vanishing mouse cursor on Ryzen 3 devices.
  - Fixed issues with non working Touchpad and Trackpoint on Lenovo laptops.
  - Hardware detect HP t430.
  - Added possibility to use AMDGPU PRO driver instead of the kernel integrated driver.  
Ryzen 3 devices (1200, 1300X, 2200G, 2200U and 2300U) will use the AMDGPU PRO driver if registry key `x.drivers.amdgpu.use_amdgpu_pro` is set to auto (default).
- New registry key (settings to this key will only work after reboot):  
[More...](#)

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Use AMDGPU PRO driver.                       |
| Registry  | <code>x.drivers.amdgpu.use_amdgpu_pro</code> |
| Range     | [Auto] [True] [False]                        |

#### Remote Management

- If TC is managed over ICG, then settings do not apply immediately when received in connection stage. The settings must be applied after user prompt dialog.

## 7.18 Notes for Release 11.01.100

|                       |                   |
|-----------------------|-------------------|
| <b>Software:</b>      | Version 11.01.100 |
| <b>Release Date:</b>  | 2019-02-15        |
| <b>Release Notes:</b> | RN-1101100-1      |
| <b>Last update:</b>   | 2019-02-15        |

- 
- [IGEL OS 11](#)(see page 1854)
  - [IGEL OS Creator \(OSC\)](#)(see page 1869)



## 7.18.1 IGEL OS 11

### Supported Devices

| <b>IGEL devices:</b> |                              |
|----------------------|------------------------------|
| UD2-LX:              | UD2-LX 40                    |
| UD3-LX:              | UD3-LX 51<br>UD3-LX 50       |
| UD5-LX:              | UD5-LX 50                    |
| UD6-LX:              | UD6-LX 51                    |
| UD7-LX:              | UD7-LX 10                    |
| UD9-LX:              | UD9-LX Touch 41<br>UD9-LX 40 |

For supported IGEL OS 11 third-party devices, see [Devices Supported by IGEL OS 11](#)<sup>447</sup>.

- [Component Versions 11.01.100](#)(see page 1854)
- [General Information 11.01.100](#)(see page 1859)
- [Known Issues 11.01.100](#)(see page 1859)
- [New Features 11.01.100](#)(see page 1860)
- [CA Certificates Contained in IGEL OS 11.01.100](#)(see page 1865)

### Component Versions 11.01.100

- **Clients**

| Product                          | Version    |
|----------------------------------|------------|
| Citrix HDX Realtime Media Engine | 2.7.0-2113 |
| Citrix Receiver                  | 13.10.0.20 |

<sup>447</sup> <https://kb.igel.com/display/hardware/Third-Party+Devices+Supported+by+IGEL+OS+11>



|                                         |                      |
|-----------------------------------------|----------------------|
| Citrix Receiver                         | 13.5.0.10185126      |
| Citrix Workspace App                    | 18.10.0.11           |
| deviceTRUST Citrix Channel              | 19.1.100.0           |
| deviceTRUST RDP Channel                 | 19.1.100.0           |
| Evidian AuthMgr                         | 1.5.6840             |
| Evince PDF Viewer                       | 3.18.2-1ubuntu4.3    |
| FabulaTech USB for Remote Desktop       | 5.2.29               |
| Firefox                                 | 60.4.0               |
| IBM iAccess Client Solutions            | 1.1.8.0              |
| IGEL RDP Client                         | 2.2                  |
| Imprivata OneSign ProveID Embedded      |                      |
| NX Client                               | 5.3.12               |
| Open VPN                                | 2.3.10-1ubuntu2.1    |
| Oracle JRE                              | 1.8.0_202            |
| Parallels Client (32 bit)               | 16.5.2.20595         |
| Parole Media Player                     | 1.0.1-0ubuntu1igel16 |
| Remote Viewer (RedHat Virtualization)   | 7.0-igel47           |
| Spice GTK (Red Hat Virtualization)      | 0.35                 |
| Spice Protocol (Red Hat Virtualization) | 0.12.14              |
| Usbredir (Red Hat Virtualization)       | 0.8.0                |
| Thinlinc Client                         | 4.9.0-5775           |
| ThinPrint Client                        | 7.5.88               |
| Totem Media Player                      | 2.30.2               |
| VMware Horizon Client                   | 4.10.0-11053294      |



|                   |                         |
|-------------------|-------------------------|
| VNC Viewer        | 1.8.0+git20180123-igel1 |
| Voip Client Ekiga | 4.0.1                   |

• **Dictation**

|                                                       |          |
|-------------------------------------------------------|----------|
| Diktamen driver for dictation                         |          |
| Driver for Grundig Business Systems dictation devices |          |
| Nuance Audio Extensions for dictation                 | B048     |
| Olympus driver for dictation                          | 20180621 |
| Philips Speech Driver                                 | 12.6.36  |

• **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.6    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.1.0    |

• **Smartcard**

|                                           |              |
|-------------------------------------------|--------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101      |
| PKCS#11 Library Athena IDProtect          | 623.07       |
| PKCS#11 Library cryptovision sc/interface | 7.1.9.620    |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0    |
| PKCS#11 Library SecMaker NetID            | 6.7.0.23     |
| Reader Driver ACS CCID                    | 1.1.6-1igel1 |
| Reader Driver Gemalto eToken              | 10.0.37-0    |
| Reader Driver HID Global Omnikey          | 4.3.3        |
| Reader Driver Identive CCID               | 5.0.35       |



|                                    |                        |
|------------------------------------|------------------------|
| Reader Driver Identive eHealth200  | 1.0.5                  |
| Reader Driver Identive SCRKBC      | 5.0.24                 |
| Reader Driver MUSCLE CCID          | 1.4.30-1igel3          |
| Reader Driver REINER SCT cyberJack | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite        | 1.8.23-1igel1          |
| Cherry USB2LAN Proxy               | 3.0.0.6                |

- **System Components**

|                                         |                              |
|-----------------------------------------|------------------------------|
| OpenSSL                                 | 1.0.2g-1ubuntu4.14           |
| OpenSSH Client                          | 7.2p2-4ubuntu2.7             |
| OpenSSH Server                          | 7.2p2-4ubuntu2.7             |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5           |
| MESA OpenGL stack                       | 18.3.3-1igel57               |
| VAAPI ABI Version                       | 0.40                         |
| VDPAU Library version                   | 1.1.1-3ubuntu1               |
| Graphics Driver INTEL                   | 2.99.917+git20181113-igel856 |
| Graphics Driver ATI/RADEON              | 18.1.0-1igel854              |
| Graphics Driver ATI/AMDGPU              | 18.1.0-1igel853              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.15-2igel775              |
| Graphics Driver Nvidia                  | 410.93-0ubuntu1              |
| Graphics Driver Vboxvideo               | 5.2.18-dfsg-2igel17          |
| Graphics Driver VMware                  | 13.3.0-2igel857              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1igel775         |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |
| Graphics Driver VESA                    | 2.4.0-1igel855               |
| Input Driver Evdev                      | 2.10.5-1ubuntu1igel750       |



|                                 |                              |
|---------------------------------|------------------------------|
| Input Driver Elographics        | 1.4.1-1build5igel633         |
| Input Driver eGalax             | 2.5.5814                     |
| Input Driver Synaptics          | 1.9.0-1ubuntu1igel748        |
| Input Driver Vmmouse            | 13.1.0-1ubuntu2igel635       |
| Input Driver Wacom              | 0.36.1-0ubuntu1igel813       |
| Kernel                          | 4.18.20 #mainline-udos-r2517 |
| Xorg X11 Server                 | 1.19.6-1ubuntu4.2igel842     |
| Xorg Xephyr                     | 1.19.6-1ubuntu4.2igel842     |
| CUPS printing daemon            | 2.1.3-4ubuntu0.7igel23       |
| PrinterLogic                    | 18.2.1.128                   |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1            |
| XFCE4 Windowmanager             | 4.12.3-1ubuntu2igel675       |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7      |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.2igel58 |
| ModemManager                    | 1.6.8-2ubuntu1igel2          |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.1           |
| GStreamer 1.x                   | 1.14.4-1ubuntu1igel203       |
| Python2                         | 2.7.12                       |
| Python3                         | 3.5.2                        |

- **Features with Limited IGEL Support**

|                          |
|--------------------------|
| Mobile Device Access USB |
|--------------------------|

|                 |
|-----------------|
| VPN OpenConnect |
|-----------------|

|                 |
|-----------------|
| Scanner support |
|-----------------|

|            |
|------------|
| VirtualBox |
|------------|

- **Features with Limited Functionality**



Cisco JVDI Client

12.1

## General Information 11.01.100

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- Ericom PowerTerm
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

## Known Issues 11.01.100

### Citrix

- With **activated DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with multimedia redirection of H.264, MPEG1 and MPEG2. GStreamer1.0 is used if **browser content redirection** is active.
- **Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix StoreFront Login** with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is inserted after start of Login.  
As a workaround, insert the smartcard before starting StoreFront Login.
- When using **Citrix Workspace App 18.10** in combination with **Philips Speech driver**, the session occasionally does not properly terminate at logoff and hangs.  
As a workaround, usage of Citrix Receiver 13.10 is recommended when Philips Speech driver is needed.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.

### VMware Horizon

- **External drives** are mounted already before connection, do not appear in the **remote desktop**.  
Workaround: Mapping the directory/media as a drive on desktop. The external devices will show up within the media drive then.



- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, when using **USB redirection for storage devices**: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using **drive mapping** instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug** has to be enabled and the **Number of storage hotplug devices** has to set to at least 1.

#### Parallels Client

- **Native USB redirection** does not work with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** once with **disabled FIPS support**.

#### Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign** smartcards.

#### Multimedia

- Multimedia redirection with **GStreamer** could fail with the Nouveau GPU driver.

#### Base system

- On **NVIDIA GPU** drivers, the **reported resolutions** of a display may contain unsupported resolutions. When any of those are configured, there are visual bugs (e.g. the desktop does not render properly).

## New Features 11.01.100

#### Base system

- Support for **IGEL OS 11 license deployment** with **IGEL UMS 6** (via 'Automatic License Deployment')
- Support for **manual license deployment** in IGEL Setup Assistant
- Support for **demo license registration** in IGEL Setup Assistant
- Unified **IGEL OS 11 firmware** for IGEL and third-party hardware (New update file prefix: lxos)
- **Writable partitions are encrypted now**
- Use **IGEL OS Creator** for IGEL OS 11 installation and recovery (Download file: OSC\_11.01.100.zip)

#### X11 system

- Reworked **user interface**
- **New wallpapers** have been added with **transparent background** so that the custom desktop color shows through. Selection of one of the new **Desktop Color** wallpapers in combination with an adjustment of desktop colors will provide this individual effect. The 2nd desktop color and the gradients also work with that.



- The new **Display Switch** tool can use **multiple different profiles**, automatically chosen at runtime depending on the currently connected monitors. A profile is created, when the current monitor layout/resolution is configured via the Display Switch utility. The profile will be associated with the currently connected displays automatically (manufacturer, model and used connector are used for allocation) and if applicable, the state of the laptop lid. The setup will be restored by hot-(un)plugging known displays, means the system will automatically switch to the already configured profile. The Display Switch utility itself got a new interface. All base functionality can be configured via Drag&Drop.

An example workflow:

- Connect the hardware and close/open lid
- Open the Display Switch Utility
  - A quick (simple) setting can be selected directly.
  - Should the desired use case be different from the provided choices, the **Advanced** button opens a drag and drop interface for further settings.
- In this interface, the **displays can be dragged and dropped** for the intended configuration. The display will snap adjacent to others.
- If a display should not be used, it can be dragged to the **Disabled** area on the top right - the screen will be reactivated when it is dragged back to the active area.
- To show the same content on multiple displays, one display should be dragged onto an other active screen. The interface will show **Mirror**. The mirroring monitor will be displayed on the lower right.
- With the **Apply** button the current state will be set, with 'Yes' on the "Keep configuration" dialog the current settings will be saved to persistent storage and associated with the profile.
- Advanced functionality** (panning/scaling/resolutions) can be configured in drop-down boxes, hidden in a **drawer on the right side**. The drawer can be expanded by clicking the '<' button on the right edge.

- For the **Display Switch** functionality the following parameters should be enabled for proper usage.

**More...**

|            |                                                     |
|------------|-----------------------------------------------------|
| IGEL Setup | <b>Accessories &gt; Display Switch &gt; Options</b> |
| Parameter  | Preserve settings over reboot                       |
| Registry   | sessions.user_display0.options.preserve_settings    |
| Value      | enabled / <u>disabled</u>                           |
| IGEL Setup | <b>Accessories &gt; Display Switch &gt; Options</b> |
| Parameter  | Smart display configuration                         |
| Registry   | x.auto_associate                                    |



|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

- The **IGEL Display Switch** utility is now used for **NVIDIA graphics** devices as well.
- Automatic DPI detection** has been added by the following parameter.

[More...](#)

|            |                                                 |
|------------|-------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Display &gt; Options</b> |
| Parameter  | Monitor DPI Detection                           |
| Registry   | x.xserver0.auto_dpi                             |
| Value      | Off / <u>Smart</u> / Pixel-Precise              |

With the **Smart** automatic DPI detection the user interface is now usable out of the box on 4k displays.

**Smart:** Auto detect the DPI but only use a few values whichever is closest to the calculated DPI value. Used DPI values: 96, 125, 150, 175, 200, 225, 250, 275, 300.

**Off:** No auto DPI detection, fixed Monitor DPI value is used.

**Pixel-Precise:** Auto detect the DPI value and use it when it is within 65-300 DPI. Otherwise, 96 DPI is used.

- Improved **High DPI** support for various applications.
- Added **xprintidle** tool to firmware.
- Added a parameter to **delay DisplayPort handling** by a certain number of seconds to mitigate disabled outputs causing a reconfiguration.

[More...](#)

|           |                                                                                                 |
|-----------|-------------------------------------------------------------------------------------------------|
| Parameter | Delay DisplayPort disconnect events by N seconds to prevent reconfiguration with weird monitors |
| Registry  | sessions.user_display0.options.delay_dp_hotplug                                                 |
| Value     | <u>2</u>                                                                                        |

## Firefox

- The Firefox configuration is now only done by global parameters found at setup pages: **IGEL Setup > Sessions > Browser > Browser Global**
- Session specific parameters are: **startup page**, **start monitor** and **autostart**

## Audio

- Added support for deployment of **Jabra Xpress** packages with **IGEL UMS 6**.

[More...](#)

|            |                                                                         |
|------------|-------------------------------------------------------------------------|
| IGEL Setup | <b>Devices &gt; Unified Communications &gt; Jabra &gt; Jabra Xpress</b> |
| Parameter  | Device Dashboard URL                                                    |



|                      |                                                                                                  |
|----------------------|--------------------------------------------------------------------------------------------------|
| Registry             | <code>jabra.xpress.device_dashboard.server_url</code>                                            |
| IGEL Setup Parameter | <b>Devices &gt; Unified Communications &gt; Jabra &gt; Jabra Xpress</b><br>Package               |
| Registry             | <code>jabra.xpress.package_name</code>                                                           |
| IGEL Setup Parameter | <b>Devices &gt; Unified Communications &gt; Jabra &gt; Jabra Xpress</b><br>Source URL            |
| Registry             | <code>jabra.xpress.package_url</code>                                                            |
| IGEL Setup Parameter | <b>Devices &gt; Unified Communications &gt; Jabra &gt; Jabra Xpress</b><br>Check SSL certificate |
| Registry             | <code>jabra.xpress.package_url_ssl_cert_check</code>                                             |
| Value                | <u>enabled</u> / disabled                                                                        |
| IGEL Setup Parameter | <b>Devices &gt; Unified Communications &gt; Jabra &gt; Jabra Xpress</b><br>Password              |
| Registry             | <code>jabra.xpress.package_url_crypt_password</code>                                             |

- Added support of **automatic suspend for wireless Jabra USB audio devices**. A device will be suspended after idle time over 5 seconds and automatically resumed again, when an application wants to playback or record audio data over the device.

[More...](#)

|                      |                                                                    |
|----------------------|--------------------------------------------------------------------|
| IGEL Setup Parameter | <b>Devices &gt; Unified Communications &gt; Jabra &gt; Options</b> |
| Parameter            | Suspend on idle                                                    |
| Registry             | <code>devices.jabra.suspend_on_idle</code>                         |
| Value                | <u>enabled</u> / disabled                                          |

TC Setup (Java)

- Local TC setup theme** can be configured now.

[More...](#)

|           |                                        |
|-----------|----------------------------------------|
| Parameter | Color Theme                            |
| Registry  | <code>userinterface.setup.theme</code> |



|       |                                            |
|-------|--------------------------------------------|
| Value | Auto / Dark / Dark & Light / Light / Ocean |
|-------|--------------------------------------------|

- Added **High DPI scaling**

#### On-screen keyboard

- Added new parameters to **auto show and hide the on-screen keyboard**. To use this feature, the on-screen keyboard should be set to **autostart** and **restart**. The on-screen keyboard will start in a hidden state and automatically appears when a text field is selected. Confirmed to work within Firefox and on lockscreen.

[More...](#)

|            |                                                                         |
|------------|-------------------------------------------------------------------------|
| IGEL Setup | <b>Accessories &gt; On-Screen Keyboard &gt; Application Integration</b> |
| Parameter  | Automatically show On-Screen Keyboard when text field is selected       |
| Registry   | userinterface.softkeyboard.autoshow                                     |
| Value      | enabled / <u>disabled</u>                                               |
| Parameter  | Automatically hide On-Screen Keyboard when text field is deselected     |
| Registry   | userinterface.softkeyboard.autohide                                     |
| Value      | enabled / <u>disabled</u>                                               |

#### Appliance Mode

- Streamlined the **on-screen keyboard** settings for appliance mode.
- Add new parameter to enable the on-screen keyboard in appliance mode. With **enabled Appliance Mode Access** the on-screen keyboard should set to auto start.

[More...](#)

|            |                                            |
|------------|--------------------------------------------|
| IGEL Setup | <b>Accessories &gt; On-Screen Keyboard</b> |
| Parameter  | Appliance Mode Access                      |
| Registry   | sessions.gtkeyboard0.appliance_mode_access |
| Value      | enabled / <u>disabled</u>                  |

- Alternatively, the button to **show/hide** the on-screen keyboard can be displayed in **appliance mode**, to provide a quick method to turn the keyboard on or off.

[More...](#)

|            |                                                                                                               |
|------------|---------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Accessories &gt; On-Screen Keyboard &gt; Application Integration &gt; On-Screen Keyboard Toggle Button</b> |
| Parameter  | Show button                                                                                                   |
| Registry   | userinterface.touchescreen.keyboard.touchkey.enable                                                           |



| Value | <u>enabled / disabled</u> |
|-------|---------------------------|
|-------|---------------------------|

- **Removed the old options** to individually enable/disable and position the on-screen keyboard for various appliance mode settings.

#### Hardware

- Added hardware support for **HP t530**.

### CA Certificates Contained in IGEL OS 11.01.100

Contained CA certificates:

- ACCVRAIZ1, expires Dec 31 09:37:37 2030 GMT (ACCVRAIZ1.crt)
- ACEDICOM Root, expires Apr 13 16:24:22 2028 GMT (ACEDICOM\_Root.crt)
- AC RAIZ FNMT-RCM, expires Jan 1 00:00:00 2030 GMT (AC\_RAIZ\_FNMT-RCM.crt)
- Actalis Authentication Root CA, expires Sep 22 11:22:02 2030 GMT (Actalis\_Authentication\_Root\_CA.crt)
- AddTrust External CA Root, expires May 30 10:48:38 2020 GMT (AddTrust\_External\_Root.crt)
- AddTrust Class 1 CA Root, expires May 30 10:38:31 2020 GMT (AddTrust\_Low-Value\_Services\_Root.crt)
- AddTrust Public CA Root, expires May 30 10:41:50 2020 GMT (AddTrust\_Public\_Services\_Root.crt)
- AddTrust Qualified CA Root, expires May 30 10:44:50 2020 GMT (AddTrust\_Qualified\_Certificates\_Root.crt)
- AffirmTrust Commercial, expires Dec 31 14:06:06 2030 GMT (AffirmTrust\_Commercial.crt)
- AffirmTrust Networking, expires Dec 31 14:08:24 2030 GMT (AffirmTrust\_Networking.crt)
- AffirmTrust Premium, expires Dec 31 14:10:36 2040 GMT (AffirmTrust\_Premium.crt)
- AffirmTrust Premium ECC, expires Dec 31 14:20:24 2040 GMT (AffirmTrust\_Premium\_ECC.crt)
- Amazon Root CA 1, expires Jan 17 00:00:00 2038 GMT (Amazon\_Root\_CA\_1.crt)
- Amazon Root CA 2, expires May 26 00:00:00 2040 GMT (Amazon\_Root\_CA\_2.crt)
- Amazon Root CA 3, expires May 26 00:00:00 2040 GMT (Amazon\_Root\_CA\_3.crt)
- Amazon Root CA 4, expires May 26 00:00:00 2040 GMT (Amazon\_Root\_CA\_4.crt)
- Atos TrustedRoot 2011, expires Dec 31 23:59:59 2030 GMT (Atos\_TrustedRoot\_2011.crt)
- Autoridad de Certificacion Firmaprofesional CIF A62634068, expires Dec 31 08:38:15 2030 GMT (Autoridad\_de\_Certificacion\_Firmaprofesional\_CIF\_A62634068.crt)
- Baltimore CyberTrust Root, expires May 12 23:59:00 2025 GMT (Baltimore\_CyberTrust\_Root.crt)
- Buypass Class 2 Root CA, expires Oct 26 08:38:03 2040 GMT (Buypass\_Class\_2\_Root\_CA.crt)
- Buypass Class 3 Root CA, expires Oct 26 08:28:58 2040 GMT (Buypass\_Class\_3\_Root\_CA.crt)
- CA Disig Root R1, expires Jul 19 09:06:56 2042 GMT (CA\_Disig\_Root\_R1.crt)
- CA Disig Root R2, expires Jul 19 09:15:30 2042 GMT (CA\_Disig\_Root\_R2.crt)
- CFCA EV ROOT, expires Dec 31 03:07:01 2029 GMT (CFCA\_EV\_ROOT.crt)
- CNNIC ROOT, expires Apr 16 07:09:14 2027 GMT (CNNIC\_ROOT.crt)
- COMODO Certification Authority, expires Dec 31 23:59:59 2029 GMT (COMODO\_Certification\_Authority.crt)
- COMODO ECC Certification Authority, expires Jan 18 23:59:59 2038 GMT (COMODO\_ECC\_Certification\_Authority.crt)
- COMODO RSA Certification Authority, expires Jan 18 23:59:59 2038 GMT (COMODO\_RSA\_Certification\_Authority.crt)
- Chambers of Commerce Root, expires Sep 30 16:13:44 2037 GMT (Camerfirma\_Chambers\_of\_Commerce\_Root.crt)
- Global Chambersign Root, expires Sep 30 16:14:18 2037 GMT (Camerfirma\_Global\_Chambersign\_Root.crt)
- Certigna, expires Jun 29 15:13:05 2027 GMT (Certigna.crt)
- Certinomis - Autorité Racine, expires Sep 17 08:28:59 2028 GMT (Certinomis\_-\_Autorité\_Racine.crt)
- Certinomis - Root CA, expires Oct 21 09:17:18 2033 GMT (Certinomis\_-\_Root\_CA.crt)



- Class 2 Primary CA, expires Jul 6 23:59:59 2019 GMT (Certplus\_Class\_2\_Primary\_CA.crt)
- Certplus Root CA G1, expires Jan 15 00:00:00 2038 GMT (Certplus\_Root\_CA\_G1.crt)
- Certplus Root CA G2, expires Jan 15 00:00:00 2038 GMT (Certplus\_Root\_CA\_G2.crt)
- Certum CA, expires Jun 11 10:46:39 2027 GMT (Certum\_Root\_CA.crt)
- Certum Trusted Network CA, expires Dec 31 12:07:37 2029 GMT (Certum\_Trusted\_Network\_CA.crt)
- Certum Trusted Network CA 2, expires Oct 6 08:39:56 2046 GMT (Certum\_Trusted\_Network\_CA\_2.crt)
- Chambers of Commerce Root - 2008, expires Jul 31 12:29:50 2038 GMT (Chambers\_of\_Commerce\_Root\_-\_2008.crt)
- China Internet Network Information Center EV Certificates Root, expires Aug 31 07:11:25 2030 GMT  
(China\_Internet\_Network\_Information\_Center\_EV\_Certificates\_Root.crt)
- AAA Certificate Services, expires Dec 31 23:59:59 2028 GMT (Comodo\_AAA\_Services\_root.crt)
- Secure Certificate Services, expires Dec 31 23:59:59 2028 GMT (Comodo\_Secure\_Services\_root.crt)
- Trusted Certificate Services, expires Dec 31 23:59:59 2028 GMT (Comodo\_Trusted\_Services\_root.crt)
- Cybertrust Global Root, expires Dec 15 08:00:00 2021 GMT (Cybertrust\_Global\_Root.crt)
- D-TRUST Root Class 3 CA 2 2009, expires Nov 5 08:35:58 2029 GMT (D-TRUST\_Root\_Class\_3\_CA\_2\_2009.crt)
- D-TRUST Root Class 3 CA 2 EV 2009, expires Nov 5 08:50:46 2029 GMT (D-TRUST\_Root\_Class\_3\_CA\_2\_EV\_2009.crt)
- DST ACES CA X6, expires Nov 20 21:19:58 2017 GMT (DST\_ACES\_CA\_X6.crt)
- DST Root CA X3, expires Sep 30 14:01:15 2021 GMT (DST\_Root\_CA\_X3.crt)
- Deutsche Telekom Root CA 2, expires Jul 9 23:59:00 2019 GMT (Deutsche\_Telekom\_Root\_CA\_2.crt)
- DigiCert Assured ID Root CA, expires Nov 10 00:00:00 2031 GMT (DigiCert\_Assured\_ID\_Root\_CA.crt)
- DigiCert Assured ID Root G2, expires Jan 15 12:00:00 2038 GMT (DigiCert\_Assured\_ID\_Root\_G2.crt)
- DigiCert Assured ID Root G3, expires Jan 15 12:00:00 2038 GMT (DigiCert\_Assured\_ID\_Root\_G3.crt)
- DigiCert Global Root CA, expires Nov 10 00:00:00 2031 GMT (DigiCert\_Global\_Root\_CA.crt)
- DigiCert Global Root G2, expires Jan 15 12:00:00 2038 GMT (DigiCert\_Global\_Root\_G2.crt)
- DigiCert Global Root G3, expires Jan 15 12:00:00 2038 GMT (DigiCert\_Global\_Root\_G3.crt)
- DigiCert High Assurance EV Root CA, expires Nov 10 00:00:00 2031 GMT (DigiCert\_High\_Assurance\_EV\_Root\_CA.crt)
- DigiCert Trusted Root G4, expires Jan 15 12:00:00 2038 GMT (DigiCert\_Trusted\_Root\_G4.crt)
- E-Tugra Certification Authority, expires Mar 3 12:09:48 2023 GMT (E-Tugra\_Certification\_Authority.crt)
- EC-ACC, expires Jan 7 22:59:59 2031 GMT (EC-ACC.crt)
- EE Certification Centre Root CA, expires Dec 17 23:59:59 2030 GMT (EE\_Certification\_Centre\_Root\_CA.crt)
- [Entrust.net](http://Entrust.net)<sup>448</sup> Certification Authority (2048), expires Jul 24 14:15:12 2029 GMT  
(Entrust.net\_Premium\_2048\_Secure\_Server\_CA.crt)
- Entrust Root Certification Authority, expires Nov 27 20:53:42 2026 GMT (Entrust\_Root\_Certification\_Authority.crt)
- Entrust Root Certification Authority - EC1, expires Dec 18 15:55:36 2037 GMT  
(Entrust\_Root\_Certification\_Authority\_-\_EC1.crt)
- Entrust Root Certification Authority - G2, expires Dec 7 17:55:54 2030 GMT (Entrust\_Root\_Certification\_Authority\_-\_G2.crt)
- GeoTrust Global CA, expires May 21 04:00:00 2022 GMT (GeoTrust\_Global\_CA.crt)
- GeoTrust Global CA 2, expires Mar 4 05:00:00 2019 GMT (GeoTrust\_Global\_CA\_2.crt)
- GeoTrust Primary Certification Authority, expires Jul 16 23:59:59 2036 GMT  
(GeoTrust\_Primary\_Certification\_Authority.crt)
- GeoTrust Primary Certification Authority - G2, expires Jan 18 23:59:59 2038 GMT  
(GeoTrust\_Primary\_Certification\_Authority\_-\_G2.crt)
- GeoTrust Primary Certification Authority - G3, expires Dec 1 23:59:59 2037 GMT  
(GeoTrust\_Primary\_Certification\_Authority\_-\_G3.crt)
- GeoTrust Universal CA, expires Mar 4 05:00:00 2029 GMT (GeoTrust\_Universal\_CA.crt)
- GeoTrust Universal CA 2, expires Mar 4 05:00:00 2029 GMT (GeoTrust\_Universal\_CA\_2.crt)
- GlobalSign, expires Jan 19 03:14:07 2038 GMT (GlobalSign\_ECC\_Root\_CA\_-\_R4.crt)

---

<sup>448</sup> <http://Entrust.net>



- GlobalSign, expires Jan 19 03:14:07 2038 GMT (GlobalSign\_ECC\_Root\_CA\_-\_R5.crt)
- GlobalSign Root CA, expires Jan 28 12:00:00 2028 GMT (GlobalSign\_Root\_CA.crt)
- GlobalSign, expires Dec 15 08:00:00 2021 GMT (GlobalSign\_Root\_CA\_-\_R2.crt)
- GlobalSign, expires Mar 18 10:00:00 2029 GMT (GlobalSign\_Root\_CA\_-\_R3.crt)
- Global Chambersign Root - 2008, expires Jul 31 12:31:40 2038 GMT (Global\_Chambersign\_Root\_-\_2008.crt)
- Go Daddy Class 2 Certification Authority, expires Jun 29 17:06:20 2034 GMT (Go\_Daddy\_Class\_2\_CA.crt)
- Go Daddy Root Certificate Authority - G2, expires Dec 31 23:59:59 2037 GMT  
(Go\_Daddy\_Root\_Certificate\_Authority\_-\_G2.crt)
- Hellenic Academic and Research Institutions ECC RootCA 2015, expires Jun 30 10:37:12 2040 GMT  
(Hellenic\_Academic\_and\_Research\_Institutions\_ECC\_RootCA\_2015.crt)
- Hellenic Academic and Research Institutions RootCA 2011, expires Dec 1 13:49:52 2031 GMT  
(Hellenic\_Academic\_and\_Research\_Institutions\_RootCA\_2011.crt)
- Hellenic Academic and Research Institutions RootCA 2015, expires Jun 30 10:11:21 2040 GMT  
(Hellenic\_Academic\_and\_Research\_Institutions\_RootCA\_2015.crt)
- Hongkong Post Root CA 1, expires May 15 04:52:29 2023 GMT (Hongkong\_Post\_Root\_CA\_1.crt)
- ISRG Root X1, expires Jun 4 11:04:38 2035 GMT (ISRG\_Root\_X1.crt)
- IdenTrust Commercial Root CA 1, expires Jan 16 18:12:23 2034 GMT (IdenTrust\_Commercial\_Root\_CA\_1.crt)
- IdenTrust Public Sector Root CA 1, expires Jan 16 17:53:32 2034 GMT (IdenTrust\_Public\_Sector\_Root\_CA\_1.crt)
- Imprivata Embedded Code Signing CA, expires Sep 7 16:20:00 2033 GMT (Imprivata.crt)
- [Izenpe.com](http://Izenpe.com)<sup>449</sup>, expires Dec 13 08:27:25 2037 GMT ([Izenpe.com](http://Izenpe.com)<sup>450</sup>.crt)
- LuxTrust Global Root 2, expires Mar 5 13:21:57 2035 GMT (LuxTrust\_Global\_Root\_2.crt)
- Microsec e-Szigno Root CA 2009, expires Dec 30 11:30:18 2029 GMT (Microsec\_e-Szigno\_Root\_CA\_2009.crt)
- NetLock Arany (Class Gold) Főtanúsítvány, expires Dec 6 15:08:21 2028 GMT  
(NetLock\_Arany\_=Class\_Gold=\_Főtanúsítvány.crt)
- Network Solutions Certificate Authority, expires Dec 31 23:59:59 2029 GMT  
(Network\_Solutions\_Certificate\_Authority.crt)
- OISTE WISEKey Global Root GA CA, expires Dec 11 16:09:51 2037 GMT (OISTE\_WISEKey\_Global\_Root\_GA\_CA.crt)
- OISTE WISEKey Global Root GB CA, expires Dec 1 15:10:31 2039 GMT (OISTE\_WISEKey\_Global\_Root\_GB\_CA.crt)
- OpenTrust Root CA G1, expires Jan 15 00:00:00 2038 GMT (OpenTrust\_Root\_CA\_G1.crt)
- OpenTrust Root CA G2, expires Jan 15 00:00:00 2038 GMT (OpenTrust\_Root\_CA\_G2.crt)
- OpenTrust Root CA G3, expires Jan 15 00:00:00 2038 GMT (OpenTrust\_Root\_CA\_G3.crt)
- Autoridad de Certificacion Raiz del Estado Venezolano, expires Dec 25 23:59:59 2020 GMT (PSCProcert.crt)
- QuoVadis Root Certification Authority, expires Mar 17 18:33:33 2021 GMT (QuoVadis\_Root\_CA.crt)
- QuoVadis Root CA 1 G3, expires Jan 12 17:27:44 2042 GMT (QuoVadis\_Root\_CA\_1\_G3.crt)
- QuoVadis Root CA 2, expires Nov 24 18:23:33 2031 GMT (QuoVadis\_Root\_CA\_2.crt)
- QuoVadis Root CA 2 G3, expires Jan 12 18:59:32 2042 GMT (QuoVadis\_Root\_CA\_2\_G3.crt)
- QuoVadis Root CA 3, expires Nov 24 19:06:44 2031 GMT (QuoVadis\_Root\_CA\_3.crt)
- QuoVadis Root CA 3 G3, expires Jan 12 20:26:32 2042 GMT (QuoVadis\_Root\_CA\_3\_G3.crt)
- SZAFIR ROOT CA2, expires Oct 19 07:43:30 2035 GMT (SZAFIR\_ROOT\_CA2.crt)
- SecureSign RootCA11, expires Apr 8 04:56:47 2029 GMT (SecureSign\_RootCA11.crt)
- SecureTrust CA, expires Dec 31 19:40:55 2029 GMT (SecureTrust\_CA.crt)
- Secure Global CA, expires Dec 31 19:52:06 2029 GMT (Secure\_Global\_CA.crt)
- Security Communication EV RootCA1, expires Jun 6 02:12:32 2037 GMT  
(Security\_Communication\_EV\_RootCA1.crt)
- Security Communication RootCA2, expires May 29 05:00:39 2029 GMT (Security\_Communication\_RootCA2.crt)
- Security Communication RootCA1, expires Sep 30 04:20:49 2023 GMT (Security\_Communication\_Root\_CA.crt)
- Sonera Class2 CA, expires Apr 6 07:29:40 2021 GMT (Sonera\_Class\_2\_Root\_CA.crt)
- Staat der Nederlanden EV Root CA, expires Dec 8 11:10:28 2022 GMT (Staat\_der\_Nederlanden\_EV\_Root\_CA.crt)

<sup>449</sup> <http://Izenpe.com><sup>450</sup> <http://Izenpe.com>



- Staat der Nederlanden Root CA - G2, expires Mar 25 11:03:10 2020 GMT (Staat\_der\_Nederlanden\_Root\_CA\_-\_G2.crt)
- Staat der Nederlanden Root CA - G3, expires Nov 13 23:00:00 2028 GMT (Staat\_der\_Nederlanden\_Root\_CA\_-\_G3.crt)
- Starfield Class 2 Certification Authority, expires Jun 29 17:39:16 2034 GMT (Starfield\_Class\_2\_CA.crt)
- Starfield Root Certificate Authority - G2, expires Dec 31 23:59:59 2037 GMT (Starfield\_Root\_Certificate\_Authority\_-\_G2.crt)
- Starfield Services Root Certificate Authority - G2, expires Dec 31 23:59:59 2037 GMT (Starfield\_Services\_Root\_Certificate\_Authority\_-\_G2.crt)
- SwissSign Gold CA - G2, expires Oct 25 08:30:35 2036 GMT (SwissSign\_Gold\_CA\_-\_G2.crt)
- SwissSign Silver CA - G2, expires Oct 25 08:32:46 2036 GMT (SwissSign\_Silver\_CA\_-\_G2.crt)
- Swisscom Root CA 1, expires Aug 18 22:06:20 2025 GMT (Swisscom\_Root\_CA\_1.crt)
- Swisscom Root CA 2, expires Jun 25 07:38:14 2031 GMT (Swisscom\_Root\_CA\_2.crt)
- Swisscom Root EV CA 2, expires Jun 25 08:45:08 2031 GMT (Swisscom\_Root\_EV\_CA\_2.crt)
- T-TeleSec GlobalRoot Class 2, expires Oct 1 23:59:59 2033 GMT (T-TeleSec\_GlobalRoot\_Class\_2.crt)
- T-TeleSec GlobalRoot Class 3, expires Oct 1 23:59:59 2033 GMT (T-TeleSec\_GlobalRoot\_Class\_3.crt)
- TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1, expires Oct 25 08:25:55 2043 GMT (TUBITAK\_Kamu\_SM\_SSL\_Kok\_Sertifikasi\_-\_Surum\_1.crt)
- TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı, expires Dec 22 18:37:19 2017 GMT (TÜRKTRUST\_Certificate\_Services\_Provider\_Root\_2007.crt)
- TWCA Global Root CA, expires Dec 31 15:59:59 2030 GMT (TWCA\_Global\_Root\_CA.crt)
- TWCA Root Certification Authority, expires Dec 31 15:59:59 2030 GMT (TWCA\_Root\_Certification\_Authority.crt)
- Government Root Certification Authority, expires Dec 5 13:23:33 2032 GMT (Taiwan\_GRCA.crt)
- TeliaSonera Root CA v1, expires Oct 18 12:00:50 2032 GMT (TeliaSonera\_Root\_CA\_v1.crt)
- Trustis FPS Root CA, expires Jan 21 11:36:54 2024 GMT (Trustis\_FPS\_Root\_CA.crt)
- TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3, expires Aug 21 11:37:07 2017 GMT (TÜBİTAK\_UEKAE\_Kök\_Sertifika\_Hizmet\_Sağlayıcısı\_-\_Sürüm\_3.crt)
- TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı H5, expires Apr 28 08:07:01 2023 GMT (TÜRKTRUST\_Elektronik\_Sertifika\_Hizmet\_Sağlayıcısı\_H5.crt)
- USERTrust ECC Certification Authority, expires Jan 18 23:59:59 2038 GMT (USERTrust\_ECC\_Certification\_Authority.crt)
- USERTrust RSA Certification Authority, expires Jan 18 23:59:59 2038 GMT (USERTrust\_RSA\_Certification\_Authority.crt)
- UTN-USERFirst-Hardware, expires Jul 9 18:19:22 2019 GMT (UTN\_USERFirst\_Hardware\_Root\_CA.crt)
- VeriSign Class 3 Public Primary Certification Authority - G4, expires Jan 18 23:59:59 2038 GMT (VeriSign\_Class\_3\_Public\_Primary\_Certification\_Authority\_-\_G4.crt)
- VeriSign Class 3 Public Primary Certification Authority - G5, expires Jul 16 23:59:59 2036 GMT (VeriSign\_Class\_3\_Public\_Primary\_Certification\_Authority\_-\_G5.crt)
- VeriSign Universal Root Certification Authority, expires Dec 1 23:59:59 2037 GMT (VeriSign\_Universal\_Root\_Certification\_Authority.crt)
- VeriSign Class 3 Public Primary Certification Authority - G3, expires Jul 16 23:59:59 2036 GMT (VeriSign\_Class\_3\_Public\_Primary\_Certification\_Authority\_-\_G3.crt)
- Visa eCommerce Root, expires Jun 24 00:16:12 2022 GMT (Visa\_eCommerce\_Root.crt)
- XRamp Global Certification Authority, expires Jan 1 05:37:19 2035 GMT (XRamp\_Global\_CA\_Root.crt)
- certSIGN ROOT CA, expires Jul 4 17:20:04 2031 GMT (certSIGN\_ROOT\_CA.crt)
- ePKI Root Certification Authority, expires Dec 20 02:31:27 2034 GMT (ePKI\_Root\_Certification\_Authority.crt)
- thawte Primary Root CA, expires Jul 16 23:59:59 2036 GMT (thawte\_Primary\_Root\_CA.crt)
- thawte Primary Root CA - G2, expires Jan 18 23:59:59 2038 GMT (thawte\_Primary\_Root\_CA\_-\_G2.crt)
- thawte Primary Root CA - G3, expires Dec 1 23:59:59 2037 GMT (thawte\_Primary\_Root\_CA\_-\_G3.crt)



## 7.18.2 IGEL OS Creator (OSC)

### Supported Devices

| IGEL devices:   |
|-----------------|
| UD2-LX 40       |
| UD3-LX 51       |
| UD3-LX 50       |
| UD5-LX 50       |
| UD6-LX 51       |
| UD7-LX 10       |
| UD9-LX Touch 41 |
| UD9-LX 40       |

For supported devices, see [Third-Party Devices Supported by IGEL OS 11](#)<sup>451</sup>.

- [General Information 11.01.100](#)(see page 1869)
- [Component Versions 11.01.100](#)(see page 1869)

### General Information 11.01.100

- **IGEL OS Creator** is used for **IGEL OS 11** installation and recovery on:
  - Supported IGEL hardware
  - IGEL UD Pocket
  - Supported x86 hardware
- Find details in the IGEL OS Creator manual at <https://kb.igel.com/osc-manual>

### Component Versions 11.01.100

- **Clients**

| Product | Version |
|---------|---------|
|         |         |

<sup>451</sup> <https://kb.igel.com/display/hardware/Third-Party+Devices+Supported+by+IGEL+OS+11>



|                                         |                              |
|-----------------------------------------|------------------------------|
| Oracle JRE                              | 1.8.0_202                    |
| <b>• Smartcard Product</b>              |                              |
| Reader Driver MUSCLE CCID               | 1.4.30-1igel3                |
| Resource Manager PC/SC Lite             | 1.8.23-1igel1                |
| <b>• System Components</b>              |                              |
| OpenSSL                                 | 1.0.2g-1ubuntu4.14           |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5           |
| MESA OpenGL stack                       | 18.3.3-1igel57               |
| VDPAU Library Version                   | 1.1.1-3ubuntu1               |
| Graphics Driver INTEL                   | 2.99.917+git20181113-igel856 |
| Graphics Driver ATI/RADEON              | 18.1.0-1igel854              |
| Graphics Driver ATI/AMDGPU              | 18.1.0-1igel853              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.15-2igel775              |
| Graphics Driver Vboxvideo               | 5.2.18-dfsg-2igel17          |
| Graphics Driver VMware                  | 13.3.0-2igel857              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1igel775         |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |
| Graphics Driver VESA                    | 2.4.0-1igel855               |
| Input Driver Evdev                      | 2.10.5-1ubuntu1igel750       |
| Input Driver Elographics                | 1.4.1-1build5igel633         |
| Input Driver Synaptics                  | 1.9.0-1ubuntu1igel748        |
| Input Driver Vmmouse                    | 13.1.0-1ubuntu2igel635       |
| Input Driver Wacom                      | 0.36.1-0ubuntu1igel813       |
| Kernel                                  | 4.18.20 #mainline-udos-r2517 |



|                                 |                          |
|---------------------------------|--------------------------|
| Xorg X11 Server                 | 1.19.6-1ubuntu4.2igel842 |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1        |
| XFCE4 Windowmanager             | 4.12.3-1ubuntu2igel675   |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7  |
| Python2                         | 2.7.12                   |
| Python3                         | 3.5.2                    |

## 7.19 Notes for Release 10.06.190

Currently, the Release Notes for IGEL OS 10.06.190 are available only in plain text format, see [lx\\_10.06.190.txt](#)<sup>452</sup>.

## 7.20 Notes for Release 10.06.170

|                       |            |             |
|-----------------------|------------|-------------|
| <b>Software:</b>      | Version    | 10.06.170   |
| <b>Release Date:</b>  | 2020-01-24 |             |
| <b>Release Notes:</b> | Version    | RN-106170-1 |
| <b>Last update:</b>   | 2020-01-23 |             |

- [IGEL Linux Universal Desktop](#)(see page 1871)
- [IGEL Universal Desktop OS 3](#)(see page 1883)

### 7.20.1 IGEL Linux Universal Desktop

#### Supported Devices

| <b>Universal Desktop:</b> |                        |
|---------------------------|------------------------|
| UD2-LX:                   | UD2-LX 40              |
| UD3-LX:                   | UD3-LX 51<br>UD3-LX 50 |

<sup>452</sup> [https://www.igel.com/wp-content/uploads/2020/06/lx\\_10.06.190.txt](https://www.igel.com/wp-content/uploads/2020/06/lx_10.06.190.txt)



|          |                                |
|----------|--------------------------------|
| UD5-LX:  | UD5-LX 50                      |
| UD6-LX:  | UD6-LX 51                      |
| UD7-LX:  | UD7-LX 10                      |
| UD9-LX:  | UD9-LX Touch 41<br>UD9-LX 40   |
| UD10-LX: | UD10-LX Touch 10<br>UD10-LX 10 |

**IGEL Zero:**

IZ2-RFX

IZ2-HDX

IZ2-HORIZON

IZ3-RFX

IZ3-HDX

IZ3-HORIZON

- Component Versions 10.06.170(see page 1872)
- General Information 10.06.170(see page 1877)
- Security Fixes 10.06.170(see page 1878)
- Known Issues 10.06.170(see page 1878)
- New Features 10.06.170(see page 1880)
- Resolved Issues 10.06.170(see page 1881)

## Component Versions 10.06.170

• **Clients**

| Product                          | Version    |
|----------------------------------|------------|
| Citrix HDX Realtime Media Engine | 2.8.0-2235 |



|                                       |                                                                        |
|---------------------------------------|------------------------------------------------------------------------|
| Citrix Workspace App                  | 18.10.0.11                                                             |
| Citrix Workspace App                  | 19.10.0.15                                                             |
| Citrix Workspace App                  | 19.12.0.19                                                             |
| deviceTRUST Citrix Channel            | 19.1.200.2                                                             |
| Ericom PowerTerm                      | 12.0.1.0.20170219.2_dev_-34574                                         |
| Evidian AuthMgr                       | 1.5.7116                                                               |
| Evince PDF Viewer                     | 3.18.2-1ubuntu4.5                                                      |
| FabulaTech USB for Remote Desktop     | 5.2.29                                                                 |
| Firefox                               | 68.4.1                                                                 |
| IBM iAccess Client Solutions          | 1.1.8.1                                                                |
| IGEL RDP Client                       | 2.2                                                                    |
| Imprivata OneSign ProveID Embedded    | onesign-bootstrap-loader_1.0.523630_amd64<br>Qualification in progress |
| deviceTRUST RDP Channel               | 19.1.200.2                                                             |
| Leostream Java Connect                | 3.3.7.0                                                                |
| NCP Secure Enterprise Client          | 5.10_rev40552                                                          |
| NX Client                             | 6.5.6                                                                  |
| Open VPN                              | 2.3.10-1ubuntu2.2                                                      |
| Zulu JRE                              | 8.38.0.13                                                              |
| Parallels Client (64 bit)             | 16.5.3.20735                                                           |
| Remote Viewer (RedHat Virtualization) | 8.0-1igel49                                                            |
| Spice GTK (Red Hat Virtualization)    | 0.36-1~git20190601igel61                                               |
| Usbredir (Red Hat Virtualization)     | 0.8.0-1igel49                                                          |
| Systancia AppliDis                    | 4.0.0.17                                                               |



|                       |                      |
|-----------------------|----------------------|
| ThinLinc Client       | 4.10.0-6068          |
| ThinPrint Client      | 7.5.88               |
| Totem Media Player    | 2.30.2               |
| Parole Media Player   | 1.0.1-0ubuntu1igel18 |
| VMware Horizon Client | 5.0.0-12557422       |
| VNC Viewer            | 1.9.0+dfsg-3igel8    |
| Voip Client Ekiga     | 4.0.1                |

- **Dictation**

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20180621 |
| Philips Speech Driver                     | 12.8.5   |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.8    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.3.2    |

- **Smartcard**

|                                           |           |
|-------------------------------------------|-----------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101   |
| PKCS#11 Library Athena IDProtect          | 623.07    |
| PKCS#11 Library cryptovision sc/interface | 7.1.20    |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0 |
| PKCS#11 Library SecMaker NetID            | 6.8.1.31  |



|                                    |                        |
|------------------------------------|------------------------|
| Reader Driver ACS CCID             | 1.1.6-1igel1           |
| Reader Driver Gemalto eToken       | 10.0.37-0              |
| Reader Driver HID Global Omnikey   | 4.3.3                  |
| Reader Driver Identive CCID        | 5.0.35                 |
| Reader Driver Identive eHealth200  | 1.0.5                  |
| Reader Driver Identive SCRKBC      | 5.0.24                 |
| Reader Driver MUSCLE CCID          | 1.4.30-1igel3          |
| Reader Driver REINER SCT cyberJack | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite        | 1.8.23-1igel8          |
| Cherry USB2LAN Proxy               | 3.2.0.3                |

- **System Components**

|                            |                                                  |
|----------------------------|--------------------------------------------------|
| OpenSSL                    | 1.0.2g-1ubuntu4.15                               |
| OpenSSH Client             | 7.2p2-4ubuntu2.8                                 |
| OpenSSH Server             | 7.2p2-4ubuntu2.8                                 |
| Bluetooth stack (bluez)    | 5.50-0ubuntu1igel5                               |
| MESA OpenGL stack          | 19.0.8-1igel73                                   |
| VAAPI ABI Version          | 0.40                                             |
| VDPAU Library version      | 1.1.1-3ubuntu1                                   |
| Graphics Driver INTEL      | 2.99.917+git20191117-igel939                     |
| Graphics Driver ATI/RADEON | 19.0.1-2igel890                                  |
| Graphics Driver ATI/AMDGPU | 19.0.1-4igel894                                  |
| Graphics Driver VIA        | 5.76.52.92-opensource-009-005f78-20150730igel871 |
| Graphics Driver FBDEV      | 0.5.0-1igel819                                   |



|                                 |                              |
|---------------------------------|------------------------------|
| Graphics Driver VESA            | 2.4.0-1igel855               |
| Input Driver Evdev              | 2.10.6-1igel888              |
| Input Driver Elographics        | 1.4.1-1build5igel633         |
| Input Driver eGalax             | 2.5.5814                     |
| Input Driver Synaptics          | 1.9.1-1ubuntu1igel866        |
| Input Driver VMmouse            | 13.1.0-1ubuntu2igel635       |
| Input Driver Wacom              | 0.36.1-0ubuntu2igel888       |
| Kernel                          | 4.19.65 #mainline-ud-r2788   |
| Xorg X11 Server                 | 1.20.5-1igel914              |
| Xorg Xephyr                     | 1.20.5-1igel914              |
| CUPS printing daemon            | 2.1.3-4ubuntu0.9igel27       |
| PrinterLogic                    | 25.1.0.303                   |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1            |
| XFCE4 Window Manager            | 4.12.3-1ubuntu2igel656       |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7      |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.3igel74 |
| ModemManager                    | 1.10.0-1~ubuntu18.04.2igel3  |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.2           |
| GStreamer 1.x                   | 1.16.0-1igel214              |
| WebKit2Gtk                      | 2.26.1-3igel25               |
| Python2                         | 2.7.12                       |
| Python3                         | 3.5.2                        |

- **Features with Limited IGEL Support**

|                                |               |
|--------------------------------|---------------|
| Mobile Device Access USB (MTP) | 1.1.16-2igel1 |
|--------------------------------|---------------|



|                                    |                                  |
|------------------------------------|----------------------------------|
| Mobile Device Access USB (imobile) | 1.2.1~git20181030.92c5462-1igel5 |
| Mobile Device Access USB (gphoto)  | 2.5.22-3igel1                    |
| VPN OpenConnect                    | 7.08-1                           |
| Scanner support / SANE             | 1.0.27-1                         |
| VirtualBox                         | 6.0.8-dfsg-4igel25               |

- **Features with Limited Functionality**

|                   |        |
|-------------------|--------|
| Cisco JVDI Client | 12.1.0 |
|-------------------|--------|

## General Information 10.06.170

The following clients and features are not supported anymore:

- Citrix Receiver 12.1 and 13.1 - 13.4;
- Citrix Access Gateway Standard Plug-in;
- Dell vWorkspace Connector for Linux;
- Ericom PowerTerm Emulation 9 and 11;
- Ericom Webconnect;
- IGEL Legacy RDP Client (rdesktop);
- Virtual Bridges VERDE Client;
- PPTP VPN Support;
- IGEL Upgrade License Tool with IGEL Smartcard Token;
- Remote Management by setup.ini file transfer (TFTP);
- Remote Access via RSH;
- Legacy Philips Speech Driver;
- T-Systems TCOS Smartcard Support;
- DUS Series touchscreens;
- Elo serial touchscreens;
- Video hardware acceleration support is discontinued on UD10-LX Touch 10 and UD10-LX 10;
- H.264 hardware acceleration support is discontinued on UD10-LX Touch 10 and UD10-LX 10;
- Java WebStart;
- Storage hotplug devices are not automatically removed anymore, instead they must always be ejected manually:
  - by a panel tray icon;
  - by an icon in the **In-Session Control Bar** (configurable under **IGEL Setup > User Interface > Desktop**);
  - by a **Safely Remove Hardware** session (configurable under **IGEL Setup > Accessories**).

The following clients and features are not available in this release:

- Cherry eGK Channel;
- Open VPN Smartcard Support;
- Asian Input Methods;
- Composite Manager.



## Security Fixes 10.06.170

### Firefox

- Updated Mozilla **Firefox** to **68.4.1esr**.
- Fix for **mfsa2020-03**, also known as CVE-2019-17026.
- Fixes for **mfsa2020-02**, also known as: CVE-2019-17016, CVE-2019-17017, CVE-2019-17022, and CVE-2019-17024.
- Fixes for **mfsa2019-37**, also known as:  
[More...](#)  
CVE-2019-17008, CVE-2019-11745, CVE-2019-17010, CVE-2019-17005, CVE-2019-17011, and CVE-2019-17012.
- Fixes for **mfsa2019-33**, also known as:  
[More...](#)  
CVE-2019-15903, CVE-2019-11757, CVE-2019-11758, CVE-2019-11759, CVE-2019-11760, CVE-2019-11761, CVE-2019-11762, CVE-2019-11763, and CVE-2019-11764.

## Known Issues 10.06.170

### Firefox

- As the behavior of Firefox has changed, following **settings for “Start in full-screen mode” and “Disable Hotkeys for open new window/tab” can be configured in first browser session only** – these are handled like a usual global setting, means the configuration within another browser session does not have an effect for these two parameters.

### Citrix

- With activated DRI3 and AMD GPU, Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H264, MPEG1 and MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.  
As a workaround, insert the smartcard before starting StoreFront login.
- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" > "For the entire screen".
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264 acceleration plugin**, the following registry key must be enabled:  
[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
|-----------|------------------------------------------------------------------|



|          |                           |
|----------|---------------------------|
| Registry | ica.workaround-dual-rtme  |
| Value    | enabled / <u>disabled</u> |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

#### VMware Horizon

- **External drives** mounted already before connection **do not appear in the remote desktop**.  
Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off.  
In the IGEL Setup client, **drive mapping** can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping**.  
It is also recommended to disable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection entirely** or at least to **deny storage devices** by adding a filter to the USB class rules.  
Furthermore, Horizon Client relies on the OS to mount the storage device itself. Enable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.

#### Parallels Client

- **Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** one time with FIPS support disabled.

#### Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice: spice-xpi** Firefox plugin **is no longer supported**. The **Console Invocation** has to allow **Native client** (auto is also possible) and it should start in fullscreen to prevent opening windows.

#### Wi-Fi

- **TP-Link Archer T2UH Wi-Fi adapters** do not work after system suspend/resume.  
Workaround: Disable system suspend under **IGEL Setup > System > Power Options > Shutdown**.

#### Base system

- Due to the removal of the Oracle JRE, **Java WebStart** is **not supported** anymore.

#### Hardware

- **Suspend on UD10** is disabled.



## New Features 10.06.170

### Citrix

- Integrated **Citrix Workspace App 19.12**
- Available **Citrix Workspace Apps** in this release: **19.12** (default), **19.10**, and **18.10**
- New **registry keys**:
  - Added a registry key for enabling **full-screen banner "Citrix Desktop Viewer"** when starting a Desktop or Application session.

[More...](#)

|           |                                   |
|-----------|-----------------------------------|
| Parameter | Show Citrix Desktop Viewer screen |
| Registry  | ica.module.cdviewerscreen         |
| Value     | <u>off</u> / <u>on</u>            |

- Added a registry key to enable usage of **Chromium Embedded Framework (CEF) for Browser Content Redirection (BCR)** [Experimental].

[More...](#)

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Use Chromium Embedded Framework (CEF) |
| Registry  | ica.allregions.usecefbrowser          |
| Value     | <u>factory default</u> / false / true |

"Factory default" means that can be set by config file.

- Added a registry key to enable/disable **Transparent User Interface [TUI] Virtual Channel [VC] protocol**. The VDTUI protocol is enabled by default.

[More...](#)

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Enable VDTUI protocol                 |
| Registry  | ica.module.virtualdriver.vdtui.enable |
| Value     | <u>off</u> / <u>on</u>                |

- Updated **libwebkit2gtk-4.0-37** to version **2.26.1**. It is now possible to enable **debug output for Citrix Browser Content Redirection** by running the script `/config/bin/install-webkit-debug`. The debug output is written to `/var/log/user/webcontainer.debug`. **CAUTION: You can run only short sessions with enabled debug output** because a lot of debugging data is written to the log file.

### Firefox

- Updated **Fluendo multimedia codecs** to the following versions:
  - gst-fluendo-h264dec - 18/09/2019 0.10.54
  - gst-fluendo-vadec - 16/10/2019 0.10.210

### Imprivata

- Usage of 500 MB for the Imprivata data partition** when **flash** is **bigger than 2 GB**.

### OS 11 Upgrade



- Add parameter to **skip battery checking in OS 11 Upgrade.**

[More...](#)

|           |                                                                                                           |
|-----------|-----------------------------------------------------------------------------------------------------------|
| Parameter | Use at your own risk! Turns Battery safety check into warning only.<br>Any unbootable systems are on you. |
| Registry  | update.battery_is_only_warning                                                                            |
| Value     | enabled / <u>disabled</u>                                                                                 |

#### IGEL Cloud Gateway

- Added **support for shadowing via ICG.**

#### Resolved Issues 10.06.170

##### Imprivata

- Fixed **race condition** that may lead to **unexpected behavior with RDP connections.**
- Fixed **VMware Horizon session disconnect.**
- Fixed **Lock-key** and **Tap-out behavior.**
- Fixed **MS RDSH session.**

##### VMware Horizon

- Fixed **sound in Horizon client 5.x** using **PCoIP** protocol.

##### Caradigm

- **Caradigm restart loops** fixed.

##### Base system

- Fixed potential temporary **settings loss** when **resuming from standby.**
- **Automatic firmware update** is now checked after retrieval of UMS settings.
- When there are any **non-applied changes in the network configuration**, the **network will be reconfigured before the firmware update** starts.
- Re-fixed broken **custom bootsplash** when doing a **reset to factory defaults via UMS.**

##### Smartcard

- Updated **SecMaker Net iD smartcard library** to version **6.8.1.31**. The changes are:
 

[More...](#)

  - Support for **Gemalto IDPrime 940** and **3940**.
  - Support for new **VRK card** (IDEA IAS ECC, spec: FINEID S1 - FINEID S1 Electronic ID Application v4.0).
  - Support for **Aventra MyEID v4.0** (customer specific card profile with read support only).
    - Fixed problem with **detection of cards in Net iD Card Portal.**
    - Other fixes, see release notes at SecMaker.
  - Fixed **smartcard user names displayed on login screen**: non-ASCII characters were not shown correctly before.
  - Fixed **error message on login screen** shown when **smartcard PIN** is locked.



- Fixed handling of smartcards in **pcsc-lite: improved transaction locking**.  
A new parameter was introduced to control the new behavior (enabled by default):  
[More...](#)

|           |                                        |
|-----------|----------------------------------------|
| Parameter | Abort stalled transactions             |
| Registry  | scard.pcscd.abort_stalled_transactions |
| Value     | <u>enabled</u> / disabled              |

- Fixed IGEL Smartcard to be able to handle **VoIP client Ekiga sessions**.

#### Driver

- Updated **Philips Speech Driver** to version **12.8.5**.
- Updated **StepOver TCP Client** to version **2.3.2**.

#### CUPS Printing

- Updated **Printer Installer client** to version **25.1.0.303**.
- **Added** missing **CUPS model names** for some CUPS printers.

#### X11 system

- Fixed an issue with **modesetting driver** and **DisplayLink USB graphic adapters**.
- **Removed** registry key `x.drivers.glamor.use_dri3` as it is of no real use.
- **Updated Intel Xorg driver** to work fix issues with **DisplayLink USB adapters**.
- Fixed issue with **Wacom Signing Pads not being recognized as displays**.

#### X server

- Fix **HP Elitebook Display** issue **with HP Ultrathin Docking Station**.

#### Network

- Fixed issue when configuring **more than one NTP server**.
- Fixed **missing library with openconnect** feature.

#### OS 11 Upgrade

- Add special **warning when not connected to power line in upgrade boot**.

#### RDP/IGEL RDP Client 2

- Fixed **RDP Web Access Domain Visibility** not working correctly.

#### Remote Management

- Fixed broken **logon into Shared Workplace** on devices that are managed over **ICG**.
- Fixed **responding to requests searching an available buddy update server**.

#### VNC

- Fixed **sporadic connection failure in the VNC server**.



## 7.20.2 IGEL Universal Desktop OS 3

### Supported Hardware

<https://kb.igel.com/udc3-supported-devices>

- [Component Versions 10.06.170](#)(see page 1883)
- [General Information 10.06.170](#)(see page 1887)
- [Security Fixes 10.06.170](#)(see page 1888)
- [Known Issues 10.06.170](#)(see page 1889)
- [New Features 10.06.170](#)(see page 1890)
- [Resolved Issues 10.06.170](#)(see page 1891)

### Component Versions 10.06.170

#### • Clients

| Product                           | Version                         |
|-----------------------------------|---------------------------------|
| Citrix HDX Realtime Media Engine  | 2.8.0-2235                      |
| Citrix Workspace App              | 18.10.0.11                      |
| Citrix Workspace App              | 19.10.0.15                      |
| Citrix Workspace App              | 19.12.0.19                      |
| deviceTRUST Citrix Channel        | 19.1.200.2                      |
| Ericom PowerTerm                  | 12.0.1.0.20170219.2-_dev_-34574 |
| Evidian AuthMgr                   | 1.5.7116                        |
| Evince PDF Viewer                 | 3.18.2-1ubuntu4.5               |
| FabulaTech USB for Remote Desktop | 5.2.29                          |
| Firefox                           | 68.4.1                          |
| IBM iAccess Client Solutions      | 1.1.8.1                         |
| IGEL RDP Client                   | 2.2                             |



|                                       |                                                                        |
|---------------------------------------|------------------------------------------------------------------------|
| Imprivata OneSign ProveID Embedded    | onesign-bootstrap-loader_1.0.523630_amd64<br>Qualification in progress |
| deviceTRUST RDP Channel               | 19.1.200.2                                                             |
| Leostream Java Connect                | 3.3.7.0                                                                |
| NCP Secure Enterprise Client          | 5.10_rev40552                                                          |
| NX Client                             | 6.5.6                                                                  |
| Open VPN                              | 2.3.10-1ubuntu2.2                                                      |
| Zulu JRE                              | 8.38.0.13                                                              |
| Parallels Client (64 bit)             | 16.5.3.20735                                                           |
| Remote Viewer (RedHat Virtualization) | 8.0-1igel49                                                            |
| Spice GTK (Red Hat Virtualization)    | 0.36-1~git20190601igel61                                               |
| Usbredir (Red Hat Virtualization)     | 0.8.0-1igel49                                                          |
| Systancia AppliDis                    | 4.0.0.17                                                               |
| ThinLinc Client                       | 4.10.0-6068                                                            |
| ThinPrint Client                      | 7.5.88                                                                 |
| Totem Media Player                    | 2.30.2                                                                 |
| Parole Media Player                   | 1.0.1-0ubuntu1igel18                                                   |
| VMware Horizon Client                 | 5.0.0-12557422                                                         |
| VNC Viewer                            | 1.9.0+dfsg-3igel8                                                      |
| Voip Client Ekiga                     | 4.0.1                                                                  |

- **Dictation**

|                                           |      |
|-------------------------------------------|------|
| Diktamen driver for dictation             |      |
| Grundig Business Systems dictation driver |      |
| Nuance Audio Extensions for dictation     | B301 |



|                              |          |
|------------------------------|----------|
| Olympus driver for dictation | 20180621 |
| Philips Speech Driver        | 12.8.5   |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.8    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.3.2    |

- **Smartcard**

|                                           |                        |
|-------------------------------------------|------------------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101                |
| PKCS#11 Library Athena IDProtect          | 623.07                 |
| PKCS#11 Library cryptovision sc/interface | 7.1.20                 |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0              |
| PKCS#11 Library SecMaker NetID            | 6.8.1.31               |
| Reader Driver ACS CCID                    | 1.1.6-1igel1           |
| Reader Driver Gemalto eToken              | 10.0.37-0              |
| Reader Driver HID Global Omnikey          | 4.3.3                  |
| Reader Driver Identive CCID               | 5.0.35                 |
| Reader Driver Identive eHealth200         | 1.0.5                  |
| Reader Driver Identive SCRKBC             | 5.0.24                 |
| Reader Driver MUSCLE CCID                 | 1.4.30-1igel3          |
| Reader Driver REINER SCT cyberJack        | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite               | 1.8.23-1igel8          |
| Cherry USB2LAN Proxy                      | 3.2.0.3                |



- System Components**

|                                         |                                                      |
|-----------------------------------------|------------------------------------------------------|
| OpenSSL                                 | 1.0.2g-1ubuntu4.15                                   |
| OpenSSH Client                          | 7.2p2-4ubuntu2.8                                     |
| OpenSSH Server                          | 7.2p2-4ubuntu2.8                                     |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5                                   |
| MESA OpenGL stack                       | 19.0.8-1igel73                                       |
| VAAPI ABI Version                       | 0.40                                                 |
| VDPAU Library version                   | 1.1.1-3ubuntu1                                       |
| Graphics Driver INTEL                   | 2.99.917+git20191117-igel939                         |
| Graphics Driver ATI/RADEON              | 19.0.1-2igel890                                      |
| Graphics Driver ATI/AMDGPU              | 19.0.1-4igel894                                      |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867                                      |
| Graphics Driver Nvidia                  | 390.116-0ubuntu0.18.10.1                             |
| Graphics Driver VIA                     | 5.76.52.92-<br>opensource-009-005f78-20150730igel871 |
| Graphics Driver Vboxvideo               | 1.0.0-igel798                                        |
| Graphics Driver VMware                  | 13.3.0-2igel857                                      |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1igel775                                 |
| Graphics Driver FBDEV                   | 0.5.0-1igel819                                       |
| Graphics Driver VESA                    | 2.4.0-1igel855                                       |
| Input Driver Evdev                      | 2.10.6-1igel888                                      |
| Input Driver Elographics                | 1.4.1-1build5igel633                                 |
| Input Driver eGalax                     | 2.5.5814                                             |
| Input Driver Synaptics                  | 1.9.1-1ubuntu1igel866                                |
| Input Driver VMmouse                    | 13.1.0-1ubuntu2igel635                               |
| Input Driver Wacom                      | 0.36.1-0ubuntu2igel888                               |



|                                 |                              |
|---------------------------------|------------------------------|
| Kernel                          | 4.19.65 #mainline-udos-r2788 |
| Xorg X11 Server                 | 1.20.5-1igel914              |
| Xorg Xephyr                     | 1.20.5-1igel914              |
| CUPS Printing Daemon            | 2.1.3-4ubuntu0.9igel27       |
| PrinterLogic                    | 25.1.0.303                   |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1            |
| XFCE4 Window Manager            | 4.12.3-1ubuntu2igel656       |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7      |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.3igel74 |
| ModemManager                    | 1.10.0-1~ubuntu18.04.2igel3  |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.2           |
| GStreamer 1.x                   | 1.16.0-1igel214              |
| WebKit2Gtk                      | 2.26.1-3igel25               |
| Python2                         | 2.7.12                       |
| Python3                         | 3.5.2                        |

- **Features with Limited IGEL Support**

|                                    |                                  |
|------------------------------------|----------------------------------|
| Mobile Device Access USB (MTP)     | 1.1.16-2igel1                    |
| Mobile Device Access USB (imobile) | 1.2.1~git20181030.92c5462-1igel5 |
| Mobile Device Access USB (gphoto)  | 2.5.22-3igel1                    |
| VPN OpenConnect                    | 7.08-1                           |
| Scanner support / SANE             | 1.0.27-1                         |
| VirtualBox                         | 6.0.8-dfsg-4igel25               |

- **Features with Limited Functionality**

|                   |        |
|-------------------|--------|
| Cisco JVDI Client | 12.1.0 |
|-------------------|--------|

## General Information 10.06.170

The following clients and features are not supported anymore:



- Citrix Receiver 12.1 and 13.1 - 13.4;
- Citrix Access Gateway Standard Plug-in;
- Dell vWorkspace Connector for Linux;
- Ericom PowerTerm Emulation 9 and 11;
- Ericom Webconnect;
- IGEL Legacy RDP Client (rdesktop);
- Virtual Bridges VERDE Client;
- PPTP VPN Support;
- IGEL Upgrade License Tool with IGEL Smartcard Token;
- Remote Management by setup.ini file transfer (TFTP);
- Remote Access via RSH;
- Legacy Philips Speech Driver;
- T-Systems TCOS Smartcard Support;
- DUS Series touchscreens;
- Elo serial touchscreens;
- VIA Graphics support;
- Java WebStart;
- Storage hotplug devices are not automatically removed anymore, instead they must be always ejected manually:
  - by panel tray icon;
  - by an icon in the **In-Session Control Bar** (configurable under **IGEL Setup > User Interface > Desktop**);
  - by a **Safely Remove Hardware** session (configurable under **IGEL Setup > Accessories**).

The following clients and features are not available in this release:

- Cherry eGK Channel;
- Open VPN Smartcard Support;
- Asian Input Methods;
- Composite Manager.

## Security Fixes 10.06.170

### Firefox

- Updated Mozilla **Firefox** to **68.4.1esr**.
- Fix for **mfsa2020-03**, also known as CVE-2019-17026.
- Fixes for **mfsa2020-02**, also known as: CVE-2019-17016, CVE-2019-17017, CVE-2019-17022, and CVE-2019-17024.
- Fixes for **mfsa2019-37**, also known as:  
[More...](#)

CVE-2019-17008, CVE-2019-11745, CVE-2019-17010,  
CVE-2019-17005, CVE-2019-17011, and CVE-2019-17012.

- Fixes for **mfsa2019-33**, also known as:  
[More...](#)



CVE-2019-15903, CVE-2019-11757, CVE-2019-11758,  
 CVE-2019-11759, CVE-2019-11760, CVE-2019-11761,  
 CVE-2019-11762, CVE-2019-11763, and CVE-2019-11764.

## Known Issues 10.06.170

### Firefox

- As the behavior of Firefox has changed, following **settings for “Start in full-screen mode” and “Disable Hotkeys for open new window/tab” can be configured in first browser session only** – these are handled like a usual global setting, means the configuration within another browser session does not have an effect for these two parameters.

### Citrix

- With activated DRI3 and AMD GPU, Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H264, MPEG1 and MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.  
 As a workaround, insert the smartcard before starting StoreFront login.
- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" > "For the entire screen".
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264 acceleration plugin**, the following registry key must be enabled:  
[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Value     | enabled / disabled                                               |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

### VMware Horizon

- External drives** mounted already before connection **do not appear in the remote desktop**.  
 Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off.  
 In the IGEL Setup client, **drive mapping** can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping**.



It is also recommended to disable local **Storage Hotplug** under Setup > **Devices > Storage Devices > Storage Hotplug**.

- On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection entirely** or at least to **deny storage devices** by adding a filter to the USB class rules.

Furthermore, Horizon Client relies on the OS to mount the storage device itself. Enable local **Storage Hotplug** under Setup >**Devices > Storage Devices > Storage Hotplug**.

#### Parallels Client

- **Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** one time with FIPS support disabled.

#### Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice: spice-xpi** Firefox plugin **is no longer supported**. The **Console Invocation** has to allow **Native client** (auto is also possible) and it should start in fullscreen to prevent opening windows.

#### Multimedia

- **Multimedia redirection with GStreamer** could fail with the **Nouveau GPU** driver.

#### Wi-Fi

- **TP-Link Archer T2UH Wi-Fi adapters** do not work after system suspend/resume.  
Workaround: Disable system suspend under **IGEL Setup > System > Power Options > Shutdown**.

#### Base system

- Due to the removal of the Oracle JRE, **Java WebStart** is **not supported** anymore.

### New Features 10.06.170

#### Citrix

- Integrated **Citrix Workspace App 19.12**
- Available **Citrix Workspace Apps** in this release: **19.12** (default), **19.10**, and **18.10**
- New **registry keys**:
  - Added a registry key for enabling **full-screen banner "Citrix Desktop Viewer"** when starting a Desktop or Application session.  
[More...](#)

|           |                                   |
|-----------|-----------------------------------|
| Parameter | Show Citrix Desktop Viewer screen |
| Registry  | ica.module.cdvviewerscreen        |
| Value     | off / on                          |

- Added a registry key to enable usage of **Chromium Embedded Framework (CEF) for Browser Content Redirection (BCR)** [Experimental].



[More...](#)

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Use Chromium Embedded Framework (CEF) |
| Registry  | ica.allregions.usecefbrowser          |
| Value     | <u>factory default</u> / false / true |

"Factory default" means that can be set by config file.

- Added a registry key to enable/disable **Transparent User Interface [TUI] Virtual Channel [VC] protocol**. The VDTUI protocol is enabled by default.

[More...](#)

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Enable VDTUI protocol                 |
| Registry  | ica.module.virtualdriver.vdtui.enable |
| Value     | off / <u>on</u>                       |

- Updated **libwebkit2gtk-4.0-37** to version **2.26.1**. It is now possible to enable **debug output for Citrix Browser Content Redirection** by running the script /config/bin/install-webkit-debug. The debug output is written to /var/log/user/webcontainer.debug. **CAUTION: You can run only short sessions with enabled debug output** because a lot of debugging data is written to the log file.

## Firefox

- Updated **Fluendo multimedia codecs** to the following versions:  
gst-fluendo-h264dec - 18/09/2019 0.10.54  
gst-fluendo-vadec - 16/10/2019 0.10.210

## Imprivata

- Usage of 500 MB for the Imprivata data partition** when **flash** is **bigger than 2 GB**.

## OS 11 Upgrade

- Add parameter to **skip battery checking in OS 11 Upgrade**.

[More...](#)

|           |                                                                                                        |
|-----------|--------------------------------------------------------------------------------------------------------|
| Parameter | Use at your own risk! Turns Battery safety check into warning only. Any unbootable systems are on you. |
| Registry  | update.battery_is_only_warning                                                                         |
| Value     | enabled / <u>disabled</u>                                                                              |

## IGEL Cloud Gateway

- Added **support for shadowing via ICG**.

## Resolved Issues 10.06.170

### Imprivata

- Fixed **race condition** that may lead to **unexpected behavior with RDP connections**.
- Fixed **VMware Horizon session disconnect**.



- Fixed **Lock-key** and **Tap-out behavior**.
- Fixed **MS RDSH** session.

#### VMware Horizon

- Fixed **sound in Horizon client 5.x** using **PCoIP** protocol.

#### Caradigm

- **Caradigm restart loops** fixed.

#### Base system

- Fixed potential temporary **settings loss** when **resuming from standby**.
- **Automatic firmware update** is now checked after retrieval of UMS settings.
- When there are any **non-applied changes in the network configuration**, the **network** will be **reconfigured before the firmware update** starts.
- Re-fixed broken **custom bootsplash** when doing a **reset to factory defaults via UMS**.

#### Smartcard

- Updated **SecMaker Net iD smartcard library** to version **6.8.1.31**. The changes are:
  - More...**
  - Support for **Gemalto IDPrime 940** and **3940**.
  - Support for new **VRK card** (IDEA IAS ECC, spec: FINEID S1 - FINEID S1 Electronic ID Application v4.0).
  - Support for **Aventra MyEID v4.0** (customer specific card profile with read support only).
  - Fixed problem with **detection of cards in Net iD Card Portal**.
  - Other fixes, see release notes at SecMaker.
- Fixed **smartcard user names displayed on login screen**: non-ASCII characters were not shown correctly before.
- Fixed **error message on login screen** shown when **smartcard PIN** is locked.
- Fixed handling of smartcards in **pcsc-lite: improved transaction locking**.  
A new parameter was introduced to control the new behavior (enabled by default):
  - More...**

|           |                                        |
|-----------|----------------------------------------|
| Parameter | Abort stalled transactions             |
| Registry  | scard.pcscd.abort_stalled_transactions |
| Value     | <u>enabled</u> / disabled              |

- Fixed IGEL Smartcard to be able to handle **VoIP client Ekiga sessions**.

#### Driver

- Updated **Philips Speech Driver** to version **12.8.5**.
- Updated **StepOver TCP Client** to version **2.3.2**.

#### CUPS Printing

- Updated **Printer Installer client** to version **25.1.0.303**.
- **Added** missing **CUPS model names** for some CUPS printers.

#### X11 system



- Fixed an issue with **modesetting driver** and **DisplayLink USB graphic adapters**.
- **Removed** registry key `x.drivers.glamor.use_dri3` as it is of no real use.
- **Updated Intel Xorg driver** to work fix issues with **DisplayLink USB adapters**.
- Fixed issue with **Wacom Signing Pads not being recognized as displays**.

#### X server

- Fix **HP Elitebook Display** issue **with HP Ultrasmart Docking Station**.

#### Network

- Fixed issue when configuring **more than one NTP server**.
- Fixed **missing library with openconnect** feature.

#### OS 11 Upgrade

- Add special **warning when not connected to power line in upgrade boot**.

#### RDP/IGEL RDP Client 2

- Fixed **RDP Web Access Domain Visibility** not working correctly.

#### Remote Management

- Fixed broken **logon into Shared Workplace** on devices that are managed over **ICG**.
- Fixed **responding to requests searching** an available **buddy update server**.

#### VNC

- Fixed **sporadic connection failure in the VNC server**.

## 7.21 Notes for Release 10.06.130

|                       |            |             |
|-----------------------|------------|-------------|
| <b>Software:</b>      | Version    | 10.06.130   |
| <b>Release Date:</b>  | 2019-09-09 |             |
| <b>Release Notes:</b> | Version    | RN-106130-1 |
| <b>Last update:</b>   | 2019-09-09 |             |

- [IGEL Linux Universal Desktop](#)(see page 1893)
- [IGEL Universal Desktop OS 3](#)(see page 1903)

### 7.21.1 IGEL Linux Universal Desktop

#### Supported Devices

##### Universal Desktop:



|          |                  |
|----------|------------------|
| UD2-LX:  | UD2-LX 40        |
| UD3-LX:  | UD3-LX 51        |
|          | UD3-LX 50        |
| UD5-LX:  | UD5-LX 50        |
| UD6-LX:  | UD6-LX 51        |
| UD7-LX:  | UD7-LX 10        |
| UD9-LX:  | UD9-LX Touch 41  |
|          | UD9-LX 40        |
| UD10-LX: | UD10-LX Touch 10 |
|          | UD10-LX 10       |

**IGEL Zero:**

IZ2-RFX

IZ2-HDX

IZ2-HORIZON

IZ3-RFX

IZ3-HDX

IZ3-HORIZON

- 
- Component Versions 10.06.130(see page 1895)
  - General Information 10.06.130(see page 1899)
  - Security Fixes 10.06.130(see page 1900)
  - Known Issues 10.06.130(see page 1900)
  - Resolved Issues 10.06.130(see page 1901)



## Component Versions 10.06.130

• **Clients**

| <b>Product</b>                     | <b>Version</b>                            |
|------------------------------------|-------------------------------------------|
| Citrix HDX Realtime Media Engine   | 2.8.0-2235                                |
| Citrix Receiver                    | 13.10.0.20                                |
| Citrix Workspace App               | 19.3.0.5                                  |
| Citrix Workspace App               | 19.6.0.60                                 |
| deviceTRUST Citrix Channel         | 19.1.200.2                                |
| Ericom PowerTerm                   | 12.0.1.0.20170219.2-_dev_-34574           |
| Evidian AuthMgr                    | 1.5.7116                                  |
| Evince PDF Viewer                  | 3.18.2-1ubuntu4.5                         |
| FabulaTech USB for Remote Desktop  | 5.2.29                                    |
| Firefox                            | 60.9.0                                    |
| IBM iAccess Client Solutions       | 1.1.8.1                                   |
| IGEL RDP Client                    | 2.2                                       |
| Imprivata OneSign ProveID Embedded | onesign-bootstrap-loader_1.0.523630_amd64 |
| deviceTRUST RDP Channel            | 19.1.200.2                                |
| Leostream Java Connect             | 3.3.7.0                                   |
| NCP Secure Enterprise Client       | 5.10_rev40552                             |
| NX Client                          | 6.5.6                                     |
| Open VPN                           | 2.3.10-1ubuntu2.2                         |
| Zulu JRE                           | 8.38.0.13                                 |
| Parallels Client (64 bit)          | 16.5.3.20735                              |



|                                       |                          |
|---------------------------------------|--------------------------|
| Remote Viewer (RedHat Virtualization) | 8.0-1igel49              |
| Spice GTK (Red Hat Virtualization)    | 0.36-1~git20190601igel61 |
| Usbredir (Red Hat Virtualization)     | 0.8.0-1igel49            |
| Systancia AppliDis                    | 4.0.0.17                 |
| ThinLinc Client                       | 4.10.0-6068              |
| ThinPrint Client                      | 7.5.88                   |
| Totem Media Player                    | 2.30.2                   |
| Parole Media Player                   | 1.0.1-0ubuntu1igel18     |
| VMware Horizon Client                 | 5.0.0-12557422           |
| VNC Viewer                            | 1.9.0+dfsg-3igel8        |
| Voip Client Ekiga                     | 4.0.1                    |

- **Dictation**

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20180621 |
| Philips Speech Driver                     | 12.7.11  |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.8    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.1.0    |

- **Smartcard**

|                                  |         |
|----------------------------------|---------|
| PKCS#11 Library A.E.T SafeSign   | 3.0.101 |
| PKCS#11 Library Athena IDProtect | 623.07  |



|                                           |                        |
|-------------------------------------------|------------------------|
| PKCS#11 Library cryptovision sc/interface | 7.1.20                 |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0              |
| PKCS#11 Library SecMaker NetID            | 6.7.2.36               |
| Reader Driver ACS CCID                    | 1.1.6-1igel1           |
| Reader Driver Gemalto eToken              | 10.0.37-0              |
| Reader Driver HID Global Omnikey          | 4.3.3                  |
| Reader Driver Identive CCID               | 5.0.35                 |
| Reader Driver Identive eHealth200         | 1.0.5                  |
| Reader Driver Identive SCRKBC             | 5.0.24                 |
| Reader Driver MUSCLE CCID                 | 1.4.30-1igel3          |
| Reader Driver REINER SCT cyberJack        | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite               | 1.8.23-1igel1          |
| Cherry USB2LAN Proxy                      | 3.2.0.3                |

- **System Components**

|                            |                              |
|----------------------------|------------------------------|
| OpenSSL                    | 1.0.2g-1ubuntu4.15           |
| OpenSSH Client             | 7.2p2-4ubuntu2.8             |
| OpenSSH Server             | 7.2p2-4ubuntu2.8             |
| Bluetooth stack (bluez)    | 5.50-0ubuntu1igel5           |
| MESA OpenGL stack          | 19.0.8-1igel73               |
| VAAPI ABI Version          | 0.40                         |
| VDPAU Library version      | 1.1.1-3ubuntu1               |
| Graphics Driver INTEL      | 2.99.917+git20190301-igel870 |
| Graphics Driver ATI/RADEON | 19.0.1-2igel890              |



|                                 |                                                  |
|---------------------------------|--------------------------------------------------|
| Graphics Driver ATI/AMDGPU      | 19.0.1-4igel894                                  |
| Graphics Driver VIA             | 5.76.52.92-opensource-009-005f78-20150730igel871 |
| Graphics Driver FBDEV           | 0.5.0-1igel819                                   |
| Graphics Driver VESA            | 2.4.0-1igel855                                   |
| Input Driver Evdev              | 2.10.6-1igel888                                  |
| Input Driver Elographics        | 1.4.1-1build5igel633                             |
| Input Driver eGalax             | 2.5.5814                                         |
| Input Driver Synaptics          | 1.9.1-1ubuntu1igel866                            |
| Input Driver VMmouse            | 13.1.0-1ubuntu2igel635                           |
| Input Driver Wacom              | 0.36.1-0ubuntu2igel888                           |
| Kernel                          | 4.19.65 #mainline-ud-r2788                       |
| Xorg X11 Server                 | 1.20.5-1igel914                                  |
| Xorg Xephyr                     | 1.20.5-1igel914                                  |
| CUPS printing daemon            | 2.1.3-4ubuntu0.9igel27                           |
| PrinterLogic                    | 18.2.1.128                                       |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1                                |
| XFCE4 Window Manager            | 4.12.3-1ubuntu2igel656                           |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7                          |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.3igel74                     |
| ModemManager                    | 1.10.0-1~ubuntu18.04.2igel3                      |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.2                               |
| GStreamer 1.x                   | 1.16.0-1igel214                                  |
| WebKit2Gtk                      | 2.24.2-0ubuntu0.19.04.1igel18                    |
| Python2                         | 2.7.12                                           |



|         |       |
|---------|-------|
| Python3 | 3.5.2 |
|---------|-------|

• **Features with Limited IGEL Support**

|                                    |                                  |
|------------------------------------|----------------------------------|
| Mobile Device Access USB (MTP)     | 1.1.16-2igel1                    |
| Mobile Device Access USB (imobile) | 1.2.1~git20181030.92c5462-1igel5 |
| Mobile Device Access USB (gphoto)  | 2.5.22-3igel1                    |
| VPN OpenConnect                    | 7.08-1                           |
| Scanner support / SANE             | 1.0.27-1                         |
| VirtualBox                         | 6.0.8-dfsg-4igel25               |

• **Features with Limited Functionality**

|                   |        |
|-------------------|--------|
| Cisco JVDI Client | 12.1.0 |
|-------------------|--------|

## General Information 10.06.130

The following clients and features are not supported anymore:

- Citrix Receiver 12.1 and 13.1 - 13.4;
- Citrix Access Gateway Standard Plug-in;
- Dell vWorkspace Connector for Linux;
- Ericom PowerTerm Emulation 9 and 11;
- Ericom Webconnect;
- IGEL Legacy RDP Client (rdesktop);
- Virtual Bridges VERDE Client;
- PPTP VPN Support;
- IGEL Upgrade License Tool with IGEL Smartcard Token;
- Remote Management by setup.ini file transfer (TFTP);
- Remote Access via RSH;
- Legacy Philips Speech Driver;
- T-Systems TCOS Smartcard Support;
- DUS Series touchscreens;
- Elo serial touchscreens;
- Video hardware acceleration support is discontinued on UD10-LX Touch 10 and UD10-LX 10;
- H.264 hardware acceleration support is discontinued on UD10-LX Touch 10 and UD10-LX 10;
- Java WebStart;
- Storage hotplug devices are not automatically removed anymore, instead they must always be ejected manually:
  - by a panel tray icon;
  - by an icon in the **In-Session Control Bar** (configurable under **IGEL Setup > User Interface > Desktop**);
  - by a **Safely Remove Hardware** session (configurable under **IGEL Setup > Accessories**).

The following clients and features are not available in this release:



- Cherry eGK Channel;
- Open VPN Smartcard Support;
- Asian Input Methods;
- Composite Manager.

## Security Fixes 10.06.130

### Firefox

- Updated **Mozilla Firefox** to version **60.9.0 ESR**.  
Including fixes from **Security Advisory 2019-27**:  
[More...](#)

CVE-2019-11746, CVE-2019-11744, CVE-2019-11753, CVE-2019-11752,  
CVE-2019-9812, CVE-2019-11743, and CVE-2019-11740.

## Known Issues 10.06.130

### Citrix

- With activated DRI3 and AMD GPU, Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H264, MPEG1 and MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.  
As a workaround, insert the smartcard before starting StoreFront login.
- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" > "For the entire screen".
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264 acceleration plugin**, the following registry key must be enabled:  
[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Value     | <u>enabled</u> / <u>disabled</u>                                 |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

### VMware Horizon

- **External drives** mounted already before connection **do not appear in the remote desktop**.  
Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.



- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off. In the IGEL Setup client, **drive mapping** can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping**. It is also recommended to disable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection entirely** or at least to **deny storage devices** by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage device itself. Enable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.

#### Parallels Client

- **Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** one time with FIPS support disabled.

#### Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice: spice-xpi** Firefox plugin **is no longer supported**. The **Console Invocation** has to allow **Native client** (auto is also possible) and it should start in fullscreen to prevent opening windows.

#### Wi-Fi

- **TP-Link Archer T2UH Wi-Fi adapters** do not work after system suspend/resume. Workaround: Disable system suspend under **IGEL Setup > System > Power Options > Shutdown**.

#### Base system

- Due to the removal of the Oracle JRE, **Java WebStart** is **not supported** anymore.

#### Hardware

- **Suspend on UD10** is disabled.

## Resolved Issues 10.06.130

#### RDP/IGEL RDP Client 2

- Fixed **RDP graphics issues with Windows 2008(R2) Server** (when **RemoteFX** is not enabled).
- Fixed some smaller **graphical RDP issues with Windows 2012 R2** if using **Clearcodec**.

#### Network

- Changed **minimally allowed MSS size** to '**750**' to avoid problems with some VPN solutions.
- Added a new registry key to be able to configure the **minimally allowed TCP MSS size**. A new registry key:



[More...](#)

|           |                                                                             |
|-----------|-----------------------------------------------------------------------------|
| Parameter | Minimal TCP send MSS size                                                   |
| Registry  | system.sysctl.tcp_min_snd_mss                                               |
| Type      | Integer                                                                     |
| Value     | 750                                                                         |
| Tooltip   | Minimal TCP send MSS size (configurable value in the area from 200 to 1450) |

#### OS 11 Upgrade

- Fixed **OS11 Upgrade failing** when IGEL Setup Assistant is auto started.

#### Base system

- Removed deprecated registry keys system.idlecommand....

#### X11 system

- Fixed problem with **modesetting driver** and **2 x 2160x1440 monitors** in extended configuration.
- Added a new registry key to enable the **use of linear framebuffer for modesetting driver**.

A new registry key:

|           |                                                          |
|-----------|----------------------------------------------------------|
| Parameter | Use linear instead of tiled framebuffer                  |
| Registry  | x.drivers.modesetting.use_linear_framebuffer             |
| Range     | [Default] [False] [True]                                 |
| Value     | "Default" (use linear framebuffer only in special cases) |

- Added a new registry key to disable/enable the use of DRI3 with GLAMOR acceleration.

A new registry key:

|           |                                                                             |
|-----------|-----------------------------------------------------------------------------|
| Parameter | Disable/Enable usage of DRI3 in GLAMOR acceleration                         |
| Registry  | x.drivers.glamor.use_dri3                                                   |
| Range     | [Auto] [False] [True]                                                       |
| Value     | "Auto" (use no DRI3 functions for modesetting driver with only DRI2 active) |

- Added new registry keys to be able to configure some modesetting options if needed.

New registry keys:

[More...](#)

|           |                                                          |
|-----------|----------------------------------------------------------|
| Parameter | Use DRI3 PageFlip feature                                |
| Registry  | x.drivers.modesetting.use_page_flip                      |
| Range     | [Default] [False] [True]                                 |
| Info      | "Default" (normally use page flip feature)               |
| Parameter | Use shadow framebuffer layer                             |
| Registry  | x.drivers.modesetting.use_shadow_fb                      |
| Range     | [Default] [False] [True]                                 |
| Info      | "Default" (normally use shadow framebuffer)              |
| Parameter | Use double shadow framebuffer to improve VNC performance |
| Registry  | x.drivers.modesetting.use_double_shadow                  |



|           |                                                              |
|-----------|--------------------------------------------------------------|
| Range     | <u>[False]</u> [True]                                        |
| Parameter | Use software cursor for modesetting driver                   |
| Registry  | x.drivers.modesetting.use_sw_cursor                          |
| Range     | <u>[Default]</u> [False] [True]                              |
| Info      | "Default" (normally false)                                   |
| Parameter | Choose acceleration method                                   |
| Registry  | x.drivers.modesetting.accel_method                           |
| Range     | <u>[Default]</u> [Glamor] [None]                             |
| Info      | "Default" (normally Glamor is used)                          |
| Parameter | Force usage of DRI3 regardless of x.drivers.use_dri3 setting |
| Registry  | x.drivers.modesetting.force_dri3                             |
| Type      | Bool                                                         |
| Value     | <u>False</u>                                                 |

## X server

- Fixed **Xorg freezes** if using **modesetting driver** and **video acceleration**.

## Hardware

- Fixed **EFI freeze** problem **after bootcode update on** devices like the **HP t630** and probably others too.
- Added support for newer **Prolific PL2303 USB serial adapters**.

## 7.21.2 IGEL Universal Desktop OS 3

Supported Hardware:

<https://kb.igel.com/udc3-supported-devices>

- Component Versions 10.06.130(see page 1903)
- General Information 10.06.130(see page 1908)
- Security Fixes 10.06.130(see page 1909)
- Known Issues 10.06.130(see page 1909)
- New Features 10.06.130(see page 1910)
- Resolved Issues 10.06.130(see page 1911)

## Component Versions 10.06.130

- **Clients**

| Product                          | Version    |
|----------------------------------|------------|
| Citrix HDX Realtime Media Engine | 2.8.0-2235 |



|                                       |                                           |
|---------------------------------------|-------------------------------------------|
| Citrix Receiver                       | 13.10.0.20                                |
| Citrix Workspace App                  | 19.3.0.5                                  |
| Citrix Workspace App                  | 19.6.0.60                                 |
| deviceTRUST Citrix Channel            | 19.1.200.2                                |
| Ericom PowerTerm                      | 12.0.1.0.20170219.2_dev_-34574            |
| Evidian AuthMgr                       | 1.5.7116                                  |
| Evince PDF Viewer                     | 3.18.2-1ubuntu4.5                         |
| FabulaTech USB for Remote Desktop     | 5.2.29                                    |
| Firefox                               | 60.9.0                                    |
| IBM iAccess Client Solutions          | 1.1.8.1                                   |
| IGEL RDP Client                       | 2.2                                       |
| Imprivata OneSign ProveID Embedded    | onesign-bootstrap-loader_1.0.523630_amd64 |
| deviceTRUST RDP Channel               | 19.1.200.2                                |
| Leostream Java Connect                | 3.3.7.0                                   |
| NCP Secure Enterprise Client          | 5.10_rev40552                             |
| NX Client                             | 6.5.6                                     |
| Open VPN                              | 2.3.10-1ubuntu2.2                         |
| Zulu JRE                              | 8.38.0.13                                 |
| Parallels Client (64 bit)             | 16.5.3.20735                              |
| Remote Viewer (RedHat Virtualization) | 8.0-1igel49                               |
| Spice GTK (Red Hat Virtualization)    | 0.36-1~git20190601igel61                  |
| Usbredir (Red Hat Virtualization)     | 0.8.0-1igel49                             |
| Systancia AppliDis                    | 4.0.0.17                                  |



|                       |                      |
|-----------------------|----------------------|
| ThinLinc Client       | 4.10.0-6068          |
| ThinPrint Client      | 7.5.88               |
| Totem Media Player    | 2.30.2               |
| Parole Media Player   | 1.0.1-0ubuntu1igel18 |
| VMware Horizon Client | 5.0.0-12557422       |
| VNC Viewer            | 1.9.0+dfsg-3igel8    |
| Voip Client Ekiga     | 4.0.1                |

- **Dictation**

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20180621 |
| Philips Speech Driver                     | 12.7.11  |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.8    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.1.0    |

- **Smartcard**

|                                           |           |
|-------------------------------------------|-----------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101   |
| PKCS#11 Library Athena IDProtect          | 623.07    |
| PKCS#11 Library cryptovision sc/interface | 7.1.20    |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0 |
| PKCS#11 Library SecMaker NetID            | 6.7.2.36  |



|                                    |                        |
|------------------------------------|------------------------|
| Reader Driver ACS CCID             | 1.1.6-1igel1           |
| Reader Driver Gemalto eToken       | 10.0.37-0              |
| Reader Driver HID Global Omnikey   | 4.3.3                  |
| Reader Driver Identive CCID        | 5.0.35                 |
| Reader Driver Identive eHealth200  | 1.0.5                  |
| Reader Driver Identive SCRKBC      | 5.0.24                 |
| Reader Driver MUSCLE CCID          | 1.4.30-1igel3          |
| Reader Driver REINER SCT cyberJack | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite        | 1.8.23-1igel1          |
| Cherry USB2LAN Proxy               | 3.2.0.3                |

- **System Components**

|                                         |                                                      |
|-----------------------------------------|------------------------------------------------------|
| OpenSSL                                 | 1.0.2g-1ubuntu4.15                                   |
| OpenSSH Client                          | 7.2p2-4ubuntu2.8                                     |
| OpenSSH Server                          | 7.2p2-4ubuntu2.8                                     |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5                                   |
| MESA OpenGL stack                       | 19.0.8-1igel73                                       |
| VAAPI ABI Version                       | 0.40                                                 |
| VDPAU Library version                   | 1.1.1-3ubuntu1                                       |
| Graphics Driver INTEL                   | 2.99.917+git20190301-igel870                         |
| Graphics Driver ATI/RADEON              | 19.0.1-2igel890                                      |
| Graphics Driver ATI/AMDGPU              | 19.0.1-4igel894                                      |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867                                      |
| Graphics Driver Nvidia                  | 390.116-0ubuntu0.18.10.1                             |
| Graphics Driver VIA                     | 5.76.52.92-<br>opensource-009-005f78-20150730igel871 |



|                                 |                               |
|---------------------------------|-------------------------------|
| Graphics Driver Vboxvideo       | 1.0.0-igel798                 |
| Graphics Driver VMware          | 13.3.0-2igel857               |
| Graphics Driver QXL (Spice)     | 0.1.5-2build1igel775          |
| Graphics Driver FBDEV           | 0.5.0-1igel819                |
| Graphics Driver VESA            | 2.4.0-1igel855                |
| Input Driver Evdev              | 2.10.6-1igel888               |
| Input Driver Elographics        | 1.4.1-1build5igel633          |
| Input Driver eGalax             | 2.5.5814                      |
| Input Driver Synaptics          | 1.9.1-1ubuntu1igel866         |
| Input Driver VMmouse            | 13.1.0-1ubuntu2igel635        |
| Input Driver Wacom              | 0.36.1-0ubuntu2igel888        |
| Kernel                          | 4.19.65 #mainline-udos-r2788  |
| Xorg X11 Server                 | 1.20.5-1igel914               |
| Xorg Xephyr                     | 1.20.5-1igel914               |
| CUPS Printing Daemon            | 2.1.3-4ubuntu0.9igel27        |
| PrinterLogic                    | 18.2.1.128                    |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1             |
| XFCE4 Window Manager            | 4.12.3-1ubuntu2igel656        |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7       |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.3igel74  |
| ModemManager                    | 1.10.0-1~ubuntu18.04.2igel3   |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.2            |
| GStreamer 1.x                   | 1.16.0-1igel214               |
| WebKit2Gtk                      | 2.24.2-0ubuntu0.19.04.1igel18 |
| Python2                         | 2.7.12                        |



|                                              |                                  |
|----------------------------------------------|----------------------------------|
| Python3                                      | 3.5.2                            |
| <b>• Features with Limited IGEL Support</b>  |                                  |
| Mobile Device Access USB (MTP)               | 1.1.16-2igel1                    |
| Mobile Device Access USB (imobile)           | 1.2.1~git20181030.92c5462-1igel5 |
| Mobile Device Access USB (gphoto)            | 2.5.22-3igel1                    |
| VPN OpenConnect                              | 7.08-1                           |
| Scanner support / SANE                       | 1.0.27-1                         |
| VirtualBox                                   | 6.0.8-dfsg-4igel25               |
| <b>• Features with Limited Functionality</b> |                                  |
| Cisco JVDI Client                            | 12.1.0                           |

## General Information 10.06.130

The following clients and features are not supported anymore:

- Citrix Receiver 12.1 and 13.1 - 13.4;
- Citrix Access Gateway Standard Plug-in;
- Dell vWorkspace Connector for Linux;
- Ericom PowerTerm Emulation 9 and 11;
- Ericom Webconnect;
- IGEL Legacy RDP Client (rdesktop);
- Virtual Bridges VERDE Client;
- PPTP VPN Support;
- IGEL Upgrade License Tool with IGEL Smartcard Token;
- Remote Management by setup.ini file transfer (TFTP);
- Remote Access via RSH;
- Legacy Philips Speech Driver;
- T-Systems TCOS Smartcard Support;
- DUS Series touchscreens;
- Elo serial touchscreens;
- VIA Graphics support;
- Java WebStart;
- Storage hotplug devices are not automatically removed anymore, instead they must be always ejected manually:
  - by panel tray icon;
  - by an icon in the **In-Session Control Bar** (configurable under **IGEL Setup > User Interface > Desktop**);
  - by a **Safely Remove Hardware** session (configurable under **IGEL Setup > Accessories**).

The following clients and features are not available in this release:



- Cherry eGK Channel;
- Open VPN Smartcard Support;
- Asian Input Methods;
- Composite Manager.

## Security Fixes 10.06.130

### Firefox

- Updated **Mozilla Firefox** to version **60.9.0 ESR**.  
Including fixes from **Security Advisory 2019-27**:  
[More...](#)

CVE-2019-11746, CVE-2019-11744, CVE-2019-11753, CVE-2019-11752,  
CVE-2019-9812, CVE-2019-11743, and CVE-2019-11740.

## Known Issues 10.06.130

### Citrix

- With activated DRI3 and AMD GPU, Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H264, MPEG1 and MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.  
As a workaround, insert the smartcard before starting StoreFront login.
- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" > "For the entire screen".
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264 acceleration plugin**, the following registry key must be enabled:  
[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Value     | <u>enabled</u> / <u>disabled</u>                                 |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

### VMware Horizon

- **External drives** mounted already before connection **do not appear in the remote desktop**.  
Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.



- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off. In the IGEL Setup client, **drive mapping** can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping**. It is also recommended to disable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection entirely** or at least to **deny storage devices** by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage device itself. Enable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.

#### Parallels Client

- **Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** one time with FIPS support disabled.

#### Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice: spice-xpi** Firefox plugin **is no longer supported**. The **Console Invocation** has to allow **Native client** (auto is also possible) and it should start in fullscreen to prevent opening windows.

#### Multimedia

- **Multimedia redirection with GStreamer** could fail with the **Nouveau GPU** driver.

#### Wi-Fi

- **TP-Link Archer T2UH Wi-Fi adapters** do not work after system suspend/resume. Workaround: Disable system suspend under **IGEL Setup > System > Power Options > Shutdown**.

#### Base system

- Due to the removal of the Oracle JRE, **Java WebStart** is **not supported** anymore.

## New Features 10.06.130

#### Hardware

- Added basic support for **HP t510** devices.
- Re-added **VIA driver for HP t510** to OS firmware (only limited support; provided "as is", without the guarantee of correct functionality).



## Resolved Issues 10.06.130

### RDP/IGEL RDP Client 2

- Fixed **RDP graphics issues with Windows 2008(R2) Server** (when **RemoteFX** is not enabled).
- Fixed some smaller **graphical RDP issues with Windows 2012 R2** if using **Clearcodec**.

### Network

- Changed **minimally allowed MSS size** to '750' to avoid problems with some VPN solutions.
- Added a new registry key to be able to configure the **minimally allowed TCP MSS size**.

A new registry key:

[More...](#)

|           |                                                                             |
|-----------|-----------------------------------------------------------------------------|
| Parameter | Minimal TCP send MSS size                                                   |
| Registry  | system.sysctl.tcp_min_snd_mss                                               |
| Type      | Integer                                                                     |
| Value     | <u>750</u>                                                                  |
| Tooltip   | Minimal TCP send MSS size (configurable value in the area from 200 to 1450) |

### OS 11 Upgrade

- Fixed **OS11 Upgrade failing** when IGEL Setup Assistant is auto started.

### Base system

- Removed deprecated registry keys `system.idlecommand` . . . .

### X11 system

- Fixed problem with **modesetting driver** and **2 x 2160x1440 monitors** in extended configuration.
- Added a new registry key to enable the **use of linear framebuffer for modesetting driver**.

A new registry key:

|           |                                                          |
|-----------|----------------------------------------------------------|
| Parameter | Use linear instead of tiled framebuffer                  |
| Registry  | x.drivers.modesetting.use_linear_framebuffer             |
| Range     | [Default] [False] [True]                                 |
| Value     | "Default" (use linear framebuffer only in special cases) |

- Added a new registry key to disable/enable the use of DRI3 with GLAMOR acceleration.

A new registry key:

|           |                                                                             |
|-----------|-----------------------------------------------------------------------------|
| Parameter | Disable/Enable usage of DRI3 in GLAMOR acceleration                         |
| Registry  | x.drivers.glamor.use_dri3                                                   |
| Range     | [Auto] [False] [True]                                                       |
| Value     | "Auto" (use no DRI3 functions for modesetting driver with only DRI2 active) |

- Added new registry keys to be able to **configure some modesetting options** if needed.

New registry keys:

[More...](#)

|           |                           |
|-----------|---------------------------|
| Parameter | Use DRI3 PageFlip feature |
|-----------|---------------------------|



|           |                                                              |
|-----------|--------------------------------------------------------------|
| Registry  | x.drivers.modesetting.use_page_flip                          |
| Range     | [Default] [False] [True]                                     |
| Info      | "Default" (normally use page flip feature)                   |
| Parameter | Use shadow framebuffer layer                                 |
| Registry  | x.drivers.modesetting.use_shadow_fb                          |
| Range     | [Default] [False] [True]                                     |
| Info      | "Default" (normally use shadow framebuffer)                  |
| Parameter | Use double shadow framebuffer to improve VNC performance     |
| Registry  | x.drivers.modesetting.use_double_shadow                      |
| Range     | [False] [True]                                               |
| Parameter | Use software cursor for modesetting driver                   |
| Registry  | x.drivers.modesetting.use_sw_cursor                          |
| Range     | [Default] [False] [True]                                     |
| Info      | "Default" (normally false)                                   |
| Parameter | Choose acceleration method                                   |
| Registry  | x.drivers.modesetting.accel_method                           |
| Range     | [Default] [Glamor] [None]                                    |
| Info      | "Default" (normally Glamor is used)                          |
| Parameter | Force usage of DRI3 regardless of x.drivers.use_dri3 setting |
| Registry  | x.drivers.modesetting.force_dri3                             |
| Type      | Bool                                                         |
| Value     | False                                                        |

## X server

- Fixed **Xorg freezes** if using **modesetting driver** and **video acceleration**.

## Hardware

- Fixed **EFI freeze** problem **after bootcode update on** devices like the **HP t630** and probably others too.
- Added support for newer **Prolific PL2303 USB serial adapters**.

## 7.22 Notes for Release 10.06.120

|                       |            |             |
|-----------------------|------------|-------------|
| <b>Software:</b>      | Version    | 10.06.120   |
| <b>Release Date:</b>  | 2019-08-23 |             |
| <b>Release Notes:</b> | Version    | RN-106120-1 |
| <b>Last update:</b>   | 2019-08-23 |             |



- [IGEL Linux Universal Desktop \(see page 1913\)](#)
- [IGEL Universal Desktop OS 3 \(see page 1925\)](#)

### 7.22.1 IGEL Linux Universal Desktop

#### Supported Devices

| <b>Universal Desktop:</b> |                                |
|---------------------------|--------------------------------|
| UD2-LX:                   | UD2-LX 40                      |
| UD3-LX:                   | UD3-LX 51<br>UD3-LX 50         |
| UD5-LX:                   | UD5-LX 50                      |
| UD6-LX:                   | UD6-LX 51                      |
| UD7-LX:                   | UD7-LX 10                      |
| UD9-LX:                   | UD9-LX Touch 41<br>UD9-LX 40   |
| UD10-LX:                  | UD10-LX Touch 10<br>UD10-LX 10 |
| <b>IGEL Zero:</b>         |                                |
| IZ2-RFX                   |                                |
| IZ2-HDX                   |                                |
| IZ2-HORIZON               |                                |
| IZ3-RFX                   |                                |
| IZ3-HDX                   |                                |
| IZ3-HORIZON               |                                |



- Component Versions 10.06.120(see page 1914)
- General Information 10.06.120(see page 1918)
- Security Fixes 10.06.120(see page 1919)
- Known Issues 10.06.120(see page 1923)
- New Features 10.06.120(see page 1925)
- Resolved Issues 10.06.120(see page 1925)

## Component Versions 10.06.120

### • Clients

| <b>Product</b>                     | <b>Version</b>                            |
|------------------------------------|-------------------------------------------|
| Citrix HDX Realtime Media Engine   | 2.8.0-2235                                |
| Citrix Receiver                    | 13.10.0.20                                |
| Citrix Workspace App               | 19.3.0.5                                  |
| Citrix Workspace App               | 19.6.0.60                                 |
| deviceTRUST Citrix Channel         | 19.1.200.2                                |
| Ericom PowerTerm                   | 12.0.1.0.20170219.2-_dev_-34574           |
| Evidian AuthMgr                    | 1.5.7116                                  |
| Evince PDF Viewer                  | 3.18.2-1ubuntu4.5                         |
| FabulaTech USB for Remote Desktop  | 5.2.29                                    |
| Firefox                            | 60.8.0                                    |
| IBM iAccess Client Solutions       | 1.1.8.1                                   |
| IGEL RDP Client                    | 2.2                                       |
| Imprivata OneSign ProveID Embedded | onesign-bootstrap-loader_1.0.523630_amd64 |
| deviceTRUST RDP Channel            | 19.1.200.2                                |
| Leostream Java Connect             | 3.3.7.0                                   |
| NCP Secure Enterprise Client       | 5.10_rev40552                             |



|                                       |                          |
|---------------------------------------|--------------------------|
| NX Client                             | 6.5.6                    |
| Open VPN                              | 2.3.10-1ubuntu2.2        |
| Zulu JRE                              | 8.38.0.13                |
| Parallels Client (64 bit)             | 16.5.3.20735             |
| Remote Viewer (RedHat Virtualization) | 8.0-1igel49              |
| Spice GTK (Red Hat Virtualization)    | 0.36-1~git20190601igel61 |
| Usbredir (Red Hat Virtualization)     | 0.8.0-1igel49            |
| Systancia AppliDis                    | 4.0.0.17                 |
| ThinLinc Client                       | 4.10.0-6068              |
| ThinPrint Client                      | 7.5.88                   |
| Totem Media Player                    | 2.30.2                   |
| Parole Media Player                   | 1.0.1-0ubuntu1igel18     |
| VMware Horizon Client                 | 5.0.0-12557422           |
| VNC Viewer                            | 1.9.0+dfsg-3igel8        |
| Voip Client Ekiga                     | 4.0.1                    |

- **Dictation**

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20180621 |
| Philips Speech Driver                     | 12.7.11  |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.8    |
| signotec VCOM Daemon      | 2.0.0    |



|                     |       |
|---------------------|-------|
| StepOver TCP Client | 2.1.0 |
|---------------------|-------|

- **Smartcard**

|                                           |                        |
|-------------------------------------------|------------------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101                |
| PKCS#11 Library Athena IDProtect          | 623.07                 |
| PKCS#11 Library cryptovision sc/interface | 7.1.20                 |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0              |
| PKCS#11 Library SecMaker NetID            | 6.7.2.36               |
| Reader Driver ACS CCID                    | 1.1.6-1igel1           |
| Reader Driver Gemalto eToken              | 10.0.37-0              |
| Reader Driver HID Global Omnikey          | 4.3.3                  |
| Reader Driver Identive CCID               | 5.0.35                 |
| Reader Driver Identive eHealth200         | 1.0.5                  |
| Reader Driver Identive SCRKBC             | 5.0.24                 |
| Reader Driver MUSCLE CCID                 | 1.4.30-1igel3          |
| Reader Driver REINER SCT cyberJack        | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite               | 1.8.23-1igel1          |
| Cherry USB2LAN Proxy                      | 3.2.0.3                |

- **System Components**

|                         |                    |
|-------------------------|--------------------|
| OpenSSL                 | 1.0.2g-1ubuntu4.15 |
| OpenSSH Client          | 7.2p2-4ubuntu2.8   |
| OpenSSH Server          | 7.2p2-4ubuntu2.8   |
| Bluetooth stack (bluez) | 5.50-0ubuntu1igel5 |
| MESA OpenGL stack       | 19.0.8-1igel73     |
| VAAPI ABI Version       | 0.40               |



|                                 |                                                  |
|---------------------------------|--------------------------------------------------|
| VDPAU Library version           | 1.1.1-3ubuntu1                                   |
| Graphics Driver INTEL           | 2.99.917+git20190301-igel870                     |
| Graphics Driver ATI/RADEON      | 19.0.1-2igel890                                  |
| Graphics Driver ATI/AMDGPU      | 19.0.1-4igel894                                  |
| Graphics Driver VIA             | 5.76.52.92-opensource-009-005f78-20150730igel871 |
| Graphics Driver FBDEV           | 0.5.0-1igel819                                   |
| Graphics Driver VESA            | 2.4.0-1igel855                                   |
| Input Driver Evdev              | 2.10.6-1igel888                                  |
| Input Driver Elographics        | 1.4.1-1build5igel633                             |
| Input Driver eGalax             | 2.5.5814                                         |
| Input Driver Synaptics          | 1.9.1-1ubuntu1igel866                            |
| Input Driver VMmouse            | 13.1.0-1ubuntu2igel635                           |
| Input Driver Wacom              | 0.36.1-0ubuntu2igel888                           |
| Kernel                          | 4.19.65 #mainline-ud-r2782                       |
| Xorg X11 Server                 | 1.20.5-1igel891                                  |
| Xorg Xephyr                     | 1.20.5-1igel891                                  |
| CUPS printing daemon            | 2.1.3-4ubuntu0.9igel27                           |
| PrinterLogic                    | 18.2.1.128                                       |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1                                |
| XFCE4 Window Manager            | 4.12.3-1ubuntu2igel656                           |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7                          |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.3igel74                     |



|                |                               |
|----------------|-------------------------------|
| ModemManager   | 1.10.0-1~ubuntu18.04.2igel3   |
| GStreamer 0.10 | 0.10.36-2ubuntu0.2            |
| GStreamer 1.x  | 1.16.0-1igel214               |
| WebKit2Gtk     | 2.24.2-0ubuntu0.19.04.1igel18 |
| Python2        | 2.7.12                        |
| Python3        | 3.5.2                         |

- **Features with Limited IGEL Support**

|                                    |                                  |
|------------------------------------|----------------------------------|
| Mobile Device Access USB (MTP)     | 1.1.16-2igel1                    |
| Mobile Device Access USB (imobile) | 1.2.1~git20181030.92c5462-1igel5 |
| Mobile Device Access USB (gphoto)  | 2.5.22-3igel1                    |
| VPN OpenConnect                    | 7.08-1                           |
| Scanner support / SANE             | 1.0.27-1                         |
| VirtualBox                         | 6.0.8-dfsg-4igel25               |

- **Features with Limited Functionality**

|                   |        |
|-------------------|--------|
| Cisco JVDI Client | 12.1.0 |
|-------------------|--------|

## General Information 10.06.120

The following clients and features are not supported anymore:

- Citrix Receiver 12.1 and 13.1 - 13.4;
- Citrix Access Gateway Standard Plug-in;
- Dell vWorkspace Connector for Linux;
- Ericom PowerTerm Emulation 9 and 11;
- Ericom Webconnect;
- IGEL Legacy RDP Client (rdesktop);
- Virtual Bridges VERDE Client;
- PPTP VPN Support;
- IGEL Upgrade License Tool with IGEL Smartcard Token;
- Remote Management by setup.ini file transfer (TFTP);
- Remote Access via RSH;
- Legacy Philips Speech Driver;
- T-Systems TCOS Smartcard Support;
- DUS Series touch screens;
- Elo serial touchscreens;
- Video hardware acceleration support is discontinued on UD10-LX Touch 10 and UD10-LX 10;
- H.264 hardware acceleration support is discontinued on UD10-LX Touch 10 and UD10-LX 10;



- Java WebStart;
- Storage hotplug devices are not automatically removed anymore, instead they must always be ejected manually:
  - by panel tray icon;
  - by an icon in the **In-Session Control Bar** (configurable under **IGEL Setup > User Interface > Desktop**);
  - by a **Safely Remove Hardware** session (configurable under **IGEL Setup > Accessories**).

The following clients and features are not available in this release:

- Cherry eGK Channel;
- Open VPN Smartcard Support;
- Asian Input Methods;
- Composite Manager.

## Security Fixes 10.06.120

### Firefox

- Updated **Firefox** browser to version **60.8.0 ESR**.
- Fixed **mfsa2019-22** security issues:  
[More...](#)

CVE-2019-9811, CVE-2019-11711, CVE-2019-11712, CVE-2019-11713, CVE-2019-11729, CVE-2019-11715, CVE-2019-11717, CVE-2019-11719, CVE-2019-11730 and CVE-2019-11709.

- Fixed **mfsa2019-19** security issue CVE-2019-11708.
  - Fixed **mfsa2019-18** security issue CVE-2019-11707.
  - Fixed **mfsa2019-08** security issues:  
[More...](#)
- CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2018-18506 and CVE-2019-9788.
- Fixed **mfsa2019-05** security issues CVE-2018-18356 and CVE-2019-5785.
  - Fixed **mfsa2019-02** security issues CVE-2018-18500, CVE-2018-18505 and CVE-2018-18501.

### Shared Workplace

- Fixed **login in Shared Workplace** which accepts any user credentials in the 10.06.100 release. However, no user settings were applied to the device.

### Base system

- Updated **kernel** to version **4.19.65**.
- Fixed security issue CVE-2019-1125 aka **Spectre SWAPGS gadget vulnerability**.
- Fixed a vulnerability in **Java configuration script**.
- Fixed possibly malicious **owner change** with TC setup configuration.
- Fixed **policykit-1** security issues CVE-2018-19788 and CVE-2019-6133.
- Fixed **NSS** security issues CVE-2018-18508, CVE-2018-12404, CVE-2018-12384 and CVE-2018-0495.
- Fixed **PPP** security issue CVE-2018-11574.
- Fixed **imagemagick** security issues.

**More...**

CVE-2018-16750, CVE-2018-16749, CVE-2018-16645, CVE-2018-16644, CVE-2018-16643, CVE-2018-16642, CVE-2018-16640, CVE-2018-16323, CVE-2018-14437, CVE-2018-14436, CVE-2018-14435, CVE-2018-14434, CVE-2017-13144, CVE-2017-12430, CVE-2019-9956, CVE-2019-7398, CVE-2019-7397, CVE-2019-7396, CVE-2019-7175, CVE-2019-11598, CVE-2019-11597, CVE-2019-11472, CVE-2019-11470, CVE-2019-10650, CVE-2019-10131, CVE-2018-20467, CVE-2018-18025, CVE-2018-18024, CVE-2018-18016, CVE-2018-17966, CVE-2018-17965, CVE-2018-16413, CVE-2018-16412, CVE-2017-12806, and CVE-2017-12805.

- Fixed **systemd** security issues.

**More...**

CVE-2018-16866, CVE-2018-16865, CVE-2018-16864, CVE-2018-15688, CVE-2019-6454, CVE-2018-1049, CVE-2018-15686 and CVE-2019-3842.

- Fixed **CUPS** security issue CVE-2018-4700.

- Fixed **libarchive** security issues.

**More...**

CVE-2019-1000020, CVE-2019-1000019, CVE-2018-1000878, CVE-2018-1000877, and CVE-2017-14502.

- Fixed **avahi** security issues CVE-2018-1000845 and CVE-2017-6519.

- Fixed **bind9** security issues CVE-2019-6465, CVE-2018-5745, and CVE-2018-5743.

- Fixed **libcaca** security issues.

**More...**

CVE-2018-20549, CVE-2018-20548, CVE-2018-20547, CVE-2018-20546, CVE-2018-20545, and CVE-2018-20544.

- Fixed **libgd2** security issues CVE-2019-6978 and CVE-2019-6977.

- Fixed **ghostscript** security issues.

**More...**

CVE-2019-6116, CVE-2018-19477, CVE-2018-19476, CVE-2018-19475, CVE-2018-19409, CVE-2018-18284, CVE-2018-18073, CVE-2018-17961, CVE-2019-3838, and CVE-2019-3835.

- Fixed **krb5** security issues.

**More...**

CVE-2018-5730, CVE-2018-5729, CVE-2017-11462, CVE-2017-11368, CVE-2016-3120, and CVE-2016-3119.

- Fixed **texlive-bin** security issue CVE-2018-17407.

- Fixed **LDB** security issue CVE-2019-3824.

- Fixed **libmspack** security issues CVE-2018-18585 and CVE-2018-18584.

- Fixed **Perl** security issues CVE-2018-18314, CVE-2018-18313, CVE-2018-18312 and CVE-2018-18311.

- Fixed **poppler** security issues.

**More...**



CVE-2019-7310, CVE-2018-20650, CVE-2018-20551, CVE-2018-20481, CVE-2018-19149, CVE-2018-19060, CVE-2018-19059, CVE-2018-19058, CVE-2018-16646, and CVE-2019-9200.

- Fixed **Python 3.5** security issues CVE-2018-14647, CVE-2018-1061, CVE-2018-1060 and CVE-2018-106.
- Fixed **Net-SNMP** security issue CVE-2018-18065.
- Fixed **OpenSSL** security issues CVE-2019-1559, CVE-2018-5407 and CVE-2018-0734.
- Fixed **TIFF** security issues.

**More...**

CVE-2018-8905, CVE-2018-7456, CVE-2018-18661, CVE-2018-18557, CVE-2018-17101, CVE-2018-17100, CVE-2018-1710, CVE-2018-10963, CVE-2019-7663, CVE-2019-6128, CVE-2018-19210, CVE-2018-17000, CVE-2018-12900, and CVE-2018-10779.

- Fixed **libvncserver** security issues.

**More...**

CVE-2018-6307, CVE-2018-20750, CVE-2018-20749, CVE-2018-20748, CVE-2018-20024, CVE-2018-20023, CVE-2018-20022, CVE-2018-20021, CVE-2018-20020, CVE-2018-20019, CVE-2018-15127, and CVE-2018-15126.

- Fixed **WavPack** security issue CVE-2018-19840.
- Fixed **Samba** security issues.

**More...**

CVE-2018-16851, CVE-2018-16841, CVE-2018-14629, CVE-2019-3880, and CVE-2018-16860.

- Fixed **libxkbcommon** security issues.

**More...**

CVE-2018-15864, CVE-2018-15863, CVE-2018-15862, CVE-2018-15861, CVE-2018-15859, CVE-2018-15858, CVE-2018-15857, CVE-2018-15856, CVE-2018-15855, CVE-2018-15854, and CVE-2018-15853.

- Fixed **OpenSSH** security issues.

**More...**

CVE-2019-6111, CVE-2019-6109, CVE-2018-20685, CVE-2018-15473, and CVE-2016-10708.

- Fixed **Python 2.7** security issues.

**More...**

CVE-2018-14647, CVE-2018-1061, CVE-2018-1060, CVE-2018-106, CVE-2018-1000802, and CVE-2018-1000030.

- Fixed **lxml** security issue CVE-2018-19787.
- Fixed **gdk-pixbuf** security issues.

**More...**

CVE-2017-6314, CVE-2017-6313, CVE-2017-6312, CVE-2017-6311, CVE-2017-2870, CVE-2017-2862, CVE-2017-1000422, CVE-2016-6352, and CVE-2017-12447.



- Fixed **file** security issues CVE-2019-8907 and CVE-2019-8905.
- Fixed **wget** security issue CVE-2019-5953.
- Fixed **libxslt** security issue CVE-2019-11068.
- Fixed **Evince** security issue CVE-2019-11459.
- Fixed **webkit2gtk** security issues.

**More...**

CVE-2019-8595, CVE-2019-8607, CVE-2019-8615, CVE-2019-6251, CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378, CVE-2018-4382, CVE-2018-4392, CVE-2018-4416, CVE-2018-4345, CVE-2018-4386, and CVE-2018-4372.

- Fixed **gst-plugins-base0.10** security issue CVE-2019-9928.
- Fixed **WPA** security issues.

**More...**

CVE-2019-9495, CVE-2019-9497, CVE-2019-9498, CVE-2019-9499, and CVE-2019-11555.

- Fixed **Heimdal** security issues CVE-2019-12098 and CVE-2018-16860.
- Fixed **libimobiledevice** security issue CVE-2016-5104.
- Fixed **libpng1.6** security issues CVE-2019-7317 and CVE-2018-13785.
- Fixed **GIMP** security issues.

**More...**

CVE-2017-17786, CVE-2017-17789, CVE-2017-17784, CVE-2017-17787, CVE-2017-17785, and CVE-2017-17788

- Fixed **libtomcrypt** security issue CVE-2018-12437.
- Fixed **curl** security issues.

**More...**

CVE-2018-16840, CVE-2018-16839, CVE-2019-3823, CVE-2019-3822, CVE-2018-16890, CVE-2019-5346.

- Fixed **gnutls28** security issues CVE-2018-10846, CVE-2018-10845, CVE-2018-10844 and CVE-2018-1084.
- Fixed **qtbase-opensource-src** security issues CVE-2018-19873, CVE-2018-19870 and CVE-2018-15518.
- Fixed **db5.3** security issue CVE-2019-8457.
- Fixed **libssh2** security issues.

**More...**

CVE-2019-3863, CVE-2019-3862, CVE-2019-3861, CVE-2019-3860, CVE-2019-3859, CVE-2019-3858, CVE-2019-3857, CVE-2019-3856, and CVE-2019-3855.

- Fixed **network-manager** security issue CVE-2018-15688.
- Fixed **elfutils** security issues.

**More...**

CVE-2019-7665, CVE-2019-7150, CVE-2019-7149, CVE-2018-18521, CVE-2018-18520, CVE-2018-18310, CVE-2018-16403, CVE-2018-16402, and CVE-2018-16062.



- Fixed **libsndfile** security issues.

**More...**

CVE-2019-3832, CVE-2018-19758, CVE-2018-19662, CVE-2018-19661, CVE-2018-19432, CVE-2018-13139, CVE-2017-6892, CVE-2017-17457, CVE-2017-17456, CVE-2017-16942, CVE-2017-14634, CVE-2017-14246, and CVE-2017-14245.

- Fixed **dbus** security issue CVE-2019-12749.
  - Fixed **Vim** security issues CVE-2019-12735 and CVE-2017-5953.
- Fixed **sqlite3** security issues.

**More...**

CVE-2019-9937, CVE-2019-9936, CVE-2019-8457, CVE-2018-20506, CVE-2018-20346, CVE-2017-2520, CVE-2017-2519, CVE-2017-2518, CVE-2017-13685, CVE-2017-10989, and CVE-2016-6153.

- Fixed **libseccomp** security issue CVE-2019-9893.
- Fixed **bzip2** security issues CVE-2019-12900 and CVE-2016-3189.
- Fixed **Expat** security issue CVE-2018-20843.
- Fixed **unzip** security issues CVE-2019-13232, CVE-2018-1000035, CVE-2016-9844 and CVE-2014-9913.
- **Mount partitions** with "**nodev**" flag option.
- The home directory of the remote users is now **/home/ruser**.
- Default **umask** is set to **0077** for all non-root users.
- Fixed a vulnerability in the **custom environment variable framework**.
- Fixed kernel **TCP** vulnerabilities CVE-2019-11477: **SACK Panic**, CVE-2019-11478: **SACK Slowness** and CVE-2019-11479: **Excess Resource Consumption Due to Low MSS Values**.
- Changed **minimally allowed MSS size** to "**1000**" to prevent possible denial-of-service attacks.

## Known Issues 10.06.120

### Citrix

- With activated DRI3 and AMD GPU, Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H264, MPEG1 and MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.  
As a workaround, insert the smartcard before starting StoreFront login.
- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" > "For the entire screen".
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264 acceleration plugin**, the following registry key must be enabled:  
**More...**



|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Value     | <u>enabled</u> / <u>disabled</u>                                 |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

#### VMware Horizon

- **Sound redirection in PCoIP** is broken when the so-called lightweight-client is used, which has become the new default.  
But Sound redirection can still be used by choosing the rollback-client instead. This can be done by setting the IGEL Registry key:  
[More...](#)

|           |                                         |
|-----------|-----------------------------------------|
| Parameter | Allow rollback to former client variant |
| Registry  | vmware.view.allow-client-rollback       |
| Value     | <u>enabled</u> / <u>disabled</u>        |

- **External drives** mounted already before connection **do not appear in the remote desktop**.  
Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off.  
In the IGEL Setup client, **drive mapping** can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping**.  
It is also recommended to disable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection entirely** or at least to **deny storage devices** by adding a filter to the USB class rules.  
Furthermore, Horizon Client relies on the OS to mount the storage device itself. Enable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.

#### Parallels Client

- **Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** one time with FIPS support disabled.

#### Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice**: spice-xpi Firefox plugin is no longer supported. The **Console Invocation** has to allow **Native client** (auto is also possible) and it should start in fullscreen to prevent opening windows.



## Wi-Fi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.  
Workaround: Disable system suspend under **IGEL Setup > System > Power Options > Shutdown**.

## Base system

- Due to the removal of the Oracle JRE, **Java WebStart** is **not supported** anymore.

## Hardware

- **Suspend on UD10** is disabled.

## New Features 10.06.120

### Citrix

- Integrated **Citrix Workspace app 19.06**.  
Available Citrix Workspace apps in this release: 19.06, 19.03 and 13.10.

## Resolved Issues 10.06.120

### VMware Horizon

- Fixed: **Client connection** to the remote desktop **using PCoIP protocol** failed occasionally.

### OS 11 Upgrade

- Fixed major **upgrade** problem **with Intel network drivers**.
- Make OS 11 Upgrade **VPN detection more lenient** to allow blocked upgrade on some devices with integrated mobile broadband modem.

### Base system

- Fixed **ActiveDirectory/Kerberos password change** with "Change Password" accessory for users who are members of many (~300+) AD groups.

### Bluetooth

- Fixed not working **bluetooth for** some **Intel Wi-Fi cards**.

### Remote Management

- Fixed: **UMS jobs** have not been executed when delivered at the next system boot.
- Fixed **automatic registering in the UMS** using DNS entry or DHCP tag.

### Caradigm

- Updated firmware **7.3.3 of RFIDeas pcProx readers**.

## 7.22.2 IGEL Universal Desktop OS 3

### Supported Hardware:

<https://kb.igel.com/igelos/en/devices-supported-by-udc3-and-ud-pocket-3117174.html>



- Component Versions 10.06.120(see page 1926)
- General Information 10.06.120(see page 1930)
- Security Fixes 10.06.120(see page 1931)
- Known Issues 10.06.120(see page 1935)
- New Features 10.06.120(see page 1937)
- Resolved Issues 10.06.120(see page 1937)

## Component Versions 10.06.120

### • Clients

| <b>Product</b>                     | <b>Version</b>                            |
|------------------------------------|-------------------------------------------|
| Citrix HDX Realtime Media Engine   | 2.8.0-2235                                |
| Citrix Receiver                    | 13.10.0.20                                |
| Citrix Workspace App               | 19.3.0.5                                  |
| Citrix Workspace App               | 19.6.0.60                                 |
| deviceTRUST Citrix Channel         | 19.1.200.2                                |
| Ericom PowerTerm                   | 12.0.1.0.20170219.2-_dev_-34574           |
| Evidian AuthMgr                    | 1.5.7116                                  |
| Evince PDF Viewer                  | 3.18.2-1ubuntu4.5                         |
| FabulaTech USB for Remote Desktop  | 5.2.29                                    |
| Firefox                            | 60.8.0                                    |
| IBM iAccess Client Solutions       | 1.1.8.1                                   |
| IGEL RDP Client                    | 2.2                                       |
| Imprivata OneSign ProveID Embedded | onesign-bootstrap-loader_1.0.523630_amd64 |
| deviceTRUST RDP Channel            | 19.1.200.2                                |
| Leostream Java Connect             | 3.3.7.0                                   |
| NCP Secure Enterprise Client       | 5.10_rev40552                             |
| NX Client                          | 6.5.6                                     |



|                                       |                          |
|---------------------------------------|--------------------------|
| Open VPN                              | 2.3.10-1ubuntu2.2        |
| Zulu JRE                              | 8.38.0.13                |
| Parallels Client (64 bit)             | 16.5.3.20735             |
| Remote Viewer (RedHat Virtualization) | 8.0-1igel49              |
| Spice GTK (Red Hat Virtualization)    | 0.36-1~git20190601igel61 |
| Usbredir (Red Hat Virtualization)     | 0.8.0-1igel49            |
| Systancia AppliDis                    | 4.0.0.17                 |
| ThinLinc Client                       | 4.10.0-6068              |
| ThinPrint Client                      | 7.5.88                   |
| Totem Media Player                    | 2.30.2                   |
| Parole Media Player                   | 1.0.1-0ubuntu1igel18     |
| VMware Horizon Client                 | 5.0.0-12557422           |
| VNC Viewer                            | 1.9.0+dfsg-3igel8        |
| Voip Client Ekiga                     | 4.0.1                    |

- **Dictation**

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20180621 |
| Philips Speech Driver                     | 12.7.11  |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.8    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.1.0    |



- **Smartcard**

|                                           |                        |
|-------------------------------------------|------------------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101                |
| PKCS#11 Library Athena IDProtect          | 623.07                 |
| PKCS#11 Library cryptovision sc/interface | 7.1.20                 |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0              |
| PKCS#11 Library SecMaker NetID            | 6.7.2.36               |
| Reader Driver ACS CCID                    | 1.1.6-1igel1           |
| Reader Driver Gemalto eToken              | 10.0.37-0              |
| Reader Driver HID Global Omnikey          | 4.3.3                  |
| Reader Driver Identive CCID               | 5.0.35                 |
| Reader Driver Identive eHealth200         | 1.0.5                  |
| Reader Driver Identive SCRKBC             | 5.0.24                 |
| Reader Driver MUSCLE CCID                 | 1.4.30-1igel3          |
| Reader Driver REINER SCT cyberJack        | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite               | 1.8.23-1igel1          |
| Cherry USB2LAN Proxy                      | 3.2.0.3                |

- **System Components**

|                         |                    |
|-------------------------|--------------------|
| OpenSSL                 | 1.0.2g-1ubuntu4.15 |
| OpenSSH Client          | 7.2p2-4ubuntu2.8   |
| OpenSSH Server          | 7.2p2-4ubuntu2.8   |
| Bluetooth stack (bluez) | 5.50-0ubuntu1igel5 |
| MESA OpenGL stack       | 19.0.8-1igel73     |
| VAAPI ABI Version       | 0.40               |
| VDPAU Library version   | 1.1.1-3ubuntu1     |



|                                         |                              |
|-----------------------------------------|------------------------------|
| Graphics Driver INTEL                   | 2.99.917+git20190301-igel870 |
| Graphics Driver ATI/RADEON              | 19.0.1-2igel890              |
| Graphics Driver ATI/AMDGPU              | 19.0.1-4igel894              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867              |
| Graphics Driver Nvidia                  | 390.116-0ubuntu0.18.10.1     |
| Graphics Driver Vboxvideo               | 1.0.0-igel798                |
| Graphics Driver VMware                  | 13.3.0-2igel857              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1igel775         |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |
| Graphics Driver VESA                    | 2.4.0-1igel855               |
| Input Driver Evdev                      | 2.10.6-1igel888              |
| Input Driver Elographics                | 1.4.1-1build5igel633         |
| Input Driver eGalax                     | 2.5.5814                     |
| Input Driver Synaptics                  | 1.9.1-1ubuntu1igel866        |
| Input Driver VMmouse                    | 13.1.0-1ubuntu2igel635       |
| Input Driver Wacom                      | 0.36.1-0ubuntu2igel888       |
| Kernel                                  | 4.19.65 #mainline-udos-r2782 |
| Xorg X11 Server                         | 1.20.5-1igel891              |
| Xorg Xephyr                             | 1.20.5-1igel891              |
| CUPS printing daemon                    | 2.1.3-4ubuntu0.9igel27       |
| PrinterLogic                            | 18.2.1.128                   |
| Lightdm graphical login manager         | 1.18.3-0ubuntu1.1            |
| XFCE4 Window Manager                    | 4.12.3-1ubuntu2igel656       |
| ISC DHCP Client                         | 4.3.3-5ubuntu12.10igel7      |



|                |                               |
|----------------|-------------------------------|
| NetworkManager | 1.2.6-0ubuntu0.16.04.3igel74  |
| ModemManager   | 1.10.0-1~ubuntu18.04.2igel3   |
| GStreamer 0.10 | 0.10.36-2ubuntu0.2            |
| GStreamer 1.x  | 1.16.0-1igel214               |
| WebKit2Gtk     | 2.24.2-0ubuntu0.19.04.1igel18 |
| Python2        | 2.7.12                        |
| Python3        | 3.5.2                         |

- **Features with Limited IGEL Support**

|                                    |                                  |
|------------------------------------|----------------------------------|
| Mobile Device Access USB (MTP)     | 1.1.16-2igel1                    |
| Mobile Device Access USB (imobile) | 1.2.1~git20181030.92c5462-1igel5 |
| Mobile Device Access USB (gphoto)  | 2.5.22-3igel1                    |
| VPN OpenConnect                    | 7.08-1                           |
| Scanner support / SANE             | 1.0.27-1                         |
| VirtualBox                         | 6.0.8-dfsg-4igel25               |

- **Features with Limited Functionality**

|                   |        |
|-------------------|--------|
| Cisco JVDI Client | 12.1.0 |
|-------------------|--------|

## General Information 10.06.120

The following clients and features are not supported anymore:

- Citrix Receiver 12.1 and 13.1 - 13.4;
- Citrix Access Gateway Standard Plug-in;
- Dell vWorkspace Connector for Linux;
- Ericom PowerTerm Emulation 9 and 11;
- Ericom Webconnect;
- IGEL Legacy RDP Client (rdesktop);
- Virtual Bridges VERDE Client;
- PPTP VPN Support;
- IGEL Upgrade License Tool with IGEL Smartcard Token;
- Remote Management by setup.ini file transfer (TFTP);
- Remote Access via RSH;
- Legacy Philips Speech Driver;
- T-Systems TCOS Smartcard Support;
- DUS Series touch screens;
- Elo serial touchscreens;



- VIA Graphics support;
- Java WebStart;
- Storage hotplug devices are not automatically removed anymore, instead they must be always ejected manually:
  - by panel tray icon;
  - by an icon in the **In-Session Control Bar** (configurable under **IGEL Setup > User Interface > Desktop**);
  - by a **Safely Remove Hardware** session (configurable under **IGEL Setup > Accessories**).

The following clients and features are not available in this release:

- Cherry eGK Channel;
- Open VPN Smartcard Support;
- Asian Input Methods;
- Composite Manager.

## Security Fixes 10.06.120

### Firefox

- Updated **Firefox** browser to version **60.8.0 ESR**.
- Fixed **mfsa2019-22** security issues:

[More...](#)

CVE-2019-9811, CVE-2019-11711, CVE-2019-11712, CVE-2019-11713, CVE-2019-11729, CVE-2019-11715, CVE-2019-11717, CVE-2019-11719, CVE-2019-11730 and CVE-2019-11709.

- Fixed **mfsa2019-19** security issue CVE-2019-11708.
- Fixed **mfsa2019-18** security issue CVE-2019-11707.
- Fixed **mfsa2019-08** security issues:

[More...](#)

CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2018-18506 and CVE-2019-9788.

- Fixed **mfsa2019-05** security issues CVE-2018-18356 and CVE-2019-5785.
- Fixed **mfsa2019-02** security issues CVE-2018-18500, CVE-2018-18505 and CVE-2018-18501.

### Shared Workplace

- Fixed **login in Shared Workplace** which accepts any user credentials in the 10.06.100 release. However, no user settings were applied to the device.

### Base system

- Updated **kernel** to version **4.19.65**.
- Fixed security issue CVE-2019-1125 aka **Spectre SWAPGS gadget vulnerability**.
- Fixed a vulnerability in **Java configuration script**.
- Fixed possibly malicious **owner change** with TC setup configuration.
- Fixed **policykit-1** security issues CVE-2018-19788 and CVE-2019-6133.
- Fixed **NSS** security issues CVE-2018-18508, CVE-2018-12404, CVE-2018-12384 and CVE-2018-0495.
- Fixed **PPP** security issue CVE-2018-11574.



- Fixed **imagemagick** security issues.

**More...**

CVE-2018-16750, CVE-2018-16749, CVE-2018-16645, CVE-2018-16644, CVE-2018-16643, CVE-2018-16642, CVE-2018-16640, CVE-2018-16323, CVE-2018-14437, CVE-2018-14436, CVE-2018-14435, CVE-2018-14434, CVE-2017-13144, CVE-2017-12430, CVE-2019-9956, CVE-2019-7398, CVE-2019-7397, CVE-2019-7396, CVE-2019-7175, CVE-2019-11598, CVE-2019-11597, CVE-2019-11472, CVE-2019-11470, CVE-2019-10650, CVE-2019-10131, CVE-2018-20467, CVE-2018-18025, CVE-2018-18024, CVE-2018-18016, CVE-2018-17966, CVE-2018-17965, CVE-2018-16413, CVE-2018-16412, CVE-2017-12806, and CVE-2017-12805.

- Fixed **systemd** security issues.

**More...**

CVE-2018-16866, CVE-2018-16865, CVE-2018-16864, CVE-2018-15688, CVE-2019-6454, CVE-2018-1049, CVE-2018-15686 and CVE-2019-3842.

- Fixed **CUPS** security issue CVE-2018-4700.

- Fixed **libarchive** security issues.

**More...**

CVE-2019-1000020, CVE-2019-1000019, CVE-2018-1000878, CVE-2018-1000877, and CVE-2017-14502.

- Fixed **avahi** security issues CVE-2018-1000845 and CVE-2017-6519.

- Fixed **bind9** security issues CVE-2019-6465, CVE-2018-5745, and CVE-2018-5743.

- Fixed **libcaca** security issues.

**More...**

CVE-2018-20549, CVE-2018-20548, CVE-2018-20547, CVE-2018-20546, CVE-2018-20545, and CVE-2018-20544.

- Fixed **libgd2** security issues CVE-2019-6978 and CVE-2019-6977.

- Fixed **ghostscript** security issues.

**More...**

CVE-2019-6116, CVE-2018-19477, CVE-2018-19476, CVE-2018-19475, CVE-2018-19409, CVE-2018-18284, CVE-2018-18073, CVE-2018-17961, CVE-2019-3838, and CVE-2019-3835.

- Fixed **krb5** security issues.

**More...**

CVE-2018-5730, CVE-2018-5729, CVE-2017-11462, CVE-2017-11368, CVE-2016-3120, and CVE-2016-3119.

- Fixed **texlive-bin** security issue CVE-2018-17407.

- Fixed **LDB** security issue CVE-2019-3824.

- Fixed **libmspack** security issues CVE-2018-18585 and CVE-2018-18584.

- Fixed **Perl** security issues CVE-2018-18314, CVE-2018-18313, CVE-2018-18312 and CVE-2018-18311.

- Fixed **poppler** security issues.

**More...**



CVE-2019-7310, CVE-2018-20650, CVE-2018-20551, CVE-2018-20481, CVE-2018-19149, CVE-2018-19060, CVE-2018-19059, CVE-2018-19058, CVE-2018-16646, and CVE-2019-9200.

- Fixed **Python 3.5** security issues CVE-2018-14647, CVE-2018-1061, CVE-2018-1060 and CVE-2018-106.
- Fixed **Net-SNMP** security issue CVE-2018-18065.
- Fixed **OpenSSL** security issues CVE-2019-1559, CVE-2018-5407 and CVE-2018-0734.
- Fixed **TIFF** security issues.

**More...**

CVE-2018-8905, CVE-2018-7456, CVE-2018-18661, CVE-2018-18557, CVE-2018-17101, CVE-2018-17100, CVE-2018-1710, CVE-2018-10963, CVE-2019-7663, CVE-2019-6128, CVE-2018-19210, CVE-2018-17000, CVE-2018-12900, and CVE-2018-10779.

- Fixed **libvncserver** security issues.

**More...**

CVE-2018-6307, CVE-2018-20750, CVE-2018-20749, CVE-2018-20748, CVE-2018-20024, CVE-2018-20023, CVE-2018-20022, CVE-2018-20021, CVE-2018-20020, CVE-2018-20019, CVE-2018-15127, and CVE-2018-15126.

- Fixed **WavPack** security issue CVE-2018-19840.
- Fixed **Samba** security issues.

**More...**

CVE-2018-16851, CVE-2018-16841, CVE-2018-14629, CVE-2019-3880, and CVE-2018-16860.

- Fixed **libxkbcommon** security issues.

**More...**

CVE-2018-15864, CVE-2018-15863, CVE-2018-15862, CVE-2018-15861, CVE-2018-15859, CVE-2018-15858, CVE-2018-15857, CVE-2018-15856, CVE-2018-15855, CVE-2018-15854, and CVE-2018-15853.

- Fixed **OpenSSH** security issues.

**More...**

CVE-2019-6111, CVE-2019-6109, CVE-2018-20685, CVE-2018-15473, and CVE-2016-10708.

- Fixed **Python 2.7** security issues.

**More...**

CVE-2018-14647, CVE-2018-1061, CVE-2018-1060, CVE-2018-106, CVE-2018-1000802, and CVE-2018-1000030.

- Fixed **lxml** security issue CVE-2018-19787.
- Fixed **gdk-pixbuf** security issues.

**More...**

CVE-2017-6314, CVE-2017-6313, CVE-2017-6312, CVE-2017-6311, CVE-2017-2870, CVE-2017-2862, CVE-2017-1000422, CVE-2016-6352, and CVE-2017-12447.



- Fixed **file** security issues CVE-2019-8907 and CVE-2019-8905.
- Fixed **wget** security issue CVE-2019-5953.
- Fixed **nvidia-graphic-drivers-390** security issue CVE-2018-6260.
- Fixed **libxslt** security issue CVE-2019-11068.
- Fixed **Evince** security issue CVE-2019-11459.
- Fixed **webkit2gtk** security issues.

[More...](#)

CVE-2019-8595, CVE-2019-8607, CVE-2019-8615, CVE-2019-6251, CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378, CVE-2018-4382, CVE-2018-4392, CVE-2018-4416, CVE-2018-4345, CVE-2018-4386, and CVE-2018-4372.

- Fixed **gst-plugins-base0.10** security issue CVE-2019-9928.
- Fixed **WPA** security issues.

[More...](#)

CVE-2019-9495, CVE-2019-9497, CVE-2019-9498, CVE-2019-9499, and CVE-2019-11555.

- Fixed **Heimdal** security issues CVE-2019-12098 and CVE-2018-16860.
- Fixed **libimobiledevice** security issue CVE-2016-5104.
- Fixed **libpng1.6** security issues CVE-2019-7317 and CVE-2018-13785.
- Fixed **GIMP** security issues.

[More...](#)

CVE-2017-17786, CVE-2017-17789, CVE-2017-17784, CVE-2017-17787, CVE-2017-17785, and CVE-2017-17788

- Fixed **libtomcrypt** security issue CVE-2018-12437.
- Fixed **curl** security issues.

[More...](#)

CVE-2018-16840, CVE-2018-16839, CVE-2019-3823, CVE-2019-3822, CVE-2018-16890, CVE-2019-5346.

- Fixed **gnutls28** security issues CVE-2018-10846, CVE-2018-10845, CVE-2018-10844 and CVE-2018-1084.
- Fixed **qtbase-opensource-src** security issues CVE-2018-19873, CVE-2018-19870 and CVE-2018-15518.
- Fixed **db5.3** security issue CVE-2019-8457.
- Fixed **libssh2** security issues.

[More...](#)

CVE-2019-3863, CVE-2019-3862, CVE-2019-3861, CVE-2019-3860, CVE-2019-3859, CVE-2019-3858, CVE-2019-3857, CVE-2019-3856, and CVE-2019-3855.

- Fixed **network-manager** security issue CVE-2018-15688.
- Fixed **elfutils** security issues.

[More...](#)



CVE-2019-7665, CVE-2019-7150, CVE-2019-7149,  
 CVE-2018-18521, CVE-2018-18520, CVE-2018-18310,  
 CVE-2018-16403, CVE-2018-16402, and CVE-2018-16062.

- Fixed **libsndfile** security issues.

**More...**

CVE-2019-3832, CVE-2018-19758, CVE-2018-19662, CVE-2018-19661, CVE-2018-19432,  
 CVE-2018-13139, CVE-2017-6892, CVE-2017-17457, CVE-2017-17456, CVE-2017-16942,  
 CVE-2017-14634, CVE-2017-14246, and CVE-2017-14245.

- Fixed **dbus** security issue CVE-2019-12749.
- Fixed **Vim** security issues CVE-2019-12735 and CVE-2017-5953.

Fixed **sqlite3** security issues.

**More...**

CVE-2019-9937, CVE-2019-9936, CVE-2019-8457, CVE-2018-20506,  
 CVE-2018-20346, CVE-2017-2520, CVE-2017-2519, CVE-2017-2518,  
 CVE-2017-13685, CVE-2017-10989, and CVE-2016-6153.

- Fixed **libseccomp** security issue CVE-2019-9893.
- Fixed **bzip2** security issues CVE-2019-12900 and CVE-2016-3189.
- Fixed **Expat** security issue CVE-2018-20843.
- Fixed **unzip** security issues CVE-2019-13232, CVE-2018-1000035, CVE-2016-9844 and  
 CVE-2014-9913.
- **Mount partitions** with "**nodev**" flag option.
- The home directory of the remote users is now **/home/ruser**.
- Default **umask** is set to **0077** for all non-root users.
- Fixed a vulnerability in the **custom environment variable framework**.
- Fixed kernel **TCP** vulnerabilities CVE-2019-11477: **SACK Panic**, CVE-2019-11478: **SACK Slowness** and CVE-2019-11479: **Excess Resource Consumption Due to Low MSS Values**.
- Changed **minimally allowed MSS size** to "**1000**" to prevent possible denial-of-service attacks.

## Known Issues 10.06.120

### Citrix

- With activated DRI3 and AMD GPU, Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H264, MPEG1 and MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.  
 As a workaround, insert the smartcard before starting StoreFront login.
- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" > "For the entire screen".



- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264 acceleration plugin**, the following registry key must be enabled:

[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Value     | <u>enabled</u> / <u>disabled</u>                                 |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

#### VMware Horizon

- Sound redirection in PCoIP** is broken when the so-called lightweight-client is used, which has become the new default.  
But Sound redirection can still be used by choosing the rollback-client instead. This can be done by setting the IGEL Registry key:

[More...](#)

|           |                                         |
|-----------|-----------------------------------------|
| Parameter | Allow rollback to former client variant |
| Registry  | vmware.view.allow-client-rollback       |
| Value     | <u>enabled</u> / <u>disabled</u>        |

- External drives** mounted already before connection **do not appear in the remote desktop**.  
Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off.  
In the IGEL Setup client, **drive mapping** can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping**.  
It is also recommended to disable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection entirely** or at least to **deny storage devices** by adding a filter to the USB class rules.  
Furthermore, Horizon Client relies on the OS to mount the storage device itself. Enable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.

#### Parallels Client

- Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** one time with FIPS support disabled.

#### Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode



- Appliance mode **RHEV/Spice**: spice-xpi Firefox plugin is no longer supported. The **Console Invocation** has to allow **Native client** (auto is also possible) and it should start in fullscreen to prevent opening windows.

#### Multimedia

- **Multimedia redirection with GStreamer** could fail with the Nouveau GPU driver.

#### Wi-Fi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.  
Workaround: Disable system suspend under **IGEL Setup > System > Power Options > Shutdown**.

#### Base system

- Due to the removal of the Oracle JRE, **Java WebStart** is **not supported** anymore.

### New Features 10.06.120

#### Citrix

- Integrated **Citrix Workspace** app **19.06**.  
Available Citrix Workspace apps in this release: 19.06, 19.03, and 13.10.

### Resolved Issues 10.06.120

#### VMware Horizon

- Fixed: **Client connection** to the remote desktop **using PCoIP protocol** failed occasionally.

#### OS 11 Upgrade

- Fixed **UD Pocket upgrade process** with Wi-Fi connection.
- Fixed major **upgrade** problem **with Intel network drivers**.
- Make OS 11 Upgrade **VPN detection more lenient** to allow blocked upgrade on some devices with integrated mobile broadband modem.

#### Base system

- Fixed **ActiveDirectory/Kerberos password change** with "Change Password" accessory for users who are members of many (~300+) AD groups.

#### Bluetooth

- Fixed not working **bluetooth for** some **Intel Wi-Fi cards**.

#### Remote Management

- Fixed: **UMS jobs** have not been executed when delivered at next system boot.
- Fixed **automatic registering in the UMS** using DNS entry or DHCP tag.

#### Caradigm

- Updated firmware **7.3.3 of RFIDEas pcProx readers**.



## 7.23 Notes for Release 10.06.110

|                       |            |             |
|-----------------------|------------|-------------|
| <b>Software:</b>      | Version    | 10.06.110   |
| <b>Release Date:</b>  | 2019-07-24 |             |
| <b>Release Notes:</b> | Version    | RN-106110-1 |
| <b>Last update:</b>   | 2019-07-24 |             |

- [IGEL Linux Universal Desktop](#)(see page 1938)
- [IGEL Universal Desktop OS 3](#)(see page 1947)

### 7.23.1 IGEL Linux Universal Desktop

#### Supported Devices

| <b>Universal Desktop:</b> |                                |
|---------------------------|--------------------------------|
| UD2-LX:                   | UD2-LX 40                      |
| UD3-LX:                   | UD3-LX 51<br>UD3-LX 50         |
| UD5-LX:                   | UD5-LX 50                      |
| UD6-LX:                   | UD6-LX 51                      |
| UD7-LX:                   | UD7-LX 10                      |
| UD9-LX:                   | UD9-LX Touch 41<br>UD9-LX 40   |
| UD10-LX:                  | UD10-LX Touch 10<br>UD10-LX 10 |
| <b>IGEL Zero:</b>         |                                |



|             |
|-------------|
| IZ2-RFX     |
| IZ2-HDX     |
| IZ2-HORIZON |
| IZ3-RFX     |
| IZ3-HDX     |
| IZ3-HORIZON |

- Component Versions 10.06.110(see page 1939)
- General Information 10.06.110(see page 1943)
- Known Issues 10.06.110(see page 1944)
- Security Fixes 10.06.110(see page 1946)
- New Features 10.06.110(see page 1946)
- Resolved Issues 10.06.110(see page 1947)

## Component Versions 10.06.110

### • Clients

| Product                           | Version                         |
|-----------------------------------|---------------------------------|
| Citrix HDX Realtime Media Engine  | 2.8.0-2235                      |
| Citrix Receiver                   | 13.10.0.20                      |
| Citrix Receiver                   | 13.5.0.10185126                 |
| Citrix Workspace App              | 19.3.0.5                        |
| deviceTRUST Citrix Channel        | 19.1.200.2                      |
| Ericom PowerTerm                  | 12.0.1.0.20170219.2-_dev_-34574 |
| Evidian AuthMgr                   | 1.5.7116                        |
| Evince PDF Viewer                 | 3.18.2-1ubuntu4.5               |
| FabulaTech USB for Remote Desktop | 5.2.29                          |



|                                       |                                           |
|---------------------------------------|-------------------------------------------|
| Firefox                               | 60.8.0                                    |
| IBM iAccess Client Solutions          | 1.1.8.1                                   |
| IGEL RDP Client                       | 2.2                                       |
| Imprivata OneSign ProveID Embedded    | onesign-bootstrap-loader_1.0.523630_amd64 |
| deviceTRUST RDP Channel               | 19.1.200.2                                |
| Leostream Java Connect                | 3.3.7.0                                   |
| NCP Secure Enterprise Client          | 5.10_rev40552                             |
| NX Client                             | 6.5.6                                     |
| Open VPN                              | 2.3.10-1ubuntu2.2                         |
| Zulu JRE                              | 8.38.0.13                                 |
| Parallels Client (64 bit)             | 16.5.3.20735                              |
| Remote Viewer (RedHat Virtualization) | 8.0-1igel49                               |
| Spice GTK (Red Hat Virtualization)    | 0.36-1~git20190601igel61                  |
| Usbredir (Red Hat Virtualization)     | 0.8.0-1igel49                             |
| Systancia AppliDis                    | 4.0.0.17                                  |
| ThinLinc Client                       | 4.10.0-6068                               |
| ThinPrint Client                      | 7.5.88                                    |
| Totem Media Player                    | 2.30.2                                    |
| Parole Media Player                   | 1.0.1-0ubuntu1igel18                      |
| VMware Horizon Client                 | 5.0.0-12557422                            |
| VNC Viewer                            | 1.9.0+dfsg-3igel8                         |
| Voip Client Ekiga                     | 4.0.1                                     |
| <b>• Dictation</b>                    |                                           |
| Diktamen driver for dictation         |                                           |



|                                           |          |
|-------------------------------------------|----------|
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20180621 |
| Philips Speech Driver                     | 12.7.11  |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.8    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.1.0    |

- **Smartcard**

|                                           |                        |
|-------------------------------------------|------------------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101                |
| PKCS#11 Library Athena IDProtect          | 623.07                 |
| PKCS#11 Library cryptovision sc/interface | 7.1.20                 |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0              |
| PKCS#11 Library SecMaker NetID            | 6.7.2.36               |
| Reader Driver ACS CCID                    | 1.1.6-1igel1           |
| Reader Driver Gemalto eToken              | 10.0.37-0              |
| Reader Driver HID Global Omnikey          | 4.3.3                  |
| Reader Driver Identive CCID               | 5.0.35                 |
| Reader Driver Identive eHealth200         | 1.0.5                  |
| Reader Driver Identive SCRKBC             | 5.0.24                 |
| Reader Driver MUSCLE CCID                 | 1.4.30-1igel3          |
| Reader Driver REINER SCT cyberJack        | 3.99.5final.sp13igel15 |



|                             |               |
|-----------------------------|---------------|
| Resource Manager PC/SC Lite | 1.8.23-1igel1 |
| Cherry USB2LAN Proxy        | 3.2.0.3       |

• **System Components**

|                            |                                                  |
|----------------------------|--------------------------------------------------|
| OpenSSL                    | 1.0.2g-1ubuntu4.15                               |
| OpenSSH Client             | 7.2p2-4ubuntu2.8                                 |
| OpenSSH Server             | 7.2p2-4ubuntu2.8                                 |
| Bluetooth stack (bluez)    | 5.50-0ubuntu1igel5                               |
| MESA OpenGL stack          | 19.0.8-1igel73                                   |
| VAAPI ABI Version          | 0.40                                             |
| VDPAU Library version      | 1.1.1-3ubuntu1                                   |
| Graphics Driver INTEL      | 2.99.917+git20190301-igel870                     |
| Graphics Driver ATI/Radeon | 19.0.1-2igel890                                  |
| Graphics Driver ATI/AMDGPU | 19.0.1-4igel894                                  |
| Graphics Driver VIA        | 5.76.52.92-opensource-009-005f78-20150730igel871 |
| Graphics Driver FBDEV      | 0.5.0-1igel819                                   |
| Graphics Driver VESA       | 2.4.0-1igel855                                   |
| Input Driver Evdev         | 2.10.6-1igel888                                  |
| Input Driver Elographics   | 1.4.1-1build5igel633                             |
| Input Driver eGalax        | 2.5.5814                                         |
| Input Driver Synaptics     | 1.9.1-1ubuntu1igel866                            |
| Input Driver VMmouse       | 13.1.0-1ubuntu2igel635                           |
| Input Driver Wacom         | 0.36.1-0ubuntu2igel888                           |
| Kernel                     | 4.19.57 #mainline-ud-r2762                       |



|                                 |                               |
|---------------------------------|-------------------------------|
| Xorg X11 Server                 | 1.20.5-1igel891               |
| Xorg Xephyr                     | 1.20.5-1igel891               |
| CUPS printing daemon            | 2.1.3-4ubuntu0.9igel27        |
| PrinterLogic                    | 18.2.1.128                    |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1             |
| XFCE4 Window Manager            | 4.12.3-1ubuntu2igel656        |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7       |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.3igel74  |
| ModemManager                    | 1.10.0-1~ubuntu18.04.2igel3   |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.2            |
| GStreamer 1.x                   | 1.16.0-1igel214               |
| WebKit2Gtk                      | 2.24.2-0ubuntu0.19.04.1igel18 |
| Python2                         | 2.7.12                        |
| Python3                         | 3.5.2                         |

- **Features with Limited IGEL Support**

|                                    |                                  |
|------------------------------------|----------------------------------|
| Mobile Device Access USB (MTP)     | 1.1.16-2igel1                    |
| Mobile Device Access USB (imobile) | 1.2.1~git20181030.92c5462-1igel5 |
| Mobile Device Access USB (gphoto)  | 2.5.22-3igel1                    |
| VPN OpenConnect                    | 7.08-1                           |
| Scanner support / SANE             | 1.0.27-1                         |
| VirtualBox                         | 6.0.8-dfsg-4igel25               |

- **Features with Limited Functionality**

|                   |        |
|-------------------|--------|
| Cisco JVDI Client | 12.1.0 |
|-------------------|--------|

## General Information 10.06.110

The following clients and features are not supported anymore:

- Citrix Receiver 12.1 and 13.1 - 13.4;
- Citrix Access Gateway Standard Plug-in;



- Dell vWorkspace Connector for Linux;
- Ericom PowerTerm Emulation 9 and 11;
- Ericom Webconnect;
- IGEL Legacy RDP Client (rdesktop);
- Virtual Bridges VERDE Client;
- PPTP VPN Support;
- IGEL Upgrade License Tool with IGEL Smartcard Token;
- Remote Management by setup.ini file transfer (TFTP);
- Remote Access via RSH;
- Legacy Philips Speech Driver;
- T-Systems TCOS Smartcard Support;
- DUS Series touch screens;
- Elo serial touchscreens;
- Video hardware acceleration support is discontinued on UD10-LX Touch 10 and UD10-LX 10;
- H.264 hardware acceleration support is discontinued on UD10-LX Touch 10 and UD10-LX 10;
- Java WebStart;
- Storage hotplug devices are not automatically removed anymore, instead they must be always ejected manually:
  - by panel tray icon;
  - by an icon in the **In-Session Control Bar** (configurable under **IGEL Setup > User Interface > Desktop**);
  - by a **Safely Remove Hardware** session (configurable under **IGEL Setup > Accessories**).

The following clients and features are not available in this release:

- Cherry eGK Channel;
- Open VPN Smartcard Support;
- Asian Input Methods;
- Composite Manager.

## Known Issues 10.06.110

### Citrix

- With activated DRI3 and AMD GPU, Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H264, MPEG1 and MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.  
As a workaround, insert the smartcard before starting StoreFront login.
- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" > "For the entire screen".



- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264 acceleration plugin**, the following registry key must be enabled:

[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Range     | <u>enabled</u> / <u>disabled</u>                                 |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

#### VMware Horizon

- External drives** mounted already before connection **do not appear in the remote desktop**. Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off. In the IGEL Setup client, **drive mapping** can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping**. It is also recommended to disable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection entirely** or at least to **deny storage devices** by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage device itself. Enable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.

#### Parallels Client

- Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** one time with FIPS support disabled.

#### Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice**: spice-xpi Firefox plugin is no longer supported. The **Console Invocation** has to allow **Native client** (auto is also possible) and it should start in fullscreen to prevent opening windows.

#### WiFi

- TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume. Workaround: Disable system suspend under **IGEL Setup > System > Power Options > Shutdown**.

#### Base system



- Due to the removal of the Oracle JRE, **Java WebStart** is **not supported** anymore.

#### Hardware

- **Suspend on UD10** is disabled.

### Security Fixes 10.06.110

#### Firefox

- Updated **Firefox** browser to version **60.8.0 ESR**.
- Fixed **mfsa2019-22** security issues:  
[More...](#)

CVE-2019-9811, CVE-2019-11711, CVE-2019-11712, CVE-2019-11713, CVE-2019-11729, CVE-2019-11715, CVE-2019-11717, CVE-2019-11719, CVE-2019-11730 and CVE-2019-11709.

- Fixed **mfsa2019-19** security issue CVE-2019-11708.
  - Fixed **mfsa2019-18** security issue CVE-2019-11707.
  - Fixed **mfsa2019-08** security issues:  
[More...](#)
- CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2018-18506 and CVE-2019-9788.
- Fixed **mfsa2019-05** security issues CVE-2018-18356 and CVE-2019-5785.
  - Fixed **mfsa2019-02** security issues CVE-2018-18500, CVE-2018-18505 and CVE-2018-18501.

#### Shared Workplace

- Fixed **login in Shared Workplace** which accepts any user credentials in the 10.06.100 release. However, no user settings were applied to the device.

### New Features 10.06.110

#### Base system

- Replaced **timesyncd** with **chrony NTP**.  
A new registry key:  
[More...](#)

|           |                                        |
|-----------|----------------------------------------|
| Parameter | Use NTP Servers from DNS SRV record    |
| Registry  | system.time.ntp_use_dnssrv_timeservers |
| Value     | <u>enabled</u> / <u>disabled</u>       |

#### Evidian

- Integrated **Evidian AuthMgr** version **1.5.7116**.

#### Hardware

- Hardware support for **HP EliteBook 840 G3**.



## Resolved Issues 10.06.110

### Base system

- Fixed **NTP synchronization** problems with changing the NTP client from **timesyncd** to **chrony**.
- Fixed **USB printer aliases**.

### X11 system

- Fixed **screen corruption with DPMS** and enabled **composite manager**.
- Added consideration of **hardware limits** for choosing **automatic resolution in Xorg config** (currently only for IGEL hardware).

### Hardware

- Fixed **black screen** issue with some monitors and 2560x1440 resolution (occurred on **UD2 LX50**).

### Caradigm

- Updated **RF IDEas** reader tool for the usage with Caradigm.

## 7.23.2 IGEL Universal Desktop OS 3

### Supported Hardware:

<https://kb.igel.com/igelos/en/devices-supported-by-udc3-and-ud-pocket-3117174.html>

- Component Versions 10.06.110(see page 1947)
- General Information 10.06.110(see page 1952)
- Known Issues 10.06.110(see page 1953)
- Security Fixes 10.06.110(see page 1954)
- New Features 10.06.110(see page 1955)
- Resolved Issues 10.06.110(see page 1955)

## Component Versions 10.06.110

- **Clients**

| Product                          | Version         |
|----------------------------------|-----------------|
| Citrix HDX Realtime Media Engine | 2.8.0-2235      |
| Citrix Receiver                  | 13.10.0.20      |
| Citrix Receiver                  | 13.5.0.10185126 |
| Citrix Workspace App             | 19.3.0.5        |



|                                       |                                           |
|---------------------------------------|-------------------------------------------|
| deviceTRUST Citrix Channel            | 19.1.200.2                                |
| Ericom PowerTerm                      | 12.0.1.0.20170219.2-_dev_-34574           |
| Evidian AuthMgr                       | 1.5.7116                                  |
| Evince PDF Viewer                     | 3.18.2-1ubuntu4.5                         |
| FabulaTech USB for Remote Desktop     | 5.2.29                                    |
| Firefox                               | 60.8.0                                    |
| IBM iAccess Client Solutions          | 1.1.8.1                                   |
| IGEL RDP Client                       | 2.2                                       |
| Imprivata OneSign ProveID Embedded    | onesign-bootstrap-loader_1.0.523630_amd64 |
| deviceTRUST RDP Channel               | 19.1.200.2                                |
| Leostream Java Connect                | 3.3.7.0                                   |
| NCP Secure Enterprise Client          | 5.10_rev40552                             |
| NX Client                             | 6.5.6                                     |
| Open VPN                              | 2.3.10-1ubuntu2.2                         |
| Zulu JRE                              | 8.38.0.13                                 |
| Parallels Client (64 bit)             | 16.5.3.20735                              |
| Remote Viewer (RedHat Virtualization) | 8.0-1igel49                               |
| Spice GTK (Red Hat Virtualization)    | 0.36-1~git20190601igel61                  |
| Usbredir (Red Hat Virtualization)     | 0.8.0-1igel49                             |
| Systancia AppliDis                    | 4.0.0.17                                  |
| ThinLinc Client                       | 4.10.0-6068                               |
| ThinPrint Client                      | 7.5.88                                    |
| Totem Media Player                    | 2.30.2                                    |



|                       |                      |
|-----------------------|----------------------|
| Parole Media Player   | 1.0.1-0ubuntu1igel18 |
| VMware Horizon Client | 5.0.0-12557422       |
| VNC Viewer            | 1.9.0+dfsg-3igel8    |
| Voip Client Ekiga     | 4.0.1                |

- **Dictation**

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20180621 |
| Philips Speech Driver                     | 12.7.11  |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.8    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.1.0    |

- **Smartcard**

|                                           |              |
|-------------------------------------------|--------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101      |
| PKCS#11 Library Athena IDProtect          | 623.07       |
| PKCS#11 Library cryptovision sc/interface | 7.1.20       |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0    |
| PKCS#11 Library SecMaker NetID            | 6.7.2.36     |
| Reader Driver ACS CCID                    | 1.1.6-1igel1 |
| Reader Driver Gemalto eToken              | 10.0.37-0    |
| Reader Driver HID Global Omnikey          | 4.3.3        |



|                                    |                        |
|------------------------------------|------------------------|
| Reader Driver Identive CCID        | 5.0.35                 |
| Reader Driver Identive eHealth200  | 1.0.5                  |
| Reader Driver Identive SCRKBC      | 5.0.24                 |
| Reader Driver MUSCLE CCID          | 1.4.30-1igel3          |
| Reader Driver REINER SCT cyberJack | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite        | 1.8.23-1igel1          |
| Cherry USB2LAN Proxy               | 3.2.0.3                |

- **System Components**

|                                         |                              |
|-----------------------------------------|------------------------------|
| OpenSSL                                 | 1.0.2g-1ubuntu4.15           |
| OpenSSH Client                          | 7.2p2-4ubuntu2.8             |
| OpenSSH Server                          | 7.2p2-4ubuntu2.8             |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5           |
| MESA OpenGL stack                       | 19.0.8-1igel73               |
| VAAPI ABI Version                       | 0.40                         |
| VDPAU Library version                   | 1.1.1-3ubuntu1               |
| Graphics Driver INTEL                   | 2.99.917+git20190301-igel870 |
| Graphics Driver ATI/RADEON              | 19.0.1-2igel890              |
| Graphics Driver ATI/AMDGPU              | 19.0.1-4igel894              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867              |
| Graphics Driver Nvidia                  | 390.116-0ubuntu0.18.10.1     |
| Graphics Driver Vboxvideo               | 1.0.0-igel798                |
| Graphics Driver VMware                  | 13.3.0-2igel857              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1igel775         |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |
| Graphics Driver VESA                    | 2.4.0-1igel855               |



|                                             |                                  |
|---------------------------------------------|----------------------------------|
| Input Driver Evdev                          | 2.10.6-1igel888                  |
| Input Driver Elographics                    | 1.4.1-1build5igel633             |
| Input Driver eGalax                         | 2.5.5814                         |
| Input Driver Synaptics                      | 1.9.1-1ubuntu1igel866            |
| Input Driver VMmouse                        | 13.1.0-1ubuntu2igel635           |
| Input Driver Wacom                          | 0.36.1-0ubuntu2igel888           |
| Kernel                                      | 4.19.57 #mainline-udos-r2762     |
| Xorg X11 Server                             | 1.20.5-1igel891                  |
| Xorg Xephyr                                 | 1.20.5-1igel891                  |
| CUPS printing daemon                        | 2.1.3-4ubuntu0.9igel27           |
| PrinterLogic                                | 18.2.1.128                       |
| Lightdm graphical login manager             | 1.18.3-0ubuntu1.1                |
| XFCE4 Window Manager                        | 4.12.3-1ubuntu2igel656           |
| ISC DHCP Client                             | 4.3.3-5ubuntu12.10igel7          |
| NetworkManager                              | 1.2.6-0ubuntu0.16.04.3igel74     |
| ModemManager                                | 1.10.0-1~ubuntu18.04.2igel3      |
| GStreamer 0.10                              | 0.10.36-2ubuntu0.2               |
| GStreamer 1.x                               | 1.16.0-1igel214                  |
| WebKit2Gtk                                  | 2.24.2-0ubuntu0.19.04.1igel18    |
| Python2                                     | 2.7.12                           |
| Python3                                     | 3.5.2                            |
| <b>• Features with Limited IGEL Support</b> |                                  |
| Mobile Device Access USB (MTP)              | 1.1.16-2igel1                    |
| Mobile Device Access USB (imobile)          | 1.2.1~git20181030.92c5462-1igel5 |



|                                   |                    |
|-----------------------------------|--------------------|
| Mobile Device Access USB (gphoto) | 2.5.22-3igel1      |
| VPN OpenConnect                   | 7.08-1             |
| Scanner support / SANE            | 1.0.27-1           |
| VirtualBox                        | 6.0.8-dfsg-4igel25 |

- **Features with Limited Functionality**

|                   |        |
|-------------------|--------|
| Cisco JVDI Client | 12.1.0 |
|-------------------|--------|

## General Information 10.06.110

The following clients and features are not supported anymore:

- Citrix Receiver 12.1 and 13.1 - 13.4;
- Citrix Access Gateway Standard Plug-in;
- Dell vWorkspace Connector for Linux;
- Ericom PowerTerm Emulation 9 and 11;
- Ericom Webconnect;
- IGEL Legacy RDP Client (rdesktop);
- Virtual Bridges VERDE Client;
- PPTP VPN Support;
- IGEL Upgrade License Tool with IGEL Smartcard Token;
- Remote Management by setup.ini file transfer (TFTP);
- Remote Access via RSH;
- Legacy Philips Speech Driver;
- T-Systems TCOS Smartcard Support;
- DUS Series touch screens;
- Elo serial touchscreens;
- VIA Graphics support;
- Java WebStart;
- Storage hotplug devices are not automatically removed anymore, instead they must be always ejected manually:
  - by panel tray icon;
  - by an icon in the **In-Session Control Bar** (configurable under **IGEL Setup > User Interface > Desktop**);
  - by a **Safely Remove Hardware** session (configurable under **IGEL Setup > Accessories**).

The following clients and features are not available in this release:

- Cherry eGK Channel;
- Open VPN Smartcard Support;
- Asian Input Methods;
- Composite Manager.



## Known Issues 10.06.110

### Citrix

- With activated DRI3 and AMD GPU, Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H264, MPEG1 and MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.  
As a workaround, insert the smartcard before starting StoreFront login.
- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" > "For the entire screen".
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264 acceleration plugin**, the following registry key must be enabled:  
[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Range     | <u>enabled</u> / <u>disabled</u>                                 |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

### VMware Horizon

- External drives** mounted already before connection **do not appear in the remote desktop**.  
Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off.  
In the IGEL Setup client, **drive mapping** can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping**.  
It is also recommended to disable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection entirely** or at least to **deny storage devices** by adding a filter to the USB class rules.  
Furthermore, Horizon Client relies on the OS to mount the storage device itself. Enable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.

### Parallels Client



- **Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** one time with FIPS support disabled.

#### Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice**: spice-xpi Firefox plugin is no longer supported. The **Console Invocation** has to allow **Native client** (auto is also possible) and it should start in fullscreen to prevent opening windows.

#### Multimedia

- **Multimedia redirection with GStreamer** could fail with the Nouveau GPU driver.

#### WiFi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.  
Workaround: Disable system suspend under **IGEL Setup > System > Power Options > Shutdown**.

#### Base system

- Due to the removal of the Oracle JRE, **Java WebStart** is **not supported** anymore.

### Security Fixes 10.06.110

#### Firefox

- Updated **Firefox** browser to version **60.8.0 ESR**.
- Fixed **mfsa2019-22** security issues:  
[More...](#)

CVE-2019-9811, CVE-2019-11711, CVE-2019-11712, CVE-2019-11713, CVE-2019-11729, CVE-2019-11715, CVE-2019-11717, CVE-2019-11719, CVE-2019-11730 and CVE-2019-11709.

- Fixed **mfsa2019-19** security issue CVE-2019-11708.
- Fixed **mfsa2019-18** security issue CVE-2019-11707.
- Fixed **mfsa2019-08** security issues:  
[More...](#)

CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2018-18506 and CVE-2019-9788.

- Fixed **mfsa2019-05** security issues CVE-2018-18356 and CVE-2019-5785.
- Fixed **mfsa2019-02** security issues CVE-2018-18500, CVE-2018-18505 and CVE-2018-18501.

#### Shared Workplace

- Fixed **login in Shared Workplace** which accepts any user credentials in the 10.06.100 release. However, no user settings were applied to the device.



## New Features 10.06.110

### Base system

- Replaced **timesyncd** with **chrony NTP**.

A new registry key:

**More...**

|           |                                        |
|-----------|----------------------------------------|
| Parameter | Use NTP Servers from DNS SRV record    |
| Registry  | system.time.ntp_use_dnssrv_timeservers |
| Value     | <u>enabled</u> / disabled              |

### Evidian

- Integrated **Evidian AuthMgr** version **1.5.7116**.

### Hardware

- Hardware support for **HP EliteBook 840 G3**.

## Resolved Issues 10.06.110

### Base system

- Fixed **NTP synchronization** problems with changing the NTP client from **timesyncd** to **chrony**.
- Fixed **USB printer aliases**.

### X11 system

- Fixed **screen corruption with DPMS** and enabled **composite manager**.

### Hardware

- Fixed **black screen** issue with some monitors and 2560x1440 resolution on Intel GPUs.

### Caradigm

- Updated **RF IDEas** reader tool for the usage with Caradigm.

## 7.24 Notes for Release 10.06.100

|                       |            |             |
|-----------------------|------------|-------------|
| <b>Software:</b>      | Version    | 10.06.100   |
| <b>Release Date:</b>  | 2019-07-16 |             |
| <b>Release Notes:</b> | Version    | RN-106100-1 |
| <b>Last update:</b>   | 2019-07-16 |             |

- 
- [IGEL Linux Universal Desktop](#)(see page 1956)



- [IGEL Universal Desktop OS 3](#)(see page 1996)

### 7.24.1 IGEL Linux Universal Desktop

#### Supported Devices

##### **Universal Desktop:**

|          |                  |
|----------|------------------|
| UD2-LX:  | UD2-LX 40        |
| UD3-LX:  | UD3-LX 51        |
|          | UD3-LX 50        |
| UD5-LX:  | UD5-LX 50        |
| UD6-LX:  | UD6-LX 51        |
| UD7-LX:  | UD7-LX 10        |
| UD9-LX:  | UD9-LX Touch 41  |
|          | UD9-LX 40        |
| UD10-LX: | UD10-LX Touch 10 |
|          | UD10-LX 10       |

##### **IGEL Zero:**

|             |
|-------------|
| IZ2-RFX     |
| IZ2-HDX     |
| IZ2-HORIZON |
| IZ3-RFX     |
| IZ3-HDX     |
| IZ3-HORIZON |



- Component Versions 10.06.100(see page 1957)
- General Information 10.06.100(see page 1961)
- Security Fixes 10.06.100(see page 1962)
- Known Issues 10.06.100(see page 1966)
- New Features 10.06.100(see page 1967)
- Resolved Issues 10.06.100(see page 1988)

## Component Versions 10.06.100

### • Clients

| Product                            | Version                                   |
|------------------------------------|-------------------------------------------|
| Citrix HDX Realtime Media Engine   | 2.8.0-2235                                |
| Citrix Receiver                    | 13.10.0.20                                |
| Citrix Receiver                    | 13.5.0.10185126                           |
| Citrix Workspace App               | 19.3.0.5                                  |
| deviceTRUST Citrix Channel         | 19.1.200.2                                |
| Ericom PowerTerm                   | 2.0.1.0.20170219.2-_dev_-34574            |
| Evidian AuthMgr                    | 1.5.6840                                  |
| Evince PDF Viewer                  | 3.18.2-1ubuntu4.5                         |
| FabulaTech USB for Remote Desktop  | 5.2.29                                    |
| Firefox                            | 60.7.2                                    |
| IBM iAccess Client Solutions       | 1.1.8.1                                   |
| IGEL RDP Client                    | 2.2                                       |
| Imprivata OneSign ProveID Embedded | onesign-bootstrap-loader_1.0.523630_amd64 |
| deviceTRUST RDP Channel            | 19.1.200.2                                |
| Leostream Java Connect             | 3.3.7.0                                   |
| NCP Secure Enterprise Client       | 5.10_rev40552                             |



|                                       |                          |
|---------------------------------------|--------------------------|
| NX Client                             | 6.5.6                    |
| Open VPN                              | 2.3.10-1ubuntu2.2        |
| Zulu JRE                              | 8.38.0.13                |
| Parallels Client (64 bit)             | 16.5.3.20735             |
| Remote Viewer (RedHat Virtualization) | 8.0-1igel49              |
| Spice GTK (Red Hat Virtualization)    | 0.36-1~git20190601igel61 |
| Usbredir (Red Hat Virtualization)     | 0.8.0-1igel49            |
| Systancia AppliDis                    | 4.0.0.17                 |
| ThinLinc Client                       | 4.10.0-6068              |
| ThinPrint Client                      | 7.5.88                   |
| Totem Media Player                    | 2.30.2                   |
| Parole Media Player                   | 1.0.1-0ubuntu1igel18     |
| VMware Horizon Client                 | 5.0.0-12557422           |
| VNC Viewer                            | 1.9.0+dfsg-3igel8        |
| Voip Client Ekiga                     | 4.0.1                    |

- **Dictation**

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20180621 |
| Philips Speech Driver                     | 12.7.11  |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.8    |
| signotec VCOM Daemon      | 2.0.0    |



|                     |       |
|---------------------|-------|
| StepOver TCP Client | 2.1.0 |
|---------------------|-------|

- **Smartcard**

|                                           |                        |
|-------------------------------------------|------------------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101                |
| PKCS#11 Library Athena IDProtect          | 623.07                 |
| PKCS#11 Library cryptovision sc/interface | 7.1.20                 |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0              |
| PKCS#11 Library SecMaker NetID            | 6.7.2.36               |
| Reader Driver ACS CCID                    | 1.1.6-1igel1           |
| Reader Driver Gemalto eToken              | 10.0.37-0              |
| Reader Driver HID Global Omnikey          | 4.3.3                  |
| Reader Driver Identive CCID               | 5.0.35                 |
| Reader Driver Identive eHealth200         | 1.0.5                  |
| Reader Driver Identive SCRKBC             | 5.0.24                 |
| Reader Driver MUSCLE CCID                 | 1.4.30-1igel3          |
| Reader Driver REINER SCT cyberJack        | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite               | 1.8.23-1igel1          |
| Cherry USB2LAN Proxy                      | 3.2.0.3                |

- **System Components**

|                         |                    |
|-------------------------|--------------------|
| OpenSSL                 | 1.0.2g-1ubuntu4.15 |
| OpenSSH Client          | 7.2p2-4ubuntu2.8   |
| OpenSSH Server          | 7.2p2-4ubuntu2.8   |
| Bluetooth stack (bluez) | 5.50-0ubuntu1igel5 |
| MESA OpenGL stack       | 19.0.8-1igel73     |
| VAAPI ABI Version       | 0.40               |



|                                 |                                                      |
|---------------------------------|------------------------------------------------------|
| VDPAU Library version           | 1.1.1-3ubuntu1                                       |
| Graphics Driver INTEL           | 2.99.917+git20190301-igel870                         |
| Graphics Driver ATI/RADEON      | 19.0.1-2igel890                                      |
| Graphics Driver ATI/AMDGPU      | 19.0.1-4igel894                                      |
| Graphics Driver VIA             | 5.76.52.92-<br>opensource-009-005f78-20150730igel871 |
| Graphics Driver FBDEV           | 0.5.0-1igel819                                       |
| Graphics Driver VESA            | 2.4.0-1igel855                                       |
| Input Driver Evdev              | 2.10.6-1igel888                                      |
| Input Driver Elographics        | 1.4.1-1build5igel633                                 |
| Input Driver eGalax             | 2.5.5814                                             |
| Input Driver Synaptics          | 1.9.1-1ubuntu1igel866                                |
| Input Driver VMmouse            | 13.1.0-1ubuntu2igel635                               |
| Input Driver Wacom              | 0.36.1-0ubuntu2igel888                               |
| Kernel                          | 4.19.57 #mainline-ud-r2762                           |
| Xorg X11 Server                 | 1.20.5-1igel891                                      |
| Xorg Xephyr                     | 1.20.5-1igel891                                      |
| CUPS printing daemon            | 2.1.3-4ubuntu0.9igel27                               |
| PrinterLogic                    | 18.2.1.128                                           |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1                                    |
| XFCE4 Window Manager            | 4.12.3-1ubuntu2igel656                               |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7                              |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.3igel74                         |



|                |                               |
|----------------|-------------------------------|
| ModemManager   | 1.10.0-1~ubuntu18.04.2igel3   |
| GStreamer 0.10 | 0.10.36-2ubuntu0.2            |
| GStreamer 1.x  | 1.16.0-1igel214               |
| WebKit2Gtk     | 2.24.2-0ubuntu0.19.04.1igel18 |
| Python2        | 2.7.12                        |
| Python3        | 3.5.2                         |

- **Features with Limited IGEL Support**

|                                    |                                  |
|------------------------------------|----------------------------------|
| Mobile Device Access USB (MTP)     | 1.1.16-2igel1                    |
| Mobile Device Access USB (imobile) | 1.2.1~git20181030.92c5462-1igel5 |
| Mobile Device Access USB (gphoto)  | 2.5.22-3igel1                    |
| VPN OpenConnect                    | 7.08-1                           |
| Scanner support / SANE             | 1.0.27-1                         |
| VirtualBox                         | 6.0.8-dfsg-4igel25               |

- **Features with Limited Functionality**

|                   |        |
|-------------------|--------|
| Cisco JVDI Client | 12.1.0 |
|-------------------|--------|

## General Information 10.06.100

The following clients and features are not supported anymore:

- Citrix Receiver 12.1 and 13.1 - 13.4;
- Citrix Access Gateway Standard Plug-in;
- Dell vWorkspace Connector for Linux;
- Ericom PowerTerm Emulation 9 and 11;
- Ericom Webconnect;
- IGEL Legacy RDP Client (rdesktop);
- Virtual Bridges VERDE Client;
- PPTP VPN Support;
- IGEL Upgrade License Tool with IGEL Smartcard Token;
- Remote Management by setup.ini file transfer (TFTP);
- Remote Access via RSH;
- Legacy Philips Speech Driver;
- T-Systems TCOS Smartcard Support;
- DUS Series touch screens;
- Elo serial touchscreens;
- Video hardware acceleration support is discontinued on UD10-LX Touch 10 and UD10-LX 10;
- H.264 hardware acceleration support is discontinued on UD10-LX Touch 10 and UD10-LX 10;



- Java WebStart;
- Storage hotplug devices are not automatically removed anymore, instead they must be always ejected manually:
  - by panel tray icon;
  - by an icon in the **In-Session Control Bar** (configurable under **IGEL Setup > User Interface > Desktop**);
  - by a **Safely Remove Hardware** session (configurable under **IGEL Setup > Accessories**).

The following clients and features are not available in this release:

- Cherry eGK Channel;
- Open VPN Smartcard Support;
- Asian Input Methods;
- Composite Manager.

## Security Fixes 10.06.100

### Firefox

- Updated Mozilla **Firefox** to version **60.7.2 ESR**.
- Fixed **mfsa2019-19** security issue CVE-2019-11708.
- Fixed **mfsa2019-18** security issue CVE-2019-11707.
- Fixed **mfsa2019-10** security issues CVE-2019-9810 and CVE-2019-9813.
- Fixed **mfsa2019-08** security issues.

[More...](#)

CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793,  
CVE-2019-9795, CVE-2019-9796, CVE-2018-18506, CVE-2019-9788.

- Fixed **mfsa2019-05** security issues CVE-2018-18356 and CVE-2019-5785.
- Fixed **mfsa2019-02** security issues CVE-2018-18500, CVE-2018-18505 and CVE-2018-18501.
- Fixed **mfsa2018-30** security issues.

[More...](#)

CVE-2018-17466, CVE-2018-18492, CVE-2018-18493,  
CVE-2018-18494, CVE-2018-18498, CVE-2018-12405.

- Allow Firefox to access YubiKey (FIDO/U2F) when AppArmor is active.

### Base system

- Fixed a vulnerability in **Java configuration script**.
- Fixed possibly malicious **owner change** with TC setup configuration.
- Fixed **policykit-1** security issues CVE-2018-19788 and CVE-2019-6133.
- Fixed **NSS** security issues CVE-2018-18508, CVE-2018-12404, CVE-2018-12384 and CVE-2018-0495.
- Fixed **PPP** security issue CVE-2018-11574.
- Fixed **imagemagick** security issues.

[More...](#)

CVE-2018-16750, CVE-2018-16749, CVE-2018-16645, CVE-2018-16644,  
CVE-2018-16643, CVE-2018-16642, CVE-2018-16640, CVE-2018-16323,  
CVE-2018-14437, CVE-2018-14436, CVE-2018-14435, CVE-2018-14434,  
CVE-2017-13144, CVE-2017-12430, CVE-2019-9956, CVE-2019-7398,



CVE-2019-7397, CVE-2019-7396, CVE-2019-7175, CVE-2019-11598, CVE-2019-11597, CVE-2019-11472, CVE-2019-11470, CVE-2019-10650, CVE-2019-10131, CVE-2018-20467, CVE-2018-18025, CVE-2018-18024, CVE-2018-18016, CVE-2018-17966, CVE-2018-17965, CVE-2018-16413, CVE-2018-16412, CVE-2017-12806, and CVE-2017-12805.

- Fixed **systemd** security issues.

[More...](#)

CVE-2018-16866, CVE-2018-16865, CVE-2018-16864, CVE-2018-15688, CVE-2019-6454, CVE-2018-1049, CVE-2018-15686 and CVE-2019-3842.

- Fixed **CUPS** security issue CVE-2018-4700.

- Fixed **libarchive** security issues.

[More...](#)

CVE-2019-1000020, CVE-2019-1000019, CVE-2018-1000878, CVE-2018-1000877, and CVE-2017-14502.

- Fixed **Avahi** security issues CVE-2018-1000845 and CVE-2017-6519.

- Fixed **bind9** security issues CVE-2019-6465, CVE-2018-5745, and CVE-2018-5743.

- Fixed **libcaca** security issues.

[More...](#)

CVE-2018-20549, CVE-2018-20548, CVE-2018-20547, CVE-2018-20546, CVE-2018-20545, and CVE-2018-20544.

- Fixed **libgd2** security issues CVE-2019-6978 and CVE-2019-6977.

- Fixed **ghostscript** security issues.

[More...](#)

CVE-2019-6116, CVE-2018-19477, CVE-2018-19476, CVE-2018-19475, CVE-2018-19409, CVE-2018-18284, CVE-2018-18073, CVE-2018-17961, CVE-2019-3838, and CVE-2019-3835.

- Fixed **krb5** security issues.

[More...](#)

CVE-2018-5730, CVE-2018-5729, CVE-2017-11462, CVE-2017-11368, CVE-2016-3120, and CVE-2016-3119.

- Fixed **texlive-bin** security issue CVE-2018-17407.

- Fixed **LDB** security issue CVE-2019-3824.

- Fixed **libmspack** security issues CVE-2018-18585 and CVE-2018-18584.

- Fixed **Perl** security issues CVE-2018-18314, CVE-2018-18313, CVE-2018-18312 and CVE-2018-18311.

- Fixed **poppler** security issues.

[More...](#)

CVE-2019-7310, CVE-2018-20650, CVE-2018-20551, CVE-2018-20481, CVE-2018-19149, CVE-2018-19060, CVE-2018-19059, CVE-2018-19058, CVE-2018-16646, and CVE-2019-9200.

- Fixed **Python 3.5** security issues CVE-2018-14647, CVE-2018-1061, CVE-2018-1060 and CVE-2018-106.

- Fixed **Net-SNMP** security issue CVE-2018-18065.



- Fixed **OpenSSL** security issues CVE-2019-1559, CVE-2018-5407 and CVE-2018-0734.

- Fixed **TIFF** security issues.

[More...](#)

CVE-2018-8905, CVE-2018-7456, CVE-2018-18661, CVE-2018-18557, CVE-2018-17101, CVE-2018-17100, CVE-2018-1710, CVE-2018-10963, CVE-2019-7663, CVE-2019-6128, CVE-2018-19210, CVE-2018-17000, CVE-2018-12900, and CVE-2018-10779.

- Fixed **libvncserver** security issues.

[More...](#)

CVE-2018-6307, CVE-2018-20750, CVE-2018-20749, CVE-2018-20748, CVE-2018-20024, CVE-2018-20023, CVE-2018-20022, CVE-2018-20021, CVE-2018-20020, CVE-2018-20019, CVE-2018-15127, and CVE-2018-15126.

- Fixed **WavPack** security issue CVE-2018-19840.

- Fixed **Samba** security issues.

[More...](#)

CVE-2018-16851, CVE-2018-16841, CVE-2018-14629, CVE-2019-3880, and CVE-2018-16860.

- Fixed **libxkbcommon** security issues.

[More...](#)

CVE-2018-15864, CVE-2018-15863, CVE-2018-15862, CVE-2018-15861, CVE-2018-15859, CVE-2018-15858, CVE-2018-15857, CVE-2018-15856, CVE-2018-15855, CVE-2018-15854, and CVE-2018-15853.

- Fixed **OpenSSH** security issues.

[More...](#)

CVE-2019-6111, CVE-2019-6109, CVE-2018-20685, CVE-2018-15473, and CVE-2016-10708.

- Fixed **Python 2.7** security issues.

[More...](#)

CVE-2018-14647, CVE-2018-1061, CVE-2018-1060, CVE-2018-106, CVE-2018-1000802, and CVE-2018-1000030.

- Fixed **lxml** security issue CVE-2018-19787.

- Fixed **gdk-pixbuf** security issues.

[More...](#)

CVE-2017-6314, CVE-2017-6313, CVE-2017-6312, CVE-2017-6311, CVE-2017-2870, CVE-2017-2862, CVE-2017-1000422, CVE-2016-6352, and CVE-2017-12447.

- Fixed **file** security issues CVE-2019-8907 and CVE-2019-8905.

- Fixed **wget** security issue CVE-2019-5953.

- Fixed **libsslt** security issue CVE-2019-11068.

- Fixed **Evince** security issue CVE-2019-11459.

- Fixed **webkit2gtk** security issues.

[More...](#)



CVE-2019-8595, CVE-2019-8607, CVE-2019-8615, CVE-2019-6251, CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378, CVE-2018-4382, CVE-2018-4392, CVE-2018-4416, CVE-2018-4345, CVE-2018-4386, and CVE-2018-4372.

- Fixed **gst-plugins-base0.10** security issue CVE-2019-9928.
- Fixed **WPA** security issues.

[More...](#)

CVE-2019-9495, CVE-2019-9497, CVE-2019-9498, CVE-2019-9499, and CVE-2019-11555.

- Fixed **Heimdal** security issues CVE-2019-12098 and CVE-2018-16860.
- Fixed **libimobiledevice** security issue CVE-2016-5104.
- Fixed **libpng1.6** security issues CVE-2019-7317 and CVE-2018-13785.
- Fixed **GIMP** security issues.

[More...](#)

CVE-2017-17786, CVE-2017-17789, CVE-2017-17784, CVE-2017-17787, CVE-2017-17785, and CVE-2017-17788

- Fixed **libtomcrypt** security issue CVE-2018-12437.
- Fixed **curl** security issues.

[More...](#)

CVE-2018-16840, CVE-2018-16839, CVE-2019-3823, CVE-2019-3822, CVE-2018-16890, CVE-2019-5346.

- Fixed **gnutls28** security issues CVE-2018-10846, CVE-2018-10845, CVE-2018-10844 and CVE-2018-1084.
- Fixed **qtbase-opensource-src** security issues CVE-2018-19873, CVE-2018-19870 and CVE-2018-15518.
- Fixed **db5.3** security issue CVE-2019-8457.
- Fixed **libssh2** security issues.

[More...](#)

CVE-2019-3863, CVE-2019-3862, CVE-2019-3861, CVE-2019-3860, CVE-2019-3859, CVE-2019-3858, CVE-2019-3857, CVE-2019-3856, and CVE-2019-3855.

- Fixed **network-manager** security issue CVE-2018-15688.
- Fixed **elfutils** security issues.

[More...](#)

CVE-2019-7665, CVE-2019-7150, CVE-2019-7149, CVE-2018-18521, CVE-2018-18520, CVE-2018-18310, CVE-2018-16403, CVE-2018-16402, and CVE-2018-16062.

- Fixed **libsndfile** security issues.

[More...](#)

CVE-2019-3832, CVE-2018-19758, CVE-2018-19662, CVE-2018-19661, CVE-2018-19432, CVE-2018-13139, CVE-2017-6892, CVE-2017-17457, CVE-2017-17456, CVE-2017-16942, CVE-2017-14634, CVE-2017-14246, and CVE-2017-14245.



- Fixed **dbus** security issue CVE-2019-12749.
- Fixed **Vim** security issues CVE-2019-12735 and CVE-2017-5953.  
Fixed **sqlite3** security issues.  
[More...](#)
- CVE-2019-9937, CVE-2019-9936, CVE-2019-8457, CVE-2018-20506, CVE-2018-20346, CVE-2017-2520, CVE-2017-2519, CVE-2017-2518, CVE-2017-13685, CVE-2017-10989, and CVE-2016-6153.
- Fixed **libseccomp** security issue CVE-2019-9893.
- Fixed **bzip2** security issues CVE-2019-12900 and CVE-2016-3189.
- Fixed **Expat** security issue CVE-2018-20843.
- Fixed **unzip** security issues CVE-2019-13232, CVE-2018-1000035, CVE-2016-9844 and CVE-2014-9913.
- **Mount partitions** with "**nodev**" flag option.
- The home directory of the remote users is now **/home/ruser**.
- Default **umask** is set to **0077** for all non-root users.
- Fixed a vulnerability in the **custom environment variable framework**.
- Fixed kernel **TCP** vulnerabilities CVE-2019-11477: **SACK Panic**, CVE-2019-11478: **SACK Slowness** and CVE-2019-11479: **Excess Resource Consumption Due to Low MSS Values**.
- Changed **minimally allowed MSS size** to "**1000**" to prevent possible denial-of-service attacks.

## Known Issues 10.06.100

### Citrix

- With activated DRI3 and AMD GPU, Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H264, MPEG1 and MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.  
As a workaround, insert the smartcard before starting StoreFront login.
- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" > "For the entire screen".
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264 acceleration plugin**, the following registry key must be enabled:  
[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | <code>ica.workaround-dual-rtme</code>                            |
| Range     | <code>enabled</code> / <code>disabled</code>                     |



This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

#### VMware Horizon

- **External drives** mounted already before connection **do not appear in the remote desktop**.  
Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off.  
In the IGEL Setup client, **drive mapping** can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping**.  
It is also recommended to disable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection entirely** or at least to **deny storage devices** by adding a filter to the USB class rules.  
Furthermore, Horizon Client relies on the OS to mount the storage device itself. Enable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.

#### Parallels Client

- **Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode** it is necessary to connect to the **Parallels RAS** one time with FIPS support disabled.

#### Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice**: spice-xpi Firefox plugin is no longer supported. The **Console Invocation** has to allow **Native client** (auto is also possible) and it should start in fullscreen to prevent opening windows.

#### WiFi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.  
Workaround: Disable system suspend under **IGEL Setup > System > Power Options > Shutdown**.

#### Base system

- Due to the removal of the Oracle JRE, **Java WebStart** is **not supported** anymore.

#### Hardware

- **Suspend on UD10** is disabled.

## New Features 10.06.100

#### OS 11 Upgrade



- It is now possible to **upgrade to IGEL OS 11**. For more information, see the how-to [Upgrading IGEL Devices from IGEL OS 10 to IGEL OS 11](#)(see page 174).

The **parameters for the upgrade**:

[More...](#)

#### IGEL Setup > System > Update > OS 11 Upgrade

|           |                                                                         |
|-----------|-------------------------------------------------------------------------|
| Parameter | Upgrade to OS 11                                                        |
| Registry  | <code>update.firmware_migrate_to_11</code>                              |
| Value     | <u>enabled</u> / <u>disabled</u>                                        |
| Parameter | Upgrade to OS 11 even if a previous upgrade attempt failed              |
| Registry  | <code>update.force_firmware_migrate_to_11</code>                        |
| Value     | <u>enabled</u> / <u>disabled</u>                                        |
| Parameter | Upgrade to OS 11 even if PowerTerm is enabled                           |
| Registry  | <code>update.migrate_to_11_with_powerterm</code>                        |
| Value     | <u>enabled</u> / <u>disabled</u>                                        |
| Parameter | Require an Enterprise Management Pack license to upgrade to OS 11       |
| Registry  | <code>update.migrate_to_11_enterprise_required</code>                   |
| Range     | [Smart] [Always] [Never]                                                |
| Parameter | Timeout waiting for OS 11 license to start automatic upgrade            |
| Registry  | <code>update.migrate_to_11_license_timeout</code>                       |
| Range     | [Disabled] [ <u>10 Minutes</u> ] [15 Minutes] [30 Minutes] [60 Minutes] |

The parameters for configuring the **desktop integration** of the **IGEL OS 11 Upgrade tool** are:

[More...](#)

#### IGEL Setup > Accessories > OS 11 Upgrade

|          |                                                        |
|----------|--------------------------------------------------------|
| Registry | <code>sessions.os11_migration0.startmenu</code>        |
| Value    | <u>enabled</u> / <u>disabled</u>                       |
| Registry | <code>sessions.os11_migration0.applaunch</code>        |
| Value    | <u>enabled</u> / <u>disabled</u>                       |
| Registry | <code>sessions.os11_migration0.startmenu_system</code> |
| Value    | <u>enabled</u> / <u>disabled</u>                       |
| Registry | <code>sessions.os11_migration0.applaunch_system</code> |
| Value    | <u>enabled</u> / <u>disabled</u>                       |
| Registry | <code>sessions.os11_migration0.menu_path</code>        |
| Registry | <code>sessions.os11_migration0.desktop_path</code>     |
| Registry | <code>sessions.os11_migration0.applaunch_path</code>   |
| Registry | <code>sessions.os11_migration0.quick_start</code>      |
| Value    | <u>enabled</u> / <u>disabled</u>                       |
| Registry | <code>sessions.os11_migration0.pwprotected</code>      |
| Range    | [None] [Administrator] [User] [Setup user]             |
| Registry | <code>sessions.os11_migration0.desktop</code>          |
| Value    | <u>enabled</u> / <u>disabled</u>                       |



|          |                                   |
|----------|-----------------------------------|
| Registry | sessions.os11_migration0.pulldown |
| Value    | <u>enabled</u> / <u>disabled</u>  |

## Citrix

- Integrated **Citrix Workspace app 19.03**.
- Added a new registry key to support **1536-bit RSA keys for client authentication**. Factory default for this release is "true".

**More...**

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Enables RSA 1536 cipher suite         |
| Registry  | ica.allregions.enable_rsa_1536        |
| Range     | <u>factory default</u> / false / true |

- Added a new **registry key** to enable **different cipher suites**. Factory default for this release is "ALL".

**More...**

|           |                                                                                                                                                          |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter | Enables different cipher suite                                                                                                                           |
| Registry  | ica.allregions.sslciphers                                                                                                                                |
| Range     | <u>factory default</u> / ALL / GOV / COM                                                                                                                 |
|           | > TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - GOV/ALL<br>> TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - GOV/ALL<br>> TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - COM/ALL |

- Added a new **registry key** to support **keyboard layout synchronization**.

**More...**

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Keyboard layout synchronization               |
| Registry  | ica.modules.virtualdriver.keyboardsync.enable |
| Value     | <u>disabled</u> / enabled                     |

- Updated **Citrix HDX RTME** used for optimization of Skype for Business to version **2.8.0-2235**.
- Added support for **Citrix Workspace Launcher** functionality as described at <https://support.citrix.com/article/CTX237727>.
- Added a Citrix plugin for **hardware accelerated VDPAU based H.264 decoding** on AMD graphics chipsets:

**More...**

|           |                                                      |
|-----------|------------------------------------------------------|
| Parameter | Enable HW accelerated H264 vdpaucodec (experimental) |
| Registry  | ica.hw-accelerated-h264-vdpaucodec                   |
| Value     | <u>enabled</u> / <u>disabled</u>                     |

## RDP/IGEL RDP Client 2

- Added a field '**Collection**' to RDP session server page.

**More...****IGEL Setup > Sessions > RDP > RDP Sessions > RDP Session > Server****IGEL Setup > Sessions > RDP > RDP Sessions > RDP Session > Options**

|           |            |
|-----------|------------|
| Parameter | Collection |
|-----------|------------|



|          |                                                  |
|----------|--------------------------------------------------|
| Registry | sessions.winconnect<NR>.option.load-balance-info |
|----------|--------------------------------------------------|

## VMware Horizon

- Updated **Horizon Client** to version **5.0.0-12557422**.
- Added parameters to specify **webcam frame size** and **rate for RTAV**.

[More...](#)

|           |                               |
|-----------|-------------------------------|
| Parameter | Webcam frame width            |
| Registry  | vmware.view.rtav-frame-width  |
| Value     | <u>&lt;empty string&gt;</u>   |
| Parameter | Webcam frame height           |
| Registry  | vmware.view.rtav-frame-height |
| Value     | <u>&lt;empty string&gt;</u>   |
| Parameter | Webcam frame rate             |
| Registry  | vmware.view.rtav-frame-rate   |
| Value     | <u>&lt;empty string&gt;</u>   |

- Added a possibility to easily evaluate **Horizon Blast decoder states**. By default, sessions are evaluated after use and the result is written to the journal log.
- Added **continuous run mode** for USB-Arbitrator.

[More...](#)

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | USB-Arbitrator continuous run mode            |
| Registry  | vmware.view.usb.arbitrator-continuous-runmode |
| Value     | <u>enabled</u> / disabled                     |

- Added **recognition for password change** and **password expired dialog** in Horizon local logon sessions or appliance mode.
- Added **switch for Blast H.264 decoding** for VMware Horizon Client.

[More...](#)

|           |                           |
|-----------|---------------------------|
| Parameter | Blast H.264 decoding      |
| Registry  | vmware.view.blast-h264    |
| Value     | <u>enabled</u> / disabled |

- Added **switch to use systemwide proxy** in VMware Horizon appliance mode.

[More...](#)

|           |                           |
|-----------|---------------------------|
| Parameter | Use the systemwide proxy  |
| Registry  | vmwarevdmapp.use_proxy    |
| Value     | <u>enabled</u> / disabled |

## Parallels Client

- Updated **Parallels Client** to version **16.5.3 (64-Bit)**.
- Added a possibility to set apps to **autostart on Parallels RAS**.

## ThinLinc

- Updated **Cendio ThinLinc** to version **4.10**.

## RedHat Enterprise Virtualization Client.



- Updated **Remote Viewer** (RedHat Virtualization) to version **8.0**.
- Updated **Spice GTK** (RedHat Virtualization) to version **0.36**.

## IBM\_5250

- Updated **IBM iAccess Client** Solutions to version **1.1.8.1**.
- **Improved startup time** of IBM iAccess Client.
- **Improved configuration** of IBM iAccess Client **via IGEL Setup**.

[More...](#)

|                |                                                                                                           |
|----------------|-----------------------------------------------------------------------------------------------------------|
| Setup          | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Connection > Advanced                   |
| Parameter      | Bypass signon                                                                                             |
| Registry Value | <code>sessions.iaccess&lt;NR&gt;.options.ssoenabled</code><br><u>enabled</u> / <u>disabled</u>            |
| Setup          | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Font                           |
| Parameter      | Antialiasing                                                                                              |
| Registry Value | <code>sessions.iaccess&lt;NR&gt;.options.textantialiasing</code><br><u>enabled</u> / <u>disabled</u>      |
| Setup          | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor                         |
| Parameter      | Allow blinking cursor                                                                                     |
| Registry Value | <code>sessions.iaccess&lt;NR&gt;.options.blinkcursor</code><br><u>enabled</u> / <u>disabled</u>           |
| Setup          | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor                         |
| Parameter      | Show blinking text with                                                                                   |
| Registry Value | <code>sessions.iaccess&lt;NR&gt;.options.blinkstate</code><br>[Blinking Text] [Host Color] [Mapped Color] |
| Setup          | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor                         |
| Parameter      | Blink Color                                                                                               |
| Registry Value | <code>sessions.iaccess&lt;NR&gt;.options.blinkcolor_fg</code><br><u>#ffc800</u>                           |
| Setup          | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor                         |



|           |                                                                                      |
|-----------|--------------------------------------------------------------------------------------|
| Parameter | Blink Color Background                                                               |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.blinkcolor_bg</code>                        |
| Value     | <code>#000000</code>                                                                 |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Rule Line |
| Parameter | Rule Line                                                                            |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.ruleline</code>                             |
| Value     | <code>enabled / disabled</code>                                                      |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Rule Line |
| Parameter | Follow Cursor                                                                        |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.rulelinefollows</code>                      |
| Value     | <code>enabled / disabled</code>                                                      |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Rule Line |
| Parameter | Style                                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.rulelinestyle</code>                        |
| Value     | <code>[Crosshair] [Vertical] [Horizontal]</code>                                     |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color     |
| Parameter | Green                                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fgn_fg</code>                         |
| Value     | <code>#00ff00</code>                                                                 |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color     |
| Parameter | Green Background                                                                     |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fgn_bg</code>                         |
| Value     | <code>#000000</code>                                                                 |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color     |
| Parameter | White                                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fwt_fg</code>                         |
| Value     | <code>#ffffff</code>                                                                 |



|           |                                                                                  |
|-----------|----------------------------------------------------------------------------------|
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | White Background                                                                 |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fwt_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Red                                                                              |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_frd_fg</code>                     |
| Value     | <u>#ff0000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Red Background                                                                   |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_frd_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Turquoise                                                                        |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_ftq_fg</code>                     |
| Value     | <u>#00ffff</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Turquoise Background                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_ftq_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Yellow                                                                           |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fyw_fg</code>                     |
| Value     | <u>#ffff00</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Yellow Background                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fyw_bg</code>                     |



|           |                                                                                  |
|-----------|----------------------------------------------------------------------------------|
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Pink                                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fpk_fg</code>                     |
| Value     | <u>#ff00ff</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Pink Background                                                                  |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fpk_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Blue                                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fbl_fg</code>                     |
| Value     | <u>#7890f0</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Blue Background                                                                  |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fbl_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Status Indicators                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_osi</code>                        |
| Value     | <u>#7890f0</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Information Indicators                                                           |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_oui</code>                        |
| Value     | <u>#ffffff</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Attention Indicators                                                             |



|           |                                                                                  |
|-----------|----------------------------------------------------------------------------------|
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_oai</code>                        |
| Value     | <u>#ffff00</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Error Indicators                                                                 |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_oei</code>                        |
| Value     | <u>#ff0000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | OIA Background                                                                   |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_oob</code>                        |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Screen Background                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_sbg</code>                        |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Highlight active field                                                           |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.actfieldhilite</code>                   |
| Value     | <u>enabled / disabled</u>                                                        |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Active Field                                                                     |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_actf_fg</code>                    |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Active Field Background                                                          |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_actf_bg</code>                    |
| Value     | <u>#ffff00</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |



|           |                                                                                              |
|-----------|----------------------------------------------------------------------------------------------|
| Parameter | Crosshair Ruler Color                                                                        |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_crc</code>                                    |
| Value     | <code>#00ff00</code>                                                                         |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color             |
| Parameter | Column Separator                                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_ccs</code>                                    |
| Value     | <code>#ffffff</code>                                                                         |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences                |
| Parameter | Start window maximized                                                                       |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.ismaximized</code>                                  |
| Value     | <code>enabled / disabled</code>                                                              |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences > Keyboard     |
| Parameter | Keyboard Remapping File                                                                      |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.keyremapfile</code>                                 |
| Value     | <code>IBMi.kmp</code>                                                                        |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences > Popup Keypad |
| Parameter | Popup Keypad File                                                                            |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.poppadfile</code>                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences > Toolbar      |
| Parameter | Toolbar File                                                                                 |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.toolbarfile</code>                                  |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup                                   |
| Parameter | Open new sessions in a new tab                                                               |
| Registry  | <code>ibm.iaccess.acssm.opensessionintab</code>                                              |
| Value     | <code>enabled / disabled</code>                                                              |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup                                   |



|           |                                                            |
|-----------|------------------------------------------------------------|
| Parameter | Always display the tab bar                                 |
| Registry  | <code>ibm.iaccess.acssm.alwaysshownabar</code>             |
| Value     | <u>enabled</u> / <u>disabled</u>                           |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup |
| Parameter | Switch to new tab when created                             |
| Registry  | <code>ibm.iaccess.acssm.switchtonewtab</code>              |
| Value     | <u>enabled</u> / <u>disabled</u>                           |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup |
| Parameter | Send a warning when closing multiple tabs                  |
| Registry  | <code>ibm.iaccess.acssm.closemultipletabwarning</code>     |
| Value     | <u>enabled</u> / <u>disabled</u>                           |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup |
| Parameter | Do not start tabbed sessions until the tab is selected     |
| Registry  | <code>ibm.iaccess.acssm.tabdelayedstart</code>             |
| Value     | <u>enabled</u> / <u>disabled</u>                           |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup |
| Parameter | New Tab Action                                             |
| Registry  | <code>ibm.iaccess.acssm.newtabaction</code>                |
| Value     | [Disable and Hide] [Run the Same] [Run Other...]           |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup |
| Parameter | Tab Placement                                              |
| Registry  | <code>ibm.iaccess.acssm.tabplacement</code>                |
| Value     | [Top] [Bottom] [Left] [Right]                              |

## Firefox

- Updated **Mozilla Firefox** to version **60.7.2 ESR**.
  - Added new keys to **auto show and hide the on-screen software keyboard**. To use this feature, the keyboard should be set to autostart. After a restart is activated, the keyboard will appear automatically when an input box is selected. Confirmed to work in Firefox and on lockscreen.
- [More...](#)



|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Automatically hide software keyboard depending on focused widget |
| Registry  | userinterface.softkeyboard.autohide                              |
| Value     | <u>enabled</u> / <u>disabled</u>                                 |
| Parameter | Automatically show software keyboard depending on focused widget |
| Registry  | userinterface.softkeyboard.autoshow                              |
| Value     | <u>enabled</u> / <u>disabled</u>                                 |

- Added new parameters: **Allow a custom command before and after browser session.**

[More...](#)

|           |                                |
|-----------|--------------------------------|
| Parameter | init_action                    |
| Registry  | sessions.browser%.init_action  |
| Value     | <u>&lt;empty_string&gt;</u>    |
| Parameter | final_action                   |
| Registry  | sessions.browser%.final_action |
| Value     | <u>&lt;empty_string&gt;</u>    |

- Added options to customize Firefox overflow menu and hide navigation buttons.

[More...](#)

|           |                                                              |
|-----------|--------------------------------------------------------------|
| Parameter | Hide Navigation buttons                                      |
| Registry  | sessions.browser<NR>.app.navigation_buttons_hidden           |
| Value     | <u>enabled</u> / <u>disabled</u>                             |
| Parameter | Overflow Menu                                                |
| Registry  | sessions.browser<NR>.app.custom_toolbar.overflow-menu        |
| Value     | <u>open-file-button,feed-button,characterencoding-button</u> |

## Imprivata

- Imprivata Appliance 6.3** or higher is needed now.
- Added a new parameter to Imprivata.conf: "**Redirection of Smartcards**".

[More...](#)

| <b>IGEL Setup &gt; Sessions &gt; Appliance Mode &gt; Imprivata</b> |                                        |
|--------------------------------------------------------------------|----------------------------------------|
| Parameter                                                          | Redirection of Smartcards              |
| Registry                                                           | imprivata.native_smartcard_redirection |
| Value                                                              | <u>enabled</u> / <u>disabled</u>       |

- Added a new parameter: "**Path to Certificate**".

[More...](#)



### IGEL Setup > Sessions > Appliance Mode > Imprivata

|           |                               |
|-----------|-------------------------------|
| Parameter | Path to Certificate           |
| Registry  | imprivata.path_to_certificate |

#### Network

- Added **NCP Secure Enterprise VPN Client** version **5.10\_rev40552** (configurable under **IGEL Setup > Network > VPN > NCP VPN Client**).
- Added a new feature: **Network status icons** are **shown on the lock and logon screens**.
- Added a mechanism for **retrieving the SCEP challenge password with a custom script**. Setting the following registry key to "true" enables the use of the script. The registry key `network.scepclient.cert%.crypt_password` will be ignored. (The script may use it for its own purpose though.)

[More...](#)

|           |                                                                      |
|-----------|----------------------------------------------------------------------|
| Parameter | Use Challenge Password Command                                       |
| Registry  | <code>network.scepclient.cert%.use_challenge_password_command</code> |
| Value     | <u>enabled</u> / <u>disabled</u>                                     |

If the above key is enabled, the value of this key will be passed to bash for execution. It happens when the SCEP challenge password is needed for creating a certificate signing request. The script is supposed to output the challenge password on its standard output. For convenience, any Carriage-Return characters are stripped off the script before execution by bash.

[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Challenge Password Command                                       |
| Registry  | <code>network.scepclient.cert%.challenge_password_command</code> |
| Value     | <u>&lt;empty_string&gt;</u>                                      |

#### Wi-Fi

- Added support for **Realtek 8821CE wireless cards**.
- Added switch to determine **the source of WiFi scan results for Wireless Manager**. Selecting default is currently identical with the old mechanism (using the iwlist command). This may change in the future. When iwlist fails, NetworkManager is automatically used as a fallback.

[More...](#)

|           |                                                                   |
|-----------|-------------------------------------------------------------------|
| Parameter | WiFi Scanner                                                      |
| Registry  | <code>network.interfaces.wirelesslan.device0.mssid_scanner</code> |
| Range     | <u>[default]</u> <u>[iwlist]</u> <u>[NetworkManager]</u>          |

#### Smartcard

- New **IGEL Smartcard** mode **without Locking Desktop** (reintroduced feature of Linux 5.x firmware).

[More...](#)

### IGEL Setup > Security > Logon > IGEL Smartcard

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Enable IGEL Smartcard without Locking Desktop |
|-----------|-----------------------------------------------|



|          |                                         |
|----------|-----------------------------------------|
| Registry | <code>scard.scardd.enable_nolock</code> |
| Value    | <u>enabled</u> / <u>disabled</u>        |

### IGEL Setup > Security > Logon > IGEL Smartcard

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | On Smartcard Removal, terminate               |
| Registry  | <code>scard.scardd.session_termination</code> |
| Value     | <u>all</u> / smartcard                        |

- Updated **MUSCLE CCID** smartcard reader driver to version **1.4.30**.
- Updated **ACS CCID** smartcard driver to version **1.1.6**.
- Updated **REINER SCT** smartcard reader driver to version **3.99.5final.sp13**.
- Updated **SecMaker NetID** to version **6.7.2.36**: now **YubiKey 5** is supported.
- Updated **cryptovision sc/interface PKCS#11** smartcard library to version **7.1.20**.
- Added configuration parameters for some settings of **smartcard library OpenSC**.  
[More...](#)

|           |                                                                      |
|-----------|----------------------------------------------------------------------|
| Parameter | Debug level                                                          |
| Registry  | <code>scard.pkcs11.opensc.default.debug</code>                       |
| Value     | <u>0</u>                                                             |
| Parameter | Debug file                                                           |
| Registry  | <code>scard.pkcs11.opensc.default.debug_file</code>                  |
| Value     | <u>stderr</u>                                                        |
| Parameter | Max. send size                                                       |
| Registry  | <code>scard.pkcs11.opensc.default.pcsc.max_send_size</code>          |
| Value     | <u>255</u>                                                           |
| Parameter | Max. receive size                                                    |
| Registry  | <code>scard.pkcs11.opensc.default.pcsc.max_recv_size</code>          |
| Value     | <u>256</u>                                                           |
| Parameter | Connect exclusive                                                    |
| Registry  | <code>scard.pkcs11.opensc.default.pcsc.connect_exclusive</code>      |
| Value     | <u>enabled</u> / <u>disabled</u>                                     |
| Parameter | Disconnect action                                                    |
| Registry  | <code>scard.pkcs11.opensc.default.pcsc.disconnect_action</code>      |
| Value     | <u>leave</u> / <u>reset</u> / <u>unpower</u>                         |
| Parameter | Transaction end action                                               |
| Registry  | <code>scard.pkcs11.opensc.default.pcsc.transaction_end_action</code> |
| Value     | <u>leave</u> / <u>reset</u> / <u>unpower</u>                         |
| Parameter | Reconnect action                                                     |
| Registry  | <code>scard.pkcs11.opensc.default.pcsc.reconnect_action</code>       |
| Value     | <u>leave</u> / <u>reset</u> / <u>unpower</u>                         |
| Parameter | Enable pinpad                                                        |
| Registry  | <code>scard.pkcs11.opensc.default.pcsc.enable_pinpad</code>          |



|           |                                                                               |
|-----------|-------------------------------------------------------------------------------|
| Value     | <u>enabled / disabled</u>                                                     |
| Parameter | Use PIN caching                                                               |
| Registry  | <code>scard.pkcs11.opensc.default.pkcs15.use_pin_caching</code>               |
| Value     | <u>enabled / disabled</u>                                                     |
| Parameter | How many times to use a PIN from cache before re-authenticating it            |
| Registry  | <code>scard.pkcs11.opensc.default.pkcs15.pin_cache_counter</code>             |
| Value     | <u>10</u>                                                                     |
| Parameter | PIN caching ignores user consent                                              |
| Registry  | <code>scard.pkcs11.opensc.default.pkcs15.pin_cache_ignore_user_consent</code> |
| Value     | <u>enabled / disabled</u>                                                     |

- Updated **CHERRY USB-LAN Proxy** to version **3.2.0.3**. This version provides enhanced configuration.

[More...](#)

#### **IGEL Setup > Security > Smartcard > Services**

|           |                                                 |
|-----------|-------------------------------------------------|
| Parameter | Bind IP                                         |
| Registry  | <code>devices.cherry.usblanproxy.bind-ip</code> |
| Value     | <u>auto</u>                                     |

#### **IGEL Setup > Security > Smartcard > Services**

|           |                                                    |
|-----------|----------------------------------------------------|
| Parameter | Https Server Port                                  |
| Registry  | <code>devices.cherry.usblanproxy.https-port</code> |
| Value     | <u>443</u>                                         |

#### **IGEL Setup > Security > Smartcard > Services**

|           |                                                           |
|-----------|-----------------------------------------------------------|
| Parameter | SICCT Announce IP                                         |
| Registry  | <code>devices.cherry.usblanproxy.sicct-announce-ip</code> |
| Value     | <u>broadcast</u>                                          |

#### **IGEL Setup > Security > Smartcard > Services**

|           |                                                             |
|-----------|-------------------------------------------------------------|
| Parameter | SICCT Announce Port                                         |
| Registry  | <code>devices.cherry.usblanproxy.sicct-announce-port</code> |
| Value     | <u>4742</u>                                                 |

#### **IGEL Setup > Security > Smartcard > Services**

|           |                                                                 |
|-----------|-----------------------------------------------------------------|
| Parameter | SICCT Announce Interval                                         |
| Registry  | <code>devices.cherry.usblanproxy.sicct-announce-interval</code> |
| Value     | <u>30</u>                                                       |

#### **IGEL Setup > Security > Smartcard > Services**

|           |                                                       |
|-----------|-------------------------------------------------------|
| Parameter | USB Fast Mode                                         |
| Registry  | <code>devices.cherry.usblanproxy.usb-fast-mode</code> |
| Value     | <u>enabled /disabled</u>                              |

#### **IGEL Setup > Security > Smartcard > Services**



|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Alternate Initialization Method for G87-1505  |
| Registry  | devices.cherry.usblanproxy.usb-1505-alt-setup |
| Value     | <u>enabled /disabled</u>                      |

## CUPS Printing

- Added **SMB Network Print** client function.

[More...](#)

**IGEL Setup > Devices > Printer > CUPS > Printers > Dialog**

|           |                                |
|-----------|--------------------------------|
| Parameter | Printer Port                   |
| Registry  | print.cups.printer<NR>.backend |
| Value     | <u>smb</u>                     |

**IGEL Setup > Devices > Printer > CUPS > Printers > Dialog**

|           |                                   |
|-----------|-----------------------------------|
| Parameter | SMB Server                        |
| Registry  | print.cups.printer<NR>.smb_server |

**IGEL Setup > Devices > Printer > CUPS > Printers > Dialog**

|           |                                      |
|-----------|--------------------------------------|
| Parameter | SMB Workgroup                        |
| Registry  | print.cups.printer<NR>.smb_workgroup |

**IGEL Setup > Devices > Printer > CUPS > Printers > Dialog**

|           |                                    |
|-----------|------------------------------------|
| Parameter | SMB Printer                        |
| Registry  | print.cups.printer<NR>.smb_printer |

**IGEL Setup > Devices > Printer > CUPS > Printers > Dialog**

|           |                                 |
|-----------|---------------------------------|
| Parameter | SMB Port                        |
| Registry  | print.cups.printer<NR>.smb_port |

**IGEL Setup > Devices > Printer > CUPS > Printers > Dialog**

|           |                                     |
|-----------|-------------------------------------|
| Parameter | Use Kerberos Authentication         |
| Registry  | print.cups.printer<NR>.smb_kerberos |
| Value     | <u>enabled / disabled</u>           |

**IGEL Setup > Devices > Printer > CUPS > Printers > Dialog**

|           |                                        |
|-----------|----------------------------------------|
| Parameter | Use Passthrough Authentication         |
| Registry  | print.cups.printer<NR>.smb_passthrough |
| Value     | <u>enabled /disabled</u>               |

**IGEL Setup > Devices > Printer > CUPS > Printers > Dialog**

|           |                                 |
|-----------|---------------------------------|
| Parameter | SMB User                        |
| Registry  | print.cups.printer<NR>.smb_user |

**IGEL Setup > Devices > Printer > CUPS > Printers > Dialog**

|           |                                       |
|-----------|---------------------------------------|
| Parameter | SMB Password                          |
| Registry  | print.cups.printer<NR>.crypt_password |

## Base system

- Updated **kernel** from 4.18.20 **to 4.19.57** version.



- Enhanced **bootloader** to allow the set of some kernel commandline parameters with registry keys:  
[More...](#)

|                                         |                                               |
|-----------------------------------------|-----------------------------------------------|
| Parameter                               | Disable use of APIC controller                |
| Registry                                | system.kernel.bootparams.noapic               |
| Value                                   | enabled /disabled                             |
| Parameter                               | Disable use of ACPI                           |
| Registry                                | system.kernel.bootparams.noacpi               |
| Value                                   | enabled /disabled                             |
| Parameter                               | Use only one CPU core and disable all others  |
| Registry                                | system.kernel.bootparams.nosmp                |
| Value                                   | enabled /disabled                             |
| Parameter                               | Enable debug console on serial port 1         |
| Registry                                | system.kernel.bootparams.serial_console_debug |
| Value                                   | enabled /disabled                             |
| Parameter                               | Limit CPU core usage (0 means no limit)       |
| Registry                                | system.kernel.bootparams.maxcpus              |
| Type                                    | Integer                                       |
| Value                                   | 0                                             |
| Parameter                               | Set maximum allowed cstate on intel cpus      |
| Registry                                | system.kernel.bootparams.max_cstate           |
| Range                                   | [No limit] [1] [2] [3] [4] [5] [6]            |
| <b>Info:</b> Do not limit Intel cstate. |                                               |

|                                     |                                       |
|-------------------------------------|---------------------------------------|
| Parameter                           | IOMMU usage setting                   |
| Registry                            | system.kernel.bootparams.iommu        |
| Range                               | [On] [Off] [Passthrough] [Force]      |
| <b>Info:</b> Use IOMMU if possible. |                                       |
| Parameter                           | IOMMU usage setting for AMD systems   |
| Registry                            | system.kernel.bootparams.amd_iommu    |
| Range                               | [On] [Off]                            |
| <b>Info:</b> Use IOMMU if possible. |                                       |
| Parameter                           | IOMMU usage setting for Intel systems |
| Registry                            | system.kernel.bootparams.intel_iommu  |
| Range                               | [On] [Off]                            |
| <b>Info:</b> Use IOMMU if possible. |                                       |

- Added a possibility to configure **scheduled commands**. Registry keys: system.cron.\*\*
- Buddy update** enhancements:
  - Automatic load balancing:**  
A client collects up to eight server candidates from which one is selected randomly.



Collection stops when the number specified in the following registry key is reached.  
Otherwise collection stops after a timeout.

[More...](#)

|           |                                    |
|-----------|------------------------------------|
| Parameter | Buddy Update Server Candidates     |
| Registry  | update.ftp.buddy_server_candidates |
| Value     | 1                                  |

- **Grouping:**

Buddy update servers and clients only interact with each other when they are in the same group determined by the following registry key (a non-negative integer number). This feature is mainly useful when different firmware versions shall be used in parallel.

[More...](#)

|           |                           |
|-----------|---------------------------|
| Parameter | Buddy Group ID            |
| Registry  | update.ftp.buddy_group_id |
| Value     | 0                         |

- Updated **libwebkit2gtk-4.0-37** to version **1.24.2**.

Security fixes:

[More...](#)

CVE-2019-8595, CVE-2019-8607, CVE-2019-8615, CVE-2019-6251,  
CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378,  
CVE-2018-4382, CVE-2018-4392, CVE-2018-4416, CVE-2018-4345,  
CVE-2018-4386, CVE-2018-4372

- Updated **Fluendo multimedia codecs** to the following versions:

[More...](#)

|                        |            |          |
|------------------------|------------|----------|
| gst-fluendo-aacdec     | 21/03/2019 | 0.10.39  |
| gst-fluendo-asfdemux   | 21/03/2019 | 0.10.89  |
| gst-fluendo-h264dec    | 21/03/2019 | 0.10.53  |
| gst-fluendo-mp3        | 21/03/2019 | 0.10.39  |
| gst-fluendo-mpeg4video | 21/03/2019 | 0.10.43  |
| gst-fluendo-vadec      | 21/03/2019 | 0.10.208 |
| gst-fluendo-wmadec     | 21/03/2019 | 0.10.68  |
| gst-fluendo-wmvdec     | 20/03/2019 | 0.10.65  |

- Added a package **ldap-utils** which can be used by custom scripts.

## Driver

- Updated **DisplayLink driver** to version **5.1.26**.
- Updated **Philips Speech Driver** to version **12.7.11** - added **support for Philips AirBridge**.
- Added registry keys to modify the Intel graphic driver usage of **framebuffer compression** and **power management**.

New registry keys:

[More...](#)



|           |                                             |
|-----------|---------------------------------------------|
| Parameter | Power saving display C-States to use        |
| Registry  | x.drivers.intel.dc_setting                  |
| Range     | [Default] [Disable] [Up to DC5] [Up to DC6] |
| Info:     | "Default" - driver default                  |
| Parameter | Use framebuffer compression                 |
| Registry  | x.drivers.intel.fbc_setting                 |
| Range     | [Default] [Disable]                         |
| Info:     | "Default" - driver default                  |

- Updated **signotec Citrix Virtual Channel** driver to version **8.0.8**.

- Updated **deviceTRUST Client** to version **19.1.200**. These are the release notes:

Welcome to the release of the deviceTRUST 19.1.200 IGEL client, providing the context of IGEL thin client and UD Pocket devices into your virtual sessions. This release includes support for logical disks attached to the IGEL endpoint, plus bug fixes and stability improvements over the previous 19.1.100 release.

## Logical Disks

We've added support for real-time properties representing the LOGICAL DISKS attached to the IGEL endpoint. This includes:

[More...](#)

DEVICE\_LOGICALDISK\_X\_TYPE – Either Fixed or Removable.

DEVICE\_LOGICALDISK\_X\_LABEL – The volume label.

DEVICE\_LOGICALDISK\_X\_FILESYSTEM – The type of file system.

DEVICE\_LOGICALDISK\_X\_PATHS – The paths that the disk is mounted.

DEVICE\_LOGICALDISK\_X\_TOTALMB – The total space available on the disk. This property is only available for mounted disks.

DEVICE\_LOGICALDISK\_X\_FREEMB – The free space available on the disk. This property is only available for mounted disks.

DEVICE\_LOGICALDISK\_X\_NAME – The name of the underlying physical disk.

DEVICE\_LOGICALDISK\_X\_VENDORID – The vendor identifier uniquely identifying the manufacturer. This property is only available for USB or PCI connected devices.

DEVICE\_LOGICALDISK\_X\_PRODUCTID – The product identifier uniquely identifying the product. This property is only available for USB or PCI connected devices.

DEVICE\_LOGICALDISK\_X\_SERIALNUMBER – The serial number of the physical disk.

DEVICE\_LOGICALDISK\_X\_BUSTYPE – The storage bus type linked to the physical disk.

DEVICE\_LOGICALDISK\_COUNT – The number of logical disks.

## X11 system

- Updated Xorg server from 1.19.6 to **1.20.5** version.
- Updated **Virtualbox** from 5.2.18 to **6.0.8** version.
- Updated **Mesa** from 18.2.1 to **19.0.8** version.
- Updated **Xorg video and input driver** to current upstream versions.
- Added new options for **laptop lid handling** dependent on power supply:

**More...**

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Lid close action while plugged in     |
| Registry  | system.actions.lid.ac                 |
| Range     | [Turn off display] [Suspend]          |
| Parameter | Lid close action while not plugged in |
| Registry  | system.actions.lid.battery            |
| Range     | [Turn off display] [Suspend]          |

- The new **Display Switch tool** can use multiple different profiles, automatically chosen at runtime depending on the currently connected monitors.

A profile is created, when the current monitor layout/resolution is configured via the Display Switch utility. The profile will be associated with the current connected displays automatically (manufacturer, model and used connector are used for allocation) and if applicable, the state of the laptop lid. The setup will be restored by hot-(un)plugging known displays, means the system will automatically switch to the already configured profile.

The Display Switch utility itself got a new interface. All base functionality can be configured via Drag&Drop.

An example workflow:

- Connect the hardware and close/open the lid.
  - Open the Display Switch Utility:
    - A quick (simple) setting can be selected directly.
    - Should the desired use case be different from the provided choices, the 'Advanced' button opens a drag&drop interface for further settings.
  - In this interface the displays can be dragged and dropped for the intended configuration. The display will snap adjacent to others.
  - If a display should not be used, it can be dragged to the 'Disabled' area on the top right - the screen will be reactivated when it is dragged back to the active area.
  - To show the same content on multiple displays, one display should be dragged onto another active screen. The interface will show "Mirror". The mirroring monitor will be displayed on the lower right.
- With the 'Apply' button the current state will be set, with 'Yes' on the "Keep configuration" dialog the current settings will be saved to persistent storage and associated with the profile.
- Advanced functionality (panning/scaling/resolutions) can be configured in drop-down boxes, hidden in a drawer on the right side. The drawer can be expanded by clicking the '<' button on the right edge.
  - For the Display Switch functionality the following parameters should be enabled for proper usage:

**More...**

**IGEL Setup > Accessories > Display Switch > Options**

|           |                               |
|-----------|-------------------------------|
| Parameter | Preserve settings over reboot |
|-----------|-------------------------------|



|          |                                                  |
|----------|--------------------------------------------------|
| Registry | sessions.user_display0.options.preserve_settings |
| Value    | enabled / <u>disabled</u>                        |

#### IGEL Setup > Accessories > Display Switch > Options

|           |                             |
|-----------|-----------------------------|
| Parameter | Smart display configuration |
| Registry  | x.auto_associate            |
| Value     | enabled / <u>disabled</u>   |

- Added a new parameter to optionally start with opened '**'Advanced'** drawer in Display Switch.  
[More...](#)

#### IGEL Setup > Accessories > Display Switch > Options

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | Preserve settings over reboot                    |
| Registry  | sessions.user_display0.options.preserve_settings |
| Value     | enabled / <u>disabled</u>                        |

#### IGEL Setup > Accessories > Display Switch > Options

|           |                                           |
|-----------|-------------------------------------------|
| Parameter | Start with the advanced drawer opened     |
| Registry  | sessions.user_display0.options.start_open |
| Value     | enabled / <u>disabled</u>                 |

- Added **xprintidle tool** to firmware.
- Added some registry keys to disable loading of **DRM kernel modules** (graphic).  
[More...](#)

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Disable the loading of the RADEON DRM driver |
| Registry  | x.drivers.ati.disable                        |
| Value     | 0                                            |

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Disable the loading of the AMDGPU DRM driver |
| Registry  | x.drivers.amdgpu.disable                     |
| Value     | 0                                            |

|           |                                            |
|-----------|--------------------------------------------|
| Parameter | Disable the loading of the i915 DRM driver |
| Registry  | x.drivers.intel.disable                    |
| Value     | 0                                          |

- Added the possibility to **change an embedded DisplayPort to a normal DisplayPort**.  
[More...](#)

|                       |                                                |
|-----------------------|------------------------------------------------|
| Parameter             | Use embedded displayport as normal displayport |
| Registry              | x.drivers.intel.edp_is_dp                      |
| Range                 | [default][enable][disable]                     |
| Info: Reboot required |                                                |

Java



- Replaced Oracle JRE by **AZUL's Zulu JRE**.
- **Removed** deprecated **Java WebStart** since it is not supported with non-Oracle JRE's.

#### X server

- Updated **Xephyr x session** to version **1.20.5**.

#### Hardware

- Added hardware support for the following headsets:  
[More...](#)

Jabra Engage 50;  
Jabra Engage 65;  
Jabra Engage 75;  
Jabra Evolve 30 II (Ver. B);  
Jabra Evolve 30 II (Ver. C);  
Jabra Evolve 40 (Ver. B) - USB-C;  
Jabra Evolve 40 (Ver. D);  
Jabra Evolve 65;  
Jabra Evolve 75;  
Plantronics Voyager 5200 UC;  
Plantronics Voyager 6200 UC;  
Plantronics Voyager 8200 UC;  
Sennheiser SC70.

#### Remote Management / IGEL Cloud Gateway

- **Connection order between UMS and ICG** can now be configured.  
[More...](#)

|           |                                                       |
|-----------|-------------------------------------------------------|
| Parameter | Prefer UMS over ICG                                   |
| Registry  | <code>system.remotemanager.icg_try_ums_connect</code> |
| Value     | <u>enabled</u> / <u>disabled</u>                      |

When an ICG connection is configured and the parameter is enabled, the device tries to connect directly to UMS. If the connection was established successfully, the device is managed by UMS and not over ICG until new start of the device or networking.

- **Firmware update scheduled on shutdown** is now invoked **on reboot** as well.
- Added some adaptations in **UMS Agent** concerning **migration to IGEL OS11**.

#### Resolved Issues 10.06.100

##### Citrix

- Now `ica.pnlogin.syncpasswordwithxscrnsrv` is removed, **ica.pnlogin.syncpasswordwithxlock** should be used, this provides the same functionality.
- Fixed **online meeting in VDI**: An enabled webcam will not cut the audio streaming anymore.
- Citrix **Workspace App 19.03**: Improved USB redirection handling.
- **Custom icons** now are visible **after StoreFront logon** using Citrix authentication method.
- **Appropriate icons** arise with IGEL and Citrix authentication.
- Fixed **stability issues** with Citrix Browser Content Redirection.



- Updated the **Nuance virtual channel** for ICA up to version **B301**.

#### RDP/IGEL RDP Client 2

- Added **Negotiate:Kerberos as fallback** if NTLM is disabled. This only works if Active Directory/Kerberos Logon is enabled.
- Added registry key to use **rdpglobal window settings for remote apps**.  
[More...](#)

|           |                                                             |
|-----------|-------------------------------------------------------------|
| Parameter | Enable global windows settings for remote app               |
| Registry  | rdp.winconnect.enable-global-window-settings-for-remote-app |
| Value     | enabled / disabled                                          |

- Fixed **empty warning window** being shown when closing RDP Web Applications started from browser.
- Fixed **smartcard redirection in RDP**: SCardGetAttrib was failing if pbAttr was NULL. The fix should help running Dutch Zorg-ID applications.

#### RD Web Access

- Fixed **RD Web Access** not working with **special characters in name or password**. This only works if Active Directory/Kerberos Logon is enabled.
- Fixed **empty warning dialogs** appearing when opening RD Web Application in the browser.
- Fixed **not starting RDP Remote Applications**.

#### VMware Horizon

- Fixed **Optimization for Skype for Business**.
- Fixed the configuration choice to use **the relative mouse feature**.

#### Parallels Client

- Updated **Parallels Client** to version **16.5.3** (64-Bit).
- Fixed: **Maximized windows** for published applications can be displayed incorrectly.
- Fixed: **Incorrect user credentials** can be picked up during connection if the same farm is registered in the client multiple times and with different user credentials.
- Fixed: Client **did not accept universal printing policies** set from the server.
- Fixed: **Module** opened in the background and **blocked the launcher** in some cases.
- Fixed: **Redirected smartcard** did not work **in a remote session**.
- Fixed: **Printers would not redirect to a remote session** when redirection is enforced via policies.

#### PowerTerm

- Fixed **editing** of parameter **sessions.powerterm\<INST>.logindialog.loginscript** in Setup Registry: now multiple lines are possible.
- PowerTerm Terminal Emulation: remove **obsolete SSH type SSH1** and **obsolete SSH cipher DES** from parameter ranges.

#### Firefox

- Fixed an issue where **Firefox does not accept proxy credentials** from setup.
- Fixed the **print hotkey disable option** with Firefox 60+.
- Fixed **browserglobal.app.local\_subdirs\_whitelist** not working.



- Fixed **Adobe Flash Player download** possibility.

## Network

- Improved **SCEP client robustness**:
  - The **cert\_agent script** doesn't terminate anymore when a problem occurs (e.g. the SCEP server is unreachable) but tries again after the expiry check interval.
  - When the client certificate has expired, there is still one attempt at renewing it. However, when that fails, a new one is requested. That obviously will fail if the client presents a challenge password that is not valid anymore.
- Restoring **WLAN/WWAN Modem state** after wakeup from standby or reboot.
- Improved **expire time of Ethernet no-link notification**.
- Added all **Ethernet network drivers from OS to LX** version.
- Changed **e1000e driver** to out of tree version **3.4.2.3** directly from Intel.
- Changed **igb driver** to out of tree version **5.3.5.22** directly from Intel.
- Fixed bug: **Failure to reach SCEP server** in the client certificate renewal phase resulted in loss of SCEP server and client certificates.
- SCEP: **A change of the CA fingerprint setting does not result in discarding all SCEP data anymore** if the fingerprint matches that of the current CA certificate. Firmware versions before 10.05.100 allowed an empty fingerprint. So, this is meant for users who must belatedly configure the fingerprint in order for client certificate renewal to work.  
A change of the **CAIdentifier** setting is not detected immediately and does not result in discarding all current data anymore. The new CAIdentifier will, however, be used in future SCEP operations.
- Fixed **instability with netmounts** with static ip configuration.
- Fixed problems with **windows share mounts**.
- Fixed **MBB router** configuration (broken since 10.05.500).
- Added a possibility to **switch between third-party** and **kernel Intel IGB network driver**.  
A new registry key:  
**More...**

|                                             |                                       |
|---------------------------------------------|---------------------------------------|
| Parameter                                   | Use thirdparty igb kernel module      |
| Registry                                    | network.drivers.igb.prefer_thirdparty |
| Range                                       | [Auto] [Yes] [No]                     |
| Info: "Auto" (use thirdparty in most cases) |                                       |

- Added a possibility to **switch between thirdparty** and **kernel Intel E1000E network driver**.  
A new registry key:

**More...**

|                                             |                                          |
|---------------------------------------------|------------------------------------------|
| Parameter                                   | Use thirdparty e1000e kernel module      |
| Registry                                    | network.drivers.e1000e.prefer_thirdparty |
| Range                                       | [Auto] [Yes] [No]                        |
| Info: "Auto" (use thirdparty in most cases) |                                          |

- Added a possibility to **switch between thirdparty r8168** and **kernel r8169 realtek network driver**.

A new registry key:

**More...**

|           |                                    |
|-----------|------------------------------------|
| Parameter | Use thirdparty r8168 kernel module |
|-----------|------------------------------------|



|                                        |                                    |
|----------------------------------------|------------------------------------|
| Registry                               | network.drivers.r8169.prefer_r8168 |
| Range                                  | [Auto] [Yes] [No]                  |
| Info: "Auto" (use r8168 in most cases) |                                    |

- Added a possibility to choose the **variant of the realtek r8168 driver**.

A new registry key:

[More...](#)

|                                          |                                                                 |
|------------------------------------------|-----------------------------------------------------------------|
| Parameter                                | Choose realtek r8168 variant (only if "prefer r8168" is chosen) |
| Registry                                 | network.drivers.r8169.r8168_variant                             |
| Range                                    | [Default] [No NAPI] [NAPI]                                      |
| Info: "Default" (use NAPI in most cases) |                                                                 |

- Fixed bug: **Second Ethernet interface** did not get configured when the first one was disabled.
- Fixed **802.1X Ethernet configuration with user interaction**.

## WiFi

- Fixed bug: **WiFi connection to hidden SSID** did not work anymore after reediting with the Wireless Manager.
- Fixed not working **Broadcom SDIO WLAN cards** as present in Advantech AIM8IAC device for example.

## Smartcard

- Fixed **Dell KB813 Smartcard Keyboard** in combination with certain smart cards driven by OpenSC PKCS#11 module. Before this fix, authentication to Citrix StoreFront and VMWare Horizon failed.
- Improved **handling of PIV/CAC smart cards** in OpenSC.
- Updated **cryptovision sc/interface PKCS#11 smart card library** to version **7.1.20**.

Changes in this revision:

- Fixed **a possible deadlock in the PKCS#11 module** on Linux if C\_Finalize is called during a PCSC event, for example C\_WaitForSlotEvent.
- **ROCA check in the Smartcard Manager**, based on the "ROCA detection tool", see <https://github.com/crocs-muni/roca>.
- **Renaming container label** in Smartcard Manager with F2 now possible.
- Fixed **OpenSC setting max\_send\_size** for reader driver pcsc in **/etc.opensc.opensc.conf**.

## Application Launcher

- Fixed **confusion in nameserver list** caused by comments in /etc/resolv.conf.

## Base system

- Fixed issues with **gen4/5 Intel graphic driver** in kernel 4.18.20.
- Fixed **Screensaver and Screenlock timeouts** to be independent. This means, if both timeouts are set, the start of Screenlock will not reset the Screensaver timeout any more.
- Fixed **retrieving of serial number of a display**.
- Fixed **playback of AAC coded audio streams** on IGEL Zero products.
- Added possibility to set **intel\_idle.max\_cstate kernel cmdline parameter** with registry keys **to work against Intel CPU freezes**.
- Ensure that the **Unit ID** for IGEL devices is the MAC address of the onboard network card.



- **Enhanced handling of Unit ID.** On IGEL hardware the Unit ID isn't stored persistently any more by default. The persistent Unit ID can be removed with command `get_unit_id -r`. The persistent Unit ID storage can be forced with `get_unit_id -i -f -p` or with `get_unit_id -m` to manually choose a Unit ID from several network interfaces found on the device. Handle with extreme care since the Unit ID is the key for handling the endpoint in UMS.
- Replaced MIT Kerberos clients by **Heimdal Kerberos clients**.
- Improved the buddy update server performance for multiple simultaneous update clients.
- Fixed handling of an "**update on shutdown**" during suspend/resume.
- Fixed **shutdown** while IGEL Setup Assistant is shown.
- Fixed **delay in logon** as local user when logon with IGEL Smartcard is also active.
- Fixed **sporadic bootsplash issue**.
- Fixed **suspend/resume hangs** when logged into Citrix sessions.
- Fixed **CPU scaler and volume control applet suspend/resume issue**.
- Added **AppArmor** rule to allow tcpdump to write to `/debuglog`.
- Fixed random 90 seconds **shutdown delay** (systemd).
- Fixed **Custom Bootsplash installation**.
- Bugfix: **Create shortcuts** for terminal shutdown, terminal restart and icon sort **directly after reconfiguration**. A reboot is not needed anymore.
- Fixed: **System logoff waits for Citrix logoff** now.
- Fixed **broken custom bootsplash** when doing a reset to factory defaults via UMS.
- Bugfix: **hotkey** setting **needs restart**.
- **IGEL Setup Assistant** will persistently **activate WiFi** when a connection is enabled instead of after finishing it, to preserve settings when UMS sends license and stops it.
- Fixed **AD/Kerberos logon** in case parameter `auth.login.krb5_enterprise` is **set to 'false'**.
- Added a new registry key to set **USB quirks**:

[More...](#)

|           |                                                                                           |
|-----------|-------------------------------------------------------------------------------------------|
| Parameter | Set XHCI USB quirks to fix some hardware issues                                           |
| Registry  | <code>system.kernel.bootparams.xhci-hcd_quirks</code>                                     |
| Range     | [No quirk] [Spurious Reboot quirk] [Spurious Wakeup quirk] [Spurious Reboot Wakeup quirk] |

- Fixed: **Migration tool** did not start with **Spanish** language setting.
- Disabled **martian packet logging**.

## Driver

- Updated **deviceTRUST** Client to version **19.1.200**.

### Bug Fixes:

- Fixed an issue **reading the DEVICE\_IGEL\_ICG\_SERVER** property.
- Fixed an issue where the **NETWORK** and **LOCATION** property providers could **cause the client to freeze** if a disconnection occurred while these property providers were checking for changes.
- Fixed an **open file handle leak** which lead to the client process reaching its file handle limits when left running for a long period of time.



- Fixed not working **WACOM** device **DTU-1141B**.

#### Custom Partition

- Fixed **ownership of extracted data**: Do not preserve owner information while extracting data into custom partition.

#### Storage Devices

- Fixed **auto mounting of storage devices** inside of Olympus DS-9500 Digital Voice Recorder.

#### Appliance Mode

- Fixed bug: **In-session control bar** could not be deactivated **in Citrix SelfService appliance mode**.

#### X11 system

- Fixed **Microsoft Surface Pro 4 screen resolution** issue.
- Fixed the **missing volume control** in the panel when the panel is configured to disappear while the login/lock screen is shown.
- There is now a **registry key to ignore a 3Dconnexion SpaceMouse** for IGEL graphical use (X11). If activated, the SpaceMouse is only passed through to the desktop session. If false, it acts also as the standard mouse.

**More...**

|           |                                                          |
|-----------|----------------------------------------------------------|
| Parameter | Deactivates a 3Dconnexion SpaceMouse as a standard mouse |
| Registry  | userinterface.mouse.spacemouse.x11_ignore                |
| Value     | <u>enabled</u> / disabled                                |

- The following **SpaceMouse** products are included:

**More...**

| VID    | PID    | Vendor         | Product                                  |
|--------|--------|----------------|------------------------------------------|
| 0x046D | 0xC603 | Logitech, Inc. | 3Dconnexion SpaceMouse Plus XT           |
| 0x046D | 0xC605 | Logitech, Inc. | 3Dconnexion CADman                       |
| 0x046D | 0xC606 | Logitech, Inc. | 3Dconnexion SpaceMouse Classic           |
| 0x046D | 0xC621 | Logitech, Inc. | 3Dconnexion SpaceBall 5000               |
| 0x046D | 0xC623 | Logitech, Inc. | 3Dconnexion SpaceTraveller 3D Mouse      |
| 0x046D | 0xC625 | Logitech, Inc. | 3Dconnexion SpacePilot 3D Mouse          |
| 0x046D | 0xC626 | Logitech, Inc. | 3Dconnexion SpaceNavigator 3D Mouse      |
| 0x046D | 0xC627 | Logitech, Inc. | 3Dconnexion SpaceExplorer 3D Mouse       |
| 0x046D | 0xC628 | Logitech, Inc. | 3Dconnexion SpaceNavigator for Notebooks |
| 0x046D | 0xC629 | Logitech, Inc. | 3Dconnexion SpacePilot Pro 3D Mouse      |
| 0x046D | 0xC62B | Logitech, Inc. | 3Dconnexion SpaceMouse Pro               |
| 0x256F | **     | 3Dconnexion    | SpaceMouse                               |

- **USB device reset** via USB powercycle is now available on **UD6/UD7**.
- Fixed **screen flicker** in some cases if **Force NumLock On** (x.global.forcenumlock) is active.



- Fixed not working **x.xserver0.screen1.flipscreens** registry key.
- Use **Index** and **Mode** from Advanced mode in Simple Mode **for Display Switch**.
- Fixed **display hotplug failing** on initial lock screen with Active Directory logon.
- The **in-session control bar** now **scales with the current DPI setting**.
- Fixed **Display Switch** utility **not starting with some translations**.
- Fixed an issue with the **noDDC mode** not always working as expected.
- Fixed a bug with thin clients **reporting the wrong monitor serial number**.

#### Window manager

- Fixed the option to **disable the local window manager**.

#### Audio

- Fixed **bad quality sound over DisplayPort** in a Citrix ICA session or other applications using ALSA API.
- Fixed **configuration of default audio output** and **input**.

#### Media Player (Parole)

- Fixed a problem where **parole media player** would **hang** instead of playing audio **while audio-visualization** is enabled.
- Fixed parole media player **not handling audio hotkeys in fullscreen mode**.

#### Multimedia

- Updated **multimedia codecs to fix freeze** when audio visualization is used.

#### Misc

- **Monitoring Agent** uses now **only the half size of the debuglog partition**.

When the setup option **log\_max\_size** with the option **log\_rotation** creates an overall consumption that is bigger than 50% of the debuglog partition size, the size for each log automatically will be decreased to a value that allows a full rotation which occupies exactly 50% of the partition size.

#### Hardware

- Fixed problems with **mouse cursor on Intel cherryview devices**.
- Added a **possibility to change** some **DRM settings** and **limit the DisplayPort lane bandwidth** on Intel devices.

Added new registry keys:

**More...**

|           |                                                           |
|-----------|-----------------------------------------------------------|
| Parameter | Use best graphic mode for all screens on console.         |
| Registry  | x.drivers.kms.best_console_mode                           |
| Range     | [Default] [Enabled] [Disabled]                            |
| Info:     | "Default" is enabled in most cases.                       |
| Parameter | Limit the maximum console resolution width to this value. |



|                                                           |                                                                                                   |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Registry                                                  | x.drivers.kms.max_console_width                                                                   |
| Type                                                      | Integer                                                                                           |
| Value                                                     | "0"                                                                                               |
| Info: "0" means default setting. Use the default setting. |                                                                                                   |
| Parameter                                                 | Limit the maximum console resolution height to this value.                                        |
| Registry                                                  | x.drivers.kms.max_console_height                                                                  |
| Type                                                      | Integer                                                                                           |
| Value                                                     | "0"                                                                                               |
| Info: "0" means default setting. Use the default setting. |                                                                                                   |
| Parameter                                                 | Set graphic kernel driver debug level.                                                            |
| Registry                                                  | x.drivers.kms.debug_level                                                                         |
| Range                                                     | [No debug] [Basic] [Basic + core] [Basic + core + atomic] [Full]                                  |
| Info: Warning log will grow very fast.                    |                                                                                                   |
| Only for Intel i915 driver:                               |                                                                                                   |
| Parameter                                                 | Limit the maximum DisplayPort lane link rate.                                                     |
| Registry                                                  | x.drivers.intel.max_dp_link_rate                                                                  |
| Range                                                     | [default] [1.62Gbps] [2.16Gbps] [2.7Gbps] [3.24Gbps]<br>[4.32Gbps] [5.4Gbps] [6.48Gbps] [8.1Gbps] |
| Info: "Default" means hardware default limit.             |                                                                                                   |

#### Remote Management / IGEL Cloud Gateway

- Fixed **wallpaper configuration** when ICG protocol is used.
- Fixed **UMS synchronization of configuration** when changes were made in "Emergency mode".
- Fixed sporadic **failures while sending data over ICG**.
- Fixed **removal from UMS** when the device was offline.
- Added: IGEL UMS agent sends **monitor information for maximum eight monitors** now.

#### Caradigm

- Fixed **Horizon session crash**.

#### IGEL Linux 10 Recovery

- Fixed **problem with forced no EFI installation**.



## 7.24.2 IGEL Universal Desktop OS 3

Supported Hardware:

<https://kb.igel.com/igelos/en/devices-supported-by-udc3-and-ud-pocket-3117174.html>

- Component Versions 10.06.100(see page 1996)
- General Information 10.06.100(see page 2000)
- Security Fixes 10.06.100(see page 2001)
- Known Issues 10.06.100(see page 2005)
- New Features 10.06.100(see page 2007)
- Resolved Issues 10.06.100(see page 2029)

### Component Versions 10.06.100

- **Clients**

| Product                           | Version                        |
|-----------------------------------|--------------------------------|
| Citrix HDX Realtime Media Engine  | 2.8.0-2235                     |
| Citrix Receiver                   | 13.10.0.20                     |
| Citrix Receiver                   | 13.5.0.10185126                |
| Citrix Workspace App              | 19.3.0.5                       |
| deviceTRUST Citrix Channel        | 19.1.200.2                     |
| Ericom PowerTerm                  | 2.0.1.0.20170219.2-_dev_-34574 |
| Evidian AuthMgr                   | 1.5.6840                       |
| Evince PDF Viewer                 | 3.18.2-1ubuntu4.5              |
| FabulaTech USB for Remote Desktop | 5.2.29                         |
| Firefox                           | 60.7.2                         |
| IBM iAccess Client Solutions      | 1.1.8.1                        |
| IGEL RDP Client                   | 2.2                            |



|                                       |                                           |
|---------------------------------------|-------------------------------------------|
| Imprivata OneSign ProveID Embedded    | onesign-bootstrap-loader_1.0.523630_amd64 |
| deviceTRUST RDP Channel               | 19.1.200.2                                |
| Leostream Java Connect                | 3.3.7.0                                   |
| NCP Secure Enterprise Client          | 5.10_rev40552                             |
| NX Client                             | 6.5.6                                     |
| Open VPN                              | 2.3.10-1ubuntu2.2                         |
| Zulu JRE                              | 8.38.0.13                                 |
| Parallels Client (64 bit)             | 16.5.3.20735                              |
| Remote Viewer (RedHat Virtualization) | 8.0-1igel49                               |
| Spice GTK (Red Hat Virtualization)    | 0.36-1~git20190601igel61                  |
| Usbredir (Red Hat Virtualization)     | 0.8.0-1igel49                             |
| Systancia AppliDis                    | 4.0.0.17                                  |
| ThinLinc Client                       | 4.10.0-6068                               |
| ThinPrint Client                      | 7.5.88                                    |
| Totem Media Player                    | 2.30.2                                    |
| Parole Media Player                   | 1.0.1-0ubuntu1igel18                      |
| VMware Horizon Client                 | 5.0.0-12557422                            |
| VNC Viewer                            | 1.9.0+dfsg-3igel8                         |
| Voip Client Ekiga                     | 4.0.1                                     |

- **Dictation**

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B301     |
| Olympus driver for dictation              | 20180621 |



|                       |         |
|-----------------------|---------|
| Philips Speech Driver | 12.7.11 |
|-----------------------|---------|

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.8    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.1.0    |

- **Smartcard**

|                                           |                        |
|-------------------------------------------|------------------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101                |
| PKCS#11 Library Athena IDProtect          | 623.07                 |
| PKCS#11 Library cryptovision sc/interface | 7.1.20                 |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0              |
| PKCS#11 Library SecMaker NetID            | 6.7.2.36               |
| Reader Driver ACS CCID                    | 1.1.6-1igel1           |
| Reader Driver Gemalto eToken              | 10.0.37-0              |
| Reader Driver HID Global Omnikey          | 4.3.3                  |
| Reader Driver Identive CCID               | 5.0.35                 |
| Reader Driver Identive eHealth200         | 1.0.5                  |
| Reader Driver Identive SCRKBC             | 5.0.24                 |
| Reader Driver MUSCLE CCID                 | 1.4.30-1igel3          |
| Reader Driver REINER SCT cyberJack        | 3.99.5final.sp13igel15 |
| Resource Manager PC/SC Lite               | 1.8.23-1igel1          |
| Cherry USB2LAN Proxy                      | 3.2.0.3                |

- **System Components**

|         |                    |
|---------|--------------------|
| OpenSSL | 1.0.2g-1ubuntu4.15 |
|---------|--------------------|



|                                         |                              |
|-----------------------------------------|------------------------------|
| OpenSSH Client                          | 7.2p2-4ubuntu2.8             |
| OpenSSH Server                          | 7.2p2-4ubuntu2.8             |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5           |
| MESA OpenGL stack                       | 19.0.8-1igel73               |
| VAAPI ABI Version                       | 0.40                         |
| VDPAU Library version                   | 1.1.1-3ubuntu1               |
| Graphics Driver INTEL                   | 2.99.917+git20190301-igel870 |
| Graphics Driver ATI/RADEON              | 19.0.1-2igel890              |
| Graphics Driver ATI/AMDGPU              | 19.0.1-4igel894              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.16-1igel867              |
| Graphics Driver Nvidia                  | 390.116-0ubuntu0.18.10.1     |
| Graphics Driver Vboxvideo               | 1.0.0-igel798                |
| Graphics Driver VMware                  | 13.3.0-2igel857              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1igel775         |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |
| Graphics Driver VESA                    | 2.4.0-1igel855               |
| Input Driver Evdev                      | 2.10.6-1igel888              |
| Input Driver Elographics                | 1.4.1-1build5igel633         |
| Input Driver eGalax                     | 2.5.5814                     |
| Input Driver Synaptics                  | 1.9.1-1ubuntu1igel866        |
| Input Driver VMmouse                    | 13.1.0-1ubuntu2igel635       |
| Input Driver Wacom                      | 0.36.1-0ubuntu2igel888       |
| Kernel                                  | 4.19.57 #mainline-udos-r2762 |
| Xorg X11 Server                         | 1.20.5-1igel891              |
| Xorg Xephyr                             | 1.20.5-1igel891              |



|                                 |                               |
|---------------------------------|-------------------------------|
| CUPS printing daemon            | 2.1.3-4ubuntu0.9igel27        |
| PrinterLogic                    | 18.2.1.128                    |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1             |
| XFCE4 Window Manager            | 4.12.3-1ubuntu2igel656        |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7       |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.3igel74  |
| ModemManager                    | 1.10.0-1~ubuntu18.04.2igel3   |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.2            |
| GStreamer 1.x                   | 1.16.0-1igel214               |
| WebKit2Gtk                      | 2.24.2-0ubuntu0.19.04.1igel18 |
| Python2                         | 2.7.12                        |
| Python3                         | 3.5.2                         |

- **Features with Limited IGEL Support**

|                                    |                                  |
|------------------------------------|----------------------------------|
| Mobile Device Access USB (MTP)     | 1.1.16-2igel1                    |
| Mobile Device Access USB (imobile) | 1.2.1~git20181030.92c5462-1igel5 |
| Mobile Device Access USB (gphoto)  | 2.5.22-3igel1                    |
| VPN OpenConnect                    | 7.08-1                           |
| Scanner support / SANE             | 1.0.27-1                         |
| VirtualBox                         | 6.0.8-dfsg-4igel25               |

- **Features with Limited Functionality**

|                   |        |
|-------------------|--------|
| Cisco JVDI Client | 12.1.0 |
|-------------------|--------|

## General Information 10.06.100

The following clients and features are not supported anymore:

- Citrix Receiver 12.1 and 13.1 - 13.4;
- Citrix Access Gateway Standard Plug-in;
- Dell vWorkspace Connector for Linux;
- Ericom PowerTerm Emulation 9 and 11;
- Ericom Webconnect;
- IGEL Legacy RDP Client (rdesktop);



- Virtual Bridges VERDE Client;
- PPTP VPN Support;
- IGEL Upgrade License Tool with IGEL Smartcard Token;
- Remote Management by setup.ini file transfer (TFTP);
- Remote Access via RSH;
- Legacy Philips Speech Driver;
- T-Systems TCOS Smartcard Support;
- DUS Series touch screens;
- Elo serial touchscreens;
- VIA graphics support;
- Java WebStart;
- Storage hotplug devices are not automatically removed anymore, instead they must be always ejected manually:
  - by panel tray icon;
  - by an icon in the **In-Session Control Bar** (configurable under **IGEL Setup > User Interface > Desktop**);
  - by a **Safely Remove Hardware** session (configurable under **IGEL Setup > Accessories**).

The following clients and features are not available in this release:

- Cherry eGK Channel;
- Open VPN Smartcard Support;
- Asian Input Methods;
- Composite Manager.

## Security Fixes 10.06.100

### Firefox

- Updated Mozilla **Firefox** to version **60.7.2 ESR**.
- Fixed **mfsa2019-19** security issue CVE-2019-11708.
- Fixed **mfsa2019-18** security issue CVE-2019-11707.
- Fixed **mfsa2019-10** security issues CVE-2019-9810 and CVE-2019-9813.
- Fixed **mfsa2019-08** security issues.

**More...**

CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793,  
CVE-2019-9795, CVE-2019-9796, CVE-2018-18506, CVE-2019-9788.

- Fixed **mfsa2019-05** security issues CVE-2018-18356 and CVE-2019-5785.
- Fixed **mfsa2019-02** security issues CVE-2018-18500, CVE-2018-18505 and CVE-2018-18501.
- Fixed **mfsa2018-30** security issues.

**More...**

CVE-2018-17466, CVE-2018-18492, CVE-2018-18493,  
CVE-2018-18494, CVE-2018-18498, CVE-2018-12405.

- Allow Firefox to access YubiKey (FIDO/U2F) when AppArmor is active.

### Base system

- Fixed a vulnerability in **Java configuration script**.



- Fixed possibly malicious **owner change** with TC setup configuration.
- Fixed **policykit-1** security issues CVE-2018-19788 and CVE-2019-6133.
- Fixed **NSS** security issues CVE-2018-18508, CVE-2018-12404, CVE-2018-12384 and CVE-2018-0495.
- Fixed **PPP** security issue CVE-2018-11574.
- Fixed **imagemagick** security issues.

**More...**

CVE-2018-16750, CVE-2018-16749, CVE-2018-16645, CVE-2018-16644, CVE-2018-16643, CVE-2018-16642, CVE-2018-16640, CVE-2018-16323, CVE-2018-14437, CVE-2018-14436, CVE-2018-14435, CVE-2018-14434, CVE-2017-13144, CVE-2017-12430, CVE-2019-9956, CVE-2019-7398, CVE-2019-7397, CVE-2019-7396, CVE-2019-7175, CVE-2019-11598, CVE-2019-11597, CVE-2019-11472, CVE-2019-11470, CVE-2019-10650, CVE-2019-10131, CVE-2018-20467, CVE-2018-18025, CVE-2018-18024, CVE-2018-18016, CVE-2018-17966, CVE-2018-17965, CVE-2018-16413, CVE-2018-16412, CVE-2017-12806, and CVE-2017-12805.

- Fixed **systemd** security issues.

**More...**

CVE-2018-16866, CVE-2018-16865, CVE-2018-16864, CVE-2018-15688, CVE-2019-6454, CVE-2018-1049, CVE-2018-15686 and CVE-2019-3842.

- Fixed **CUPS** security issue CVE-2018-4700.
- Fixed **libarchive** security issues.

**More...**

CVE-2019-1000020, CVE-2019-1000019, CVE-2018-1000878, CVE-2018-1000877, and CVE-2017-14502.

- Fixed **Avahi** security issues CVE-2018-1000845 and CVE-2017-6519.
- Fixed **bind9** security issues CVE-2019-6465, CVE-2018-5745, and CVE-2018-5743.
- Fixed **libcaca** security issues.

**More...**

CVE-2018-20549, CVE-2018-20548, CVE-2018-20547, CVE-2018-20546, CVE-2018-20545, and CVE-2018-20544.

- Fixed **libgd2** security issues CVE-2019-6978 and CVE-2019-6977.
- Fixed **ghostscript** security issues.

**More...**

CVE-2019-6116, CVE-2018-19477, CVE-2018-19476, CVE-2018-19475, CVE-2018-19409, CVE-2018-18284, CVE-2018-18073, CVE-2018-17961, CVE-2019-3838, and CVE-2019-3835.

- Fixed **krb5** security issues.

**More...**

CVE-2018-5730, CVE-2018-5729, CVE-2017-11462, CVE-2017-11368, CVE-2016-3120, and CVE-2016-3119.

- Fixed **texlive-bin** security issue CVE-2018-17407.
- Fixed **LDB** security issue CVE-2019-3824.
- Fixed **libmspack** security issues CVE-2018-18585 and CVE-2018-18584.



- Fixed **Perl** security issues CVE-2018-18314, CVE-2018-18313, CVE-2018-18312 and CVE-2018-18311.
- Fixed **poppler** security issues.

[More...](#)

CVE-2019-7310, CVE-2018-20650, CVE-2018-20551, CVE-2018-20481, CVE-2018-19149, CVE-2018-19060, CVE-2018-19059, CVE-2018-19058, CVE-2018-16646, and CVE-2019-9200.

- Fixed **Python 3.5** security issues CVE-2018-14647, CVE-2018-1061, CVE-2018-1060 and CVE-2018-106.

- Fixed **Net-SNMP** security issue CVE-2018-18065.

- Fixed **OpenSSL** security issues CVE-2019-1559, CVE-2018-5407 and CVE-2018-0734.

- Fixed **TIFF** security issues.

[More...](#)

CVE-2018-8905, CVE-2018-7456, CVE-2018-18661, CVE-2018-18557, CVE-2018-17101, CVE-2018-17100, CVE-2018-1710, CVE-2018-10963, CVE-2019-7663, CVE-2019-6128, CVE-2018-19210, CVE-2018-17000, CVE-2018-12900, and CVE-2018-10779.

- Fixed **libvncserver** security issues.

[More...](#)

CVE-2018-6307, CVE-2018-20750, CVE-2018-20749, CVE-2018-20748, CVE-2018-20024, CVE-2018-20023, CVE-2018-20022, CVE-2018-20021, CVE-2018-20020, CVE-2018-20019, CVE-2018-15127, and CVE-2018-15126.

- Fixed **WavPack** security issue CVE-2018-19840.

- Fixed **Samba** security issues.

[More...](#)

CVE-2018-16851, CVE-2018-16841, CVE-2018-14629, CVE-2019-3880, and CVE-2018-16860.

- Fixed **libxkbcommon** security issues.

[More...](#)

CVE-2018-15864, CVE-2018-15863, CVE-2018-15862, CVE-2018-15861, CVE-2018-15859, CVE-2018-15858, CVE-2018-15857, CVE-2018-15856, CVE-2018-15855, CVE-2018-15854, and CVE-2018-15853.

- Fixed **OpenSSH** security issues.

[More...](#)

CVE-2019-6111, CVE-2019-6109, CVE-2018-20685, CVE-2018-15473, and CVE-2016-10708.

- Fixed **Python 2.7** security issues.

[More...](#)

CVE-2018-14647, CVE-2018-1061, CVE-2018-1060, CVE-2018-106, CVE-2018-1000802, and CVE-2018-1000030.

- Fixed **lxml** security issue CVE-2018-19787.

- Fixed **gdk-pixbuf** security issues.

[More...](#)



CVE-2017-6314, CVE-2017-6313, CVE-2017-6312, CVE-2017-6311, CVE-2017-2870, CVE-2017-2862, CVE-2017-1000422, CVE-2016-6352, and CVE-2017-12447.

- Fixed **file** security issues CVE-2019-8907 and CVE-2019-8905.
- Fixed **wget** security issue CVE-2019-5953.
- Fixed **nvidia-graphic-drivers-390** security issue CVE-2018-6260.
- Fixed **libxslt** security issue CVE-2019-11068.
- Fixed **Evince** security issue CVE-2019-11459.
- Fixed **webkit2gtk** security issues.

[More...](#)

CVE-2019-8595, CVE-2019-8607, CVE-2019-8615, CVE-2019-6251, CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378, CVE-2018-4382, CVE-2018-4392, CVE-2018-4416, CVE-2018-4345, CVE-2018-4386, and CVE-2018-4372.

- Fixed **gst-plugins-base0.10** security issue CVE-2019-9928.
- Fixed **WPA** security issues.

[More...](#)

CVE-2019-9495, CVE-2019-9497, CVE-2019-9498, CVE-2019-9499, and CVE-2019-11555.

- Fixed **Heimdal** security issues CVE-2019-12098 and CVE-2018-16860.
- Fixed **libimobiledevice** security issue CVE-2016-5104.
- Fixed **libpng1.6** security issues CVE-2019-7317 and CVE-2018-13785.
- Fixed **GIMP** security issues.

[More...](#)

CVE-2017-17786, CVE-2017-17789, CVE-2017-17784, CVE-2017-17787, CVE-2017-17785, and CVE-2017-17788

- Fixed **libtomcrypt** security issue CVE-2018-12437.
- Fixed **curl** security issues.

[More...](#)

CVE-2018-16840, CVE-2018-16839, CVE-2019-3823, CVE-2019-3822, CVE-2018-16890, CVE-2019-5346.

- Fixed **gnutls28** security issues CVE-2018-10846, CVE-2018-10845, CVE-2018-10844 and CVE-2018-1084.
- Fixed **qtbase-opensource-src** security issues CVE-2018-19873, CVE-2018-19870 and CVE-2018-15518.
- Fixed **db5.3** security issue CVE-2019-8457.
- Fixed **libssh2** security issues.

[More...](#)

CVE-2019-3863, CVE-2019-3862, CVE-2019-3861, CVE-2019-3860, CVE-2019-3859, CVE-2019-3858, CVE-2019-3857, CVE-2019-3856, and CVE-2019-3855.

- Fixed **network-manager** security issue CVE-2018-15688.
- Fixed **elfutils** security issues.

**More...**

CVE-2019-7665, CVE-2019-7150, CVE-2019-7149,  
CVE-2018-18521, CVE-2018-18520, CVE-2018-18310,  
CVE-2018-16403, CVE-2018-16402, and CVE-2018-16062.

- Fixed **libsndfile** security issues.

**More...**

CVE-2019-3832, CVE-2018-19758, CVE-2018-19662, CVE-2018-19661, CVE-2018-19432,  
CVE-2018-13139, CVE-2017-6892, CVE-2017-17457, CVE-2017-17456, CVE-2017-16942,  
CVE-2017-14634, CVE-2017-14246, and CVE-2017-14245.

- Fixed **dbus** security issue CVE-2019-12749.
- Fixed **Vim** security issues CVE-2019-12735 and CVE-2017-5953.  
Fixed **sqlite3** security issues.

**More...**

CVE-2019-9937, CVE-2019-9936, CVE-2019-8457, CVE-2018-20506,  
CVE-2018-20346, CVE-2017-2520, CVE-2017-2519, CVE-2017-2518,  
CVE-2017-13685, CVE-2017-10989, and CVE-2016-6153.

- Fixed **libseccomp** security issue CVE-2019-9893.
- Fixed **bzip2** security issues CVE-2019-12900 and CVE-2016-3189.
- Fixed **Expat** security issue CVE-2018-20843.
- Fixed **unzip** security issues CVE-2019-13232, CVE-2018-1000035, CVE-2016-9844 and  
CVE-2014-9913.
- **Mount partitions** with "**nodev**" flag option.
- The home directory of the remote users is now **/home/ruser**.
- Default **umask** is set to **0077** for all non-root users.
- Fixed a vulnerability in the **custom environment variable framework**.
- Fixed kernel **TCP** vulnerabilities CVE-2019-11477: **SACK Panic**, CVE-2019-11478: **SACK Slowness**  
and CVE-2019-11479: **Excess Resource Consumption Due to Low MSS Values**.
- Changed **minimally allowed MSS size** to "**1000**" to prevent possible denial-of-service attacks.

## Known Issues 10.06.100

### Citrix

- With activated DRI3 and AMD GPU, Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected by this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H264, MPEG1 and MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.  
As a workaround, insert the smartcard before starting StoreFront login.



- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" > "For the entire screen".
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264 acceleration plugin**, the following registry key must be enabled:  
[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Range     | <u>enabled</u> / <u>disabled</u>                                 |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

#### VMware Horizon

- **External drives** mounted already before connection **do not appear in the remote desktop**.  
Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off.  
In the IGEL Setup client, **drive mapping** can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping**.  
It is also recommended to disable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection entirely** or at least to **deny storage devices** by adding a filter to the USB class rules.  
Furthermore, Horizon Client relies on the OS to mount the storage device itself. Enable local **Storage Hotplug** under **Setup > Devices > Storage Devices > Storage Hotplug**.

#### Parallels Client

- **Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode** it is necessary to connect to the **Parallels RAS** one time with FIPS support disabled.

#### Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice**: spice-xpi Firefox plugin is no longer supported. The **Console Invocation** has to allow **Native client** (auto is also possible) and it should start in fullscreen to prevent opening windows.

#### Multimedia

- **Multimedia redirection with GStreamer** could **fail with the Nouveau GPU driver**.



## WiFi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.  
Workaround: Disable system suspend under **IGEL Setup > System > Power Options > Shutdown**.

## Base system

- Due to the removal of the Oracle JRE, **Java WebStart** is **not supported** anymore.

## New Features 10.06.100

## OS 11 Upgrade

- It is now possible to **upgrade to IGEL OS 11**. For more information, see the how-to [Upgrading IGEL Devices from IGEL OS 10 to IGEL OS 11](#)(see page 174).

The **parameters for the upgrade**:

[More...](#)

| <b>IGEL Setup &gt; System &gt; Update &gt; OS 11 Upgrade</b> |                                                                   |
|--------------------------------------------------------------|-------------------------------------------------------------------|
| Parameter                                                    | Upgrade to OS 11                                                  |
| Registry                                                     | <code>update.firmware_migrate_to_11</code>                        |
| Value                                                        | <u>enabled</u> / <u>disabled</u>                                  |
| Parameter                                                    | Upgrade to OS 11 even if a previous upgrade attempt failed        |
| Registry                                                     | <code>update.force_firmware_migrate_to_11</code>                  |
| Value                                                        | <u>enabled</u> / <u>disabled</u>                                  |
| Parameter                                                    | Upgrade to OS 11 even if PowerTerm is enabled                     |
| Registry                                                     | <code>update.migrate_to_11_with_powerterm</code>                  |
| Value                                                        | <u>enabled</u> / <u>disabled</u>                                  |
| Parameter                                                    | Require an Enterprise Management Pack license to upgrade to OS 11 |
| Registry                                                     | <code>update.migrate_to_11_enterprise_required</code>             |
| Range                                                        | [Smart] [Always] [Never]                                          |
| Parameter                                                    | Timeout waiting for OS 11 license to start automatic upgrade      |
| Registry                                                     | <code>update.migrate_to_11_license_timeout</code>                 |
| Range                                                        | [Disabled] [10 Minutes] [15 Minutes] [30 Minutes] [60 Minutes]    |



|          |                                            |
|----------|--------------------------------------------|
| Value    | <u>enabled</u> / disabled                  |
| Registry | sessions.os11_migration0.menu_path         |
| Registry | sessions.os11_migration0.desktop_path      |
| Registry | sessions.os11_migration0.applaunch_path    |
| Registry | sessions.os11_migration0.quick_start       |
| Value    | <u>enabled</u> / <u>disabled</u>           |
| Registry | sessions.os11_migration0.pwprotected       |
| Range    | [None] [Administrator] [User] [Setup user] |
| Registry | sessions.os11_migration0.desktop           |
| Value    | <u>enabled</u> / <u>disabled</u>           |
| Registry | sessions.os11_migration0.pulldown          |
| Value    | <u>enabled</u> / <u>disabled</u>           |

## Citrix

- Integrated **Citrix Workspace app 19.03**.
- Added a new registry key to support **1536-bit RSA keys for client authentication**. Factory default for this release is "true".

**More...**

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Enables RSA 1536 cipher suite         |
| Registry  | ica.allregions.enable_rsa_1536        |
| Range     | <u>factory default</u> / false / true |

- Added a new **registry key** to enable **different cipher suites**. Factory default for this release is "ALL".

**More...**

|           |                                          |
|-----------|------------------------------------------|
| Parameter | Enables different cipher suite           |
| Registry  | ica.allregions.sslciphers                |
| Range     | <u>factory default</u> / ALL / GOV / COM |

> TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 - GOV/ALL  
 > TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 - GOV/ALL  
 > TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA - COM/ALL

- Added a new **registry key** to support **keyboard layout synchronization**.

**More...**

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Keyboard layout synchronization               |
| Registry  | ica.modules.virtualdriver.keyboardsync.enable |
| Value     | <u>disabled</u> / enabled                     |

- Updated **Citrix HDX RTME** used for optimization of Skype for Business to version **2.8.0-2235**.
- Added support for **Citrix Workspace Launcher** functionality as described at <https://support.citrix.com/article/CTX237727>.
- Added a Citrix plugin for **hardware accelerated VDPAU based H.264 decoding** on AMD graphics chipsets:

**More...**



|           |                                                       |
|-----------|-------------------------------------------------------|
| Parameter | Enable HW accelerated H264 vdpau codec (experimental) |
| Registry  | ica.hw-accelerated-h264-vdpau-codec                   |
| Value     | <u>enabled</u> / <u>disabled</u>                      |

## RDP/IGEL RDP Client 2

- Added a field '**Collection**' to RDP session server page.

[More...](#)

**IGEL Setup > Sessions > RDP > RDP Sessions > RDP Session > Server**

**IGEL Setup > Sessions > RDP > RDP Sessions > RDP Session > Options**

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | Collection                                       |
| Registry  | sessions.winconnect<NR>.option.load-balance-info |

## VMware Horizon

- Updated **Horizon Client** to version **5.0.0-12557422**.
- Added parameters to specify **webcam frame size** and **rate for RTAV**.

[More...](#)

|           |                               |
|-----------|-------------------------------|
| Parameter | Webcam frame width            |
| Registry  | vmware.view.rtav-frame-width  |
| Value     | <u>&lt;empty string&gt;</u>   |
| Parameter | Webcam frame height           |
| Registry  | vmware.view.rtav-frame-height |
| Value     | <u>&lt;empty string&gt;</u>   |
| Parameter | Webcam frame rate             |
| Registry  | vmware.view.rtav-frame-rate   |
| Value     | <u>&lt;empty string&gt;</u>   |

- Added a possibility to easily evaluate **Horizon Blast decoder states**. By default, sessions are evaluated after use and the result is written to the journal log.
- Added **continuous run mode** for USB-Arbitrator.

[More...](#)

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | USB-Arbitrator continuous run mode            |
| Registry  | vmware.view.usb.arbitrator-continuous-runmode |
| Value     | <u>enabled</u> / <u>disabled</u>              |

- Added **recognition for password change** and **password expired dialog** in Horizon local logon sessions or appliance mode.
- Added **switch for Blast H.264 decoding** for VMware Horizon Client.

[More...](#)

|           |                                  |
|-----------|----------------------------------|
| Parameter | Blast H.264 decoding             |
| Registry  | vmware.view.blast-h264           |
| Value     | <u>enabled</u> / <u>disabled</u> |

- Added **switch to use systemwide proxy** in VMware Horizon appliance mode.

[More...](#)



|           |                                     |
|-----------|-------------------------------------|
| Parameter | Use the systemwide proxy            |
| Registry  | <code>vmwarevdmapp.use_proxy</code> |
| Value     | <u>enabled</u> / <u>disabled</u>    |

#### Parallels Client

- Updated **Parallels Client** to version **16.5.3 (64-Bit)**.
- Added a possibility to set apps to **autostart on Parallels RAS**.

#### ThinLinc

- Updated **Cendio ThinLinc** to version **4.10**.

#### RedHat Enterprise Virtualization Client.

- Updated **Remote Viewer** (RedHat Virtualization) to version **8.0**.
- Updated **Spice GTK** (RedHat Virtualization) to version **0.36**.

#### IBM\_5250

- Updated **IBM iAccess Client** Solutions to version **1.1.8.1**.
- **Improved startup time** of IBM iAccess Client.
- **Improved configuration** of IBM iAccess Client **via IGEL Setup**.  
[More...](#)

|           |                                                                                         |
|-----------|-----------------------------------------------------------------------------------------|
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Connection > Advanced |
| Parameter | Bypass signon                                                                           |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.ssoenabled</code>                              |
| Value     | <u>enabled</u> / <u>disabled</u>                                                        |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Font         |
| Parameter | Antialiasing                                                                            |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.textantialiasing</code>                        |
| Value     | <u>enabled</u> / <u>disabled</u>                                                        |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor       |
| Parameter | Allow blinking cursor                                                                   |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.blinkcursor</code>                             |
| Value     | <u>enabled</u> / <u>disabled</u>                                                        |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor       |



|           |                                                                                      |
|-----------|--------------------------------------------------------------------------------------|
| Parameter | Show blinking text with                                                              |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.blinkstate</code>                           |
| Value     | [Blinking Text] [Host Color] [Mapped Color]                                          |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor    |
| Parameter | Blink Color                                                                          |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.blinkcolor_fg</code>                        |
| Value     | <code>#ffc800</code>                                                                 |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor    |
| Parameter | Blink Color Background                                                               |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.blinkcolor_bg</code>                        |
| Value     | <code>#000000</code>                                                                 |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Rule Line |
| Parameter | Rule Line                                                                            |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.ruleline</code>                             |
| Value     | <code>enabled / disabled</code>                                                      |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Rule Line |
| Parameter | Follow Cursor                                                                        |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.rulelinefollows</code>                      |
| Value     | <code>enabled / disabled</code>                                                      |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Rule Line |
| Parameter | Style                                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.rulelinestyle</code>                        |
| Value     | [Crosshair] [Vertical] [Horizontal]                                                  |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color     |
| Parameter | Green                                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fgn_fg</code>                         |
| Value     | <code>#00ff00</code>                                                                 |



|           |                                                                                  |
|-----------|----------------------------------------------------------------------------------|
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Green Background                                                                 |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fgn_bg</code>                     |
| Value     | <code>#000000</code>                                                             |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | White                                                                            |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fwt_fg</code>                     |
| Value     | <code>#ffffff</code>                                                             |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | White Background                                                                 |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fwt_bg</code>                     |
| Value     | <code>#000000</code>                                                             |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Red                                                                              |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_frd_fg</code>                     |
| Value     | <code>#ff0000</code>                                                             |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Red Background                                                                   |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_frd_bg</code>                     |
| Value     | <code>#000000</code>                                                             |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Turquoise                                                                        |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_ftq_fg</code>                     |
| Value     | <code>#00ffff</code>                                                             |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Turquoise Background                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_ftq_bg</code>                     |



|           |                                                                                  |
|-----------|----------------------------------------------------------------------------------|
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Yellow                                                                           |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fyw_fg</code>                     |
| Value     | <u>#ffff00</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Yellow Background                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fyw_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Pink                                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fpk_fg</code>                     |
| Value     | <u>#ff00ff</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Pink Background                                                                  |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fpk_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Blue                                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fbl_fg</code>                     |
| Value     | <u>#7890f0</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Blue Background                                                                  |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fbl_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Status Indicators                                                                |



|           |                                                                                  |
|-----------|----------------------------------------------------------------------------------|
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_osi</code>                        |
| Value     | <u>#7890f0</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Information Indicators                                                           |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_oii</code>                        |
| Value     | <u>#ffffff</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Attention Indicators                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_oai</code>                        |
| Value     | <u>#ffff00</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Error Indicators                                                                 |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_oei</code>                        |
| Value     | <u>#ff0000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | OIA Background                                                                   |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_oob</code>                        |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Screen Background                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_sbg</code>                        |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Highlight active field                                                           |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.actfieldhilite</code>                   |
| Value     | <u>enabled / disabled</u>                                                        |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |



|           |                                                                                              |
|-----------|----------------------------------------------------------------------------------------------|
| Parameter | Active Field                                                                                 |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_actf_fg</code>                                |
| Value     | <code>#000000</code>                                                                         |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color             |
| Parameter | Active Field Background                                                                      |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_actf_bg</code>                                |
| Value     | <code>#ffff00</code>                                                                         |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color             |
| Parameter | Crosshair Ruler Color                                                                        |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_crc</code>                                    |
| Value     | <code>#00ff00</code>                                                                         |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color             |
| Parameter | Column Separator                                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_ccs</code>                                    |
| Value     | <code>#ffffff</code>                                                                         |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences                |
| Parameter | Start window maximized                                                                       |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.ismaximized</code>                                  |
| Value     | <code>enabled / disabled</code>                                                              |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences > Keyboard     |
| Parameter | Keyboard Remapping File                                                                      |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.keyremapfile</code>                                 |
| Value     | <code>IBMi.kmp</code>                                                                        |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences > Popup Keypad |
| Parameter | Popup Keypad File                                                                            |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.poppadfile</code>                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences > Toolbar      |



|           |                                                             |
|-----------|-------------------------------------------------------------|
| Parameter | Toolbar File                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.toolbarfile</code> |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup  |
| Parameter | Open new sessions in a new tab                              |
| Registry  | <code>ibm.iaccess.acssm.opensessionintab</code>             |
| Value     | <u>enabled</u> / <u>disabled</u>                            |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup  |
| Parameter | Always display the tab bar                                  |
| Registry  | <code>ibm.iaccess.acssm.alwaysshownabar</code>              |
| Value     | <u>enabled</u> / <u>disabled</u>                            |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup  |
| Parameter | Switch to new tab when created                              |
| Registry  | <code>ibm.iaccess.acssm.switchtonewtab</code>               |
| Value     | <u>enabled</u> / <u>disabled</u>                            |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup  |
| Parameter | Send a warning when closing multiple tabs                   |
| Registry  | <code>ibm.iaccess.acssm.closemultipletabwarning</code>      |
| Value     | <u>enabled</u> / <u>disabled</u>                            |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup  |
| Parameter | Do not start tabbed sessions until the tab is selected      |
| Registry  | <code>ibm.iaccess.acssm.tabdelayedstart</code>              |
| Value     | <u>enabled</u> / <u>disabled</u>                            |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup  |
| Parameter | New Tab Action                                              |
| Registry  | <code>ibm.iaccess.acssm.newtabaction</code>                 |
| Value     | [Disable and Hide] [Run the Same] [Run Other...]            |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup  |



|           |                                |
|-----------|--------------------------------|
| Parameter | Tab Placement                  |
| Registry  | ibm.iaccess.acssm.tabplacement |
| Value     | [Top] [Bottom] [Left] [Right]  |

## Firefox

- Updated **Mozilla Firefox** to version **60.7.2 ESR**.
- Added new keys to **auto show and hide the on-screen software keyboard**. To use this feature, the keyboard should be set to autostart. After a restart is activated, the keyboard will appear automatically when an input box is selected. Confirmed to work in Firefox and on lockscreen.

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Automatically hide software keyboard depending on focused widget |
| Registry  | userinterface.softkeyboard.autohide                              |
| Value     | enabled / <u>disabled</u>                                        |
| Parameter | Automatically show software keyboard depending on focused widget |
| Registry  | userinterface.softkeyboard.autoshow                              |
| Value     | enabled / <u>disabled</u>                                        |

- Added new parameters: **Allow a custom command before and after browser session**.

|           |                                |
|-----------|--------------------------------|
| Parameter | init_action                    |
| Registry  | sessions.browser%.init_action  |
| Value     | <empty_string>                 |
| Parameter | final_action                   |
| Registry  | sessions.browser%.final_action |
| Value     | <empty_string>                 |

- Added options to customize Firefox overflow menu and hide navigation buttons.

|           |                                                       |
|-----------|-------------------------------------------------------|
| Parameter | Hide Navigation buttons                               |
| Registry  | sessions.browser<NR>.app.navigation_buttons_hidden    |
| Value     | enabled / <u>disabled</u>                             |
| Parameter | Overflow Menu                                         |
| Registry  | sessions.browser<NR>.app.custom_toolbar.overflow-menu |
| Value     | open-file-button,feed-button,characterencoding-button |

Imprivata



- **Imprivata Appliance 6.3** or higher is needed now.
- Added a new parameter to Imprivata.conf: "**Redirection of Smartcards**".  
[More...](#)

#### **IGEL Setup > Sessions > Appliance Mode > Imprivata**

|           |                                        |
|-----------|----------------------------------------|
| Parameter | Redirection of Smartcards              |
| Registry  | imprivata.native_smartcard_redirection |
| Value     | <u>enabled</u> / <u>disabled</u>       |

- Added a new parameter: "**Path to Certificate**".  
[More...](#)

#### **IGEL Setup > Sessions > Appliance Mode > Imprivata**

|           |                               |
|-----------|-------------------------------|
| Parameter | Path to Certificate           |
| Registry  | imprivata.path_to_certificate |

### Network

- Added **NCP Secure Enterprise VPN Client** version **5.10\_rev40552** (configurable under **IGEL Setup > Network > VPN > NCP VPN Client**).
- Added a new feature: **Network status icons** are **shown on the lock and logon screens**.
- Added a mechanism for **retrieving the SCEP challenge password with a custom script**. Setting the following registry key to "true" enables the use of the script. The registry key `network.scepclient.cert%.crypt_password` will be ignored. (The script may use it for its own purpose though.)  
[More...](#)

|           |                                                                      |
|-----------|----------------------------------------------------------------------|
| Parameter | Use Challenge Password Command                                       |
| Registry  | <code>network.scepclient.cert%.use_challenge_password_command</code> |
| Value     | <u>enabled</u> / <u>disabled</u>                                     |

If the above key is enabled, the value of this key will be passed to bash for execution. It happens when the SCEP challenge password is needed for creating a certificate signing request. The script is supposed to output the challenge password on its standard output. For convenience, any Carriage-Return characters are stripped off the script before execution by bash.  
[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Challenge Password Command                                       |
| Registry  | <code>network.scepclient.cert%.challenge_password_command</code> |
| Value     | <u>&lt;empty string&gt;</u>                                      |

### WiFi

- Added support for **Realtek 8821CE wireless cards**.
- Added switch to determine the **source of WiFi scan results for Wireless Manager**. Selecting default is currently identical with the old mechanism (using the iwlist command). This may change in the future. When iwlist fails, NetworkManager is automatically used as a fallback.  
[More...](#)



|           |                                                      |
|-----------|------------------------------------------------------|
| Parameter | WiFi Scanner                                         |
| Registry  | network.interfaces.wirelesslan.device0.mssid_scanner |
| Range     | [default][iwlist][NetworkManager]                    |

## Smartcard

- New **IGEL Smartcard** mode **without Locking Desktop** (reintroduced feature of Linux 5.x firmware).

[More...](#)**IGEL Setup > Security > Logon > IGEL Smartcard**

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Enable IGEL Smartcard without Locking Desktop |
| Registry  | scard.scardd.enable_nolock                    |
| Value     | enabled / <u>disabled</u>                     |

**IGEL Setup > Security > Logon > IGEL Smartcard**

|           |                                  |
|-----------|----------------------------------|
| Parameter | On Smartcard Removal, terminate  |
| Registry  | scard.scardd.session_termination |
| Value     | <u>all</u> / smartcard           |

- Updated **MUSCLE CCID** smartcard reader driver to version **1.4.30**.
- Updated **ACS CCID** smartcard driver to version **1.1.6**.
- Updated **REINER SCT** smartcard reader driver to version **3.99.5final.sp13**.
- Updated **SecMaker NetID** to version **6.7.2.36**: now **YubiKey 5** is supported.
- Updated **cryptovision sc/interface PKCS#11** smartcard library to version **7.1.20**.
- Added configuration parameters for some settings of **smartcard library OpenSC**.

[More...](#)

|           |                                                    |
|-----------|----------------------------------------------------|
| Parameter | Debug level                                        |
| Registry  | scard.pkcs11.opensc.default.debug                  |
| Value     | <u>0</u>                                           |
| Parameter | Debug file                                         |
| Registry  | scard.pkcs11.opensc.default.debug_file             |
| Value     | <u>stderr</u>                                      |
| Parameter | Max. send size                                     |
| Registry  | scard.pkcs11.opensc.default.pcsc.max_send_size     |
| Value     | <u>255</u>                                         |
| Parameter | Max. receive size                                  |
| Registry  | scard.pkcs11.opensc.default.pcsc.max_recv_size     |
| Value     | <u>256</u>                                         |
| Parameter | Connect exclusive                                  |
| Registry  | scard.pkcs11.opensc.default.pcsc.connect_exclusive |
| Value     | enabled / <u>disabled</u>                          |
| Parameter | Disconnect action                                  |



|           |                                                                               |
|-----------|-------------------------------------------------------------------------------|
| Registry  | <code>scard.pkcs11.opensc.default.pcsc.disconnect_action</code>               |
| Value     | <u>leave</u> / reset / unpower                                                |
| Parameter | Transaction end action                                                        |
| Registry  | <code>scard.pkcs11.opensc.default.pcsc.transaction_end_action</code>          |
| Value     | <u>leave</u> / reset / unpower                                                |
| Parameter | Reconnect action                                                              |
| Registry  | <code>scard.pkcs11.opensc.default.pcsc.reconnect_action</code>                |
| Value     | <u>leave</u> / reset / unpower                                                |
| Parameter | Enable pinpad                                                                 |
| Registry  | <code>scard.pkcs11.opensc.default.pcsc.enable_pinpad</code>                   |
| Value     | <u>enabled</u> / disabled                                                     |
| Parameter | Use PIN caching                                                               |
| Registry  | <code>scard.pkcs11.opensc.default.pkcs15.use_pin_caching</code>               |
| Value     | <u>enabled</u> / disabled                                                     |
| Parameter | How many times to use a PIN from cache before re-authenticating it            |
| Registry  | <code>scard.pkcs11.opensc.default.pkcs15.pin_cache_counter</code>             |
| Value     | <u>10</u>                                                                     |
| Parameter | PIN caching ignores user consent                                              |
| Registry  | <code>scard.pkcs11.opensc.default.pkcs15.pin_cache_ignore_user_consent</code> |
| Value     | <u>enabled</u> / disabled                                                     |

- Updated **CHERRY USB-LAN Proxy** to version **3.2.0.3**. This version provides enhanced configuration.

[More...](#)

#### **IGEL Setup > Security > Smartcard > Services**

|           |                                                 |
|-----------|-------------------------------------------------|
| Parameter | Bind IP                                         |
| Registry  | <code>devices.cherry.usblanproxy.bind-ip</code> |
| Value     | <u>auto</u>                                     |

#### **IGEL Setup > Security > Smartcard > Services**

|           |                                                    |
|-----------|----------------------------------------------------|
| Parameter | Https Server Port                                  |
| Registry  | <code>devices.cherry.usblanproxy.https-port</code> |
| Value     | <u>443</u>                                         |

#### **IGEL Setup > Security > Smartcard > Services**

|           |                                                           |
|-----------|-----------------------------------------------------------|
| Parameter | SICCT Announce IP                                         |
| Registry  | <code>devices.cherry.usblanproxy.sicct-announce-ip</code> |
| Value     | <u>broadcast</u>                                          |

#### **IGEL Setup > Security > Smartcard > Services**

|           |                                                             |
|-----------|-------------------------------------------------------------|
| Parameter | SICCT Announce Port                                         |
| Registry  | <code>devices.cherry.usblanproxy.sicct-announce-port</code> |



|                                                              |                                                    |
|--------------------------------------------------------------|----------------------------------------------------|
| Value                                                        | <u>4742</u>                                        |
| <b>IGEL Setup &gt; Security &gt; Smartcard &gt; Services</b> |                                                    |
| Parameter                                                    | SICCT Announce Interval                            |
| Registry                                                     | devices.cherry.usblanproxy.sicct-announce-interval |
| Value                                                        | <u>30</u>                                          |
| <b>IGEL Setup &gt; Security &gt; Smartcard &gt; Services</b> |                                                    |
| Parameter                                                    | USB Fast Mode                                      |
| Registry                                                     | devices.cherry.usblanproxy.usb-fast-mode           |
| Value                                                        | <u>enabled /disabled</u>                           |
| <b>IGEL Setup &gt; Security &gt; Smartcard &gt; Services</b> |                                                    |
| Parameter                                                    | Alternate Initialization Method for G87-1505       |
| Registry                                                     | devices.cherry.usblanproxy.usb-1505-alt-setup      |
| Value                                                        | <u>enabled /disabled</u>                           |

## CUPS Printing

- Added **SMB Network Print** client function.
- [More...](#)

|                                                                                 |                                      |
|---------------------------------------------------------------------------------|--------------------------------------|
| <b>IGEL Setup &gt; Devices &gt; Printer &gt; CUPS &gt; Printers &gt; Dialog</b> |                                      |
| Parameter                                                                       | Printer Port                         |
| Registry                                                                        | print.cups.printer<NR>.backend       |
| Value                                                                           | <u>smb</u>                           |
| <b>IGEL Setup &gt; Devices &gt; Printer &gt; CUPS &gt; Printers &gt; Dialog</b> |                                      |
| Parameter                                                                       | SMB Server                           |
| Registry                                                                        | print.cups.printer<NR>.smb_server    |
| <b>IGEL Setup &gt; Devices &gt; Printer &gt; CUPS &gt; Printers &gt; Dialog</b> |                                      |
| Parameter                                                                       | SMB Workgroup                        |
| Registry                                                                        | print.cups.printer<NR>.smb_workgroup |
| <b>IGEL Setup &gt; Devices &gt; Printer &gt; CUPS &gt; Printers &gt; Dialog</b> |                                      |
| Parameter                                                                       | SMB Printer                          |
| Registry                                                                        | print.cups.printer<NR>.smb_printer   |
| <b>IGEL Setup &gt; Devices &gt; Printer &gt; CUPS &gt; Printers &gt; Dialog</b> |                                      |
| Parameter                                                                       | SMB Port                             |
| Registry                                                                        | print.cups.printer<NR>.smb_port      |
| <b>IGEL Setup &gt; Devices &gt; Printer &gt; CUPS &gt; Printers &gt; Dialog</b> |                                      |
| Parameter                                                                       | Use Kerberos Authentication          |
| Registry                                                                        | print.cups.printer<NR>.smb_kerberos  |
| Value                                                                           | <u>enabled / disabled</u>            |
| <b>IGEL Setup &gt; Devices &gt; Printer &gt; CUPS &gt; Printers &gt; Dialog</b> |                                      |



|           |                                        |
|-----------|----------------------------------------|
| Parameter | Use Passthrough Authentication         |
| Registry  | print.cups.printer<NR>.smb_passthrough |
| Value     | <u>enabled</u> / <u>disabled</u>       |

#### **IGEL Setup > Devices > Printer > CUPS > Printers > Dialog**

|           |                                 |
|-----------|---------------------------------|
| Parameter | SMB User                        |
| Registry  | print.cups.printer<NR>.smb_user |

#### **IGEL Setup > Devices > Printer > CUPS > Printers > Dialog**

|           |                                       |
|-----------|---------------------------------------|
| Parameter | SMB Password                          |
| Registry  | print.cups.printer<NR>.crypt_password |

Base system

- Updated **kernel** from 4.18.20 **to 4.19.57** version.
- Enhanced **bootloader** to allow the set of some kernel commandline parameters with registry keys:  
[More...](#)

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Disable use of APIC controller                |
| Registry  | system.kernel.bootparams.noapic               |
| Value     | <u>enabled</u> / <u>disabled</u>              |
| Parameter | Disable use of ACPI                           |
| Registry  | system.kernel.bootparams.noacpi               |
| Value     | <u>enabled</u> / <u>disabled</u>              |
| Parameter | Use only one CPU core and disable all others  |
| Registry  | system.kernel.bootparams.nosmp                |
| Value     | <u>enabled</u> / <u>disabled</u>              |
| Parameter | Enable debug console on serial port 1         |
| Registry  | system.kernel.bootparams.serial_console_debug |
| Value     | <u>enabled</u> / <u>disabled</u>              |
| Parameter | Limit CPU core usage (0 means no limit)       |
| Registry  | system.kernel.bootparams.maxcpus              |
| Type      | Integer                                       |
| Value     | 0                                             |
| Parameter | Set maximum allowed cstate on intel cpus      |
| Registry  | system.kernel.bootparams.max_cstate           |
| Range     | [No limit] [1] [2] [3] [4] [5] [6]            |

**Info:** Do not limit Intel cstate.

|              |                                  |
|--------------|----------------------------------|
| Parameter    | IOMMU usage setting              |
| Registry     | system.kernel.bootparams.iommu   |
| Range        | [On] [Off] [Passthrough] [Force] |
| <b>Info:</b> | Use IOMMU if possible.           |

|           |                                     |
|-----------|-------------------------------------|
| Parameter | IOMMU usage setting for AMD systems |
|-----------|-------------------------------------|



|          |                                    |
|----------|------------------------------------|
| Registry | system.kernel.bootparams.amd_iommu |
| Range    | [On] [Off]                         |

Info: Use IOMMU if possible.

|           |                                       |
|-----------|---------------------------------------|
| Parameter | IOMMU usage setting for Intel systems |
| Registry  | system.kernel.bootparams.intel_iommu  |
| Range     | [On] [Off]                            |

Info: Use IOMMU if possible.

- Added a possibility to configure **scheduled commands**. Registry keys: system.cron.\*\*
- Buddy update** enhancements:

- Automatic load balancing:**

A client collects up to eight server candidates from which one is selected randomly. Collection stops when the number specified in the following registry key is reached. Otherwise collection stops after a timeout.

[More...](#)

|           |                                    |
|-----------|------------------------------------|
| Parameter | Buddy Update Server Candidates     |
| Registry  | update.ftp.buddy_server_candidates |
| Value     | 1                                  |

- Grouping:**

Buddy update servers and clients only interact with each other when they are in the same group determined by the following registry key (a non-negative integer number). This feature is mainly useful when different firmware versions shall be used in parallel.

[More...](#)

|           |                           |
|-----------|---------------------------|
| Parameter | Buddy Group ID            |
| Registry  | update.ftp.buddy_group_id |
| Value     | 0                         |

- Updated **libwebkit2gtk-4.0-37** to version **1.24.2**.

Security fixes:

[More...](#)

CVE-2019-8595, CVE-2019-8607, CVE-2019-8615, CVE-2019-6251,  
 CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378,  
 CVE-2018-4382, CVE-2018-4392, CVE-2018-4416, CVE-2018-4345,  
 CVE-2018-4386, CVE-2018-4372

- Updated **Fluendo multimedia codecs** to the following versions:

[More...](#)

|                        |            |          |
|------------------------|------------|----------|
| gst-fluendo-aacdec     | 21/03/2019 | 0.10.39  |
| gst-fluendo-asfdemux   | 21/03/2019 | 0.10.89  |
| gst-fluendo-h264dec    | 21/03/2019 | 0.10.53  |
| gst-fluendo-mp3        | 21/03/2019 | 0.10.39  |
| gst-fluendo-mpeg4video | 21/03/2019 | 0.10.43  |
| gst-fluendo-vadec      | 21/03/2019 | 0.10.208 |



|                    |            |         |
|--------------------|------------|---------|
| gst-fluendo-wmadec | 21/03/2019 | 0.10.68 |
| gst-fluendo-wmvdec | 20/03/2019 | 0.10.65 |

- Added a package **ldap-utils** which can be used by custom scripts.

## Driver

- Updated **DisplayLink driver** to version **5.1.26**.
- Updated **Philips Speech Driver** to version **12.7.11** - added **support for Philips AirBridge**.
- Added registry keys to modify the Intel graphic driver usage of **framebuffer compression** and **power management**.

New registry keys:

[More...](#)

|           |                                             |
|-----------|---------------------------------------------|
| Parameter | Power saving display C-States to use        |
| Registry  | x.drivers.intel.dc_setting                  |
| Range     | [Default] [Disable] [Up to DC5] [Up to DC6] |
| Info:     | "Default" - driver default                  |
| Parameter | Use framebuffer compression                 |
| Registry  | x.drivers.intel.fbc_setting                 |
| Range     | [Default] [Disable]                         |
| Info:     | "Default" - driver default                  |

- Updated **signotec Citrix Virtual Channel** driver to version **8.0.8**.
- Updated **deviceTRUST Client** to version **19.1.200**. These are the release notes:  
Welcome to the release of the deviceTRUST 19.1.200 IGEL client, providing the context of IGEL thin client and UD Pocket devices into your virtual sessions. This release includes support for logical disks attached to the IGEL endpoint, plus bug fixes and stability improvements over the previous 19.1.100 release.

## Logical Disks

We've added support for real-time properties representing the LOGICAL DISKS attached to the IGEL endpoint. This includes:

[More...](#)

DEVICE\_LOGICALDISK\_X\_TYPE – Either Fixed or Removable.

DEVICE\_LOGICALDISK\_X\_LABEL – The volume label.

DEVICE\_LOGICALDISK\_X\_FILESYSTEM – The type of file system.

DEVICE\_LOGICALDISK\_X\_PATHS – The paths that the disk is mounted.

DEVICE\_LOGICALDISK\_X\_TOTALMB – The total space available on the disk. This property is only available for mounted disks.

DEVICE\_LOGICALDISK\_X\_FREEMB – The free space available on the disk. This property is only available for mounted disks.

DEVICE\_LOGICALDISK\_X\_NAME – The name of the underlying physical disk.

DEVICE\_LOGICALDISK\_X\_VENDORID – The vendor identifier uniquely identifying the manufacturer. This



property is only available for USB or PCI connected devices.

DEVICE\_LOGICALDISK\_X\_PRODUCTID – The product identifier uniquely identifying the product. This property is only available for USB or PCI connected devices.

DEVICE\_LOGICALDISK\_X\_SERIALNUMBER – The serial number of the physical disk.

DEVICE\_LOGICALDISK\_X\_BUSTYPE – The storage bus type linked to the physical disk.

DEVICE\_LOGICALDISK\_COUNT – The number of logical disks.

## X11 system

- Updated Xorg server from 1.19.6 to **1.20.5** version.
- Updated **Virtualbox** from 5.2.18 to **6.0.8** version.
- Updated **Mesa** from 18.2.1 to **19.0.8** version.
- Updated **Nvidia driver** from 410.93 to **418.56** version.
- Updated **Xorg video and input driver** to current upstream versions.
- Added new options for **laptop lid handling** dependent on power supply:  
**More...**

|           |                                                      |
|-----------|------------------------------------------------------|
| Parameter | Lid close action while plugged in                    |
| Registry  | <a href="#">system.actions.lid.ac</a> <sup>453</sup> |
| Range     | [Turn off display] [Suspend]                         |
| Parameter | Lid close action while not plugged in                |
| Registry  | <a href="#">system.actions.lid.battery</a>           |
| Range     | [Turn off display] [Suspend]                         |

- The new **Display Switch tool** can use multiple different profiles, automatically chosen at runtime depending on the currently connected monitors.

A profile is created, when the current monitor layout/resolution is configured via the Display Switch utility. The profile will be associated with the current connected displays automatically (manufacturer, model and used connector are used for allocation) and if applicable, the state of the laptop lid. The setup will be restored by hot-(un)plugging known displays, means the system will automatically switch to the already configured profile.

The Display Switch utility itself got a new interface. All base functionality can be configured via Drag&Drop.

An example workflow:

- Connect the hardware and close/open the lid.
- Open the Display Switch Utility:
  - A quick (simple) setting can be selected directly.
  - Should the desired use case be different from the provided choices, the 'Advanced' button opens a drag&drop interface for further settings.

---

<sup>453</sup> <http://system.actions.lid.ac>



- In this interface the displays can be dragged and dropped for the intended configuration. The display will snap adjacent to others.
  - If a display should not be used, it can be dragged to the 'Disabled' area on the top right - the screen will be reactivated when it is dragged back to the active area.
  - To show the same content on multiple displays, one display should be dragged onto another active screen. The interface will show "Mirror". The mirroring monitor will be displayed on the lower right.
- With the 'Apply' button the current state will be set, with 'Yes' on the "Keep configuration" dialog the current settings will be saved to persistent storage and associated with the profile.
- Advanced functionality (panning/scaling/resolutions) can be configured in drop-down boxes, hidden in a drawer on the right side. The drawer can be expanded by clicking the '<' button on the right edge.
  - For the Display Switch functionality the following parameters should be enabled for proper usage:

[More...](#)

#### IGEL Setup > Accessories > Display Switch > Options

|           |                                                               |
|-----------|---------------------------------------------------------------|
| Parameter | Preserve settings over reboot                                 |
| Registry  | <code>sessions.user_display0.options.preserve_settings</code> |
| Value     | <u>enabled</u> / <u>disabled</u>                              |

#### IGEL Setup > Accessories > Display Switch > Options

|           |                                  |
|-----------|----------------------------------|
| Parameter | Smart display configuration      |
| Registry  | <code>x.auto_associate</code>    |
| Value     | <u>enabled</u> / <u>disabled</u> |

- The **IGEL Display Switch** utility is **now usable for NVIDIA graphics devices** as well.
- Added a new parameter to optionally start with opened '**Advanced**' drawer in **Display Switch**.

[More...](#)

#### IGEL Setup > Accessories > Display Switch > Options

|           |                                                               |
|-----------|---------------------------------------------------------------|
| Parameter | Preserve settings over reboot                                 |
| Registry  | <code>sessions.user_display0.options.preserve_settings</code> |
| Value     | <u>enabled</u> / <u>disabled</u>                              |

#### IGEL Setup > Accessories > Display Switch > Options

|           |                                                        |
|-----------|--------------------------------------------------------|
| Parameter | Start with the advanced drawer opened                  |
| Registry  | <code>sessions.user_display0.options.start_open</code> |
| Value     | <u>enabled</u> / <u>disabled</u>                       |

- Added **xprintidle tool** to firmware.
- Added some registry keys to disable loading of **DRM kernel modules** (graphic).

[More...](#)

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Disable the loading of the RADEON DRM driver. |
| Registry  | <code>x.drivers.ati.disable</code>            |



|                                                                                                             |                                                  |
|-------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| Value                                                                                                       | <u>"0"</u>                                       |
| Parameter                                                                                                   | Disable the loading of the AMDGPU DRM driver.    |
| Registry                                                                                                    | x.drivers.amdgpu.disable                         |
| Value                                                                                                       | <u>"0"</u>                                       |
| Parameter                                                                                                   | Disable the loading of the i915 DRM driver.      |
| Registry                                                                                                    | x.drivers.intel.disable                          |
| Value                                                                                                       | <u>"0"</u>                                       |
| Parameter                                                                                                   | Disable the loading of the NVIDIA kernel driver. |
| Registry                                                                                                    | x.drivers.nvidia.disable                         |
| Value                                                                                                       | <u>"0"</u>                                       |
| Parameter                                                                                                   | Disable the loading of the NOUVEAU DRM driver.   |
| Registry                                                                                                    | x.drivers.nouveau.disable                        |
| Value                                                                                                       | <u>"0"</u>                                       |
| Parameter                                                                                                   | Disable the loading of the QXL DRM driver.       |
| Registry                                                                                                    | x.drivers.qxl.disable                            |
| Value                                                                                                       | <u>"0"</u>                                       |
| Parameter                                                                                                   | Disable the loading of the VMGFX DRM driver.     |
| Registry                                                                                                    | x.drivers.vmware.disable                         |
| Value                                                                                                       | <u>"0"</u>                                       |
| Parameter                                                                                                   | Disable the loading of the VBOXVIDEO DRM driver. |
| Registry                                                                                                    | x.drivers.vboxvideo.disable                      |
| Value                                                                                                       | <u>"0"</u>                                       |
| • Added the possibility to <b>change an embedded DisplayPort to a normal DisplayPort.</b><br><b>More...</b> |                                                  |
| Parameter                                                                                                   | Use embedded displayport as normal displayport   |
| Registry                                                                                                    | x.drivers.intel.edp_is_dp                        |
| Range                                                                                                       | [default][enable][disable]                       |



**Info:** Reboot required

#### Java

- Replaced Oracle JRE by **AZUL's Zulu JRE**.
- **Removed** deprecated **Java WebStart** since it is not supported with non-Oracle JRE's.

#### X server

- Updated **Xephyr x session** to version **1.20.5**.

#### Hardware

- Added hardware support for **HP t530**.
- Added hardware support for **HP Compaq Elite 8300**.
- Added hardware support for **HP EliteDesk 800 G3 mini**.
- Added hardware support for **HP EliteDesk 800 G3 SFF**.
- Added hardware support for **HP EliteDesk 800 G1 SFF**.
- Added hardware support for **Fujitsu Esprimo Q957**.
- Added hardware support for **Dell OptiPlex 9020**.
- Added hardware support for **Dell Latitude E6440**.
- Added hardware support for the following headsets:

[More...](#)

Jabra Engage 50;  
 Jabra Engage 65;  
 Jabra Engage 75;  
 Jabra Evolve 30 II (Ver. B);  
 Jabra Evolve 30 II (Ver. C);  
 Jabra Evolve 40 (Ver. B) - USB-C;  
 Jabra Evolve 40 (Ver. D);  
 Jabra Evolve 65;  
 Jabra Evolve 75;  
 Plantronics Voyager 5200 UC;  
 Plantronics Voyager 6200 UC;  
 Plantronics Voyager 8200 UC;  
 Sennheiser SC70.

#### Remote Management / IGEL Cloud Gateway

- **Connection order between UMS and ICG** can now be configured.  
[More...](#)

|           |                                                       |
|-----------|-------------------------------------------------------|
| Parameter | Prefer UMS over ICG                                   |
| Registry  | <code>system.remotemanager.icg_try_ums_connect</code> |
| Value     | <code>enabled</code> / <code>disabled</code>          |

When an ICG connection is configured and the parameter is enabled, the device tries to connect directly to UMS. If the connection was established successfully, the device is managed by UMS and not over ICG until new start of the device or networking.

- **Firmware update scheduled on shutdown** is now invoked **on reboot** as well.
- Added some adaptations in **UMS Agent** concerning **migration to IGEL OS11**.



## Resolved Issues 10.06.100

### Citrix

- Now ica.pnlogin.syncpasswordwithxscrnsrv is removed, **ica.pnlogin.syncpasswordwithxlock** should be used, this provides the same functionality.
- Fixed **online meeting in VDI**: An enabled webcam will not cut the audio streaming anymore.
- Citrix **Workspace App 19.03**: Improved USB redirection handling.
- Custom icons** now are visible **after StoreFront logon** using Citrix authentication method.
- Appropriate icons** arise with IGEL and Citrix authentication.
- Fixed **stability issues** with Citrix Browser Content Redirection.
- Updated the **Nuance virtual channel** for ICA up to version **B301**.

### RDP/IGEL RDP Client 2

- Added **Negotiate:Kerberos as fallback** if NTLM is disabled. This only works if Active Directory/Kerberos Logon is enabled.
- Added registry key to use **rdpglobal window settings for remote apps**.

**More...**

|           |                                                             |
|-----------|-------------------------------------------------------------|
| Parameter | Enable global window settings for remote app                |
| Registry  | rdp.winconnect.enable-global-window-settings-for-remote-app |
| Value     | <u>enabled</u> / <u>disabled</u>                            |

- Fixed **empty warning window** being shown when closing RDP Web Applications started from browser.
- Fixed **smartcard redirection in RDP**: SCardGetAttrib was failing if pbAttr was NULL. The fix should help running Dutch Zorg-ID applications.

### RD Web Access

- Fixed **RD Web Access** not working with **special characters in name or password**. This only works if Active Directory/Kerberos Logon is enabled.
- Fixed **empty warning dialogs** appearing when opening RD Web Application in the browser.
- Fixed **not starting RDP Remote Applications**.

### VMware Horizon

- Fixed **Optimization for Skype for Business**.
- Fixed the configuration choice to use **the relative mouse feature**.

### Parallels Client

- Updated **Parallels Client** to version **16.5.3** (64-Bit).
- Fixed: **Maximized windows** for published applications can be displayed incorrectly.
- Fixed: **Incorrect user credentials** can be picked up during connection if the same farm is registered in the client multiple times and with different user credentials.
- Fixed: Client **did not accept universal printing policies** set from the server.
- Fixed: **Module** opened in the background and **blocked the launcher** in some cases.
- Fixed: **Redirected smartcard** did not work **in a remote session**.
- Fixed: **Printers would not redirect to a remote session** when redirection is enforced via policies.



## PowerTerm

- Fixed **editing** of parameter **sessions.powerterm|<INST>.logindialog.loginscript** in Setup Registry: now multiple lines are possible.
- PowerTerm Terminal Emulation: remove **obsolete SSH type SSH1** and **obsolete SSH cipher DES** from parameter ranges.

## Firefox

- Fixed an issue where **Firefox does not accept proxy credentials** from setup.
- Fixed the **print hotkey disable option** with Firefox 60+.
- Fixed **browserglobal.app.local\_subdirs\_whitelist** not working.
- Fixed **Adobe Flash Player download** possibility.

## Network

- Improved **SCEP client robustness**:
  - The **cert\_agent script** doesn't terminate anymore when a problem occurs (e.g. the SCEP server is unreachable) but tries again after the expiry check interval.
  - When the client certificate has expired, there is still one attempt at renewing it. However, when that fails, a new one is requested. That obviously will fail if the client presents a challenge password that is not valid anymore.
- Restoring **WLAN/WWAN Modem state** after wakeup from standby or reboot.
- Improved **expire time of Ethernet no-link notification**.
- Added all **Ethernet network drivers from OS to LX** version.
- Changed **e1000e driver** to out of tree version **3.4.2.3** directly from Intel.
- Changed **igb driver** to out of tree version **5.3.5.22** directly from Intel.
- Fixed bug: **Failure to reach SCEP server** in the client certificate renewal phase resulted in loss of SCEP server and client certificates.
- SCEP: A change of the **CA fingerprint** setting **does not result in discarding all SCEP data anymore** if the fingerprint matches that of the current CA certificate. Firmware versions before 10.05.100 allowed an empty fingerprint. So, this is meant for users who must belatedly configure the fingerprint in order for client certificate renewal to work.

A change of the **CAIdentifier** setting is not detected immediately and does not result in discarding all current data anymore. The new CAIdentifier will, however, be used in future SCEP operations.

- Fixed **instability with netmounts** with static ip configuration.
- Fixed problems with **windows share mounts**.
- Fixed **MBB router** configuration (broken since 10.05.500).
- Added a possibility to **switch between third-party** and **kernel Intel IGB network driver**.

A new registry key:

**More...**

|                                             |                                       |
|---------------------------------------------|---------------------------------------|
| Parameter                                   | Use thirdparty igb kernel module      |
| Registry                                    | network.drivers.igb.prefer_thirdparty |
| Range                                       | [Auto] [Yes] [No]                     |
| Info: "Auto" (use thirdparty in most cases) |                                       |

- Added a possibility to **switch between thirdparty** and **kernel Intel E1000E network driver**.

A new registry key:

**More...**



|           |                                          |
|-----------|------------------------------------------|
| Parameter | Use thirdparty e1000e kernel module      |
| Registry  | network.drivers.e1000e.prefer_thirdparty |
| Range     | [Auto] [Yes] [No]                        |

Info: "Auto" (use thirdparty in most cases)

- Added a possibility to **switch between thirdparty r8168 and kernel r8169 realtek network driver.**

A new registry key:

**More...**

|           |                                    |
|-----------|------------------------------------|
| Parameter | Use thirdparty r8168 kernel module |
| Registry  | network.drivers.r8169.prefer_r8168 |
| Range     | [Auto] [Yes] [No]                  |

Info: "Auto" (use r8168 in most cases)

- Added a possibility to choose the **variant of the realtek r8168 driver.**

A new registry key:

**More...**

|           |                                                                 |
|-----------|-----------------------------------------------------------------|
| Parameter | Choose realtek r8168 variant (only if "prefer r8168" is chosen) |
| Registry  | network.drivers.r8169.r8168_variant                             |
| Range     | [Default] [No NAPI] [NAPI]                                      |

Info: "Default" (use NAPI in most cases)

- Fixed bug: **Second Ethernet interface** did not get configured when the first one was disabled.
- Fixed **802.1X Ethernet configuration with user interaction.**

## WiFi

- Fixed bug: **WiFi connection to hidden SSID** did not work anymore after re-editing with the Wireless Manager.
- Fixed not working **Broadcom SDIO WLAN cards** as present in Advantech AIM8IAC device for example.

## Smartcard

- Fixed **Dell KB813 Smartcard Keyboard** in combination with certain smart cards driven by OpenSC PKCS#11 module. Before this fix, authentication to Citrix StoreFront and VMWare Horizon failed.
  - Improved **handling of PIV/CAC smart cards** in OpenSC.
  - Updated **cryptovision sc/interface PKCS#11 smart card library** to version **7.1.20**.
- Changes in this revision:
- Fixed **a possible deadlock in the PKCS#11 module** on Linux if C\_Finalize is called during a PCSC event, for example, C\_WaitForSlotEvent.
  - **ROCA check in the Smartcard Manager**, based on the "ROCA detection tool", see <https://github.com/crocs-muni/roca>.
  - **Renaming container label** in Smartcard Manager with F2 now possible.
  - Fixed **OpenSC setting max\_send\_size** for reader driver pcsc in **/etc/opensc/opensc.conf**.

## Application Launcher

- Fixed **confusion in nameserver list** caused by comments in /etc/resolv.conf.

## Base system



- Fixed: **Zotac Zbox will not shutdown.**
- Fixed issues with **gen4/5 Intel graphic driver** in kernel 4.18.20.
- Fixed **Screensaver and Screenlock timeouts** to be independent. This means, if both timeouts are set, the start of Screenlock will not reset the Screensaver timeout any more.
- Fixed **retrieving of serial number of a display.**
- Fixed **playback of AAC coded audio streams** on IGEL Zero products.
- Do not auto-start **UD-Pocket license browser** when the device has a proper license.
- Added possibility to set **intel\_idle.max\_cstate kernel cmdline parameter** with registry keys **to work against Intel CPU freezes.**
- **Enhanced handling of Unit ID.** The persistent Unit ID can be removed with command `get_unit_id -r`. The persistent Unit ID storage can be forced with `get_unit_id -i -f -p` or with `get_unit_id -m` to manually choose a Unit ID from several network interfaces found on the device. Handle with extreme care since the Unit ID is the key for handling the endpoint in UMS.
- Replaced MIT Kerberos clients by **Heimdal Kerberos clients**.
- Improved the buddy update server performance for multiple simultaneous update clients.
- Fixed handling of an "**update on shutdown**" during suspend/resume.
- Fixed **NVIDIA driver kernel warning messages**.
- Allow to **configure NVIDIA graphics cards** (rotation/resolution) **via Setup** again.
- Fixed **shutdown** while IGEL Setup Assistant is shown.
- Fixed **delay in logon** as local user when logon with IGEL Smartcard is also active.
- Fixed **sporadic bootsplash issue**.
- Fixed **suspend/resume hangs** when logged into Citrix sessions.
- Fixed **CPU scaler and volume control applet suspend/resume** issue.
- Added **AppArmor rule** to allow `tcpdump` to write to **/debuglog**.
- Fixed random 90 seconds **shutdown delay** (systemd).
- Fixed **Custom Bootsplash installation**.
- Bugfix: **Create shortcuts** for terminal shutdown, terminal restart and icon sort **directly after reconfiguration**. A reboot is not needed anymore.
- Fixed: **System logoff waits for Citrix logoff** now.
- Fixed **broken custom bootsplash** when doing a reset to factory defaults via UMS.
- Bugfix: **hotkey** setting **needs restart**.
- **IGEL Setup Assistant** will persistently **activate WiFi** when a connection is enabled instead of after finishing it, to preserve settings when UMS sends license and stops it.
- Fixed **AD/Kerberos logon** in case parameter **auth.login.krb5\_enterprise** is **set to 'false'**.
- Added a new registry key to set **USB quirks**:  
**More...**

|           |                                                                                              |
|-----------|----------------------------------------------------------------------------------------------|
| Parameter | Set XHCI USB quirks to fix some hardware issues                                              |
| Registry  | <code>system.kernel.bootparams.xhci-hcd_quirks</code>                                        |
| Range     | [No quirk] [Spurious Reboot quirk] [Spurious Wakeup quirk]<br>[Spurious Reboot Wakeup quirk] |

- **Lenovo ThinkCentre M73** needs the `system.kernel.bootparams.xhci-hcd_quirks` registry key set to "**Spurious Reboot quirk**" to fix reboot after shutdown problem.



- Fixed: **Migration tool** did not start with **Spanish** language setting.
- Disabled **martian packet logging**.

#### Driver

- Updated **deviceTRUST** Client to version **19.1.200**.

#### Bug Fixes:

- Fixed an issue **reading the DEVICE\_IGEL\_ICG\_SERVER** property.
- Fixed an issue where the **NETWORK** and **LOCATION** property providers could **cause the client to freeze** if a disconnection occurred while these property providers were checking for changes.
- Fixed an **open file handle leak** which lead to the client process reaching its file handle limits when left running for a long period of time.
- Fixed not working **WACOM** device **DTU-1141B**.

#### Custom Partition

- Fixed **ownership of extracted data**: Do not preserve owner information while extracting data into custom partition.

#### Storage Devices

- Fixed **auto mounting of storage devices** inside of Olympus DS-9500 Digital Voice Recorder.

#### Appliance Mode

- Fixed bug: **In-session control bar** could not be deactivated **in Citrix SelfService appliance mode**.

#### X11 system

- Fixed **Microsoft Surface Pro 4 screen resolution** issue.
- Fixed the **missing volume control** in the panel when the panel is configured to disappear while the login/lock screen is shown.
- There is now a **registry key to ignore a 3Dconnexion SpaceMouse** for IGEL graphical use (X11). If activated, the SpaceMouse is only passed through to the desktop session. If false, it acts also as the standard mouse.

[More...](#)

|           |                                                          |
|-----------|----------------------------------------------------------|
| Parameter | Deactivates a 3Dconnexion SpaceMouse as a standard mouse |
| Registry  | userinterface.mouse.spacemouse.x11_ignore                |
| Value     | <u>enabled</u> / disabled                                |

- The following **SpaceMouse** products are included:

[More...](#)

| VID    | PID    | Vendor         | Product                        |
|--------|--------|----------------|--------------------------------|
| 0x046D | 0xC603 | Logitech, Inc. | 3Dconnexion SpaceMouse Plus XT |
| 0x046D | 0xC605 | Logitech, Inc. | 3Dconnexion CADman             |
| 0x046D | 0xC606 | Logitech, Inc. | 3Dconnexion SpaceMouse Classic |
| 0x046D | 0xC621 | Logitech, Inc. | 3Dconnexion SpaceBall 5000     |



| <b>VID</b> | <b>PID</b> | <b>Vendor</b>  | <b>Product</b>                           |
|------------|------------|----------------|------------------------------------------|
| 0x046D     | 0xC623     | Logitech, Inc. | 3Dconnexion SpaceTraveller 3D Mouse      |
| 0x046D     | 0xC625     | Logitech, Inc. | 3Dconnexion SpacePilot 3D Mouse          |
| 0x046D     | 0xC626     | Logitech, Inc. | 3Dconnexion SpaceNavigator 3D Mouse      |
| 0x046D     | 0xC627     | Logitech, Inc. | 3Dconnexion SpaceExplorer 3D Mouse       |
| 0x046D     | 0xC628     | Logitech, Inc. | 3Dconnexion SpaceNavigator for Notebooks |
| 0x046D     | 0xC629     | Logitech, Inc. | 3Dconnexion SpacePilot Pro 3D Mouse      |
| 0x046D     | 0xC62B     | Logitech, Inc. | 3Dconnexion SpaceMouse Pro               |
| 0x256F     | **         | 3Dconnexion    | SpaceMouse                               |

- Fixed **screen flicker** in some cases if **Force NumLock On** (x.global.forcenumlock) is active.
- Fixed not working **x.xserver0.screen1.flipscreens** registry key.
- Fixed **problems with internal graphic cards** and **NVIDIA graphic cards**.
- Use **Index** and **Mode** from Advanced mode in Simple Mode **for Display Switch**.
- Fixed **display hotplug failing** on initial lock screen with Active Directory logon.
- The **in-session control bar** now **scales with the current DPI** setting.
- Fixed **Display Switch** utility **not starting with some translations**.
- Fixed an issue with the **noDDC mode** not always working as expected.
- Fixed some **multimonitor (>4) issues with NVIDIA graphic cards**.
- Fixed **monitor screen ID** shown **with NVIDIA NV810 GPU**.
- Fixed a bug with thin clients **reporting the wrong monitor serial number**.

#### Window manager

- Fixed the option to **disable the local window manager**.

#### Audio

- Fixed **bad quality sound over DisplayPort** in a Citrix ICA session or other applications using ALSA API.
- Fixed **jack detection** of the headphone port **in Dell Wyse 3040**.
- Fixed **configuration of default audio output and input**.

#### Media Player (Parole)

- Fixed a problem where **parole media player** would **hang** instead of playing audio **while audio-visualization** is enabled.
- Fixed parole media player **not handling audio hotkeys in fullscreen mode**.

#### Multimedia

- Updated **multimedia codecs to fix freeze** when audio visualization is used.

#### Misc

- **Monitoring Agent** uses now **only the half size of the debuglog partition**.

When the setup option **log\_max\_size** with the option **log\_rotation** creates an overall consumption that is bigger than 50% of the debuglog partition size, the size for each log automatically will be decreased to a value that allows a full rotation which occupies exactly 50% of the partition size.



## Hardware

- Fixed wrongly detected **embedded DisplayPort on Dell Wyse 5070 Extended hardware.**
- Fixed **wakeup from suspend for Lenovo Ideapad 320-15IAP.**
- Fixed not working **network on Beckhoff CB3163, CB6263** and **CB6363** systems.
- Fixed not working **network on Lex 3I380D.**
- Fixed **shutdown issue of Lenovo ThinkCentre M73** (rebooted 2 - 3 seconds after power off).
- Fixed problems with **mouse cursor on Intel cherryview devices.**
- Fixed **detection of Dell Wyse 5070** for the non-extended version.
- Fixed not working **Laptop Display for Dell Latitude E5510.**
- Added a **possibility to change** some **DRM settings** and **limit the DisplayPort lane bandwidth** on Intel devices.

Added new registry keys:

**More...**

|                                                           |                                                                  |
|-----------------------------------------------------------|------------------------------------------------------------------|
| Parameter                                                 | Use best graphic mode for all screens on console.                |
| Registry                                                  | x.drivers.kms.best_console_mode                                  |
| Range                                                     | [Default] [Enabled] [Disabled]                                   |
| Info: "Default" is enabled in most cases.                 |                                                                  |
| Parameter                                                 | Limit the maximum console resolution width to this value.        |
| Registry                                                  | x.drivers.kms.max_console_width                                  |
| Type                                                      | Integer                                                          |
| Value                                                     | "0"                                                              |
| Info: "0" means default setting. Use the default setting. |                                                                  |
| Parameter                                                 | Limit the maximum console resolution height to this value.       |
| Registry                                                  | x.drivers.kms.max_console_height                                 |
| Type                                                      | Integer                                                          |
| Value                                                     | "0"                                                              |
| Info: "0" means default setting. Use the default setting. |                                                                  |
| Parameter                                                 | Set graphic kernel driver debug level.                           |
| Registry                                                  | x.drivers.kms.debug_level                                        |
| Range                                                     | [No debug] [Basic] [Basic + core] [Basic + core + atomic] [Full] |
| Info: Warning log will grow very fast.                    |                                                                  |

Only for Intel i915 driver:



|                                               |                                                                                                            |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Parameter                                     | Limit the maximum DisplayPort lane link rate.                                                              |
| Registry                                      | x.drivers.intel.max_dp_link_rate                                                                           |
| Range                                         | [ <u>default</u> ] [1.62Gbps] [2.16Gbps] [2.7Gbps] [3.24Gbps]<br>[4.32Gbps] [5.4Gbps] [6.48Gbps] [8.1Gbps] |
| Info: "Default" means hardware default limit. |                                                                                                            |

#### Remote Management / IGEL Cloud Gateway

- Fixed **wallpaper configuration** when ICG protocol is used.
- Fixed **UMS synchronization of configuration** when changes were made in "Emergency mode".
- Fixed sporadic **failures while sending data over ICG**.
- Fixed **removal from UMS** when the device was offline.
- Added: IGEL UMS agent sends **monitor information for maximum eight monitors** now.

#### Caradigm

- Fixed **Horizon session crash**.

## 7.25 Notes for Release 10.05.830

|                       |            |             |
|-----------------------|------------|-------------|
| <b>Software:</b>      | Version    | 10.05.830   |
| <b>Release Date:</b>  | 2019-07-05 |             |
| <b>Release Notes:</b> | Version    | RN-105830-1 |
| <b>Last update:</b>   | 2019-07-05 |             |

- 
- [IGEL Linux Universal Desktop](#)(see page 2036)
  - [IGEL Universal Desktop OS 3](#)(see page 2057)

### 7.25.1 IGEL Linux Universal Desktop

#### Supported Devices

|                           |           |
|---------------------------|-----------|
| <b>Universal Desktop:</b> |           |
| UD2-LX:                   | UD2-LX 40 |



|          |                                                  |
|----------|--------------------------------------------------|
| UD3-LX:  | UD3-LX 51<br>UD3-LX 50<br>UD3-LX 42<br>UD3-LX 41 |
| UD5-LX:  | UD5-LX 50                                        |
| UD6-LX:  | UD6-LX 51                                        |
| UD7-LX:  | UD7-LX 10                                        |
| UD9-LX:  | UD9-LX Touch 41<br>UD9-LX 40                     |
| UD10-LX: | UD10-LX Touch 10<br>UD10-LX 10                   |

**IGEL Zero:**

IZ2-RFX

IZ2-HDX

IZ2-HORIZON

IZ3-RFX

IZ3-HDX

IZ3-HORIZON

- Component Versions 10.05.830(see page 2038)
- General Information 10.05.830(see page 2042)
- Known Issues 10.05.830(see page 2043)
- New Features 10.05.830(see page 2044)
- Resolved Issues 10.05.830(see page 2053)
- Security Fixes 10.05.830(see page 2057)



## Component Versions 10.05.830

• **Clients**

| <b>Product</b>                     | <b>Version</b>                  |
|------------------------------------|---------------------------------|
| Citrix HDX Realtime Media Engine   | 2.8.0-2235                      |
| Citrix Receiver                    | 13.10.0.20                      |
| Citrix Receiver                    | 13.5.0.10185126                 |
| Citrix Workspace App               | 19.3.0.5                        |
| deviceTRUST Citrix Channel         | 19.1.200.2                      |
| Ericom PowerTerm                   | 12.0.1.0.20170219.2-_dev_-34574 |
| Evidian AuthMgr                    | 1.5.6840                        |
| Evince PDF Viewer                  | 3.18.2-1ubuntu4.3               |
| FabulaTech USB for Remote Desktop  | 5.2.29                          |
| Firefox                            | 60.7.2                          |
| IBM iAccess Client Solutions       | 1.1.8.1                         |
| IGEL RDP Client                    | 2.2                             |
| Imprivata OneSign ProveID Embedded |                                 |
| deviceTRUST RDP Channel            | 19.1.200.2                      |
| Leostream Java Connect             | 3.3.7.0                         |
| NCP Secure Enterprise Client       | 5.10_rev40552                   |
| NX Client                          | 5.3.12                          |
| Open VPN                           | 2.3.10-1ubuntu2.1               |
| Oracle JRE                         | 1.8.0_202                       |
| Parallels Client (64 bit)          | 16.5.2.20595                    |



|                                         |                         |
|-----------------------------------------|-------------------------|
| Remote Viewer (RedHat Virtualization)   | 7.0-igel47              |
| Spice GTK (Red Hat Virtualization)      | 0.35                    |
| Spice Protocol (Red Hat Virtualization) | 0.12.14                 |
| Usbredir (Red Hat Virtualization)       | 0.8.0                   |
| Systancia AppliDis                      | 4.0.0.17                |
| Thinlinc Client                         | 4.9.0-5775              |
| ThinPrint Client                        | 7.5.88                  |
| Totem Media Player                      | 2.30.2                  |
| Parole Media Player                     | 1.0.1-0ubuntu1igel16    |
| VMware Horizon Client                   | 4.10.0-11053294         |
| VNC Viewer                              | 1.8.0+git20180123-igel1 |
| Voip Client Ekiga                       | 4.0.1                   |

- **Dictation**

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B048     |
| Olympus driver for dictation              | 20180621 |
| Philips Speech Driver                     | 12.6.36  |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.6    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.1.0    |

- **Smartcard**

|                                |         |
|--------------------------------|---------|
| PKCS#11 Library A.E.T SafeSign | 3.0.101 |
|--------------------------------|---------|



|                                           |                  |
|-------------------------------------------|------------------|
| PKCS#11 Library Athena IDProtect          | 623.07           |
| PKCS#11 Library cryptovision sc/interface | 7.1.9.620        |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0        |
| PKCS#11 Library SecMaker NetID            | 6.7.2.36         |
| Reader Driver ACS CCID                    | 1.1.5            |
| Reader Driver Gemalto eToken              | 10.0.37-0        |
| Reader Driver HID Global Omnikey          | 4.3.3            |
| Reader Driver Identive CCID               | 5.0.35           |
| Reader Driver Identive eHealth200         | 1.0.5            |
| Reader Driver Identive SCRKBC             | 5.0.24           |
| Reader Driver MUSCLE CCID                 | 1.4.28           |
| Reader Driver REINER SCT cyberJack        | 3.99.5final.SP11 |
| Resource Manager PC/SC Lite               | 1.8.23-1igel1    |
| Cherry USB2LAN Proxy                      | 3.0.0.6          |

- **System Components**

|                         |                              |
|-------------------------|------------------------------|
| OpenSSL                 | 1.0.2g-1ubuntu4.13           |
| OpenSSH Client          | 7.2p2-4ubuntu2.4             |
| OpenSSH Server          | 7.2p2-4ubuntu2.4             |
| Bluetooth stack (bluez) | 5.50-0ubuntu1igel5           |
| MESA OpenGL stack       | 18.2.1-1igel51               |
| VAAPI ABI Version       | 0.40                         |
| VDPAU Library version   | 1.1.1-3ubuntul               |
| Graphics Driver INTEL   | 2.99.917+git20181113-igel846 |



|                                 |                                |
|---------------------------------|--------------------------------|
| Graphics Driver ATI/RADEON      | 18.0.1-1igel831                |
| Graphics Driver ATI/AMDGPU      | 18.0.1-1igel831                |
| Graphics Driver VIA             | 5.76.52.92-009-005f78-20150730 |
| Graphics Driver FBDEV           | 0.5.0-1igel819                 |
| Graphics Driver VESA            | 2.3.4-1build2igel639           |
| Input Driver Evdev              | 2.10.5-1ubuntu1igel750         |
| Input Driver Elographics        | 1.4.1-1build5igel633           |
| Input Driver eGalax             | 2.5.5814                       |
| Input Driver Synaptics          | 1.9.0-1ubuntu1igel748          |
| Input Driver VMmouse            | 13.1.0-1ubuntu2igel635         |
| Input Driver Wacom              | 0.36.1-0ubuntu1igel813         |
| Kernel                          | 4.18.20 #mainline-ud-r2755     |
| Xorg X11 Server                 | 1.19.6-1ubuntu4igel838         |
| Xorg Xephyr                     | 1.19.6-1ubuntu4igel832         |
| CUPS printing daemon            | 2.1.3-4ubuntu0.7igel23         |
| PrinterLogic                    | 18.2.1.128                     |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1              |
| XFCE4 Windowmanager             | 4.12.3-1ubuntu2igel653         |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7        |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.2igel58   |
| ModemManager                    | 1.6.8-2igel1                   |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.1             |
| GStreamer 1.x                   | 1.14.2-1ubuntu1igel192         |



|                                              |        |
|----------------------------------------------|--------|
| Python2                                      | 2.7.12 |
| Python3                                      | 3.5.2  |
| <b>• Features with Limited IGEL Support</b>  |        |
| Mobile Device Access USB                     |        |
| VPN OpenConnect                              |        |
| Scanner support                              |        |
| VirtualBox                                   |        |
| <b>• Features with Limited Functionality</b> |        |
| Cisco JVDI Client                            | 12.1   |

## General Information 10.05.830

The following clients and features are not supported anymore:

- Citrix Receiver 12.1 and 13.1 - 13.4;
- Citrix Access Gateway Standard Plug-in;
- Dell vWorkspace Connector for Linux;
- Ericom PowerTerm Emulation 9 and 11;
- Ericom Webconnect;
- IGEL Legacy RDP Client (rdesktop);
- Virtual Bridges VERDE Client;
- PPTP VPN Support;
- IGEL Upgrade License Tool with IGEL Smartcard Token;
- Remote Management by setup.ini file transfer (TFTP);
- Remote Access via RSH;
- Legacy Philips Speech Driver;
- t-Systems TCOS Smartcard Support;
- DUS Series touchscreens;
- Elo serial touchscreens;
- IGEL smartcard without locking desktop;
- Video Hardware Acceleration Support is discontinued on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, UD10-LX 10;
- H.264 Hardware Acceleration Support is discontinued on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, UD10-LX 10;
- Storage Hotplug devices are not automatically removed anymore, instead they must be always ejected manually:
  - by panel tray icon;
  - by an icon in the 'In-Session Control Bar' (configurable at **IGEL Setup > User Interface > Desktop**);
  - by a 'Safely Remove Hardware' session (configurable at **IGEL Setup > Accessories**).

The following clients and features are not available in this release:



- Cherry eGK Channel;
- Open VPN Smartcard Support;
- Asian Input Methods;
- Composite Manager.

## Known Issues 10.05.830

### Citrix

- With activated DRI3 and an AMD GPU, Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **gstreamer1.0** which describe problems with **multimedia redirection of H264, MPEG1 and MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.  
As a workaround, insert the smartcard before starting StoreFront login.
- When using **Citrix Workspace App 18.10** in combination with **Philips Speech** driver, the session occasionally terminates improperly at logout and hangs.  
As a workaround, the usage of **Citrix Receiver 13.10** is recommended when Philips Speech driver is needed.
- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" > "For the entire screen".
- When **Expand the session over a self-selected number of monitors** (for **Multimonitor full-screen mode**) is used and Setup is restarted, **Restrict full-screen session to one monitor** is indicated and the monitor selection is greyed out. The functionality is available, only the notification in setup is broken.
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264 acceleration plugin**, the following registry key must be enabled:  
[More...](#)

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Range     | enabled / <u>disabled</u>                                        |

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

### VMware Horizon

- **External drives** mounted already before connection **do not appear in the remote desktop**.  
Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off.



In the IGEL Setup client, **drive mapping** can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping**.

It is also recommended to disable local **Storage Hotplug** under Setup > **Devices > Storage Devices > Storage Hotplug**.

- On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection entirely** or at least to **deny storage devices** by adding a filter to the USB class rules.

Furthermore, Horizon Client relies on the OS to mount the storage device itself. Enable local **Storage Hotplug** under Setup >**Devices > Storage Devices > Storage Hotplug**.

#### Parallels Client

- **Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode** it is necessary to connect to the **Parallels RAS** one time with FIPS support disabled.

#### Smartcard

- In some cases, there are instabilities when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice**: spice-xpi Firefox plugin is no longer supported. The **Console Invocation** has to allow **Native client** (auto is also possible) and it should start in fullscreen to prevent opening windows.

#### Hardware

- Suspend on **UD10** is disabled.

### New Features 10.05.830

#### Citrix

- Added support for **Citrix Workspace Launcher** functionality as described at <https://support.citrix.com/article/CTX237727>.
- Updated **Citrix HDX RTME** used for optimization of Skype for Business to version **2.8.0-2235**.
- Integrated **Citrix Workspace App 19.03**.
- Added: new registry key supports **1536-bit RSA keys for client authentication**.  
**More...**

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Enable RSA 1536 cipher suite          |
| Registry  | ica.allregions.enabl_rsa_1536         |
| Range     | <u>factory default</u> / false / true |

- Added: new registry key to enable different **cipher suites client authentication**.  
**More...**

|           |                                 |
|-----------|---------------------------------|
| Parameter | Enables different cipher suites |
|-----------|---------------------------------|



|                                                 |                                          |
|-------------------------------------------------|------------------------------------------|
| Registry                                        | <code>ica.allregions.sslciphers</code>   |
| Range                                           | <u>factory default</u> / ALL / GOV / COM |
| <b>Info:</b>                                    |                                          |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – GOV/ALL |                                          |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – GOV/ALL |                                          |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA – COM/ALL    |                                          |

## VMware Horizon

- Added possibility to easily evaluate **Horizon Blast decoder states**. By default, sessions are evaluated after the use and the result is put to the journal log. But it can also be used with GUI notifications at runtime.

## Driver

- Added registry keys to modify the Intel graphic driver usage of **framebuffer compression** and **power management**.

New registry keys:

[More...](#)

|                                         |                                                    |
|-----------------------------------------|----------------------------------------------------|
| Parameter                               | Power saving display C-States to use.              |
| Registry                                | <code>x.drivers.intel.dc_setting</code>            |
| Range                                   | <u>[Default]</u> [Disable] [Up to DC5] [Up to DC6] |
| <b>Info:</b> "Default" - driver default |                                                    |
| Parameter                               | Use framebuffer compression.                       |
| Registry                                | <code>x.drivers.intel.fbc_setting</code>           |
| Range                                   | <u>[Default]</u> [Disable]                         |
| <b>Info:</b> "Default" - driver default |                                                    |

## X11 system

- Added some registry keys to disable loading of **DRM kernel modules** (graphic).

New registry keys:

[More...](#)

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Disable the loading of the RADEON DRM driver. |
| Registry  | <code>x.drivers.ati.disable</code>            |
| Value     | <u>"0"</u>                                    |
| Parameter | Disable the loading of the AMDGPU DRM driver. |



|           |                                                  |
|-----------|--------------------------------------------------|
| Registry  | x.drivers.amdgpu.disable                         |
| Value     | <u>"0"</u>                                       |
| Parameter | Disable the loading of the i915 DRM driver.      |
| Registry  | x.drivers.intel.disable                          |
| Value     | <u>"0"</u>                                       |
| Parameter | Disable the loading of the NVIDIA kernel driver. |
| Registry  | x.drivers.nvidia.disable                         |
| Value     | <u>"0"</u>                                       |
| Parameter | Disable the loading of the NOUVEAU DRM driver.   |
| Registry  | x.drivers.nouveau.disable                        |
| Value     | <u>"0"</u>                                       |
| Parameter | Disable the loading of the QXL DRM driver.       |
| Registry  | x.drivers.qxl.disable                            |
| Value     | <u>"0"</u>                                       |
| Parameter | Disable the loading of the VMGFX DRM driver.     |
| Registry  | x.drivers.vmware.disable                         |
| Value     | <u>"0"</u>                                       |
| Parameter | Disable the loading of the VBOXVIDEO DRM driver. |
| Registry  | x.drivers.vboxvideo.disable                      |
| Value     | <u>"0"</u>                                       |

## IBM\_5250

- Improved **startup time** of IBM iAccess Client.
  - Improved **configuration** of IBM iAccess Client **via IGEL Setup.**
- More...**

|       |                                                                                         |
|-------|-----------------------------------------------------------------------------------------|
| Setup | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Connection > Advanced |
|-------|-----------------------------------------------------------------------------------------|



|           |                                                                                      |
|-----------|--------------------------------------------------------------------------------------|
| Parameter | Bypass signon                                                                        |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.ssoenabled</code>                           |
| Value     | <code>true/false</code>                                                              |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Font      |
| Parameter | Antialiasing                                                                         |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.textantialiasing</code>                     |
| Value     | <code>true/false</code>                                                              |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor    |
| Parameter | Allow blinking cursor                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.blinkcursor</code>                          |
| Value     | <code>true/false</code>                                                              |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor    |
| Parameter | Show blinking text with                                                              |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.blinkstate</code>                           |
| Value     | <code>[Blinking Text] [Host Color] [Mapped Color]</code>                             |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor    |
| Parameter | Blink Color                                                                          |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.blinkcolor_fg</code>                        |
| Value     | <code>#ffc800</code>                                                                 |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor    |
| Parameter | Blink Color Background                                                               |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.blinkcolor_bg</code>                        |
| Value     | <code>#000000</code>                                                                 |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Rule Line |
| Parameter | Rule Line                                                                            |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.ruleline</code>                             |
| Value     | <code>true/false</code>                                                              |



|           |                                                                                      |
|-----------|--------------------------------------------------------------------------------------|
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Rule Line |
| Parameter | Follow Cursor                                                                        |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.rulelinefollows</code>                      |
| Value     | <code>true/ false</code>                                                             |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Rule Line |
| Parameter | Style                                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.rulelinestyle</code>                        |
| Value     | <code>[Crosshair] [Vertical] [Horizontal]</code>                                     |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color     |
| Parameter | Green                                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fgn_fg</code>                         |
| Value     | <code>#00ff00</code>                                                                 |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color     |
| Parameter | Green Background                                                                     |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fgn_bg</code>                         |
| Value     | <code>#000000</code>                                                                 |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color     |
| Parameter | White                                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fwt_fg</code>                         |
| Value     | <code>#ffffff</code>                                                                 |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color     |
| Parameter | White Background                                                                     |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fwt_bg</code>                         |
| Value     | <code>#000000</code>                                                                 |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color     |
| Parameter | Red                                                                                  |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_frd_fg</code>                         |



|           |                                                                                  |
|-----------|----------------------------------------------------------------------------------|
| Value     | <u>#ff0000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Red Background                                                                   |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_frd_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Turquoise                                                                        |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_ftq_fg</code>                     |
| Value     | <u>#00ffff</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Turquoise Background                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_ftq_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Yellow                                                                           |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fyw_fg</code>                     |
| Value     | <u>#ffff00</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Yellow Background                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fyw_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Pink                                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fpk_fg</code>                     |
| Value     | <u>#ff00ff</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Pink Background                                                                  |



|           |                                                                                  |
|-----------|----------------------------------------------------------------------------------|
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fpk_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Blue                                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fbl_fg</code>                     |
| Value     | <u>#7890f0</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Blue Background                                                                  |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fbl_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Status Indicators                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_osi</code>                        |
| Value     | <u>#7890f0</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Information Indicators                                                           |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_oui</code>                        |
| Value     | <u>#ffffff</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Attention Indicators                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_oai</code>                        |
| Value     | <u>#ffff00</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Error Indicators                                                                 |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_oei</code>                        |
| Value     | <u>#ff0000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |



|           |                                                                                  |
|-----------|----------------------------------------------------------------------------------|
| Parameter | OIA Background                                                                   |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_oob</code>                        |
| Value     | <code>#000000</code>                                                             |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Screen Background                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_sbg</code>                        |
| Value     | <code>#000000</code>                                                             |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Highlight active field                                                           |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.actfieldhilite</code>                   |
| Value     | <code>true/ false</code>                                                         |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Active Field                                                                     |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_actf_fg</code>                    |
| Value     | <code>#000000</code>                                                             |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Active Field Background                                                          |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_actf_bg</code>                    |
| Value     | <code>#ffff00</code>                                                             |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Crosshair Ruler Color                                                            |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_crc</code>                        |
| Value     | <code>#00ff00</code>                                                             |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Column Separator                                                                 |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_ccs</code>                        |
| Value     | <code>#ffffff</code>                                                             |



|           |                                                                                              |
|-----------|----------------------------------------------------------------------------------------------|
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences                |
| Parameter | Start window maximized                                                                       |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.ismaximized</code>                                  |
| Value     | <u>true/false</u>                                                                            |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences > Keyboard     |
| Parameter | Keyboard Remapping File                                                                      |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.keyremapfile</code>                                 |
| Value     | <u>IBMi.kmp</u>                                                                              |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences > Popup Keypad |
| Parameter | Popup Keypad File                                                                            |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.poppadfile</code>                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences > Toolbar      |
| Parameter | Toolbar File                                                                                 |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.toolbarfile</code>                                  |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup                                   |
| Parameter | Open new sessions in a new tab                                                               |
| Registry  | <code>ibm.iaccess.acssm.opensessionintab</code>                                              |
| Value     | <u>true/false</u>                                                                            |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup                                   |
| Parameter | Always display the tab bar                                                                   |
| Registry  | <code>ibm.iaccess.acssm.alwaysshownabar</code>                                               |
| Value     | <u>true/false</u>                                                                            |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup                                   |
| Parameter | Switch to new tab when created                                                               |
| Registry  | <code>ibm.iaccess.acssm.switchtonewtab</code>                                                |
| Value     | <u>true/false</u>                                                                            |



|           |                                                            |
|-----------|------------------------------------------------------------|
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup |
| Parameter | Send a warning when closing multiple tabs                  |
| Registry  | <code>ibm.iaccess.acssm.closemultipletabwarning</code>     |
| Value     | <u>true</u> / <u>false</u>                                 |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup |
| Parameter | Do not start tabbed sessions until the tab is selected     |
| Registry  | <code>ibm.iaccess.acssm.tabdelayedstart</code>             |
| Value     | <u>true</u> / <u>false</u>                                 |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup |
| Parameter | New Tab Action                                             |
| Registry  | <code>ibm.iaccess.acssm.newtabaction</code>                |
| Value     | [Disable and Hide] [Run the Same] [Run Other...]           |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup |
| Parameter | Tab Placement                                              |
| Registry  | <code>ibm.iaccess.acssm.tabplacement</code>                |
| Value     | [Top] [Bottom] [Left] [Right]                              |

## Resolved Issues 10.05.830

### Firefox

- Fixed not working **browserglobal.app.local\_subdirs\_whitelist**.
- Fixed **print hotkey disable** option with Firefox 60+.

### RDP/IGEL RDP Client 2

- Fixed **smart card redirection in RDP: SCardGetAttrib** was failing if **pbAttr** was NULL. The fix should help running Dutch Zorg-ID applications.

### VMware Horizon

- Fixed: the configuration choice to **use the relative mouse feature**.

### Citrix

- Citrix Workspace App 19.03: Improved **USB redirection handling**.
- Issue solved: **Online meeting in VDI**: "enable webcam will cut the audio streaming".
- Fixed **stability issues** with Citrix Browser Content Redirection.



## Citrix Receiver 13

- Added a switch to enable the **possibility to launch multiple desktop sessions** with **RTME** and **H264 acceleration**. This switch should not be used when "Enable Secure ICA" is active for the specific delivery group.

**More...**

|          |                           |
|----------|---------------------------|
| Registry | ica.workaround-dual-rtme  |
| Value    | enabled / <u>disabled</u> |

## Network

- Fixed: The **second Ethernet interface** did not get configured when the first one was disabled.
- Added a possibility to switch between the third party **r8168** and **kernel r8169 realtek network driver**.

New registry key:

**More...**

|                                        |                                     |
|----------------------------------------|-------------------------------------|
| Parameter                              | Use thirdparty r8168 kernel module. |
| Registry                               | network.drivers.r8169.prefer_r8168  |
| Range                                  | [Auto] [Yes] [No]                   |
| Info: "Auto" (use r8169 in most cases) |                                     |

- Added a possibility to **choose the variant of the realtek r8168 driver**.

New registry key:

**More...**

|                                          |                                                                       |
|------------------------------------------|-----------------------------------------------------------------------|
| Parameter                                | Choose realtek r8168 variant (only if <b>prefer r8168</b> is chosen). |
| Registry                                 | network.drivers.r8169.r8168_variant                                   |
| Range                                    | [Default] [No NAPI] [NAPI]                                            |
| Info: "Default" (use NAPI in most cases) |                                                                       |

## Base system

- Fixed: **System logout** waits for Citrix logout now.
- Fixed: **Migration tool** did not start with the **Spanish** language setting.
- Added new registry key to set **USB quirks**.

**More...**

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | Set XHCI USB quirks to fix some hardware issues. |
| Registry  | system.kernel.bootparams.xhci-hcd_quirks         |



|       |                                                                                              |
|-------|----------------------------------------------------------------------------------------------|
| Range | [No quirk] [Spurious Reboot quirk] [Spurious Wakeup quirk]<br>[Spurious Reboot Wakeup quirk] |
|-------|----------------------------------------------------------------------------------------------|

- **Lenovo ThinkCentre M73** needs the system.kernel.bootparams.xhci-hcd\_quirks registry key set to "Spurious Reboot quirk" to fix reboot after shutdown problem.

X11 system

- There is now a **registry key to ignore a 3Dconnexion SpaceMouse** for IGEL graphical use (X11). If activated, the SpaceMouse is only passed through to the desktop session. If disabled, it acts also as the standard mouse.

[More...](#)

|           |                                                           |
|-----------|-----------------------------------------------------------|
| Parameter | Deactivates a 3Dconnexion SpaceMouse as a standard mouse. |
| Registry  | userinterface.mouse.spacemouse.x11_ignore                 |
| Value     | <u>enabled</u> / disabled                                 |

- The following **SpaceMouse** products are included:

[More...](#)

| VID    | PID    | Vendor         | Product                                  |
|--------|--------|----------------|------------------------------------------|
| 0x046D | 0xC603 | Logitech, Inc. | 3Dconnexion SpaceMouse Plus XT           |
| 0x046D | 0xC605 | Logitech, Inc. | 3Dconnexion CADman                       |
| 0x046D | 0xC606 | Logitech, Inc. | 3Dconnexion SpaceMouse Classic           |
| 0x046D | 0xC621 | Logitech, Inc. | 3Dconnexion SpaceBall 5000               |
| 0x046D | 0xC623 | Logitech, Inc. | 3Dconnexion SpaceTraveller 3D Mouse      |
| 0x046D | 0xC625 | Logitech, Inc. | 3Dconnexion SpacePilot 3D Mouse          |
| 0x046D | 0xC626 | Logitech, Inc. | 3Dconnexion SpaceNavigator 3D Mouse      |
| 0x046D | 0xC627 | Logitech, Inc. | 3Dconnexion SpaceExplorer 3D Mouse       |
| 0x046D | 0xC628 | Logitech, Inc. | 3Dconnexion SpaceNavigator for Notebooks |
| 0x046D | 0xC629 | Logitech, Inc. | 3Dconnexion SpacePilot Pro 3D Mouse      |
| 0x046D | 0xC62B | Logitech, Inc. | 3Dconnexion SpaceMouse Pro               |
| 0x256F | **     | 3Dconnexion    | SpaceMouse                               |

- **USB device reset** via USB powercycle is now available on **UD6/UD7**.
- Fixed problems with **internal graphic cards** and **NVIDIA graphic cards**.
- Fixed **Display Switch** utility not starting with some translations.
- Fixed an issue with the **noDDC mode** not always working as expected.
- Fixed some **multimonitor** (>4) issues with **Nvidia** graphic cards.
- Updated **DisplayLink driver** to version **5.1.26** to solve some startup issues.

Driver

- Fixed not working **WACOM** device **DTU-1141B**.

Hardware



- Fixed **not working network** on Beckhoff CB3163, CB6263 and CB6363 systems.
- Fixed **not working network** on Lex 3I380D.
- Fixed **black screen issue** with some monitors and 2560x1440 resolution (occurred on UD2 LX50).
- Added possibility to **change** some **DRM settings** and limit the **DisplayPort lane bandwidth** on Intel devices.
- Added new registry keys:  
[More...](#)

|                                                           |                                                                  |
|-----------------------------------------------------------|------------------------------------------------------------------|
| Parameter                                                 | Use best graphic mode for all screens on console.                |
| Registry                                                  | x.drivers.kms.best_console_mode                                  |
| Range                                                     | [Default] [Enabled] [Disabled]                                   |
| Info: "Default" is enabled in most cases.                 |                                                                  |
| Parameter                                                 | Limit the maximum console resolution width to this value.        |
| Registry                                                  | x.drivers.kms.max_console_width                                  |
| Type                                                      | Integer                                                          |
| Value                                                     | "0"                                                              |
| Info: "0" means default setting. Use the default setting. |                                                                  |
| Parameter                                                 | Limit the maximum console resolution height to this value.       |
| Registry                                                  | x.drivers.kms.max_console_height                                 |
| Type                                                      | Integer                                                          |
| Value                                                     | "0"                                                              |
| Info: "0" means default setting. Use the default setting. |                                                                  |
| Parameter                                                 | Set graphic kernel driver debug level.                           |
| Registry                                                  | x.drivers.kms.debug_level                                        |
| Range                                                     | [No debug] [Basic] [Basic + core] [Basic + core + atomic] [Full] |
| Info: Warning log will grow very fast.                    |                                                                  |
| Only for Intel i915 driver:                               |                                                                  |
| Parameter                                                 | Limit the maximum DisplayPort lane link rate.                    |
| Registry                                                  | x.drivers.intel.max_dp_link_rate                                 |



|       |                                                                                                   |
|-------|---------------------------------------------------------------------------------------------------|
| Range | [default] [1.62Gbps] [2.16Gbps] [2.7Gbps] [3.24Gbps]<br>[4.32Gbps] [5.4Gbps] [6.48Gbps] [8.1Gbps] |
|-------|---------------------------------------------------------------------------------------------------|

Info: "Default" means hardware default limit.

## Security Fixes 10.05.830

### Firefox

- Updated Mozilla **Firefox** to version **60.7.2 ESR**.
- Fixed **mfsa2019-19** security issue CVE-2019-11708.
- Fixed **mfsa2019-18** security issue CVE-2019-11707.
- Fixed **mfsa2019-10** security issues CVE-2019-9810 and CVE-2019-9813.
- Fixed **mfsa2019-08** security issues.

[More...](#)

CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793,  
CVE-2019-9795, CVE-2019-9796, CVE-2018-18506, CVE-2019-9788.

- Fixed **mfsa2019-05** security issues CVE-2018-18356 and CVE-2019-5785.
- Fixed **mfsa2019-02** security issues CVE-2018-18500, CVE-2018-18505 and CVE-2018-18501.
- Fixed **mfsa2018-30** security issues.

[More...](#)

CVE-2018-17466, CVE-2018-18492, CVE-2018-18493,  
CVE-2018-18494, CVE-2018-18498, CVE-2018-12405.

### Base system

- Fixed kernel TCP vulnerabilities **CVE-2019-11477**: SACK Panic, **CVE-2019-11478**: SACK Slowness and **CVE-2019-11479**: Excess Resource Consumption Due to Low MSS Values.
- Changed **minimally allowed MSS size** to '1000' to prevent possible Denial-of-Service attacks.
- Updated **libwebkit2gtk-4.0-37** to version **1.24.2**.

[More...](#)

CVE-2019-8595, CVE-2019-8607, CVE-2019-8615, CVE-2019-6251,  
CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378,  
CVE-2018-4382, CVE-2018-4392, CVE-2018-4416, CVE-2018-4345,  
CVE-2018-4386, CVE-2018-4372

## 7.25.2 IGEL Universal Desktop OS 3

### Supported Hardware:

<https://kb.igel.com/igelos/en/devices-supported-by-udc3-and-ud-pocket-3117174.html>

- 
- Component Versions 10.05.830(see page 2058)
  - General Information 10.05.830(see page 2062)
  - Known Issues 10.05.830(see page 2063)



- [New Features 10.05.830\(see page 2064\)](#)
- [Resolved Issues 10.05.830\(see page 2073\)](#)
- [Security Fixes 10.05.830\(see page 2077\)](#)

## Component Versions 10.05.830

- **Clients**

| <b>Product</b>                     | <b>Version</b>                  |
|------------------------------------|---------------------------------|
| Citrix HDX Realtime Media Engine   | 2.8.0-2235                      |
| Citrix Receiver                    | 13.10.0.20                      |
| Citrix Receiver                    | 13.5.0.10185126                 |
| Citrix Workspace App               | 19.3.0.5                        |
| deviceTRUST Citrix Channel         | 19.1.200.2                      |
| Ericom PowerTerm                   | 12.0.1.0.20170219.2-_dev_-34574 |
| Evidian AuthMgr                    | 1.5.6840                        |
| Evince PDF Viewer                  | 3.18.2-1ubuntu4.3               |
| FabulaTech USB for Remote Desktop  | 5.2.29                          |
| Firefox                            | 60.7.2                          |
| IBM iAccess Client Solutions       | 1.1.8.1                         |
| IGEL RDP Client                    | 2.2                             |
| Imprivata OneSign ProveID Embedded |                                 |
| deviceTRUST RDP Channel            | 19.1.200.2                      |
| Leostream Java Connect             | 3.3.7.0                         |
| NCP Secure Enterprise Client       | 5.10_rev40552                   |
| NX Client                          | 5.3.12                          |
| Open VPN                           | 2.3.10-1ubuntu2.1               |



|                                         |                         |
|-----------------------------------------|-------------------------|
| Oracle JRE                              | 1.8.0_202               |
| Parallels Client (64 bit)               | 16.5.2.20595            |
| Remote Viewer (RedHat Virtualization)   | 7.0-igel47              |
| Spice GTK (Red Hat Virtualization)      | 0.35                    |
| Spice Protocol (Red Hat Virtualization) | 0.12.14                 |
| Usbredir (Red Hat Virtualization)       | 0.8.0                   |
| Systancia AppliDis                      | 4.0.0.17                |
| ThinLinc Client                         | 4.9.0-5775              |
| ThinPrint Client                        | 7.5.88                  |
| Totem Media Player                      | 2.30.2                  |
| Parole Media Player                     | 1.0.1-0ubuntu1igel16    |
| VNC Viewer                              | 1.8.0+git20180123-igel1 |
| VMware Horizon Client                   | 4.10.0-11053294         |
| Voip Client Ekiga                       | 4.0.1                   |

- **Dictation**

|                                           |          |
|-------------------------------------------|----------|
| Diktamen driver for dictation             |          |
| Grundig Business Systems dictation driver |          |
| Nuance Audio Extensions for dictation     | B048     |
| Olympus driver for dictation              | 20180621 |
| Philips Speech Driver                     | 12.6.36  |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.6    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.1.0    |



- **Smartcard**

|                                           |                  |
|-------------------------------------------|------------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101          |
| PKCS#11 Library Athena IDProtect          | 623.07           |
| PKCS#11 Library cryptovision sc/interface | 7.1.9.620        |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0        |
| PKCS#11 Library SecMaker NetID            | 6.7.2.36         |
| Reader Driver ACS CCID                    | 1.1.5            |
| Reader Driver Gemalto eToken              | 10.0.37-0        |
| Reader Driver HID Global Omnikey          | 4.3.3            |
| Reader Driver Identive CCID               | 5.0.35           |
| Reader Driver Identive eHealth200         | 1.0.5            |
| Reader Driver Identive SCRKBC             | 5.0.24           |
| Reader Driver MUSCLE CCID                 | 1.4.28           |
| Reader Driver REINER SCT cyberJack        | 3.99.5final.sp11 |
| Resource Manager PC/SC Lite               | 1.8.23-1igel1    |
| Cherry USB2LAN Proxy                      | 3.0.0.6          |

- **System Components**

|                         |                    |
|-------------------------|--------------------|
| OpenSSL                 | 1.0.2g-1ubuntu4.13 |
| OpenSSH Client          | 7.2p2-4ubuntu2.4   |
| OpenSSH Server          | 7.2p2-4ubuntu2.4   |
| Bluetooth stack (bluez) | 5.50-0ubuntu1igel5 |
| MESA OpenGL stack       | 18.2.1-1igel51     |
| VAAPI ABI Version       | 0.40               |



|                                         |                              |
|-----------------------------------------|------------------------------|
| VDPAU Library version                   | 1.1.1-3ubuntu1               |
| Graphics Driver INTEL                   | 2.99.917+git20181113-igel846 |
| Graphics Driver ATI/RADEON              | 18.0.1-1igel831              |
| Graphics Driver ATI/AMDGPU              | 18.0.1-1igel83               |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.15-2igel775              |
| Graphics Driver Nvidia                  | 390.87-0ubuntu1              |
| Graphics Driver Vboxvideo               | 5.2.18-dfsg-2igel17          |
| Graphics Driver VMware                  | 13.3.0-2igel812              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1igel775         |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |
| Graphics Driver VESA                    | 2.3.4-1build2igel639         |
| Input Driver Evdev                      | 2.10.5-1ubuntu1igel750       |
| Input Driver Elographics                | 1.4.1-1build5igel633         |
| Input Driver eGalax                     | 2.5.5814                     |
| Input Driver Synaptics                  | 1.9.0-1ubuntu1igel748        |
| Input Driver VMMouse                    | 13.1.0-1ubuntu2igel635       |
| Input Driver Wacom                      | 0.36.1-0ubuntu1igel813       |
| Kernel                                  | 4.18.20 #mainline-udos-r2755 |
| Xorg X11 Server                         | 1.19.6-1ubuntu4igel838       |
| Xorg Xephyr                             | 1.19.6-1ubuntu4igel832       |
| CUPS Printing Daemon                    | 2.1.3-4ubuntu0.7igel23       |
| PrinterLogic                            | 18.2.1.128                   |
| Lightdm Graphical Login Manager         | 1.18.3-0ubuntu1.1            |
| XFCE4 Window Manager                    | 4.12.3-1ubuntu2igel653       |



|                 |                              |
|-----------------|------------------------------|
| ISC DHCP Client | 4.3.3-5ubuntu12.10igel7      |
| NetworkManager  | 1.2.6-0ubuntu0.16.04.2igel58 |
| ModemManager    | 1.6.8-2igel1                 |
| GStreamer 0.10  | 0.10.36-2ubuntu0.1           |
| GStreamer 1.x   | 1.14.2-1ubuntu1igel192       |
| Python2         | 2.7.12                       |
| Python3         | 3.5.2                        |

- **Features with Limited IGEL Support**

|                          |
|--------------------------|
| Mobile Device Access USB |
|--------------------------|

|                 |
|-----------------|
| VPN OpenConnect |
|-----------------|

|                 |
|-----------------|
| Scanner support |
|-----------------|

|            |
|------------|
| VirtualBox |
|------------|

- **Features with Limited Functionality**

|                   |      |
|-------------------|------|
| Cisco JVDI Client | 12.1 |
|-------------------|------|

## General Information 10.05.830

The following clients and features are not supported anymore:

- Citrix Receiver 12.1 and 13.1-13.4
- Citrix Access Gateway Standard Plug-in
- Dell vWorkspace Connector for Linux
- Ericom PowerTerm Emulation 9 and 11
- Ericom Webconnect
- IGEL Legacy RDP Client (rdesktop)
- Virtual Bridges VERDE Client
- PPTP VPN Support
- IGEL Upgrade License Tool with IGEL Smartcard Token
- Remote Management by setup.ini file transfer (TFTP)
- Remote Access via RSH
- Legacy Philips Speech Driver
- t-Systems TCOS Smartcard Support
- DUS Series touchscreens
- Elo serial touchscreens
- IGEL smartcard without locking desktop
- VIA Graphics Support
- Storage Hotplug devices are not automatically removed anymore, instead they must be always ejected manually:



- by panel tray icon;
- by an icon in the 'In-Session Control Bar' (configurable at **IGEL Setup > User Interface > Desktop**);
- by a 'Safely Remove Hardware' session (configurable at **IGEL Setup > Accessories**).

The following clients and features are not available in this release:

- Cherry eGK Channel
- Open VPN Smartcard Support
- Asian Input Methods
- Composite Manager

## Known Issues 10.05.830

### Citrix

- With activated **DRI3** and an AMD GPU Citrix **H264 acceleration plugin** could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer 1.0** which describe problems with **multimedia redirection** of H264, MPEG1 and MPEG2. GStreamer 1.0 is used if browser content redirection is active.
- Browser content redirection does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront Login** with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is inserted after start of login.  
As a workaround, insert the smartcard before starting StoreFront Login.
- When using **Citrix Workspace App 18.10** in combination with **Philips Speech driver**, the **session** occasionally **terminates improperly at logout** and hangs.  
As a workaround, the usage of Citrix Receiver 13.10 is recommended when Philips Speech driver is needed.
- **Citrix H264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" > "For the entire screen".
- When "Expand the session over a self-selected number of monitors" (for "Multimonitor full-screen mode") is used and Setup is restarted, "Restrict full-screen session to one monitor" is indicated and the **monitor selection** is **greyed out**. The functionality is available, only the notification in Setup is broken.
- To launch **multiple desktop sessions** with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following **registry key** must be enabled:  
**More...**

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Activate workaround for dual RTME sessions and H264 acceleration |
| Registry  | ica.workaround-dual-rtme                                         |
| Range     | enabled / <u>disabled</u>                                        |



This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

#### VMware Horizon

- **External drives** mounted already before connection **do not appear in the remote desktop**.  
Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices, you should note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off.  
In the **IGEL Setup** client drive mapping can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**.  
It is also recommended to **disable** local **Storage Hotplug** under Setup > **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection** entirely or at least to **deny storage devices** by adding a filter to the USB class rules. Furthermore, since Horizon Client relies on the OS to mount the storage devices itself, go to Setup > **Devices > Storage Devices > Storage Hotplug**, enable **dynamic drive mapping** and put **number of storage hotplug devices** to at least **1**.

#### Parallels Client

- **Native USB redirection** does not work with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** one time with FIPS support disabled.

#### Smartcard

- In some cases, there are instabilities when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice**: spice-xpi firefox plugin is no longer supported. The **Console Invocation** has to allow **Native client** (auto is also possible) and it should start in fullscreen to prevent opening windows.

#### Base system

- **Display resolution and rotation** could not be changed with NVIDIA GPU driver via tcsetup.

#### Multimedia

- **Multimedia redirection** with **GStreamer** could fail with Nouveau GPU driver.

## New Features 10.05.830

#### Citrix

- Added support for **Citrix Workspace Launcher** functionality as described at <https://support.citrix.com/article/CTX237727>.
- Updated **Citrix HDX RTME** used for optimization of Skype for Business to version **2.8.0-2235**.



- Integrated **Citrix Workspace App 19.03**.
- Added: new registry key supports **1536-bit RSA keys for client authentication**.  
[More...](#)

|                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                          |           |                                 |          |                           |       |                                          |                                                                                                                                                             |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|-----------|---------------------------------|----------|---------------------------|-------|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| Parameter                                                                                                                                                                                                                                                                                                                                                                                                                              | Enable RSA 1536 cipher suite             |           |                                 |          |                           |       |                                          |                                                                                                                                                             |  |
| Registry                                                                                                                                                                                                                                                                                                                                                                                                                               | ica.allregions.enable_rsa_1536           |           |                                 |          |                           |       |                                          |                                                                                                                                                             |  |
| Range                                                                                                                                                                                                                                                                                                                                                                                                                                  | <u>factory default</u> / false / true    |           |                                 |          |                           |       |                                          |                                                                                                                                                             |  |
| • Added: new registry key to enable different <b>cipher suites client authentication</b> .<br><a href="#">More...</a>                                                                                                                                                                                                                                                                                                                  |                                          |           |                                 |          |                           |       |                                          |                                                                                                                                                             |  |
| <table border="1"> <tr> <td>Parameter</td><td>Enables different cipher suites</td></tr> <tr> <td>Registry</td><td>ica.allregions.sslciphers</td></tr> <tr> <td>Range</td><td><u>factory default</u> / ALL / GOV / COM</td></tr> <tr> <td colspan="2">Info:<br/>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – GOV/ALL<br/>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – GOV/ALL<br/>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA – COM/ALL</td></tr> </table> |                                          | Parameter | Enables different cipher suites | Registry | ica.allregions.sslciphers | Range | <u>factory default</u> / ALL / GOV / COM | Info:<br>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – GOV/ALL<br>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – GOV/ALL<br>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA – COM/ALL |  |
| Parameter                                                                                                                                                                                                                                                                                                                                                                                                                              | Enables different cipher suites          |           |                                 |          |                           |       |                                          |                                                                                                                                                             |  |
| Registry                                                                                                                                                                                                                                                                                                                                                                                                                               | ica.allregions.sslciphers                |           |                                 |          |                           |       |                                          |                                                                                                                                                             |  |
| Range                                                                                                                                                                                                                                                                                                                                                                                                                                  | <u>factory default</u> / ALL / GOV / COM |           |                                 |          |                           |       |                                          |                                                                                                                                                             |  |
| Info:<br>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – GOV/ALL<br>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – GOV/ALL<br>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA – COM/ALL                                                                                                                                                                                                                                                                            |                                          |           |                                 |          |                           |       |                                          |                                                                                                                                                             |  |

#### VMware Horizon

- Added possibility to easily evaluate **Horizon Blast decoder states**. By default, sessions are evaluated after the use and the result is put to the journal log. But it can also be used with GUI notifications at runtime.

#### Driver

- Added registry keys to modify the Intel graphic driver usage of **framebuffer compression** and **power management**.

New registry keys:

[More...](#)

|                                                                                                                                                                                                                                                                                           |                                                    |           |                              |          |                             |       |                            |                                  |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|-----------|------------------------------|----------|-----------------------------|-------|----------------------------|----------------------------------|--|
| Parameter                                                                                                                                                                                                                                                                                 | Power saving display C-States to use.              |           |                              |          |                             |       |                            |                                  |  |
| Registry                                                                                                                                                                                                                                                                                  | x.drivers.intel.dc_setting                         |           |                              |          |                             |       |                            |                                  |  |
| Range                                                                                                                                                                                                                                                                                     | <u>[Default]</u> [Disable] [Up to DC5] [Up to DC6] |           |                              |          |                             |       |                            |                                  |  |
| Info: "Default" - driver default                                                                                                                                                                                                                                                          |                                                    |           |                              |          |                             |       |                            |                                  |  |
| <table border="1"> <tr> <td>Parameter</td><td>Use framebuffer compression.</td></tr> <tr> <td>Registry</td><td>x.drivers.intel.fbc_setting</td></tr> <tr> <td>Range</td><td><u>[Default]</u> [Disable]</td></tr> <tr> <td colspan="2">Info: "Default" - driver default</td></tr> </table> |                                                    | Parameter | Use framebuffer compression. | Registry | x.drivers.intel.fbc_setting | Range | <u>[Default]</u> [Disable] | Info: "Default" - driver default |  |
| Parameter                                                                                                                                                                                                                                                                                 | Use framebuffer compression.                       |           |                              |          |                             |       |                            |                                  |  |
| Registry                                                                                                                                                                                                                                                                                  | x.drivers.intel.fbc_setting                        |           |                              |          |                             |       |                            |                                  |  |
| Range                                                                                                                                                                                                                                                                                     | <u>[Default]</u> [Disable]                         |           |                              |          |                             |       |                            |                                  |  |
| Info: "Default" - driver default                                                                                                                                                                                                                                                          |                                                    |           |                              |          |                             |       |                            |                                  |  |



## X11 system

- Added some registry keys to disable loading of **DRM kernel modules** (graphic).

New registry keys:

[More...](#)

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | Disable the loading of the RADEON DRM driver.    |
| Registry  | x.drivers.ati.disable                            |
| Value     | <u>"0"</u>                                       |
| Parameter | Disable the loading of the AMDGPU DRM driver.    |
| Registry  | x.drivers.amdgpu.disable                         |
| Value     | <u>"0"</u>                                       |
| Parameter | Disable the loading of the i915 DRM driver.      |
| Registry  | x.drivers.intel.disable                          |
| Value     | <u>"0"</u>                                       |
| Parameter | Disable the loading of the NVIDIA kernel driver. |
| Registry  | x.drivers.nvidia.disable                         |
| Value     | <u>"0"</u>                                       |
| Parameter | Disable the loading of the NOUVEAU DRM driver.   |
| Registry  | x.drivers.nouveau.disable                        |
| Value     | <u>"0"</u>                                       |
| Parameter | Disable the loading of the QXL DRM driver.       |
| Registry  | x.drivers.qxl.disable                            |
| Value     | <u>"0"</u>                                       |
| Parameter | Disable the loading of the VMGFX DRM driver.     |
| Registry  | x.drivers.vmware.disable                         |
| Value     | <u>"0"</u>                                       |
| Parameter | Disable the loading of the VBOXVIDEO DRM driver. |



|          |                             |
|----------|-----------------------------|
| Registry | x.drivers.vboxvideo.disable |
| Value    | <u>"0"</u>                  |

## IBM\_5250

- Improved **startup time** of IBM iAccess Client.
- Improved **configuration** of IBM iAccess Client **via IGEL Setup**.

**More...**

|           |                                                                                         |
|-----------|-----------------------------------------------------------------------------------------|
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Connection > Advanced |
| Parameter | Bypass signon                                                                           |
| Registry  | sessions.iaccess<NR>.options.ssoenabled                                                 |
| Value     | true/ <u>false</u>                                                                      |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Font         |
| Parameter | Antialiasing                                                                            |
| Registry  | sessions.iaccess<NR>.options.textantialiasing                                           |
| Value     | true/ <u>false</u>                                                                      |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor       |
| Parameter | Allow blinking cursor                                                                   |
| Registry  | sessions.iaccess<NR>.options.blinkcursor                                                |
| Value     | true/ <u>false</u>                                                                      |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor       |
| Parameter | Show blinking text with                                                                 |
| Registry  | sessions.iaccess<NR>.options.blinkstate                                                 |
| Value     | [Blinking Text] [ <u>Host Color</u> ] [Mapped Color]                                    |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor       |
| Parameter | Blink Color                                                                             |
| Registry  | sessions.iaccess<NR>.options.blinkcolor_fg                                              |
| Value     | #ffc800                                                                                 |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor       |



|           |                                                                                      |
|-----------|--------------------------------------------------------------------------------------|
| Parameter | Blink Color Background                                                               |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.blinkcolor_bg</code>                        |
| Value     | <code>#000000</code>                                                                 |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Rule Line |
| Parameter | Rule Line                                                                            |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.ruleline</code>                             |
| Value     | <code>true/ false</code>                                                             |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Rule Line |
| Parameter | Follow Cursor                                                                        |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.rulelinefollows</code>                      |
| Value     | <code>true/ false</code>                                                             |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Rule Line |
| Parameter | Style                                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.rulelinestyle</code>                        |
| Value     | <code>[Crosshair] [Vertical] [Horizontal]</code>                                     |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color     |
| Parameter | Green                                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fgn_fg</code>                         |
| Value     | <code>#00ff00</code>                                                                 |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color     |
| Parameter | Green Background                                                                     |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fgn_bg</code>                         |
| Value     | <code>#000000</code>                                                                 |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color     |
| Parameter | White                                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fwt_fg</code>                         |
| Value     | <code>#ffffff</code>                                                                 |



|           |                                                                                  |
|-----------|----------------------------------------------------------------------------------|
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | White Background                                                                 |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fwt_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Red                                                                              |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_frd_fg</code>                     |
| Value     | <u>#ff0000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Red Background                                                                   |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_frd_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Turquoise                                                                        |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_ftq_fg</code>                     |
| Value     | <u>#00ffff</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Turquoise Background                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_ftq_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Yellow                                                                           |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fyw_fg</code>                     |
| Value     | <u>#ffff00</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Yellow Background                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fyw_bg</code>                     |



|           |                                                                                  |
|-----------|----------------------------------------------------------------------------------|
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Pink                                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fpk_fg</code>                     |
| Value     | <u>#ff00ff</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Pink Background                                                                  |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fpk_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Blue                                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fbl_fg</code>                     |
| Value     | <u>#7890f0</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Blue Background                                                                  |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_fbl_bg</code>                     |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Status Indicators                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_osi</code>                        |
| Value     | <u>#7890f0</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Information Indicators                                                           |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_oui</code>                        |
| Value     | <u>#ffffff</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Attention Indicators                                                             |



|           |                                                                                  |
|-----------|----------------------------------------------------------------------------------|
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_oai</code>                        |
| Value     | <u>#ffff00</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Error Indicators                                                                 |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_oei</code>                        |
| Value     | <u>#ff0000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | OIA Background                                                                   |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_oob</code>                        |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Screen Background                                                                |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_sbg</code>                        |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Highlight active field                                                           |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.actfieldhilite</code>                   |
| Value     | <u>true/ false</u>                                                               |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Active Field                                                                     |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_actf_fg</code>                    |
| Value     | <u>#000000</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |
| Parameter | Active Field Background                                                          |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_actf_bg</code>                    |
| Value     | <u>#ffff00</u>                                                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color |



|           |                                                                                              |
|-----------|----------------------------------------------------------------------------------------------|
| Parameter | Crosshair Ruler Color                                                                        |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_crc</code>                                    |
| Value     | <code>#00ff00</code>                                                                         |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color             |
| Parameter | Column Separator                                                                             |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.color_ccs</code>                                    |
| Value     | <code>#ffffff</code>                                                                         |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences                |
| Parameter | Start window maximized                                                                       |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.ismaximized</code>                                  |
| Value     | <code>true/ false</code>                                                                     |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences > Keyboard     |
| Parameter | Keyboard Remapping File                                                                      |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.keyremapfile</code>                                 |
| Value     | <code>IBMi.kmp</code>                                                                        |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences > Popup Keypad |
| Parameter | Popup Keypad File                                                                            |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.poppadfile</code>                                   |
| Setup     | Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences > Toolbar      |
| Parameter | Toolbar File                                                                                 |
| Registry  | <code>sessions.iaccess&lt;NR&gt;.options.toolbarfile</code>                                  |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup                                   |
| Parameter | Open new sessions in a new tab                                                               |
| Registry  | <code>ibm.iaccess.acssm.opensessionintab</code>                                              |
| Value     | <code>true/ false</code>                                                                     |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup                                   |



|           |                                                            |
|-----------|------------------------------------------------------------|
| Parameter | Always display the tab bar                                 |
| Registry  | <code>ibm.iaccess.acssm.alwaysshownabar</code>             |
| Value     | <u>true/ false</u>                                         |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup |
| Parameter | Switch to new tab when created                             |
| Registry  | <code>ibm.iaccess.acssm.switchtonewtab</code>              |
| Value     | <u>true/ false</u>                                         |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup |
| Parameter | Send a warning when closing multiple tabs                  |
| Registry  | <code>ibm.iaccess.acssm.closemultipletabwarning</code>     |
| Value     | <u>true/ false</u>                                         |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup |
| Parameter | Do not start tabbed sessions until the tab is selected     |
| Registry  | <code>ibm.iaccess.acssm.tabdelayedstart</code>             |
| Value     | <u>true/ false</u>                                         |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup |
| Parameter | New Tab Action                                             |
| Registry  | <code>ibm.iaccess.acssm.newtabaction</code>                |
| Value     | [Disable and Hide] [Run the Same] [Run Other...]           |
| Setup     | Sessions > IBM iAccess Client > iAccess Global > Tab Setup |
| Parameter | Tab Placement                                              |
| Registry  | <code>ibm.iaccess.acssm.tabplacement</code>                |
| Value     | [Top] [Bottom] [Left] [Right]                              |

## Resolved Issues 10.05.830

### Firefox

- Fixed not working **browserglobal.app.local\_subdirs\_whitelist**.
- Fixed **print hotkey disable** option with Firefox 60+.



## RDP/IGEL RDP Client 2

- Fixed **smart card redirection in RDP: SCardGetAttrib** was failing if **pbAttr** was NULL. The fix should help running Dutch Zorg-ID applications.

## VMware Horizon

- Fixed: the configuration choice to **use the relative mouse feature**.

## Citrix

- Citrix Workspace App 19.03: Improved **USB redirection handling**.
- Issue solved: **Online meeting in VDI**: "enable webcam will cut the audio streaming".
- Fixed **stability issues** with Citrix Browser Content Redirection.

## Citrix Receiver 13

- Added a switch to enable the **possibility to launch multiple desktop sessions** with **RTME** and **H264 acceleration**. This switch should not be used when "Enable Secure ICA" is active for the specific delivery group.

**More...**

|          |                                  |
|----------|----------------------------------|
| Registry | ica.workaround-dual-rtme         |
| Value    | <u>enabled</u> / <u>disabled</u> |

## Network

- Fixed: The **second Ethernet interface** did not get configured when the first one was disabled.
- Added a possibility to switch between the third party **r8168** and **kernel r8169 realtek network driver**.

New registry key:

**More...**

|                                        |                                     |
|----------------------------------------|-------------------------------------|
| Parameter                              | Use thirdparty r8168 kernel module. |
| Registry                               | network.drivers.r8169.prefer_r8168  |
| Range                                  | [Auto] [Yes] [No]                   |
| Info: "Auto" (use r8169 in most cases) |                                     |

- Added a possibility to **choose the variant of the realtek r8168 driver**.

New registry key:

**More...**

|                                          |                                                                       |
|------------------------------------------|-----------------------------------------------------------------------|
| Parameter                                | Choose realtek r8168 variant (only if <b>prefer r8168</b> is chosen). |
| Registry                                 | network.drivers.r8169.r8168_variant                                   |
| Range                                    | [Default] [No NAPI] [NAPI]                                            |
| Info: "Default" (use NAPI in most cases) |                                                                       |



## Base system

- Fixed: **System logout** waits for Citrix logout now.
- Fixed: **Migration tool** did not start with the **Spanish** language setting.
- Added new registry key to set **USB quirks**.

[More...](#)

|           |                                                                                                       |
|-----------|-------------------------------------------------------------------------------------------------------|
| Parameter | Set XHCI USB quirks to fix some hardware issues.                                                      |
| Registry  | system.kernel.bootparams.xhci-hcd_quirks                                                              |
| Range     | [ <u>No quirk</u> ] [Spurious Reboot quirk] [Spurious Wakeup quirk]<br>[Spurious Reboot Wakeup quirk] |

- **Lenovo ThinkCentre M73** needs the system.kernel.bootparams.xhci-hcd\_quirks registry key set to "Spurious Reboot quirk" to fix reboot after shutdown problem.

## X11 system

- There is now a **registry key to ignore a 3Dconnexion SpaceMouse** for IGEL graphical use (X11). If activated, the SpaceMouse is only passed through to the desktop session. If disabled, it acts also as the standard mouse.

[More...](#)

|           |                                                           |
|-----------|-----------------------------------------------------------|
| Parameter | Deactivates a 3Dconnexion SpaceMouse as a standard mouse. |
| Registry  | userinterface.mouse.spacemouse.x11_ignore                 |
| Value     | <u>enabled</u> / disabled                                 |

- The following **SpaceMouse** products are included:

[More...](#)

| VID    | PID    | Vendor         | Product                                  |
|--------|--------|----------------|------------------------------------------|
| 0x046D | 0xC603 | Logitech, Inc. | 3Dconnexion SpaceMouse Plus XT           |
| 0x046D | 0xC605 | Logitech, Inc. | 3Dconnexion CADman                       |
| 0x046D | 0xC606 | Logitech, Inc. | 3Dconnexion SpaceMouse Classic           |
| 0x046D | 0xC621 | Logitech, Inc. | 3Dconnexion SpaceBall 5000               |
| 0x046D | 0xC623 | Logitech, Inc. | 3Dconnexion SpaceTraveller 3D Mouse      |
| 0x046D | 0xC625 | Logitech, Inc. | 3Dconnexion SpacePilot 3D Mouse          |
| 0x046D | 0xC626 | Logitech, Inc. | 3Dconnexion SpaceNavigator 3D Mouse      |
| 0x046D | 0xC627 | Logitech, Inc. | 3Dconnexion SpaceExplorer 3D Mouse       |
| 0x046D | 0xC628 | Logitech, Inc. | 3Dconnexion SpaceNavigator for Notebooks |
| 0x046D | 0xC629 | Logitech, Inc. | 3Dconnexion SpacePilot Pro 3D Mouse      |
| 0x046D | 0xC62B | Logitech, Inc. | 3Dconnexion SpaceMouse Pro               |
| 0x256F | **     | 3Dconnexion    | SpaceMouse                               |



- **USB device reset** via USB powercycle is now available on **UD6/UD7**.
- Fixed problems with **internal graphic cards** and **NVIDIA graphic cards**.
- Fixed **Display Switch** utility not starting with some translations.
- Fixed an issue with the **noDDC mode** not always working as expected.
- Fixed some **multimonitor** (>4) issues with **Nvidia** graphic cards.
- Updated **DisplayLink driver** to version **5.1.26** to solve some startup issues.

#### Driver

- Fixed not working **WACOM** device **DTU-1141B**.

#### Hardware

- Fixed **not working network** on Beckhoff CB3163, CB6263 and CB6363 systems.
- Fixed **not working network** on Lex 3I380D.
- Fixed **black screen issue** with some monitors and 2560x1440 resolution (occurred on UD2 LX50).
- Added possibility to **change** some **DRM settings** and limit the **DisplayPort lane bandwidth** on Intel devices.
- Added new registry keys:  
[More...](#)

|                                                           |                                                            |
|-----------------------------------------------------------|------------------------------------------------------------|
| Parameter                                                 | Use best graphic mode for all screens on console.          |
| Registry                                                  | x.drivers.kms.best_console_mode                            |
| Range                                                     | [Default] [Enabled] [Disabled]                             |
| Info: "Default" is enabled in most cases.                 |                                                            |
| Parameter                                                 | Limit the maximum console resolution width to this value.  |
| Registry                                                  | x.drivers.kms.max_console_width                            |
| Type                                                      | Integer                                                    |
| Value                                                     | "0"                                                        |
| Info: "0" means default setting. Use the default setting. |                                                            |
| Parameter                                                 | Limit the maximum console resolution height to this value. |
| Registry                                                  | x.drivers.kms.max_console_height                           |
| Type                                                      | Integer                                                    |
| Value                                                     | "0"                                                        |
| Info: "0" means default setting. Use the default setting. |                                                            |
| Parameter                                                 | Set graphic kernel driver debug level.                     |
| Registry                                                  | x.drivers.kms.debug_level                                  |



|       |                                                                                                                                                  |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Range | <a href="#">[No debug]</a> <a href="#">[Basic]</a> <a href="#">[Basic + core]</a> <a href="#">[Basic + core + atomic]</a> <a href="#">[Full]</a> |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------|

[Info: Warning log will grow very fast.](#)

Only for Intel i915 driver:

|           |                                                                                                                                                                                                                                                |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter | Limit the maximum DisplayPort lane link rate.                                                                                                                                                                                                  |
| Registry  | x.drivers.intel.max_dp_link_rate                                                                                                                                                                                                               |
| Range     | <a href="#">[default]</a> <a href="#">[1.62Gbps]</a> <a href="#">[2.16Gbps]</a> <a href="#">[2.7Gbps]</a> <a href="#">[3.24Gbps]</a> <a href="#">[4.32Gbps]</a> <a href="#">[5.4Gbps]</a> <a href="#">[6.48Gbps]</a> <a href="#">[8.1Gbps]</a> |

[Info: "Default" means hardware default limit.](#)

## Security Fixes 10.05.830

### Firefox

- Updated Mozilla **Firefox** to version **60.7.2 ESR**.
- Fixed **mfsa2019-19** security issue CVE-2019-11708.
- Fixed **mfsa2019-18** security issue CVE-2019-11707.
- Fixed **mfsa2019-10** security issues CVE-2019-9810 and CVE-2019-9813.
- Fixed **mfsa2019-08** security issues.

[More...](#)

CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2018-18506, CVE-2019-9788.

- Fixed **mfsa2019-05** security issues CVE-2018-18356 and CVE-2019-5785.
- Fixed **mfsa2019-02** security issues CVE-2018-18500, CVE-2018-18505 and CVE-2018-18501.
- Fixed **mfsa2018-30** security issues.

[More...](#)

CVE-2018-17466, CVE-2018-18492, CVE-2018-18493, CVE-2018-18494, CVE-2018-18498, CVE-2018-12405.

### Base system

- Fixed kernel TCP vulnerabilities CVE-2019-11477: **SACK Panic**, CVE-2019-11478: **SACK Slowness** and CVE-2019-11479: **Excess Resource Consumption Due to Low MSS Values**.
- Changed **minimally allowed MSS size** to '1000' to prevent possible denial-of-service attacks.
- Updated **libwebkit2gtk-4.0-37** to version **1.24.2**.

[More...](#)

CVE-2019-8595, CVE-2019-8607, CVE-2019-8615, CVE-2019-6251, CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378, CVE-2018-4382, CVE-2018-4392, CVE-2018-4416, CVE-2018-4345, CVE-2018-4386, CVE-2018-4372



## 7.26 Notes for Release 10.05.800

|                       |            |             |
|-----------------------|------------|-------------|
| <b>Software:</b>      | Version    | 10.05.800   |
| <b>Release Date:</b>  | 2019-05-08 |             |
| <b>Release Notes:</b> | Version    | RN-105800-1 |
| <b>Last update:</b>   | 2019-05-08 |             |

- [IGEL Linux Universal Desktop](#)(see page 2078)
- [IGEL Universal Desktop OS 3](#)(see page 2092)

### 7.26.1 IGEL Linux Universal Desktop

#### Supported Devices

| <b>Universal Desktop:</b> |                                                  |
|---------------------------|--------------------------------------------------|
| UD2-LX:                   | UD2-LX 40                                        |
| UD3-LX:                   | UD3-LX 51<br>UD3-LX 50<br>UD3-LX 42<br>UD3-LX 41 |
| UD5-LX:                   | UD5-LX 50                                        |
| UD6-LX:                   | UD6-LX 51                                        |
| UD7-LX:                   | UD7-LX 10                                        |
| UD9-LX:                   | UD9-LX Touch 41<br>UD9-LX 40                     |



|                   |                                |
|-------------------|--------------------------------|
| UD10-LX:          | UD10-LX Touch 10<br>UD10-LX 10 |
| <b>IGEL Zero:</b> |                                |
| IZ2-RFX           |                                |
| IZ2-HDX           |                                |
| IZ2-HORIZON       |                                |
| IZ3-RFX           |                                |
| IZ3-HDX           |                                |
| IZ3-HORIZON       |                                |

- Component Versions 10.05.800(see page 2079)
- General Information 10.05.800(see page 2083)
- Known Issues 10.05.800(see page 2084)
- New Features 10.05.800(see page 2086)
- Resolved Issues 10.05.800(see page 2089)

## Component Versions 10.05.800

### • Clients

| Product                          | Version                         |
|----------------------------------|---------------------------------|
| Citrix HDX Realtime Media Engine | 2.7.0-2113                      |
| Citrix Receiver                  | 13.10.0.20                      |
| Citrix Receiver                  | 13.5.0.10185126                 |
| Citrix Workspace App             | 18.10.0.11                      |
| deviceTRUST Citrix Channel       | 19.1.200.2                      |
| deviceTRUST RDP Channel          | 19.1.200.2                      |
| Ericom PowerTerm                 | 12.0.1.0.20170219.2-_dev_-34574 |



|                                         |                         |
|-----------------------------------------|-------------------------|
| Evidian AuthMgr                         | 1.5.6840                |
| Evince PDF Viewer                       | 3.18.2-1ubuntu4.3       |
| FabulaTech USB for Remote Desktop       | 5.2.29                  |
| Firefox                                 | 60.6.2                  |
| IBM iAccess Client Solutions            | 1.1.8.1                 |
| IGEL RDP Client                         | 2.2                     |
| Imprivata OneSign ProveID Embedded      |                         |
| Leostream Java Connect                  | 3.3.7.0                 |
| NCP Secure Enterprise Client            | 5.10_rev40552           |
| NX Client                               | 5.3.12                  |
| Open VPN                                | 2.3.10-1ubuntu2.1       |
| Oracle JRE                              | 1.8.0_202               |
| Parallels Client (64 bit)               | 16.5.2.20595            |
| Remote Viewer (RedHat Virtualization)   | 7.0-igel47              |
| Spice GTK (Red Hat Virtualization)      | 0.35                    |
| Spice Protocol (Red Hat Virtualization) | 0.12.14                 |
| Usbredir (Red Hat Virtualization)       | 0.8.0                   |
| Systancia AppliDis                      | 4.0.0.17                |
| Thinlinc Client                         | 4.9.0-5775              |
| ThinPrint Client                        | 7.5.88                  |
| Totem Media Player                      | 2.30.2                  |
| Parole Media Player                     | 1.0.1-0ubuntu1igel16    |
| VMware Horizon Client                   | 4.10.0-11053294         |
| VNC Viewer                              | 1.8.0+git20180123-igel1 |



|                                                       |           |
|-------------------------------------------------------|-----------|
| Voip Client Ekiga                                     | 4.0.1     |
| <b>• Dictation</b>                                    |           |
| Diktamen driver for dictation                         |           |
| Driver for Grundig Business Systems dictation devices |           |
| Nuance Audio Extensions for dictation                 | B048      |
| Olympus driver for dictation                          | 20180621  |
| Philips Speech Driver                                 | 12.6.36   |
| <b>• Signature</b>                                    |           |
| Kofax SPVC Citrix Channel                             | 3.1.41.0  |
| signotec Citrix Channel                               | 8.0.6     |
| signotec VCOM Daemon                                  | 2.0.0     |
| StepOver TCP Client                                   | 2.1.0     |
| <b>• Smartcard</b>                                    |           |
| PKCS#11 Library A.E.T SafeSign                        | 3.0.101   |
| PKCS#11 Library Athena IDProtect                      | 623.07    |
| PKCS#11 Library cryptovision sc/interface             | 7.1.9.620 |
| PKCS#11 Library Gemalto SafeNet                       | 10.0.37-0 |
| PKCS#11 Library SecMaker NetID                        | 6.7.2.36  |
| Reader Driver ACS CCID                                | 1.1.5     |
| Reader Driver Gemalto eToken                          | 10.0.37-0 |
| Reader Driver HID Global Omnikey                      | 4.3.3     |
| Reader Driver Identive CCID                           | 5.0.35    |



|                                    |                  |
|------------------------------------|------------------|
| Reader Driver Identive eHealth200  | 1.0.5            |
| Reader Driver Identive SCRKBC      | 5.0.24           |
| Reader Driver MUSCLE CCID          | 1.4.28           |
| Reader Driver REINER SCT cyberJack | 3.99.5final.SP11 |
| Resource Manager PC/SC Lite        | 1.8.23-1igel1    |
| Cherry USB2LAN Proxy               | 3.0.0.6          |

- System Components**

|                            |                                |
|----------------------------|--------------------------------|
| OpenSSL                    | 1.0.2g-1ubuntu4.13             |
| OpenSSH Client             | 7.2p2-4ubuntu2.4               |
| OpenSSH Server             | 7.2p2-4ubuntu2.4               |
| Bluetooth stack (bluez)    | 5.50-0ubuntu1igel5             |
| MESA OpenGL stack          | 18.2.1-1igel51                 |
| VAAPI ABI Version          | 0.40                           |
| VDPAU Library version      | 1.1.1-3ubuntu1                 |
| Graphics Driver INTEL      | 2.99.917+git20181113-igel846   |
| Graphics Driver ATI/RADEON | 18.0.1-1igel831                |
| Graphics Driver ATI/AMDGPU | 18.0.1-1igel831                |
| Graphics Driver VIA        | 5.76.52.92-009-005f78-20150730 |
| Graphics Driver FBDEV      | 0.5.0-1igel819                 |
| Graphics Driver VESA       | 2.3.4-1build2igel639           |
| Input Driver Evdev         | 2.10.5-1ubuntu1igel750         |
| Input Driver Elographics   | 1.4.1-1build5igel633           |
| Input Driver eGalax        | 2.5.5814                       |



|                                 |                              |
|---------------------------------|------------------------------|
| Input Driver Synaptics          | 1.9.0-1ubuntu1igel748        |
| Input Driver Vmmouse            | 13.1.0-1ubuntu2igel635       |
| Input Driver Wacom              | 0.36.1-0ubuntu1igel813       |
| Kernel                          | 4.18.20 #mainline-ud-r2531   |
| Xorg X11 Server                 | 1.19.6-1ubuntu4igel838       |
| Xorg Xephyr                     | 1.19.6-1ubuntu4igel832       |
| CUPS printing daemon            | 2.1.3-4ubuntu0.5igel20       |
| PrinterLogic                    | 18.2.1.128                   |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1            |
| XFCE4 Windowmanager             | 4.12.3-1ubuntu2igel653       |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7      |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.2igel58 |
| ModemManager                    | 1.6.8-2igel1                 |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.1           |
| GStreamer 1.x                   | 1.14.2-1ubuntu1igel192       |
| Python2                         | 2.7.12                       |
| Python3                         | 3.5.2                        |

- **Features with Limited IGEL Support**

|                          |
|--------------------------|
| Mobile Device Access USB |
|--------------------------|

|                 |
|-----------------|
| VPN OpenConnect |
|-----------------|

|                 |
|-----------------|
| Scanner support |
|-----------------|

|            |
|------------|
| VirtualBox |
|------------|

- **Features with Limited Functionality**

|                   |      |
|-------------------|------|
| Cisco JVDI Client | 12.1 |
|-------------------|------|

## General Information 10.05.800

The following clients and features are not supported anymore



- Citrix Receiver 12.1 and 13.1 - 13.4
- Citrix Access Gateway Standard Plug-in
- Dell vWorkspace Connector for Linux
- Ericom PowerTerm Emulation 9 and 11
- Ericom Webconnect
- IGEL Legacy RDP Client (rdesktop)
- Virtual Bridges VERDE Client
- PPTP VPN Support
- IGEL Upgrade License Tool with IGEL Smartcard Token
- Remote Management by setup.ini file transfer (TFTP)
- Remote Access via RSH
- Legacy Philips Speech Driver
- t-Systems TCOS Smartcard Support
- DUS Series touch screens
- Elo serial touch screens
- IGEL Smartcard without locking desktop
- Video Hardware Acceleration Support is discontinued on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, UD10-LX 10
- H.264 Hardware Acceleration Support is discontinued on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, UD10-LX 10
- Storage Hotplug devices are not automatically removed anymore, instead they must be always ejected manually:
  - by panel tray icon
  - by an icon in the 'In-Session Control Bar' (configurable at **IGEL Setup > User Interface > Desktop**)
  - by a 'Safely Remove Hardware' session (configurable at **IGEL Setup > Accessories**)

The following clients and features are not available in this release

- Cherry eGK Channel
- Open VPN Smartcard Support
- Asian Input Methods
- Composite Manager

## Known Issues 10.05.800

### Citrix

- With **activated DRI3** and an **amd gpu** citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (api v2) is not affected from this issue.
- Citrix has known issues with **gstreamer1.0** which describe problems with **multimedia redirection of H264, MPEG1 and MPEG2**. Gstreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.



- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.  
As a workaround, insert the smartcard before starting StoreFront login.
- When using **Citrix Workspace App 18.10** in combination with **Philips Speech** driver, the session occasionally **does not proper terminate** at logoff and hangs.  
As a workaround, usage of **Citrix Receiver 13.10** is recommended when Philips Speech driver is needed.
- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression** > \*\*For the entire screen\*\*.
- When **Expand the session over a self-selected number of monitors** (for **Multi-monitor full screen mode**) is used and setup is restarted, **Restrict full screen session to one monitor** is indicated and the **monitor selection is greyed out**. The functionality is available, only the notification in setup is broken.

#### VMware Horizon

- **External drives** mounted already before connection **do not appear in the remote desktop**.  
Workaround: map the directory /media as a drive in your desktop. Then the external devices will show up inside the media drive.
- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping is switched off**.  
In the **IGEL Setup** client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**.  
It is also recommended to **disable local Storage Hotplug**: On page **Devices > Storage Devices > Storage Hotplug**, put **number** of storage hotplug devices to **0**.
  - On the other hand, if you use **drive mapping** instead, it is recommended that you should either **switch off USB redirection entirely** or at least **deny storage devices** by adding a filter to the USB class rules. And because Horizon Client relies on the OS to mount the storage devices itself, please go to setup page: **Devices > Storage Devices > Storage Hotplug** and switch on **Enable dynamic drive mapping** and put **Number of storage hotplug devices** to at least **1**.

#### Parallels Client

- **Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode** it is necessary to connect to the **Parallels RAS** one time with FIPS support disabled.

#### Smartcard

- In some cases there are instabilities when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice**: spice-xpi firefox plugin is no longer supported. The **Console Invocation** has to allow **Native client** (auto is also possible) and it should start in fullscreen to prevent opening windows.



## Hardware

- Suspend on **UD10** is disabled.

## New Features 10.05.800

### OS 11 Upgrade

- It is now possible to **upgrade to IGEL OS 11**. For more information, please see [Upgrading IGEL Devices from IGEL OS 10 to IGEL OS 11](#)(see page 174). The parameters for the upgrade:  
[More...](#)

|            |                                                                   |
|------------|-------------------------------------------------------------------|
| IGEL Setup | <b>System &gt; Update &gt; OS 11 Upgrade</b>                      |
| Parameter  | Upgrade to OS 11                                                  |
| Registry   | update.firmware_migrate_to_11                                     |
| Value      | enabled / <u>disabled</u>                                         |
| IGEL Setup | <b>System &gt; Update &gt; OS 11 Upgrade</b>                      |
| Parameter  | Upgrade to OS 11 even if a previous upgrade attempt failed        |
| Registry   | update.force_firmware_migrate_to_11                               |
| Value      | enabled / <u>disabled</u>                                         |
| IGEL Setup | <b>System &gt; Update &gt; OS 11 Upgrade</b>                      |
| Parameter  | Upgrade to OS 11 even if PowerTerm is enabled                     |
| Registry   | update.migrate_to_11_with_powerterm                               |
| Value      | enabled / <u>disabled</u>                                         |
| IGEL Setup | <b>System &gt; Update &gt; OS 11 Upgrade</b>                      |
| Parameter  | Require an Enterprise Management Pack license to upgrade to OS 11 |
| Registry   | update.migrate_to_11_enterprise_required                          |
| Value      | [Smart] [Always] [Never]                                          |
| IGEL Setup | <b>System &gt; Update &gt; OS 11 Upgrade</b>                      |



|           |                                                                         |
|-----------|-------------------------------------------------------------------------|
| Parameter | Timeout waiting for OS 11 license to start automatic upgrade            |
| Registry  | update.migrate_to_11_license_timeout                                    |
| Value     | [Disabled] [ <u>10 Minutes</u> ] [15 Minutes] [30 Minutes] [60 Minutes] |

- The parameters for configuring the desktop integration of the **IGEL OS 11 Upgrade tool** are:  
[More...](#)

|            |                                           |
|------------|-------------------------------------------|
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>     |
| Parameter  | Start menu                                |
| Registry   | sessions.os11_migration0.startmenu        |
| Value      | <u>enabled</u> / <u>disabled</u>          |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>     |
| Parameter  | Application Launcher                      |
| Registry   | sessions.os11_migration0.applaunch        |
| Value      | <u>enabled</u> / <u>disabled</u>          |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>     |
| Parameter  | System tab of start menu                  |
| Registry   | sessions.os11_migration0.startmenu_system |
| Value      | <u>enabled</u> / <u>disabled</u>          |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>     |
| Parameter  | System tab of Application Launcher        |
| Registry   | sessions.os11_migration0.applaunch_system |
| Value      | <u>enabled</u> / <u>disabled</u>          |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>     |
| Parameter  | Menu folder                               |



|            |                                            |
|------------|--------------------------------------------|
| Registry   | sessions.os11_migration0.menu_path         |
| Value      | enabled / <u>disabled</u>                  |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>      |
| Parameter  | Desktop folder                             |
| Registry   | sessions.os11_migration0.desktop_path      |
| Value      | enabled / <u>disabled</u>                  |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>      |
| Parameter  | Application Launcher folder                |
| Registry   | sessions.os11_migration0.applaunch_path    |
| Value      | enabled / <u>disabled</u>                  |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>      |
| Parameter  | Quick start panel                          |
| Registry   | sessions.os11_migration0.quick_start       |
| Value      | enabled / <u>disabled</u>                  |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>      |
| Parameter  | Password protection                        |
| Registry   | sessions.os11_migration0.pwprotected       |
| Value      | [None] [Administrator] [User] [Setup user] |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>      |
| Parameter  | Desktop                                    |
| Registry   | sessions.os11_migration0.desktop           |
| Value      | enabled / <u>disabled</u>                  |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>      |
| Parameter  | Desktop context menu                       |



|          |                                   |
|----------|-----------------------------------|
| Registry | sessions.os11_migration0.pulldown |
| Value    | enabled / <u>disabled</u>         |

## Firefox

- Updated **Mozilla Firefox to version 60.6.2ESR**: Repaired certificate chain to re-enable web extensions that had been disabled.

## Network

- Added **NCP Secure Enterprise** VPN Client version **5.10\_rev40552**: Configurable at IGEL Setup > Network > VPN > NCP VPN Client

## Driver

- Updated **deviceTRUST Client to version 19.1.200**. These are the release notes: Welcome to the release of the deviceTRUST 19.1.200 IGEL client, providing the context of IGEL thin client and UD Pocket devices into your virtual sessions. This release includes support for logical disks attached to the IGEL endpoint, plus bug fixes and stability improvements over the previous 19.1.100 release.

### Logical Disks

Added support for real-time properties representing the LOGICAL DISKS attached to the IGEL endpoint.

#### This includes...

- DEVICE\_LOGICALDISK\_X\_TYPE – Either Fixed or Removable.
- DEVICE\_LOGICALDISK\_X\_LABEL – The volume label.
- DEVICE\_LOGICALDISK\_X\_FILESYSTEM – The type of file system.
- DEVICE\_LOGICALDISK\_X\_PATHS – The paths that the disk is mounted.
- DEVICE\_LOGICALDISK\_X\_TOTALMB – The total space available on the disk. This property is only available for mounted disks.
- DEVICE\_LOGICALDISK\_X\_FREEMB – The free space available on the disk. This property is only available for mounted disks.
- DEVICE\_LOGICALDISK\_X\_NAME – The name of the underlying physical disk.
- DEVICE\_LOGICALDISK\_X\_VENDORID – The vendor identifier uniquely identifying the manufacturer. This property is only available for USB or PCI connected devices.
- DEVICE\_LOGICALDISK\_X\_PRODUCTID – The product identifier uniquely identifying the product. This property is only available for USB or PCI connected devices.
- DEVICE\_LOGICALDISK\_X\_SERIALNUMBER – The serial number of the physical disk.
- DEVICE\_LOGICALDISK\_X\_BUSTYPE – The storage bus type linked to the physical disk.
- DEVICE\_LOGICALDISK\_COUNT – The number of logical disks.

## Resolved Issues 10.05.800

### Network

- Added possibility to **switch between thirdparty r8168 and kernel r8169 realtek network driver**. [More...](#)



|                                       |                                     |
|---------------------------------------|-------------------------------------|
| Parameter                             | Use thirdparty r8168 kernel module. |
| Registry                              | network.drivers.r8169.prefer_r8168  |
| Range                                 | [Auto] [Yes] [No]                   |
| Info: "Auto" uses r8169 in most cases |                                     |

## WiFi

- Fixed non working **TP Link Archer T2UH**.

## Base system

- Added possibility to set `intel_idle.max_cstate` kernel cmdline parameter with registry keys to work against **Intel CPU freezes**.
- Enhanced **bootloader** to allow the setting of some kernel commandline parameters with registry keys.

[More...](#)

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Disable use of APIC controller.               |
| Registry  | system.kernel.bootparams.noapic               |
| Value     | <u>enabled</u> / <u>disabled</u>              |
| Parameter | Disable use of ACPI.                          |
| Registry  | system.kernel.bootparams.noacpi               |
| Value     | <u>enabled</u> / <u>disabled</u>              |
| Parameter | Use only one CPU core and disable all others. |
| Registry  | system.kernel.bootparams.nosmp                |
| Value     | <u>enabled</u> / <u>disabled</u>              |
| Parameter | Enable debug console on serial port 1.        |
| Registry  | system.kernel.bootparams.serial_console_debug |
| Value     | <u>enabled</u> / <u>disabled</u>              |
| Parameter | Limit CPU core usage (0 means no limit).      |
| Registry  | system.kernel.bootparams.maxcpus              |
| Value     | "0"                                           |



|           |                                           |
|-----------|-------------------------------------------|
| Parameter | Set maximum allowed cstate on intel cpus. |
| Registry  | system.kernel.bootparams.max_cstate       |
| Range     | [No limit] [1] [2] [3] [4] [5] [6]        |
| Info:     | do not limit intel cstate                 |
| Parameter | IOMMU usage setting.                      |
| Registry  | system.kernel.bootparams.iommu            |
| Range     | [On] [Off] [Passthrough] [Force]          |
| Info:     | Use IOMMU if possible                     |
| Parameter | IOMMU usage setting for AMD systems.      |
| Registry  | system.kernel.bootparams.amd_iommu        |
| Range     | [On] [Off]                                |
| Info:     | Use IOMMU if possible                     |
| Parameter | IOMMU usage setting for Intel systems.    |
| Registry  | system.kernel.bootparams.intel_iommu      |
| Range     | [On] [Off]                                |
| Info:     | Use IOMMU if possible                     |

## Driver

- Updated **deviceTRUST** Client to version **19.1.200**. Bug Fixes:
  - Fixed an issue reading the **DEVICE\_IGEL\_ICG\_SERVER** property.
  - Fixed an issue where the **NETWORK** and **LOCATION** property providers could cause the client to freeze if a disconnection occurred whilst these property providers were checking for changes.
  - Fixed an **open file handle leak** which lead to the client process reaching its file handle limits when left running for a long period of time.

## X11 system

- Fixed a bug with thinclients **reporting the wrong monitor serial number**.

## Hardware

- Updated **AMDGPU Pro driver to 19.10** version. The new version fixes a disappearing mouse cursor issue. Enable AMDGPU Pro driver instead of kernel integrated driver by registry key (settings to this key will only work after reboot):
   
**More...**



|           |                                 |
|-----------|---------------------------------|
| Parameter | Use AMDGPU PRO driver.          |
| Registry  | x.drivers.amdgpu.use_amdgpu_pro |
| Range     | [Auto] [Yes] [No]               |

## 7.26.2 IGEL Universal Desktop OS 3

Supported Hardware:

<https://kb.igel.com/igelos/en/devices-supported-by-udc3-and-ud-pocket-3117174.html>

- Component Versions 10.05.800(see page 2092)
- General Information 10.05.800(see page 2096)
- Known Issues 10.05.800(see page 2097)
- New Features 10.05.800(see page 2099)
- Resolved Issues 10.05.800(see page 2106)

### Component Versions 10.05.800

- **Clients**

| Product                           | Version                         |
|-----------------------------------|---------------------------------|
| Citrix HDX Realtime Media Engine  | 2.7.0-2113                      |
| Citrix Receiver                   | 13.10.0.20                      |
| Citrix Receiver                   | 13.5.0.10185126                 |
| Citrix Workspace App              | 18.10.0.11                      |
| deviceTRUST Citrix Channel        | 19.1.200.2                      |
| deviceTRUST RDP Channel           | 19.1.200.2                      |
| Ericom PowerTerm                  | 12.0.1.0.20170219.2-_dev_-34574 |
| Evidian AuthMgr                   | 1.5.6840                        |
| Evince PDF Viewer                 | 3.18.2-1ubuntu4.3               |
| FabulaTech USB for Remote Desktop | 5.2.29                          |



|                                         |                         |
|-----------------------------------------|-------------------------|
| Firefox                                 | 60.6.2                  |
| IBM iAccess Client Solutions            | 1.1.8.1                 |
| IGEL RDP Client                         | 2.2                     |
| Imprivata OneSign ProveID Embedded      |                         |
| deviceTRUST RDP Channel                 | 19.1.200.2              |
| Leostream Java Connect                  | 3.3.7.0                 |
| NCP Secure Enterprise Client            | 5.10_rev40552           |
| NX Client                               | 5.3.12                  |
| Open VPN                                | 2.3.10-1ubuntu2.1       |
| Oracle JRE                              | 1.8.0_202               |
| Parallels Client (64 bit)               | 16.5.2.20595            |
| Parole Media Player                     | 1.0.1-0ubuntu1igel16    |
| Remote Viewer (RedHat Virtualization)   | 7.0-igel47              |
| Spice GTK (Red Hat Virtualization)      | 0.35                    |
| Spice Protocol (Red Hat Virtualization) | 0.12.14                 |
| Usbredir (Red Hat Virtualization)       | 0.8.0                   |
| Systancia AppliDis                      | 4.0.0.17                |
| Thinlinc Client                         | 4.9.0-5775              |
| ThinPrint Client                        | 7.5.88                  |
| Totem Media Player                      | 2.30.2                  |
| Parole Media Player                     | 1.0.1-0ubuntu1igel16    |
| VMware Horizon Client                   | 4.10.0-11053294         |
| VNC Viewer                              | 1.8.0+git20180123-igel1 |
| Voip Client Ekiga                       | 4.0.1                   |

- **Dictation**



|                                                       |          |
|-------------------------------------------------------|----------|
| Diktamen driver for dictation                         |          |
| Driver for Grundig Business Systems dictation devices |          |
| Nuance Audio Extensions for dictation                 | B048     |
| Olympus driver for dictation                          | 20180621 |
| Philips Speech Driver                                 | 12.6.36  |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.6    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.1.0    |

- **Smartcard**

|                                           |           |
|-------------------------------------------|-----------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101   |
| PKCS#11 Library Athena IDProtect          | 623.07    |
| PKCS#11 Library cryptovision sc/interface | 7.1.9.620 |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0 |
| PKCS#11 Library SecMaker NetID            | 6.7.2.36  |
| Reader Driver ACS CCID                    | 1.1.5     |
| Reader Driver Gemalto eToken              | 10.0.37-0 |
| Reader Driver HID Global Omnikey          | 4.3.3     |
| Reader Driver Identive CCID               | 5.0.35    |
| Reader Driver Identive eHealth200         | 1.0.5     |
| Reader Driver Identive SCRKBC             | 5.0.24    |



|                                    |                  |
|------------------------------------|------------------|
| Reader Driver MUSCLE CCID          | 1.4.28           |
| Reader Driver REINER SCT cyberJack | 3.99.5final.SP11 |
| Resource Manager PC/SC Lite        | 1.8.23-1igel1    |
| Cherry USB2LAN Proxy               | 3.0.0.6          |

- **System Components**

|                                         |                              |
|-----------------------------------------|------------------------------|
| OpenSSL                                 | 1.0.2g-1ubuntu4.13           |
| OpenSSH Client                          | 7.2p2-4ubuntu2.4             |
| OpenSSH Server                          | 7.2p2-4ubuntu2.4             |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5           |
| MESA OpenGL stack                       | 18.2.1-1igel51               |
| VAAPI ABI Version                       | 0.40                         |
| VDPAU Library version                   | 1.1.1-3ubuntu1               |
| Graphics Driver INTEL                   | 2.99.917+git20181113-igel846 |
| Graphics Driver ATI/Radeon              | 18.0.1-1igel831              |
| Graphics Driver ATI/AMDGPU              | 18.0.1-1igel831              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.15-2igel775              |
| Graphics Driver Nvidia                  | 390.87-0ubuntu1              |
| Graphics Driver Vboxvideo               | 5.2.18-dfsg-2igel17          |
| Graphics Driver VMware                  | 13.3.0-2igel812              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1igel775         |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |
| Graphics Driver VESA                    | 2.3.4-1build2igel639         |
| Input Driver Evdev                      | 2.10.5-1ubuntu1igel750       |
| Input Driver Elographics                | 1.4.1-1build5igel633         |
| Input Driver eGalax                     | 2.5.5814                     |



|                                 |                              |
|---------------------------------|------------------------------|
| Input Driver Synaptics          | 1.9.0-1ubuntu1igel748        |
| Input Driver Vmmouse            | 13.1.0-1ubuntu2igel635       |
| Input Driver Wacom              | 0.36.1-0ubuntu1igel813       |
| Kernel                          | 4.18.20 #mainline-udos-r2531 |
| Xorg X11 Server                 | 1.19.6-1ubuntu4igel838       |
| Xorg Xephyr                     | 1.19.6-1ubuntu4igel832       |
| CUPS printing daemon            | 2.1.3-4ubuntu0.5igel20       |
| PrinterLogic                    | 18.2.1.128                   |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1            |
| XFCE4 Windowmanager             | 4.12.3-1ubuntu2igel653       |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7      |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.2igel58 |
| ModemManager                    | 1.6.8-2igel1                 |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.1           |
| GStreamer 1.x                   | 1.14.2-1ubuntu1igel192       |
| Python2                         | 2.7.12                       |
| Python3                         | 3.5.2                        |

- **Features with Limited IGEL Support**

|                          |
|--------------------------|
| Mobile Device Access USB |
|--------------------------|

|                 |
|-----------------|
| VPN OpenConnect |
|-----------------|

|                 |
|-----------------|
| Scanner support |
|-----------------|

|            |
|------------|
| VirtualBox |
|------------|

- **Features with Limited Functionality**

|                   |      |
|-------------------|------|
| Cisco JVDI Client | 12.1 |
|-------------------|------|

## General Information 10.05.800

The following clients and features are not supported anymore:



- Citrix Receiver 12.1 and 13.1 - 13.4
- Citrix Access Gateway Standard Plug-in
- Dell vWorkspace Connector for Linux
- Ericom PowerTerm Emulation 9 and 11
- Ericom Webconnect
- IGEL Legacy RDP Client (rdesktop)
- Virtual Bridges VERDE Client
- PPTP VPN Support
- IGEL Upgrade License Tool with IGEL Smartcard Token
- Remote Management by setup.ini file transfer (TFTP)
- Remote Access via RSH
- Legacy Philips Speech Driver
- t-Systems TCOS Smartcard Support
- DUS Series touch screens
- Elo serial touch screens
- IGEL Smartcard without locking desktop
- VIA Graphics Support
- Storage Hotplug devices are not automatically removed anymore, instead they must be always ejected manually:
  - by panel tray icon
  - by an icon in the 'In-Session Control Bar' (configurable at **IGEL Setup > User Interface > Desktop**)
  - by a 'Safely Remove Hardware' session (configurable at **IGEL Setup > Accessories**)

The following clients and features are not available in this release:

- Cherry eGK Channel
- Open VPN Smartcard Support
- Asian Input Methods
- Composite Manager

## Known Issues 10.05.800

### Citrix

- With **activated DRI3** and an AMD GPU Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer 1.0** which describe problems with **multimedia redirection of H264, MPEG1 and MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of login.  
As a workaround, insert the smartcard before starting StoreFront login.



- When using **Citrix Workspace App 18.10** in combination with **Philips Speech** driver, the **session** occasionally **terminates improperly** at logout and hangs.  
As a workaround, usage of **Citrix Receiver 13.10** is recommended when Philips Speech driver is needed.
- Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression** > "For the entire screen".
- When "Expand the session over a self-selected number of monitors" (for "Multimonitor full-screen mode") is used and Setup is restarted, "Restrict full screen session to one monitor" is indicated and the **monitor selection is greyed out**. The functionality is available, only the notification in Setup is broken.

#### VMware Horizon

- External drives** mounted already before connection **do not appear in the remote desktop**.  
Workaround: map the directory /media as a drive in your desktop. Then the external devices will show up inside the media drive.
- Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping is switched off**. In the **IGEL Setup** client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to **disable local Storage Hotplug**: On page **Devices > Storage Devices > Storage Hotplug**, put **number** of storage hotplug devices to **0**.
  - On the other hand, if you use **drive mapping** instead, it is recommended that you should either **switch off USB redirection entirely** or at least **deny storage devices** by adding a filter to the USB class rules. And because Horizon Client relies on the OS to mount the storage devices itself, please go to setup page: **Devices > Storage Devices > Storage Hotplug** and switch on **Enable dynamic drive mapping** and put **Number of storage hotplug devices** to at least **1**.

#### Parallels Client

- Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** one time with FIPS support disabled.

#### Smartcard

- In some cases, there are instabilities when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice**: spice-xpi firefox plugin is no longer supported. The **Console Invocation** has to allow **Native client** (auto is also possible) and it should start in fullscreen to prevent opening windows.

#### Base system

- Display resolution and rotation** could not be changed with NVIDIA GPU driver via tcsetup.

#### Multimedia



- **Multimedia redirection** with **GStreamer** could fail with Nouveau GPU driver.

## New Features 10.05.800

### RDP/IGEL RDP Client 2

- Add **field collection** to RDP session **server** page.  
[More...](#)

|            |                                                                          |
|------------|--------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; RDP &gt; RDP Sessions &gt; RDP Session &gt; Server</b>  |
|            | <b>Sessions &gt; RDP &gt; RDP Sessions &gt; RDP Session &gt; Options</b> |
| Parameter  | Collection                                                               |
| Registry   | sessions.winconnect<NR>.option.load-balance-info                         |

### VMware Horizon

- Added parameters to **specify webcam frame size** and **rate for RTAV**.  
[More...](#)

|           |                               |
|-----------|-------------------------------|
| Parameter | Webcam frame width            |
| Registry  | vmware.view.rtav-frame-width  |
| Value     | <empty_string>                |
| Parameter | Webcam frame height           |
| Registry  | vmware.view.rtav-frame-height |
| Value     | <empty_string>                |
| Parameter | Webcam frame rate             |
| Registry  | vmware.view.rtav-frame-rate   |
| Value     | <empty_string>                |

### Firefox

- Updated **Mozilla Firefox** to version **60.6.2ESR**:  
 Repaired certificate chain to re-enable web extensions that had been disabled.
- Fixes for **mfsa2019-10**, also known as: CVE-2019-9810, CVE-2019-9813.



- Fixes for **mfsa2019-08**, also known as: CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2018-18506, CVE-2019-9788.
- Fixes for **mfsa2019-05**, also known as: CVE-2018-18356, CVE-2019-5785.
- Fixes for **mfsa2019-02**, also known as: CVE-2018-18500, CVE-2018-18505, CVE-2018-18501.
- Fixes for **mfsa2018-30**, also known as: CVE-2018-17466, CVE-2018-18492, CVE-2018-18493, CVE-2018-18494, CVE-2018-18498, CVE-2018-12405.
- Added new parameters: Allow a **custom command** before and after browser session.

[More...](#)

|           |                                |
|-----------|--------------------------------|
| Parameter | Initial Action                 |
| Registry  | sessions.browser%.init_action  |
| Value     | <empty_string>                 |
| Parameter | Final Action                   |
| Registry  | sessions.browser%.final_action |
| Value     | <empty_string>                 |

#### OS 11 Upgrade

- It is now possible to **upgrade to IGEL OS 11**. For more information, please see [Upgrading IGEL Devices from IGEL OS 10 to IGEL OS 11](#)<sup>454</sup>. The parameters for the upgrade:

[More...](#)

|            |                                                            |
|------------|------------------------------------------------------------|
| IGEL Setup | <b>System &gt; Update &gt; OS 11 Upgrade</b>               |
| Parameter  | Upgrade to OS 11                                           |
| Registry   | update.firmware_migrate_to_11                              |
| Value      | enabled / <u>disabled</u>                                  |
| IGEL Setup | <b>System &gt; Update &gt; OS 11 Upgrade</b>               |
| Parameter  | Upgrade to OS 11 even if a previous upgrade attempt failed |
| Registry   | update.force_firmware_migrate_to_11                        |
| Value      | enabled / <u>disabled</u>                                  |
| IGEL Setup | <b>System &gt; Update &gt; OS 11 Upgrade</b>               |

<sup>454</sup> <https://kb.igel.com/igelos-10.05.800/en/upgrading-udc3-devices-from-igel-os-10-to-igel-os-11-23517181.html>



|            |                                                                         |
|------------|-------------------------------------------------------------------------|
| Parameter  | Upgrade to OS 11 even if PowerTerm is enabled                           |
| Registry   | update.migrate_to_11_with_powerterm                                     |
| Value      | enabled / <u>disabled</u>                                               |
| IGEL Setup | <b>System &gt; Update &gt; OS 11 Upgrade</b>                            |
| Parameter  | Require an Enterprise Management Pack license to upgrade to OS 11       |
| Registry   | update.migrate_to_11_enterprise_required                                |
| Value      | [Smart] [Always] [Never]                                                |
| IGEL Setup | <b>System &gt; Update &gt; OS 11 Upgrade</b>                            |
| Parameter  | Timeout waiting for OS 11 license to start automatic upgrade            |
| Registry   | update.migrate_to_11_license_timeout                                    |
| Value      | [Disabled] [ <u>10 Minutes</u> ] [15 Minutes] [30 Minutes] [60 Minutes] |

- The parameters for configuring the desktop integration of the **IGEL OS 11 Upgrade tool** are:  
[More...](#)

|            |                                       |
|------------|---------------------------------------|
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b> |
| Parameter  | Start menu                            |
| Registry   | sessions.os11_migration0.startmenu    |
| Value      | enabled / <u>disabled</u>             |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b> |
| Parameter  | Application Launcher                  |
| Registry   | sessions.os11_migration0.applaunch    |
| Value      | enabled / <u>disabled</u>             |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b> |
| Parameter  | System tab of start menu              |



|            |                                           |
|------------|-------------------------------------------|
| Registry   | sessions.os11_migration0.startmenu_system |
| Value      | <u>enabled</u> / disabled                 |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>     |
| Parameter  | System tab of Application Launcher        |
| Registry   | sessions.os11_migration0.applaunch_system |
| Value      | <u>enabled</u> / disabled                 |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>     |
| Parameter  | Menu folder                               |
| Registry   | sessions.os11_migration0.menu_path        |
| Value      | <u>enabled</u> / <u>disabled</u>          |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>     |
| Parameter  | Desktop folder                            |
| Registry   | sessions.os11_migration0.desktop_path     |
| Value      | <u>enabled</u> / <u>disabled</u>          |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>     |
| Parameter  | Application Launcher folder               |
| Registry   | sessions.os11_migration0.applaunch_path   |
| Value      | <u>enabled</u> / <u>disabled</u>          |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>     |
| Parameter  | Quick start panel                         |
| Registry   | sessions.os11_migration0.quick_start      |
| Value      | <u>enabled</u> / <u>disabled</u>          |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>     |
| Parameter  | Password protection                       |



|            |                                            |
|------------|--------------------------------------------|
| Registry   | sessions.os11_migration0.pwprotected       |
| Value      | [None] [Administrator] [User] [Setup user] |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>      |
| Parameter  | Desktop                                    |
| Registry   | sessions.os11_migration0.desktop           |
| Value      | enabled / <u>disabled</u>                  |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>      |
| Parameter  | Desktop context menu                       |
| Registry   | sessions.os11_migration0.pulldown          |
| Value      | enabled / <u>disabled</u>                  |

## Citrix

- Updated **Citrix HDX RTME** used for optimization of **Skype for Business** to version **2.7.0-2113**.

## Parallels Client

- Updated Parallels Client to **version 16.5.2 (64-Bit)**

## CUPS Printing

- Added **SMB Network Print Client** function. The printer could be created on page **Devices > Printer > CUPS > Printers > Dialog**, **SMB Network Printer** as **Printer Port**. The settings for the SMB printer must be done in Setup Registry:  
[More...](#)

|            |                                                                                                                                                     |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Devices &gt; Printer &gt; CUPS &gt; Printers &gt; Dialog</b>                                                                                     |
| Parameter  | Printer Port                                                                                                                                        |
| Registry   | print.cups.printer<NR>.backend                                                                                                                      |
| Value      | [Parallel Port Printer] [Serial Port Printer] [USB Printer] [LPD Network Printer] [TCP Network Printer] [IPP Network Printer] [SMB Network Printer] |
| Parameter  | SMB Server                                                                                                                                          |
| Registry   | print.cups.printer<NR>.smb_server                                                                                                                   |



|           |                                       |
|-----------|---------------------------------------|
| Parameter | SMB Workgroup                         |
| Registry  | print.cups.printer<NR>.smb_workgroup  |
| Parameter | SMB Port                              |
| Registry  | print.cups.printer<NR>.smb_port       |
| Value     | 0                                     |
| Parameter | SMB Printer                           |
| Registry  | print.cups.printer<NR>.smb_printer    |
| Parameter | SMB User                              |
| Registry  | print.cups.printer<NR>.smb_user       |
| Parameter | SMB Password                          |
| Registry  | print.cups.printer<NR>.crypt_password |

## IBM\_5250

- Updated **IBM iAccess Client Solutions** to version **1.1.8.1**.

## WiFi

- Added support for **Realtek 8821CE wireless cards**.
- Added switch to determine the **source of WiFi scan results** within the **Wireless Manager**. Selecting default is currently identical with the old mechanism (using the iwlist command). This may change in the future. When iwlist fails, **NetworkManager** is automatically used as a fallback.

[More...](#)

|                                                |                                                      |
|------------------------------------------------|------------------------------------------------------|
| Parameter                                      | WiFi Scanner                                         |
| Registry                                       | network.interfaces.wirelesslan.device0.mssid_scanner |
| Range                                          | <u>default</u> / iwlist / NetworkManager             |
| Info: "default" is currently equal to "iwlist" |                                                      |

## X11 System

- Added **xprintidle** tool to firmware.
- The new **Display Switch** tool can use **multiple different profiles**, automatically chosen **at runtime** depending on the currently connected monitors. A profile is created, when the current



monitor layout/resolution is configured via the **Display Switch** utility. The profile will be associated with the **current connected displays** automatically (manufacturer, model and used connector are used for allocation) and if applicable, the state of the **laptop lid**. The setup will be restored by hot-(un)plugging known displays, means the system will automatically switch to the already configured profile. The **Display Switch** utility itself got a new interface. All base functionality can be configured via drag & drop.

An example workflow:

- Connect the hardware and **close/open lid**
- Open the **Display Switch** Utility
  - A quick (simple) setting can be selected directly.
  - Should the desired application deviate from the possibilities provided, the **Advanced** button opens a drag & drop interface for further settings.
- In this interface the displays can be **dragged and dropped** for the intended configuration. The **display will snap adjacent** to others.
- If a **display should not be used**, it can be dragged to the **Disabled** area on the top right - the screen will be reactivated when it is dragged back to the active area.
- To show the **same content on multiple displays**, one display should be dragged onto an other active screen. The interface will show **Mirror**. The mirroring monitor will be displayed on the lower right.
- With the **Apply** button the current state will be set, with **Yes** on the **Keep configuration** dialog the current settings will be saved to persistent storage and associated with the profile.
- **Advanced functionality** (panning/scaling/resolutions) can be configured in drop-down boxes, hidden in a **drawer** on the right side. The drawer can be expanded by clicking the < button on the right edge.
- For the **Display Switch** functionality the following parameters should be enabled for proper usage:  
**More...**

|            |                                                     |
|------------|-----------------------------------------------------|
| IGEL Setup | <b>Accessories &gt; Display Switch &gt; Options</b> |
| Parameter  | Preserve settings over reboot                       |
| Registry   | sessions.user_display0.options.preserve_settings    |
| Value      | enabled / disabled                                  |
| IGEL Setup | <b>Accessories &gt; Display Switch &gt; Options</b> |
| Parameter  | Smart display configuration                         |
| Registry   | x.auto_associate                                    |
| Value      | enabled / disabled                                  |

- The **IGEL Display Switch** utility is now used for **NVIDIA graphics** devices as well.

Network



- Added **NCP Secure Enterprise** VPN Client version 5.10\_rev40552: Configurable at **IGEL Setup > Network > VPN > NCP VPN Client**

#### Driver

- Updated **deviceTRUST** Client to version **19.1.200**. These are the release notes:  
Welcome to the release of the deviceTRUST 19.1.200 IGEL client, providing the context of IGEL thin client and UD Pocket devices into your virtual sessions. This release includes support for logical disks attached to the IGEL endpoint, plus bug fixes and stability improvements over the previous 19.1.100 release.

#### Logical Disks

We've added support for real-time properties representing the LOGICAL DISKS attached to the IGEL endpoint.

##### This includes...

- DEVICE\_LOGICALDISK\_X\_TYPE – Either Fixed or Removable.
- DEVICE\_LOGICALDISK\_X\_LABEL – The volume label.
- DEVICE\_LOGICALDISK\_X\_FILESYSTEM – The type of file system.
- DEVICE\_LOGICALDISK\_X\_PATHS – The paths that the disk is mounted.
- DEVICE\_LOGICALDISK\_X\_TOTALMB – The total space available on the disk. This property is only available for mounted disks.
- DEVICE\_LOGICALDISK\_X\_FREEMB – The free space available on the disk. This property is only available for mounted disks.
- DEVICE\_LOGICALDISK\_X\_NAME – The name of the underlying physical disk.
- DEVICE\_LOGICALDISK\_X\_VENDORID – The vendor identifier uniquely identifying the manufacturer. This property is only available for USB or PCI connected devices.
- DEVICE\_LOGICALDISK\_X\_PRODUCTID – The product identifier uniquely identifying the product. This property is only available for USB or PCI connected devices.
- DEVICE\_LOGICALDISK\_X\_SERIALNUMBER – The serial number of the physical disk.
- DEVICE\_LOGICALDISK\_X\_BUSTYPE – The storage bus type linked to the physical disk.
- DEVICE\_LOGICALDISK\_COUNT – The number of logical disks.

#### Resolved Issues 10.05.800

##### Citrix Receiver 13

- Fixed crash when **H.264 acceleration** and **RTME** will be used on two or more concurrent VDI sessions.

##### VMware Horizon

- Fixed optimization for **Skype for Business**.
  - Added switch to use **system-wide proxy** in VMware Horizon appliance mode.
- More...**

|           |                           |
|-----------|---------------------------|
| Parameter | Use the systemwide proxy. |
| Registry  | vmwarevdmapp.use_proxy    |



|       |                           |
|-------|---------------------------|
| Range | <u>enabled / disabled</u> |
|-------|---------------------------|

## PowerTerm

- Fixed editing of parameter sessions.powerterm\<INST>.logindialog.loginscript in Setup Registry: **now multiple lines are possible.**

## Network

- Changed **e1000e** driver to **3.4.2.3** - directly from Intel.
  - Changed **igb** driver to **5.3.5.22** - also directly from Intel.
  - Added possibility to switch between thirdparty r8168 and kernel r8169 realtek network driver.
- More...**

|           |                                     |
|-----------|-------------------------------------|
| Parameter | Use thirdparty r8168 kernel module. |
| Registry  | network.drivers.r8169.prefer_r8168  |
| Range     | <u>[Auto]</u> [Yes] [No]            |

Info: use r8169 in most cases

## Base system

- Added package **ldap-utils** which could be used via **custom scripts**.
  - Fixed **delay in logon as local user**, when logon with **IGEL Smartcard** is also active.
  - Fixed **random 90 seconds shutdown delay** (systemd).
  - Fixed **custom bootsplash** installation.
  - Added possibility to set intel\_idle.max\_cstate kernel cmdline parameter with registry keys to work against **Intel CPU freezes**.
  - Enhanced **bootloader** to allow the setting of some kernel commandline parameters with registry keys.
- More...**

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Disable use of APIC controller.               |
| Registry  | system.kernel.bootparams.noapic               |
| Value     | <u>enabled / disabled</u>                     |
| Parameter | Disable use of ACPI.                          |
| Registry  | system.kernel.bootparams.noacpi               |
| Value     | <u>enabled / disabled</u>                     |
| Parameter | Use only one CPU core and disable all others. |
| Registry  | system.kernel.bootparams.nosmp                |
| Value     | <u>enabled / disabled</u>                     |



|                                        |                                               |
|----------------------------------------|-----------------------------------------------|
| Parameter                              | Enable debug console on serial port 1.        |
| Registry                               | system.kernel.bootparams.serial_console_debug |
| Value                                  | enabled / <u>disabled</u>                     |
| Parameter                              | Limit CPU core usage (0 means no limit).      |
| Registry                               | system.kernel.bootparams.maxcpus              |
| Value                                  | "0"                                           |
| Parameter                              | Set maximum allowed cstate on intel cpus.     |
| Registry                               | system.kernel.bootparams.max_cstate           |
| Range                                  | [No limit] [1] [2] [3] [4] [5] [6]            |
| <i>Info:</i> do not limit intel cstate |                                               |
| Parameter                              | IOMMU usage setting.                          |
| Registry                               | system.kernel.bootparams.iommu                |
| Range                                  | [On] [Off] [Passthrough] [Force]              |
| <i>Info:</i> Use IOMMU if possible     |                                               |
| Parameter                              | IOMMU usage setting for AMD systems.          |
| Registry                               | system.kernel.bootparams.amd_iommu            |
| Range                                  | [On] [Off]                                    |
| <i>Info:</i> Use IOMMU if possible     |                                               |
| Parameter                              | IOMMU usage setting for Intel systems.        |
| Registry                               | system.kernel.bootparams.intel_iommu          |
| Range                                  | [On] [Off]                                    |
| <i>Info:</i> Use IOMMU if possible     |                                               |

## Storage Devices

- Fixed **auto mounting of storage devices** inside of **Olympus DS-9500 Digital Voice Recorder**.

## WiFi

- Fixed non working TP Link Archer T2UH.

## Driver



- Updated deviceTRUST Client to version 19.1.200. Bug Fixes:
  - Fixed an issue reading the DEVICE\_IGEL\_ICG\_SERVER property.
  - Fixed an issue where the NETWORK and LOCATION property providers could cause the client to freeze if a disconnection occurred whilst these property providers were checking for changes.
  - Fixed an open file handle leak which lead to the client process reaching its file handle limits when left running for a long period of time.

#### X11 system

- Fixed a bug with thinclients reporting the **wrong monitor serial number**.
- There is now a registry key to **ignore a 3Dconnexion SpaceMouse** for IGEL graphical use (X11). If activated, the **SpaceMouse** is only passed thru to the desktop session. If false, it acts like the standard mouse.
- The following **SpaceMouse** products are included (VID, PID, Vendor, Product).

[More...](#)

0x046D; 0xC603; Logitech, Inc.; 3Dconnexion Spacemouse Plus XT  
 0x046D; 0xC605; Logitech, Inc.; 3Dconnexion CADman  
 0x046D; 0xC606; Logitech, Inc.; 3Dconnexion Spacemouse Classic  
 0x046D; 0xC621; Logitech, Inc.; 3Dconnexion Spaceball 5000  
 0x046D; 0xC623; Logitech, Inc.; 3Dconnexion Space Traveller 3D Mouse  
 0x046D; 0xC625; Logitech, Inc.; 3Dconnexion Space Pilot 3D Mouse  
 0x046D; 0xC626; Logitech, Inc.; 3Dconnexion Space Navigator 3D Mouse  
 0x046D; 0xC627; Logitech, Inc.; 3Dconnexion Space Explorer 3D Mouse  
 0x046D; 0xC628; Logitech, Inc.; 3Dconnexion Space Navigator for Notebooks  
 0x046D; 0xC629; Logitech, Inc.; 3Dconnexion SpacePilot Pro 3D Mouse  
 0x046D; 0xC62B; Logitech, Inc.; 3Dconnexion Space Mouse Pro  
 0x256F; \*\*; 3Dconnexion; SpaceMouse

- **USB device reset via USB powercycle on UD6 / UD7 available.**
- Fixed **screen flicker** in some cases if **Force NumLock On** (x.global.forceenumlock) is active.

#### Window manager

- Fixed option to **disable the local window manager**.

#### Hardware

- Fixed non working **Laptop Display** for **Dell Latitude E5510**
- **Ryzen 3 devices** (1200, 1300X, 2200G, 2200U and 2300U) will use the **AMDGPU PRO** driver if registry key x.drivers.amdgpu.use\_amdgpu\_pro is set to auto (default).
- Added **AMDGPU Pro driver 19.10** version. The new version fixes a disappearing mouse cursor issue. Enable AMDGPU Pro driver instead of kernel integrated driver by registry key (settings to this key will only work after reboot).

[More...](#)



|                                                         |                                 |
|---------------------------------------------------------|---------------------------------|
| Parameter                                               | Use AMDGPU PRO driver           |
| Registry                                                | x.drivers.amdgpu.use_amdgpu_pro |
| Value                                                   | [Auto] [True] [False]           |
| Info: Settings to this key will only work after reboot. |                                 |

## IGEL Cloud Gateway

- Fixed support for **UMS file transfer status** in **ICG protocol**.
- When TC is managed over ICG, settings received in connection stage will not be applied immediately. **The settings must be applied after user prompt dialog**.

## 7.27 Notes for Release 10.05.700

|                       |            |             |
|-----------------------|------------|-------------|
| <b>Software:</b>      | Version    | 10.05.700   |
| <b>Release Date:</b>  | 2019-04-12 |             |
| <b>Release Notes:</b> | Version    | RN-105700-1 |
| <b>Last update:</b>   | 2019-04-12 |             |

- [IGEL Linux Universal Desktop](#)(see page 2111)



## 7.27.1 IGEL Linux Universal Desktop

### Supported Devices

#### **Universal Desktop:**

|          |                  |
|----------|------------------|
| UD2-LX:  | UD2-LX 40        |
| UD3-LX:  | UD3-LX 51        |
|          | UD3-LX 50        |
|          | UD3-LX 42        |
|          | UD3-LX 41        |
| UD5-LX:  | UD5-LX 50        |
| UD6-LX:  | UD6-LX 51        |
| UD7-LX:  | UD7-LX 10        |
| UD9-LX:  | UD9-LX Touch 41  |
|          | UD9-LX 40        |
| UD10-LX: | UD10-LX Touch 10 |
|          | UD10-LX 10       |

#### **IGEL Zero:**

|             |
|-------------|
| IZ2-RFX     |
| IZ2-HDX     |
| IZ2-HORIZON |
| IZ3-RFX     |
| IZ3-HDX     |



## IZ3-HORIZON

- Component Versions 10.05.700(see page 2112)
- General Information 10.05.700(see page 2116)
- Known Issues 10.05.700(see page 2117)
- New Features 10.05.700(see page 2118)
- Resolved Issues 10.05.700(see page 2125)

## Component Versions 10.05.700

• **Clients**

| <b>Product</b>                     | <b>Version</b>                  |
|------------------------------------|---------------------------------|
| Citrix HDX Realtime Media Engine   | 2.7.0-2113                      |
| Citrix Receiver                    | 13.10.0.20                      |
| Citrix Receiver                    | 13.5.0.10185126                 |
| Citrix Workspace App               | 18.10.0.11                      |
| deviceTRUST Citrix Channel         | 19.1.100.0                      |
| deviceTRUST RDP Channel            | 19.1.100.0                      |
| Ericom PowerTerm                   | 12.0.1.0.20170219.2-_dev_-34574 |
| Evidian AuthMgr                    | 1.5.6840                        |
| Evince PDF Viewer                  | 3.18.2-1ubuntu4.3               |
| FabulaTech USB for Remote Desktop  | 5.2.29                          |
| Firefox                            | 60.6.1                          |
| IBM iAccess Client Solutions       | 1.1.8.1                         |
| IGEL RDP Client                    | 2.2                             |
| Imprivata OneSign ProveID Embedded |                                 |
| deviceTRUST RDP Channel            | 19.1.100.0                      |



|                                         |                         |
|-----------------------------------------|-------------------------|
| Leostream Java Connect                  | 3.3.7.0                 |
| NX Client                               | 5.3.12                  |
| Open VPN                                | 2.3.10-1ubuntu2.1       |
| Oracle JRE                              | 1.8.0_202               |
| Parallels Client (64 bit)               | 16.5.2.20595            |
| Parole Media Player                     | 1.0.1-0ubuntu1igel16    |
| Remote Viewer (RedHat Virtualization)   | 7.0-igel47              |
| Spice GTK (Red Hat Virtualization)      | 0.35                    |
| Spice Protocol (Red Hat Virtualization) | 0.12.14                 |
| Usbredir (Red Hat Virtualization)       | 0.8.0                   |
| Systancia AppliDis                      | 4.0.0.17                |
| Thinlinc Client                         | 4.9.0-5775              |
| ThinPrint Client                        | 7.5.88                  |
| Totem Media Player                      | 2.30.2                  |
| Parole Media Player                     | 1.0.1-0ubuntu1igel16    |
| VMware Horizon Client                   | 4.10.0-11053294         |
| VNC Viewer                              | 1.8.0+git20180123-igel1 |
| Voip Client Ekiga                       | 4.0.1                   |

- **Dictation**

|                                                       |          |
|-------------------------------------------------------|----------|
| Diktamen driver for dictation                         |          |
| Driver for Grundig Business Systems dictation devices |          |
| Nuance Audio Extensions for dictation                 | B048     |
| Olympus driver for dictation                          | 20180621 |
| Philips Speech Driver                                 | 12.6.36  |



- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.6    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.1.0    |

- **Smartcard**

|                                           |                  |
|-------------------------------------------|------------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101          |
| PKCS#11 Library Athena IDProtect          | 623.07           |
| PKCS#11 Library cryptovision sc/interface | 7.1.9.620        |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0        |
| PKCS#11 Library SecMaker NetID            | 6.7.2.36         |
| Reader Driver ACS CCID                    | 1.1.5            |
| Reader Driver Gemalto eToken              | 10.0.37-0        |
| Reader Driver HID Global Omnikey          | 4.3.3            |
| Reader Driver Identive CCID               | 5.0.35           |
| Reader Driver Identive eHealth200         | 1.0.5            |
| Reader Driver Identive SCRKBC             | 5.0.24           |
| Reader Driver MUSCLE CCID                 | 1.4.28           |
| Reader Driver REINER SCT cyberJack        | 3.99.5final.SP11 |
| Resource Manager PC/SC Lite               | 1.8.23-1igel1    |
| Cherry USB2LAN Proxy                      | 3.0.0.6          |

- **System Components**

|                |                    |
|----------------|--------------------|
| OpenSSL        | 1.0.2g-1ubuntu4.13 |
| OpenSSH Client | 7.2p2-4ubuntu2.4   |



|                                 |                                |
|---------------------------------|--------------------------------|
| OpenSSH Server                  | 7.2p2-4ubuntu2.4               |
| Bluetooth stack (bluez)         | 5.50-0ubuntu1igel5             |
| MESA OpenGL stack               | 18.2.1-1igel51                 |
| VAAPI ABI Version               | 0.40                           |
| VDPAU Library version           | 1.1.1-3ubuntu1                 |
| Graphics Driver INTEL           | 2.99.917+git20181113-igel846   |
| Graphics Driver ATI/RADEON      | 18.0.1-1igel831                |
| Graphics Driver ATI/AMDGPU      | 18.0.1-1igel831                |
| Graphics Driver VIA             | 5.76.52.92-009-005f78-20150730 |
| Graphics Driver FBDEV           | 0.5.0-1igel819                 |
| Graphics Driver VESA            | 2.3.4-1build2igel639           |
| Input Driver Evdev              | 2.10.5-1ubuntu1igel750         |
| Input Driver Elographics        | 1.4.1-1build5igel633           |
| Input Driver eGalax             | 2.5.5814                       |
| Input Driver Synaptics          | 1.9.0-1ubuntu1igel748          |
| Input Driver Vmmouse            | 13.1.0-1ubuntu2igel635         |
| Input Driver Wacom              | 0.36.1-0ubuntu1igel813         |
| Kernel                          | 4.18.20 #mainline-ud-r2531     |
| Xorg X11 Server                 | 1.19.6-1ubuntu4igel838         |
| Xorg Xephyr                     | 1.19.6-1ubuntu4igel832         |
| CUPS printing daemon            | 2.1.3-4ubuntu0.5igel20         |
| PrinterLogic                    | 18.2.1.128                     |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1              |



|                     |                              |
|---------------------|------------------------------|
| XFCE4 Windowmanager | 4.12.3-1ubuntu2igel653       |
| ISC DHCP Client     | 4.3.3-5ubuntu12.10igel7      |
| NetworkManager      | 1.2.6-0ubuntu0.16.04.2igel58 |
| ModemManager        | 1.6.8-2igel1                 |
| GStreamer 0.10      | 0.10.36-2ubuntu0.1           |
| GStreamer 1.x       | 1.14.2-1ubuntu1igel192       |
| Python2             | 2.7.12                       |
| Python3             | 3.5.2                        |

- **Features with Limited IGEL Support**

Mobile Device Access USB

VPN OpenConnect

Scanner support

VirtualBox

- **Features with Limited Functionality**

|                   |      |
|-------------------|------|
| Cisco JVDI Client | 12.1 |
|-------------------|------|

## General Information 10.05.700

The following clients and features are **not supported** anymore:

- Citrix Receiver 12.1 and 13.1 - 13.4
- Citrix Access Gateway Standard Plug-in
- Dell vWorkspace Connector for Linux
- Ericom PowerTerm Emulation 9 and 11
- Ericom Webconnect
- IGEL Legacy RDP Client (rdesktop)
- Virtual Bridges VERDE Client
- PPTP VPN Support
- IGEL Upgrade License Tool with IGEL Smartcard Token
- Remote Management by setup.ini file transfer (TFTP)
- Remote Access via RSH
- Legacy Philips Speech Driver
- t-Systems TCOS Smartcard Support
- DUS Series touch screens
- Elo serial touch screens
- IGEL Smartcard without locking desktop



- **Video Hardware Acceleration** support is discontinued on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, UD10-LX 10
- **H.264 Hardware Acceleration** support is discontinued on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, UD10-LX 10
- **Storage Hotplug devices are not automatically removed anymore**, instead they must be always ejected manually:
  - by panel tray icon
  - by an icon in the 'In-Session Control Bar' (configurable at `IGEL Setup > User Interface > Desktop`)
  - by a 'Safely Remove Hardware' session (configurable at `IGEL Setup > Accessories`)

The following clients and features are **not available** in this release:

- Cherry eGK Channel
- Open VPN Smartcard Support
- NCP Secure Client
- Asian Input Methods
- Composite Manager

## Known Issues 10.05.700

### Citrix

- With **activated DRI3** and an **amd gpu** citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (api v2) is not affected from this issue.
- Citrix has known issues with **gstreamer1.0** which describe problems with **multimedia redirection of H264, MPEG1 and MPEG2**. Gstreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.  
As a workaround, insert the smartcard before starting StoreFront login.
- When using **Citrix Workspace App 18.10** in combination with **Philips Speech** driver, the session occasionally **does not proper terminate** at logoff and hangs.  
As a workaround, usage of **Citrix Receiver 13.10** is recommended when Philips Speech driver is needed.

Citrix **H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression** > \*"For the entire screen"\*\*.

- When **Expand the session over a self-selected number of monitors** (for **Multi-monitor full screen mode**) is used and setup is restarted, **Restrict full screen session to one monitor** is indicated and the **monitor selection is greyed out**. The functionality is available, only the notification in setup is broken.

### VMware Horizon

- **External drives** mounted already before connection **do not appear in the remote desktop**.  
Workaround: map the directory /media as a drive in your desktop. Then the external devices will show up inside the media drive.



- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping is switched off**. In the **IGEL Setup** client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to **disable local Storage Hotplug**: On page **Devices > Storage Devices > Storage Hotplug**, put **number** of storage hotplug devices to **0**.
  - On the other hand, if you use **drive mapping** instead, it is recommended that you should either **switch off USB redirection entirely** or at least **deny storage devices** by adding a filter to the USB class rules. And because Horizon Client relies on the OS to mount the storage devices itself, please go to setup page: **Devices > Storage Devices > Storage Hotplug** and switch on **Enable dynamic drive mapping** and put **Number of storage hotplug devices** to at least **1**.

#### Parallels Client

- **Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode** it is necessary to connect to the **Parallels RAS** one time with FIPS support disabled.

#### Smartcard

- In some cases there are instabilities when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- Appliance mode **RHEV/Spice**: spice-xpi firefox plugin is no longer supported. The **Console Invocation** has to allow **Native client** (auto is also possible) and it should start in fullscreen to prevent opening windows.

#### Hardware

- Suspend on **UD10** is disabled.

#### New Features 10.05.700

##### RDP/IGEL RDP Client 2

- Add **field collection** to RDP session **server** page.  
**More...**

|            |                                                                          |
|------------|--------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; RDP &gt; RDP Sessions &gt; RDP Session &gt; Server</b>  |
|            | <b>Sessions &gt; RDP &gt; RDP Sessions &gt; RDP Session &gt; Options</b> |
| Parameter  | Collection                                                               |



|          |                                                 |
|----------|-------------------------------------------------|
| Registry | sessions.winconnect<NR>.option.loadbalance-info |
|----------|-------------------------------------------------|

## VMware Horizon

- Added parameters to **specify webcam frame size** and **rate for RTAV**.  
[More...](#)

|           |                               |
|-----------|-------------------------------|
| Parameter | Webcam frame width            |
| Registry  | vmware.view.rtav-frame-width  |
| Value     | <empty_string>                |
| Parameter | Webcam frame height           |
| Registry  | vmware.view.rtav-frame-height |
| Value     | <empty_string>                |
| Parameter | Webcam frame rate             |
| Registry  | vmware.view.rtav-frame-rate   |
| Value     | <empty_string>                |

## Firefox

- Updated **Mozilla Firefox** to version **60.6.1ESR**.
- Fixes for **mfsa2019-10**, also known as: CVE-2019-9810, CVE-2019-9813.
- Fixes for **mfsa2019-08**, also known as: CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2018-18506, CVE-2019-9788.
- Fixes for **mfsa2019-05**, also known as: CVE-2018-18356, CVE-2019-5785.
- Fixes for **mfsa2019-02**, also known as: CVE-2018-18500, CVE-2018-18505, CVE-2018-18501.
- Fixes for **mfsa2018-30**, also known as: CVE-2018-17466, CVE-2018-18492, CVE-2018-18493, CVE-2018-18494, CVE-2018-18498, CVE-2018-12405.
- Added new parameters: Allow a **custom command** before and after browser session.  
[More...](#)

|           |                                |
|-----------|--------------------------------|
| Parameter | Initial Action                 |
| Registry  | sessions.browser%.init_action  |
| Value     | <empty_string>                 |
| Parameter | Final Action                   |
| Registry  | sessions.browser%.final_action |



|       |                |
|-------|----------------|
| Value | <empty_string> |
|-------|----------------|

## OS 11 Upgrade

- It is now possible to **upgrade to IGEL OS 11**. For more information, please see the particular section in kb.igel.com. The parameters for the upgrade:

**More...**

|            |                                                                   |
|------------|-------------------------------------------------------------------|
| IGEL Setup | <b>System &gt; Update &gt; OS 11 Upgrade</b>                      |
| Parameter  | Upgrade to OS 11                                                  |
| Registry   | update.firmware_migrate_to_11                                     |
| Value      | enabled / <u>disabled</u>                                         |
| IGEL Setup | <b>System &gt; Update &gt; OS 11 Upgrade</b>                      |
| Parameter  | Upgrade to OS 11 even if a previous upgrade attempt failed        |
| Registry   | update.force_firmware_migrate_to_11                               |
| Value      | enabled / <u>disabled</u>                                         |
| IGEL Setup | <b>System &gt; Update &gt; OS 11 Upgrade</b>                      |
| Parameter  | Upgrade to OS 11 even if PowerTerm is enabled                     |
| Registry   | update.migrate_to_11_with_powerterm                               |
| Value      | enabled / <u>disabled</u>                                         |
| IGEL Setup | <b>System &gt; Update &gt; OS 11 Upgrade</b>                      |
| Parameter  | Require an Enterprise Management Pack license to upgrade to OS 11 |
| Registry   | update.migrate_to_11_enterprise_required                          |
| Value      | [Smart] [Always] [Never]                                          |
| IGEL Setup | <b>System &gt; Update &gt; OS 11 Upgrade</b>                      |
| Parameter  | Timeout waiting for OS 11 license to start automatic upgrade      |



|          |                                                                         |
|----------|-------------------------------------------------------------------------|
| Registry | update.migrate_to_11_license_timeout                                    |
| Value    | [Disabled] [ <u>10 Minutes</u> ] [15 Minutes] [30 Minutes] [60 Minutes] |

- The parameters for configuring the desktop integration of the **IGEL OS 11 Upgrade tool** are:  
[More...](#)

|            |                                           |
|------------|-------------------------------------------|
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>     |
| Parameter  | Start menu                                |
| Registry   | sessions.os11_migration0.startmenu        |
| Value      | <u>enabled</u> / <u>disabled</u>          |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>     |
| Parameter  | Application Launcher                      |
| Registry   | sessions.os11_migration0.applaunch        |
| Value      | <u>enabled</u> / <u>disabled</u>          |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>     |
| Parameter  | System tab of start menu                  |
| Registry   | sessions.os11_migration0.startmenu_system |
| Value      | <u>enabled</u> / <u>disabled</u>          |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>     |
| Parameter  | System tab of Application Launcher        |
| Registry   | sessions.os11_migration0.applaunch_system |
| Value      | <u>enabled</u> / <u>disabled</u>          |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>     |
| Parameter  | Menu folder                               |
| Registry   | sessions.os11_migration0.menu_path        |
| Value      | <u>enabled</u> / <u>disabled</u>          |



|            |                                            |
|------------|--------------------------------------------|
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>      |
| Parameter  | Desktop folder                             |
| Registry   | sessions.os11_migration0.desktop_path      |
| Value      | enabled / <u>disabled</u>                  |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>      |
| Parameter  | Application Launcher folder                |
| Registry   | sessions.os11_migration0.applaunch_path    |
| Value      | enabled / <u>disabled</u>                  |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>      |
| Parameter  | Quick start panel                          |
| Registry   | sessions.os11_migration0.quick_start       |
| Value      | enabled / <u>disabled</u>                  |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>      |
| Parameter  | Password protection                        |
| Registry   | sessions.os11_migration0.pwprotected       |
| Value      | [None] [Administrator] [User] [Setup user] |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>      |
| Parameter  | Desktop                                    |
| Registry   | sessions.os11_migration0.desktop           |
| Value      | enabled / <u>disabled</u>                  |
| IGEL Setup | <b>Accessories &gt; OS 11 Upgrade</b>      |
| Parameter  | Desktop context menu                       |
| Registry   | sessions.os11_migration0.pulldown          |
| Value      | enabled / <u>disabled</u>                  |



## Citrix

- Updated **Citrix HDX RTME** used for optimization of **Skype for Business** to version **2.7.0-2113**.

## Parallels Client

- Updated Parallels Client to **version 16.5.2 (64-Bit)**

## CUPS Printing

- Added **SMB Network Print Client** function. The printer could be created on page **Devices > Printer > CUPS > Printers > Dialog**, **SMB Network Printer** as **Printer Port**. The settings for the SMB printer must be done in Setup Registry:  
[More...](#)

| IGEL Setup | <b>Devices &gt; Printer &gt; CUPS &gt; Printers &gt; Dialog</b>                                                                                     |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter  | Printer Port                                                                                                                                        |
| Registry   | print.cups.printer<NR>.backend                                                                                                                      |
| Value      | [Parallel Port Printer] [Serial Port Printer] [USB Printer] [LPD Network Printer] [TCP Network Printer] [IPP Network Printer] [SMB Network Printer] |
| Parameter  | SMB Server                                                                                                                                          |
| Registry   | print.cups.printer<NR>.smb_server                                                                                                                   |
| Parameter  | SMB Workgroup                                                                                                                                       |
| Registry   | print.cups.printer<NR>.smb_workgroup                                                                                                                |
| Parameter  | SMB Port                                                                                                                                            |
| Registry   | print.cups.printer<NR>.smb_port                                                                                                                     |
| Value      | 0                                                                                                                                                   |
| Parameter  | SMB Printer                                                                                                                                         |
| Registry   | print.cups.printer<NR>.smb_printer                                                                                                                  |
| Parameter  | SMB User                                                                                                                                            |
| Registry   | print.cups.printer<NR>.smb_user                                                                                                                     |
| Parameter  | SMB Password                                                                                                                                        |



|          |                                       |
|----------|---------------------------------------|
| Registry | print.cups.printer<NR>.crypt_password |
|----------|---------------------------------------|

## IBM\_5250

- Updated **IBM iAccess Client Solutions** to version **1.1.8.1**.

## WiFi

- Added support for **Realtek 8821CE wireless cards**.
- Added switch to determine the **source of WiFi scan results** within the **Wireless Manager**. Selecting default is currently identical with the old mechanism (using the iwlist command). This may change in the future. When iwlist fails, **NetworkManager** is automatically used as a fallback.

**More...**

|           |                                                          |
|-----------|----------------------------------------------------------|
| Parameter | WiFi Scanner                                             |
| Registry  | network.interfaces.wirelesslan.device0.mssid<br>_scanner |
| Range     | <u>default</u> / iwlist / NetworkManager                 |

Info: "default" is currently equal to "iwlist"

## X11 System

- Added **xprintidle** tool to firmware.
- The new **Display Switch** tool can use **multiple different profiles**, automatically chosen **at runtime** depending on the currently connected monitors. A profile is created, when the current monitor layout/resolution is configured via the **Display Switch** utility. The profile will be associated with the **current connected displays** automatically (manufacturer, model and used connector are used for allocation) and if applicable, the state of the **laptop lid**. The setup will be restored by hot-(un)plugging known displays, means the system will automatically switch to the already configured profile. The **Display Switch** utility itself got a new interface. All base functionality can be configured via drag & drop.

An example workflow:

- Connect the hardware and **close/open lid**
- Open the **Display Switch** Utility
  - A quick (simple) setting can be selected directly.
  - Should the desired application deviate from the possibilities provided, the **Advanced** button opens a drag & drop interface for further settings.
- In this interface the displays can be **dragged and dropped** for the intended configuration. The **display will snap adjacent** to others.
- If a **display should not be used**, it can be dragged to the **Disabled** area on the top right - the screen will be reactivated when it is dragged back to the active area.
- To show the **same content on multiple displays**, one display should be dragged onto an other active screen. The interface will show **Mirror**. The mirroring monitor will be displayed on the lower right.



- With the **Apply** button the current state will be set, with **Yes** on the **Keep configuration** dialog the current settings will be saved to persistent storage and associated with the profile.
- Advanced functionality** (panning/scaling/resolutions) can be configured in drop-down boxes, hidden in a **drawer** on the right side. The drawer can be expanded by clicking the < button on the right edge.
- For the **Display Switch** functionality the following parameters should be enabled for proper usage:  
[More...](#)

|            |                                                     |
|------------|-----------------------------------------------------|
| IGEL Setup | <b>Accessories &gt; Display Switch &gt; Options</b> |
| Parameter  | Preserve settings over reboot                       |
| Registry   | sessions.user_display0.options.preserve_settings    |
| Value      | enabled / <u>disabled</u>                           |
| IGEL Setup | <b>Accessories &gt; Display Switch &gt; Options</b> |
| Parameter  | Smart display configuration                         |
| Registry   | x.auto_associate                                    |
| Value      | enabled / <u>disabled</u>                           |

- The **IGEL Display Switch** utility is now used for **NVIDIA graphics** devices as well.

#### Smartcard

- Updated **SecMaker NetiD** to version **6.7.2.36**: now **Yubikey 5** is supported.

#### Resolved Issues 10.05.700

##### Citrix

- Appropriate icons** arise with IGEL and Citrix authentication
- Fixed crash when **H.264 acceleration** and **RTME** will be used on two or more concurrent VDI sessions.

##### VMware Horizon

- Added recognition for **password-change-dialog** in Horizon **local-logon** sessions or appliance mode.
- Fixed optimization for **Skype for Business**.
- Added switch to use **system-wide proxy** in VMware Horizon appliance mode.  
[More...](#)

|           |                          |
|-----------|--------------------------|
| Parameter | Use the systemwide proxy |
|-----------|--------------------------|



|          |                           |
|----------|---------------------------|
| Registry | vmwarevdmapp.use_proxy    |
| Value    | <u>enabled</u> / disabled |

#### Parallels Client

- Fixed: **Maximized windows** for published applications can be displayed incorrectly.
- Fixed: Incorrect **user credentials** can be picked up during connection, when same farm is registered multiple times with different user credentials
- Fixed: **Linux** client not consider **universal printing policies**, set from the server

#### PowerTerm

- Fixed editing of parameter sessions.powerterm\<INST>.logindialog.loginscript in Setup Registry: **now multiple lines are possible**.

#### Firefox

- Fixed an occasional issue with Firefox **not being in fullscreen** after a suspend.

#### Network

- Improved **SCEP** client robustness
  - The **cert\_agent script** does not terminate anymore, when a problem occurs (e.g. the SCEP server is unreachable) but tries again after the expiry check interval.
  - When the **client certificate has expired**, there is still one attempt for a renewal. However, when that fails, a new one is requested. That obviously will fail, if the client presents a challenge password that is not valid anymore.
- Improved expiration time of **ethernet no-link notification**
- Fixed **MBB router configuration** (broken since 10.05.500)
- Added all **Ethernet network drivers** from OS to LX version.
- Changed **e1000e** driver to **3.4.2.3** - directly from Intel.
- Changed **igb** driver to **5.3.5.22** - also directly from Intel.

#### Smartcard

- Fixed **OpenSC** setting **max\_send\_size** for reader driver **pcsc** in /etc/opensc/opensc.conf.
- Fixed **Dell KB813 Smartcard Keyboard** in combination with certain smartcards, driven by **OpenSC PKCS#11 module**. Before this fix, authentication to Citrix StoreFront and VMWare Horizon failed.

#### Application Launcher

- Fixed confusion in **nameserver list** caused by comments in /etc/resolv.conf

#### Base system

- Fixed sporadic **bootsplash** issue.
- Fixed **Screensaver** and **Screenlock timeouts** to be independent. When both timeouts are set, the start of screenlock will not reset the screensaver timeout anymore.
- Added package **ldap-utils** which could be used via **custom scripts**.
- Fixed playback of **AAC coded audio streams** on **IGEL Zero** products.
- Fixed **delay in logon as local user**, when logon with **IGEL Smartcard** is also active.
- Fixed **random 90 seconds shutdown delay** (systemd).



- Fixed **custom bootsplash** installation.

#### Appliance Mode

- Fixed a **regression in 10.05.570** that prevents appliance mode from restarting after a suspend.

#### Storage Devices

- Fixed **auto mounting of storage devices** inside of **Olympus DS-9500 Digital Voice Recorder**.

#### Base System

- Fixed issues with **gen4/5 intel graphic driver** in kernel **4.18.20**.
- Fixed **suspend/resume hangs** when logged into **Citrix sessions**.
- Fixed **CPU scaler and volume control** applet suspend/resume issue.

#### X11 system

- Fixed the **missing volume control** in the panel, when the panel is configured to disappear while the login/lock screen is shown.
- The **In-Session Control Bar** now scales with the current DPI setting.
- There is now a registry key to **ignore a 3Dconnexion SpaceMouse** for IGEL graphical use (X11). If activated, the **SpaceMouse** is only passed thru to the desktop session. If false, it acts like the standard mouse.

[More...](#)

|           |                                                          |
|-----------|----------------------------------------------------------|
| Parameter | Deactivates a 3Dconnexion SpaceMouse as a standard mouse |
| Registry  | <code>userinterface.mouse.spacemouse.x11_ignore</code>   |
| Value     | <u>enabled</u> / disabled                                |

- The following **SpaceMouse** products are included (VID, PID, Vendor, Product).

[More...](#)

0x046D; 0xC603; Logitech, Inc.; 3Dconnexion Spacemouse Plus XT  
 0x046D; 0xC605; Logitech, Inc.; 3Dconnexion CADman  
 0x046D; 0xC606; Logitech, Inc.; 3Dconnexion Spacemouse Classic  
 0x046D; 0xC621; Logitech, Inc.; 3Dconnexion Spaceball 5000  
 0x046D; 0xC623; Logitech, Inc.; 3Dconnexion Space Traveller 3D Mouse  
 0x046D; 0xC625; Logitech, Inc.; 3Dconnexion Space Pilot 3D Mouse  
 0x046D; 0xC626; Logitech, Inc.; 3Dconnexion Space Navigator 3D Mouse  
 0x046D; 0xC627; Logitech, Inc.; 3Dconnexion Space Explorer 3D Mouse  
 0x046D; 0xC628; Logitech, Inc.; 3Dconnexion Space Navigator for Notebooks  
 0x046D; 0xC629; Logitech, Inc.; 3Dconnexion SpacePilot Pro 3D Mouse  
 0x046D; 0xC62B; Logitech, Inc.; 3Dconnexion Space Mouse Pro  
 0x256F; \*\*; 3Dconnexion; SpaceMouse



- **USB device reset via USB powercycle on UD6 / UD7 available.**
- Fixed **screen flicker** in some cases if **Force NumLock On** (x.global.forcenumlock) is active.

#### Caradigm

- Fixed **Horizon session** teardown.

#### Window manager

- Fixed option to **disable the local window manager**.

#### Audio

- Fixed bad quality sound over **DisplayPort** in a **Citrix ICA session** or other applications using **ALSA API**.
- Fixed configuration of **default audio** output and input.

#### Hardware

- Added possibility to use **AMDGPU PRO** driver instead of the kernel integrated driver.  
**More...**

|           |                                 |
|-----------|---------------------------------|
| Parameter | Use AMDGPU PRO driver           |
| Registry  | x.drivers.amdgpu.use_amdgpu_pro |
| Value     | [Auto] [True] [False]           |

Info: Settings to this key will only work after reboot.

#### IGEL Cloud Gateway

- Fixed support for **UMS file transfer status** in **ICG protocol**.
- When TC is managed over ICG, settings received in connection stage will not be applied immediately. **The settings must be applied after user prompt dialog**.

## 7.28 Notes for Release 10.05.500

|                       |            |             |
|-----------------------|------------|-------------|
| <b>Software:</b>      | Version    | 10.05.500   |
| <b>Release Date:</b>  | 2018-12-20 |             |
| <b>Release Notes:</b> | Version    | RN-105500-1 |
| <b>Last update:</b>   | 2018-12-20 |             |

- [IGEL Linux Universal Desktop](#)(see page 2129)
- [IGEL Universal Desktop OS3/IGEL UD Pocket](#)(see page 2146)
- [IGEL Universal Desktop Converter \(UDC3\)](#)(see page 2163)



## 7.28.1 IGEL Linux Universal Desktop

### Supported Devices

#### **Universal Desktop:**

|          |                  |
|----------|------------------|
| UD2-LX:  | UD2-LX 40        |
| UD3-LX:  | UD3-LX 51        |
|          | UD3-LX 50        |
|          | UD3-LX 42        |
|          | UD3-LX 41        |
| UD5-LX:  | UD5-LX 50        |
| UD6-LX:  | UD6-LX 51        |
| UD7-LX:  | UD7-LX 10        |
| UD9-LX:  | UD9-LX Touch 41  |
|          | UD9-LX 40        |
| UD10-LX: | UD10-LX Touch 10 |
|          | UD10-LX 10       |

#### **IGEL Zero:**

|             |
|-------------|
| IZ2-RFX     |
| IZ2-HDX     |
| IZ2-HORIZON |
| IZ3-RFX     |
| IZ3-HDX     |



## IZ3-HORIZON

- Component Versions 10.05.500(see page 2130)
- General Information 10.05.500(see page 2134)
- Known Issues 10.05.500(see page 2135)
- New Features 10.05.500(see page 2136)
- Resolved Issues 10.05.500(see page 2143)

## Component Versions 10.05.500

• **Clients**

| <b>Product</b>                     | <b>Version</b>                  |
|------------------------------------|---------------------------------|
| Citrix HDX Realtime Media Engine   | 2.6.0-2030                      |
| Citrix Receiver                    | 13.10.0.20                      |
| Citrix Receiver                    | 13.5.0.10185126                 |
| Citrix Workspace App               | 18.10.0.11                      |
| deviceTRUST Citrix Channel         | 19.1.100.0                      |
| deviceTRUST RDP Channel            | 19.1.100.0                      |
| Ericom PowerTerm                   | 12.0.1.0.20170219.2-_dev_-34574 |
| Evidian AuthMgr                    | 1.5.6840                        |
| Evince PDF Viewer                  | 3.18.2-1ubuntu4.3               |
| FabulaTech USB for Remote Desktop  | 5.2.29                          |
| Firefox                            | 60.3.0                          |
| IBM iAccess Client Solutions       | 1.1.5.0                         |
| IGEL RDP Client                    | 2.2                             |
| Imprivata OneSign ProveID Embedded |                                 |
| Leostream Java Connect             | 3.3.7.0                         |



|                                         |                         |
|-----------------------------------------|-------------------------|
| NX Client                               | 5.3.12                  |
| Open VPN                                | 2.3.10-1ubuntu2.1       |
| Oracle JRE                              | 1.8.0_192               |
| Parallels Client (32 bit)               | 16.5.2.20588            |
| Parole Media Player                     | 1.0.1-0ubuntu1igel16    |
| Remote Viewer (RedHat Virtualization)   | 7.0-igel47              |
| Spice GTK (Red Hat Virtualization)      | 0.35                    |
| Spice Protocol (Red Hat Virtualization) | 0.12.14                 |
| Usbredir (Red Hat Virtualization)       | 0.8.0                   |
| Systancia AppliDis                      | 4.0.0.17                |
| Thinlinc Client                         | 4.9.0-5775              |
| ThinPrint Client                        | 7.5.88                  |
| Totem Media Player                      | 2.30.2                  |
| VMware Horizon Client                   | 4.10.0-11053294         |
| VNC Viewer                              | 1.8.0+git20180123-igel1 |
| Voip Client Ekiga                       | 4.0.1                   |

- **Dictation**

|                                                       |          |
|-------------------------------------------------------|----------|
| Diktamen driver for dictation                         |          |
| Driver for Grundig Business Systems dictation devices |          |
| Nuance Audio Extensions for dictation                 | B048     |
| Olympus driver for dictation                          | 20180621 |
| Philips Speech Driver                                 | 12.6.36  |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
|---------------------------|----------|



|                         |       |
|-------------------------|-------|
| signotec Citrix Channel | 8.0.6 |
| signotec VCOM Daemon    | 2.0.0 |
| StepOver TCP Client     | 2.1.0 |

- **Smartcard**

|                                           |                  |
|-------------------------------------------|------------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101          |
| PKCS#11 Library Athena IDProtect          | 623.07           |
| PKCS#11 Library cryptovision sc/interface | 7.1.9.620        |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0        |
| PKCS#11 Library SecMaker NetID            | 6.7.0.23         |
| Reader Driver ACS CCID                    | 1.1.5            |
| Reader Driver Gemalto eToken              | 10.0.37-0        |
| Reader Driver HID Global Omnikey          | 4.3.3            |
| Reader Driver Identive CCID               | 5.0.35           |
| Reader Driver Identive eHealth200         | 1.0.5            |
| Reader Driver Identive SCRKBC             | 5.0.24           |
| Reader Driver MUSCLE CCID                 | 1.4.28           |
| Reader Driver REINER SCT cyberJack        | 3.99.5final.SP11 |
| Resource Manager PC/SC Lite               | 1.8.23-1igel1    |
| Cherry USB2LAN Proxy                      | 3.0.0.6          |

- **System Components**

|                |                    |
|----------------|--------------------|
| OpenSSL        | 1.0.2g-1ubuntu4.13 |
| OpenSSH Client | 7.2p2-4ubuntu2.4   |
| OpenSSH Server | 7.2p2-4ubuntu2.4   |



|                                 |                                |
|---------------------------------|--------------------------------|
| Bluetooth stack (bluez)         | 5.50-0ubuntu1igel5             |
| MESA OpenGL stack               | 18.2.1-1igel51                 |
| VAAPI ABI Version               | 0.40                           |
| VDPAU Library version           | 1.1.1-3ubuntu1                 |
| Graphics Driver INTEL           | 2.99.917+git20181113-igel846   |
| Graphics Driver ATI/RADEON      | 18.0.1-1igel831                |
| Graphics Driver ATI/AMDGPU      | 18.0.1-1igel831                |
| Graphics Driver VIA             | 5.76.52.92-009-005f78-20150730 |
| Graphics Driver FBDEV           | 0.5.0-1igel819                 |
| Graphics Driver VESA            | 2.3.4-1build2igel639           |
| Input Driver Evdev              | 2.10.5-1ubuntu1igel750         |
| Input Driver Elographics        | 1.4.1-1build5igel633           |
| Input Driver eGalax             | 2.5.5814                       |
| Input Driver Synaptics          | 1.9.0-1ubuntu1igel748          |
| Input Driver Vmmouse            | 13.1.0-1ubuntu2igel635         |
| Input Driver Wacom              | 0.36.1-0ubuntu1igel813         |
| Kernel                          | 4.18.20 #mainline-ud-r2481     |
| Xorg X11 Server                 | 1.19.6-1ubuntu4igel838         |
| Xorg Xephyr                     | 1.19.6-1ubuntu4igel832         |
| CUPS printing daemon            | 2.1.3-4ubuntu0.5igel20         |
| PrinterLogic                    | 18.2.1.128                     |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1              |



|                     |                              |
|---------------------|------------------------------|
| XFCE4 Windowmanager | 4.12.3-1ubuntu2igel653       |
| ISC DHCP Client     | 4.3.3-5ubuntu12.10igel7      |
| NetworkManager      | 1.2.6-0ubuntu0.16.04.2igel58 |
| ModemManager        | 1.6.8-2igel1                 |
| GStreamer 0.10      | 0.10.36-2ubuntu0.1           |
| GStreamer 1.x       | 1.14.2-1ubuntu1igel192       |
| Python2             | 2.7.12                       |
| Python3             | 3.5.2                        |

- **Features with Limited IGEL Support**

|                          |
|--------------------------|
| Mobile Device Access USB |
|--------------------------|

|                 |
|-----------------|
| VPN OpenConnect |
|-----------------|

|                 |
|-----------------|
| Scanner support |
|-----------------|

|            |
|------------|
| VirtualBox |
|------------|

- **Features with Limited Functionality**

|                   |      |
|-------------------|------|
| Cisco JVDI Client | 12.1 |
|-------------------|------|

## General Information 10.05.500

The following clients and features are **not supported** anymore:

- **Citrix Receiver 12.1 and 13.1 - 13.4**
- **Citrix Access Gateway** Standard Plug-in
- **Dell vWorkspace Connector** for Linux
- **Ericom PowerTerm Emulation 9** and **11**
- **Ericom Webconnect**
- **IGEL Legacy RDP Client** (rdesktop)
- Virtual Bridges **VERDE Client**
- **PPTP VPN** Support
- **IGEL Upgrade License Tool** with **IGEL Smartcard Token**
- Remote Management by **setup.ini file transfer** (TFTP)
- Remote Access via **RSH**
- Legacy **Philips Speech Driver**
- t-Systems **TCOS Smartcard Support**
- **DUS Series** touch screens
- **Elo serial** touch screens
- **IGEL Smartcard without locking desktop**



- **Video Hardware Acceleration Support is discontinued** on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, UD10-LX 10
- **H.264 Hardware Acceleration Support is discontinued** on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, UD10-LX 10
- **Storage Hotplug devices are not automatically removed anymore**, instead they must be always ejected manually:
  - by panel tray icon
  - by an icon in the **In-Session Control Bar** (configurable at **IGEL Setup > User Interface > Desktop**)
  - by a **Safely Remove Hardware** session (configurable at **IGEL Setup > Accessories**)

The following clients and features are **not available** in this release:

- **Cherry eGK Channel**
- **Open VPN Smartcard Support**
- **NCP Secure Client**
- **Asian Input Methods**
- **Composite Manager**

## Known Issues 10.05.500

### Citrix

- **With activated DRI3 and an amd gpu citrix h264 acceleration plugin could freeze.** Selective H.264 mode (api v2) is not affected from this issue.
- Citrix has known issues with **gstreamer1.0** which describe problems with multimedia redirection of H264, MPEG1 and PEG2. Gstreamer1.0 is used if browser content redirection is active.
- **Browser content redirection does not work with** activated DRI3 and hardware accelerated H.264 deep compression codec.
- **Citrix StoreFront Login with Gemalto smartcard middleware does not detect smartcard correctly** if the card is inserted after start of Login. As a workaround, insert the smartcard before starting StoreFront Login.
- When using **Citrix Workspace App 18.10 in combination with Philips Speech driver**, the session occasionally does not properly terminate at logoff and hangs. As a workaround, usage of **Citrix Receiver 13.10** is recommended when Philips Speech driver is needed.
- **Citrix H264 acceleration plugin does not work with \*\*enabled\*\* server policy "Optimize for 3D graphics workload"** in combination with server policy **Use video codec compression > For the entire screen**.
- When **Expand the session over a self-selected number of monitors** (for "Multi-Monitor full screen mode") is used and setup is restarted, **Restrict full screen session to one monitor** is indicated and the monitor selection is greyed out. **The functionality is available, only the notification in setup is broken.**

### VMware Horizon



- **External drives** mounted already before connection **do not appear in the remote desktop**.  
Workaround: map the directory /media as a drive in your desktop. Then the external devices will show up inside the media drive.
- **Client drive mapping** and **USB redirection for storage devices** should **not** be enabled both at the same time.
  - On the one hand, if you want to use USB redirection for your storage devices.

Note that the USB on-insertion feature is only working if the **Client Drive Mapping** is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**.

It is also recommended to disable local **Storage Hotplug**: On page **Devices > Storage Devices > Storage Hotplug**, put number of storage hotplug devices to 0.

- On the other hand, if you use drive mapping instead, it is recommended that you should either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. And because Horizon Client relies on the OS to mount the storage devices itself, please go to setup page: **Devices > Storage Devices > Storage Hotplug** and switch on **Enable dynamic drive mapping** and put **Number of storage hotplug devices** to at least 1.

#### Parallels Client

- **Native USB redirection** does not work with Parallels Client.
- For using the new **FIPS 140-2 compliance mode** it is necessary to connect to the Parallels RAS one time with FIPS support disabled.

#### Smartcard

- In some cases, there are instabilities when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- **Appliance mode RHEV/Spice**: spice-xpi firefox plugin is no longer supported. The "Console Invocation" has to allow Native client (auto is also possible) and it should start in fullscreen to prevent opening windows.

#### Hardware

- **Suspend on UD10 is disabled**.

#### IGEL Cloud Gateway

- **No support for UMS file transfer status** in ICG protocol.

## New Features 10.05.500

#### Citrix

- Integrated **Citrix Workspace app 18.10**.
  - There is now a registry key to enable **Citrix Workspace App selfservice web UI mode**.  
[More...](#)



|           |                                                      |
|-----------|------------------------------------------------------|
| Parameter | Enable Citrix Workspace app self-service web UI mode |
| Registry  | ica.authman.cwacapableenabled                        |
| Value     | <u>enabled</u> / disabled                            |

- There is now a registry key to make a **Bloomberg v4 keyboard** available across multiple sessions. Additionally USB redirection has to be enabled at least for this device: vid=1188 pid=9545.

[More...](#)

|           |                                     |
|-----------|-------------------------------------|
| Parameter | Bloomberg v4 keyboard               |
| Registry  | ica.allregions.bloombergredirection |
| Value     | <u>default</u> / true / false       |

- Removed parameter for **Citrix Cloud**. This parameter is not needed anymore.

[More...](#)

#### IGEL Setup **Sessions > Citrix > Citrix Global > Options**

Parameter Connect to cloud

Registry ica.cloudconnect

- Citrix client version 13.9.1 was removed.

Available Citrix client versions: **13.5.0, 13.10, 18.10** (default)

- It is now possible to **span a Citrix session over a self-defined number of consecutive monitors**. For this, the parameter ica.wfclient.usexdgfullscreen must be deactivated and ica.pnlogin.spanmonitorenable activated. The selection must be defined in the parameter ica.pnlogin.spanmonitor.

[More...](#)

#### IGEL Setup **Sessions > Citrix > Citrix Global > Window**

Parameter Expand the session over a self-selected number of monitors

Registry ica.pnlogin.spanmonitorenable

Value enabled / disabled

#### IGEL Setup **Sessions > Citrix > Citrix Global > Window**

Parameter Monitor selection

Registry ica.pnlogin.spanmonitor



|                                                                                                                                  |     |
|----------------------------------------------------------------------------------------------------------------------------------|-----|
| Value                                                                                                                            | " " |
| Sample: When using four monitors and expansion of session across monitor 2, 3 and 4 is wanted, insertion should be 2,3,4 or 2,4. |     |

- **Setup renaming**

[More...](#)

| Old Name                                     | New Name                                |
|----------------------------------------------|-----------------------------------------|
| Citrix XenDesktop / XenApp                   | Citrix                                  |
| Citrix Receiver Selection                    | Citrix Workspace Client Selection       |
| Citrix Receiver version                      | Citrix Client version                   |
| HDX / ICA Global                             | Citrix Global                           |
| Legacy ICA Sessions                          | Citrix Legacy ICA Sessions              |
| Citrix Storefront/Webinterface               | Citrix Storefront                       |
| XenApp                                       | Citrix Virtual Apps                     |
| XenDesktop                                   | Citrix Virtual Desktops                 |
| XenApp / XenDesktop                          | Citrix Virtual Apps / Desktops          |
| Server Location: XenApp 6.x or older         | Server Location: Web Interface          |
| Server Location: XenApp/XenDesktop 7.x Store | Server Location: Storefront             |
| Server Location: XenApp/XenDesktop 7.x       | Server Location: StoreFront Legacy Mode |
| Legacy Mode                                  |                                         |

- Updated **deviceTrust** client to version **19.1.100**.

#### IGEL Linux Recovery

- Enhanced **IGEL Linux Recovery installer** by a new option to force a legacy installation if booted in EFI mode.
- Updated **preparestick** tool to version 3.3.0.0 with the following fixes:
  - WMI NullReferenceException
  - dd.exe Processbar asynchronous
  - diskpart->clean failed with access denied

#### RDP/IGEL RDP Client 2

- Updated **deviceTrust** client to version 19.1.100.

#### VMware Horizon

- Updated **Horizon Client** for Linux to **version 4.10.0-11053294**. Added support for the new features:
  - **H.264 High Color Accuracy**
  - [More...](#)

|            |                                                                                    |
|------------|------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Server Options</b> |
| Parameter  | High Color Accuracy mode                                                           |



|          |                                                   |
|----------|---------------------------------------------------|
| Registry | <code>vmware.view.high-color-accuracy-mode</code> |
| Value    | <u>enabled / disabled</u>                         |

- **Serial port redirection support**

[More...](#)

|            |                                                                                             |
|------------|---------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Serial Port Redirection</b> |
| Parameter  | Serial Port Redirection                                                                     |
| Registry   | <code>vmware.view.high-color-accuracy-mode</code>                                           |
| Value      | <u>enabled / disabled</u>                                                                   |

- **High resolution display scaling and DPI synchronisation**

[More...](#)

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Display Scaling                              |
| Registry  | <code>vmware.view.use-display-scaling</code> |
| Value     | <u>enabled / disabled</u>                    |

- **Relative mouse support**

[More...](#)

|           |                                                |
|-----------|------------------------------------------------|
| Parameter | Relative Mouse Feature for a Remote Desktop    |
| Registry  | <code>vmware.view.enable-relative-mouse</code> |
| Value     | <u>enabled / disabled</u>                      |

- **Automatically hide toolbar**

[More...](#)

|           |                                             |
|-----------|---------------------------------------------|
| Parameter | Auto-hide menu bar (tool bar)               |
| Registry  | <code>vmware.view.menu-bar-auto-hide</code> |
| Value     | <u>enabled / disabled</u>                   |

## Parallels Client

- Updated Parallels Client to **version 16.5.2**
  - Fixed: Remote session closes triggered by audio playback

## IBM\_5250

- Enhanced configuration of **IBM iAccess Client**. The following parameters were added:  
[More...](#)



|           |                                                           |
|-----------|-----------------------------------------------------------|
| Parameter | Open new sessions in a new tab                            |
| Registry  | ibm.iaccess.acssm.opensessionintab                        |
| Value     | <u>enabled</u> / disabled                                 |
| Parameter | Always display the tab bar                                |
| Registry  | ibm.iaccess.acssm.alwaysshownabar                         |
| Value     | enabled / <u>disabled</u>                                 |
| Parameter | Switch to new tab when created                            |
| Registry  | ibm.iaccess.acssm.switchtonewtab                          |
| Value     | <u>enabled</u> / disabled                                 |
| Parameter | Send a warning when closing multiple tabs                 |
| Registry  | ibm.iaccess.acssm.closemultipletabwarning                 |
| Value     | <u>enabled</u> / disabled                                 |
| Parameter | Do not start tabbed sessions until the tab is selected    |
| Registry  | ibm.iaccess.acssm.tabdelayedstart                         |
| Value     | <u>enabled</u> / <u>disabled</u>                          |
| Parameter | New Tab Action                                            |
| Registry  | ibm.iaccess.acssm.newtabaction                            |
| Range     | [Disable and Hide] [ <u>Run the Same</u> ] [Run Other...] |
| Parameter | Tab Placement                                             |
| Registry  | ibm.iaccess.acssm.tabplacement                            |
| Range     | [Top][Bottom] [Left] [Right]                              |
| Parameter | List of visible menu entries                              |
| Registry  | ibm.sessions.iaccess%.options.deletemenus                 |
| Value     | list of visible menu entries                              |



## Firefox

- Updated Mozilla Firefox to **version 60.3.0ESR**  
Fixes for **mfsa2018-27**, also known as: CVE-2018-12392, CVE-2018-12393, CVE-2018-12395, CVE-2018-12396, CVE-2018-12397, CVE-2018-12389, CVE-2018-12390.

## Cisco JVDI Client

- Updated Cisco JVDI client to **version 12.1**

## Base system

- Updated **French** and **Dutch** user interface translation.

## Driver

- **Philips Speech Drivers** for Citrix and RDP version 12.6.36  
Support of the new Philips dictation devices **SpeechOne 6000** and **SpeechAir 2000**

## Audio

- Added support for **Jabra Xpress** mechanism to deploy firmware updates and settings on **Jabra USB headsets**.

[More...](#)

|           |                                             |
|-----------|---------------------------------------------|
| Parameter | File name of Xpress package                 |
| Registry  | jabra.xpress.package_name                   |
| Parameter | URL hosting Xpress packages                 |
| Registry  | jabra.xpress.package_url                    |
| Parameter | Login name for access to Xpress package URL |
| Registry  | jabra.xpress.package_url_login              |
| Parameter | Password for access to Xpress package URL   |
| Registry  | jabra.xpress.package_url_crypt_password     |
| Parameter | Check SSL certificate                       |
| Registry  | jabra.xpress.package_url_ssl_cert_check     |
| Value     | <u>enabled</u> / disabled                   |
| Parameter | URL of the Audio Device Dashboard server    |
| Registry  | jabra.xpress.device_dashboard.server_url    |



- Added suspend on idle for **Jabra wireless headsets**. The headsets are set to offline state after 5 seconds of idle time.

**More...**

|           |                               |
|-----------|-------------------------------|
| Parameter | Suspend on idle               |
| Registry  | devices.jabra.suspend_on_idle |
| Value     | <u>enabled</u> / disabled     |

- Added parameters to configure the **deferred volume synchronization** in **Pulseaudio**.

**More...**

|           |                                                                 |
|-----------|-----------------------------------------------------------------|
| Parameter | Enable deferred volume                                          |
| Registry  | multimedia.pulseaudio.daemon.enable-deferred-volume             |
| Value     | <u>enabled</u> / disabled                                       |
| Parameter | Safety margin                                                   |
| Registry  | multimedia.pulseaudio.daemon.deferred-volume-safety-margin-usec |
| Value     | 8000                                                            |
| Parameter | Extra delay                                                     |
| Registry  | multimedia.pulseaudio.daemon.deferred-volume-extra-delay-usec   |
| Value     | 0                                                               |

- Added a parameter to force **configured volumes** for in- and output devices in **Pulseaudio**.

**More...**

|           |                                  |
|-----------|----------------------------------|
| Parameter | Force Volume Settings            |
| Registry  | userinterface.sound.force        |
| Value     | <u>enabled</u> / <u>disabled</u> |

## Java

- Updated Oracle Java Runtime Environment to **version 1.8.0 U192**.

## IGEL Cloud Gateway

- Added support for ICG High Availability and ICG load balancing to the **IGEL remote management service**.



## Resolved Issues 10.05.500

### Citrix

- Fixed tool **icacontrol**
- Added: clear error message is returned when a **published desktop is occupied by another user**.
- Added: clear error message is returned when **misconfiguration inhibits start of an application**.

### RDP/IGEL RDP Client 2

- Fixed login error message being displayed in **English** only.
- **Allow server side per user scaling for multimonitor configurations** as well (RDP sessions desktop scaling factor must be set to 100% for this to work):
  - Global setting
  - [More...](#)

| IGEL Setup | <b>Sessions &gt; RDP &gt; RDP Global &gt; Window</b> |
|------------|------------------------------------------------------|
| Parameter  | Desktop scale factor                                 |
| Registry   | rdp.winconnect.desktop-scale-factor                  |
| Value      | <u>auto</u> / 100% / 125% / 150%                     |

- Session setting
- [More...](#)

| IGEL Setup | <b>Sessions &gt; RDP &gt; RDP Sessions &gt; **RDP Session** &gt; Window</b> |
|------------|-----------------------------------------------------------------------------|
| Parameter  | Desktop scale factor                                                        |
| Registry   | sessions.winconnect%.option.desktop-scale-factor                            |
| Value      | Global setting / auto / 100% / 125% / 150%                                  |

### Evidian

- Fixed **NLA support** in Evidian AuthMgr RDP session type

### Network

- Fixed handling of the following registry keys:
  - network.interfaces.wirelesslan.device0.driver.disable\_ht
  - network.interfaces.wirelesslan.device0.driver.chain\_num
  - network.interfaces.wirelesslan.device0.driver.cfg80211.cfg80211\_disable\_40mhz\_24ghz

The first and the second parameters only affect the driver **rt2800ub** (used e.g. for Ralink RT3372 and RT5572)



- Fixed **iptables IPv6 support** by adding IPv6 netfilter kernel modules.

#### WiFi

- Fixed connection to **hidden WiFi networks**

#### Cisco JVDI Client

- Fixed: Applications are now startable via **desktop**, start menu and **application launcher**.
- Fixed Webcam support with **32Bit Citrix Receiver** for JVDI.

#### Open VPN

- Fixed **desktop folder support** for OpenVPN session.

#### Smartcard

- Improved **waiting for smartcard events**.

#### Base system

- **IGEL Setup Assistant will no longer start multiple times**, the existing instance will be raised instead.
- Fixed **automatic firmware update** on shutdown.

#### Storage Devices

- Fixed potential **hangs on suspend/shutdown** when a **USB memory stick** was in use at that time.

#### X11 system

- Fixed **huge icons** in GTK applications when DPI setting was below 96.
- Fixed problems with **Avaya VDI Communicator** and webcams.
- **Disabled SNA sprite X video support as default** because it is unstable and could crash X server.
  - New registry key:  
[More...](#)

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | Use SNA sprite video feature (could be unstable) |
| Registry  | x.drivers.intel.sprite_video                     |
| Value     | enabled / <u>disabled</u>                        |

#### Window manager

- Fixed the **custom UI colors for the window manager decoration** that was broken in 10.05.100. The custom UI colors are now applied to the window borders again.

#### Audio

- Applied workarounds concerning **USB control requests on Plantronics C510 and 520**.
- Fixed **initialization of sound card** in **Dell Wyse 3040**.
- Fixed blocking mode in compatibility **Pulseaudio PCM plugin for ALSA**. The blocking mode is used by Parallels client to playback sound.

#### Media Player (Parole)



- Parole media player now displays a **looping animation** while initiating the connection for **rtmp streams**.
- **Extended integration** of Parole media player configuration in the setup. The following configuration keys are now respected.

[More...](#)

|            |                                                                                                                                                                 |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Media Player &gt; Media Player Global &gt; Window</b>                                                                                          |
| Parameter  | Automatically resize the player window when a new video is loaded                                                                                               |
| Registry   | multimedia.mediaplayer.auto_resize                                                                                                                              |
| Value      | enabled / <u>disabled</u>                                                                                                                                       |
| IGEL Setup | <b>Sessions &gt; Media Player &gt; Media Player Global &gt; Window</b>                                                                                          |
| Parameter  | Main window should stay on top                                                                                                                                  |
| Registry   | multimedia.mediaplayer.window_on_top                                                                                                                            |
| Value      | enabled / <u>disabled</u>                                                                                                                                       |
| IGEL Setup | <b>Sessions &gt; Media Player &gt; Media Player Global &gt; Options</b>                                                                                         |
| Parameter  | Network connection speed                                                                                                                                        |
| Registry   | multimedia.mediaplayer.connection_speed                                                                                                                         |
| Range      | [56 kbps Modem/ISDN] [112 kbps Dual ISDN/DSL]<br>[256 kbps DSL/Cable] [384 kbps DSL/Cable]<br>[512 kbps DSL/Cable] [1.5 mbps T1/Intranet/LAN]<br>[Intranet/LAN] |
| Parameter  | Enable debug                                                                                                                                                    |
| Registry   | multimedia.mediaplayer.debug                                                                                                                                    |



|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

## Evidian

- Added support to **log out Citrix session type** on tap event.

**More...**

|           |                                                    |
|-----------|----------------------------------------------------|
| Parameter | Logout behavior                                    |
| Registry  | evidian.sessiontype.ctx.pnlogout                   |
| Value     | <u>[Default]</u> [Force disconnect] [Force logoff] |

## Hardware

- Fixed problems with **mouse cursor on intel cherryview devices**.

## 7.28.2 IGEL Universal Desktop OS3/IGEL UD Pocket

## Supported Hardware:

<https://kb.igel.com/igelos/en/devices-supported-by-udc3-and-ud-pocket-3117174.html>

- 
- Component Versions 10.05.500(see page 2146)
  - General Information 10.05.500(see page 2151)
  - Known Issues 10.05.500(see page 2151)
  - New Features 10.05.500(see page 2153)
  - Resolved Issues 10.05.500(see page 2159)

## Component Versions 10.05.500

- Clients**

| Product                          | Version         |
|----------------------------------|-----------------|
| Citrix HDX Realtime Media Engine | 2.6.0-2030      |
| Citrix Receiver                  | 13.10.0.20      |
| Citrix Receiver                  | 13.5.0.10185126 |
| Citrix Workspace App             | 18.10.0.11      |
| deviceTRUST Citrix Channel       | 19.1.100.0      |



|                                         |                                 |
|-----------------------------------------|---------------------------------|
| deviceTRUST RDP Channel                 | 19.1.100.0                      |
| Ericom PowerTerm                        | 12.0.1.0.20170219.2-_dev_-34574 |
| Evidian AuthMgr                         | 1.5.6840                        |
| Evince PDF Viewer                       | 3.18.2-1ubuntu4.3               |
| FabulaTech USB for Remote Desktop       | 5.2.29                          |
| Firefox                                 | 60.3.0                          |
| IBM iAccess Client Solutions            | 1.1.5.0                         |
| IGEL RDP Client                         | 2.2                             |
| Imprivata OneSign ProveID Embedded      |                                 |
| Leostream Java Connect                  | 3.3.7.0                         |
| NX Client                               | 5.3.12                          |
| Open VPN                                | 2.3.10-1ubuntu2.1               |
| Oracle JRE                              | 1.8.0_192                       |
| Parallels Client (32 bit)               | 16.5.2.20588                    |
| Parole Media Player                     | 1.0.1-0ubuntu1igel16            |
| Remote Viewer (RedHat Virtualization)   | 7.0-igel47                      |
| Spice GTK (Red Hat Virtualization)      | 0.35                            |
| Spice Protocol (Red Hat Virtualization) | 0.12.14                         |
| Usbredir (Red Hat Virtualization)       | 0.8.0                           |
| Systancia AppliDis                      | 4.0.0.17                        |
| Thinlinc Client                         | 4.9.0-5775                      |
| ThinPrint Client                        | 7.5.88                          |
| Totem Media Player                      | 2.30.2                          |



|                       |                         |
|-----------------------|-------------------------|
| VMware Horizon Client | 4.10.0-11053294         |
| VNC Viewer            | 1.8.0+git20180123-igel1 |
| Voip Client Ekiga     | 4.0.1                   |

- **Dictation**

|                                                       |          |
|-------------------------------------------------------|----------|
| Diktamen driver for dictation                         |          |
| Driver for Grundig Business Systems dictation devices |          |
| Nuance Audio Extensions for dictation                 | B048     |
| Olympus driver for dictation                          | 20180621 |
| Philips Speech Driver                                 | 12.6.36  |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.6    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.1.0    |

- **Smartcard**

|                                           |           |
|-------------------------------------------|-----------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101   |
| PKCS#11 Library Athena IDProtect          | 623.07    |
| PKCS#11 Library cryptovision sc/interface | 7.1.9.620 |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0 |
| PKCS#11 Library SecMaker NetID            | 6.7.0.23  |
| Reader Driver ACS CCID                    | 1.1.5     |
| Reader Driver Gemalto eToken              | 10.0.37-0 |
| Reader Driver HID Global Omnikey          | 4.3.3     |



|                                    |                  |
|------------------------------------|------------------|
| Reader Driver Identive CCID        | 5.0.35           |
| Reader Driver Identive eHealth200  | 1.0.5            |
| Reader Driver Identive SCRKBC      | 5.0.24           |
| Reader Driver MUSCLE CCID          | 1.4.28           |
| Reader Driver REINER SCT cyberJack | 3.99.5final.SP11 |
| Resource Manager PC/SC Lite        | 1.8.23-1igel1    |
| Cherry USB2LAN Proxy               | 3.0.0.6          |

- **System Components**

|                                         |                              |
|-----------------------------------------|------------------------------|
| OpenSSL                                 | 1.0.2g-1ubuntu4.13           |
| OpenSSH Client                          | 7.2p2-4ubuntu2.4             |
| OpenSSH Server                          | 7.2p2-4ubuntu2.4             |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5           |
| MESA OpenGL stack                       | 18.2.1-1igel51               |
| VAAPI ABI Version                       | 0.40                         |
| VDPAU Library version                   | 1.1.1-3ubuntu1               |
| Graphics Driver INTEL                   | 2.99.917+git20181113-igel846 |
| Graphics Driver ATI/RADEON              | 18.0.1-1igel831              |
| Graphics Driver ATI/AMDGPU              | 18.0.1-1igel831              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.15-2igel775              |
| Graphics Driver Nvidia                  | 390.87-0ubuntu1              |
| Graphics Driver Vboxvideo               | 5.2.18-dfsg-2igel17          |
| Graphics Driver VMware                  | 13.3.0-2igel812              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1igel775         |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |
| Graphics Driver VESA                    | 2.3.4-1build2igel639         |



|                                 |                              |
|---------------------------------|------------------------------|
| Input Driver Evdev              | 2.10.5-1ubuntu1igel750       |
| Input Driver Elographics        | 1.4.1-1build5igel633         |
| Input Driver eGalax             | 2.5.5814                     |
| Input Driver Synaptics          | 1.9.0-1ubuntu1igel748        |
| Input Driver Vmmouse            | 13.1.0-1ubuntu2igel635       |
| Input Driver Wacom              | 0.36.1-0ubuntu1igel813       |
| Kernel                          | 4.18.20 #mainline-udos-r2481 |
| Xorg X11 Server                 | 1.19.6-1ubuntu4igel838       |
| Xorg Xephyr                     | 1.19.6-1ubuntu4igel832       |
| CUPS printing daemon            | 2.1.3-4ubuntu0.5igel20       |
| PrinterLogic                    | 18.2.1.128                   |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1            |
| XFCE4 Windowmanager             | 4.12.3-1ubuntu2igel653       |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7      |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.2igel58 |
| ModemManager                    | 1.6.8-2igel1                 |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.1           |
| GStreamer 1.x                   | 1.14.2-1ubuntu1igel192       |
| Python2                         | 2.7.12                       |
| Python3                         | 3.5.2                        |

- **Features with Limited IGEL Support**

|                          |
|--------------------------|
| Mobile Device Access USB |
| VPN OpenConnect          |
| Scanner support          |
| VirtualBox               |



- **Features with Limited Functionality**

|                   |      |
|-------------------|------|
| Cisco JVDI Client | 12.1 |
|-------------------|------|

## General Information 10.05.500

The following clients and features are **not supported** anymore:

- **Citrix Receiver 12.1 and 13.1 - 13.4**
- **Citrix Access Gateway** Standard Plug-in
- **Dell vWorkspace Connector** for Linux
- **Ericom PowerTerm Emulation 9 and 11**
- **Ericom Webconnect**
- **IGEL Legacy RDP Client** (rdesktop)
- Virtual Bridges **VERDE Client**
- **PPTP VPN** Support
- **IGEL Upgrade License Tool with IGEL Smartcard Token**
- Remote Management by **setup.ini file transfer** (TFTP)
- Remote Access via **RSH**
- Legacy **Philips Speech Driver**
- t-Systems **TCOS Smartcard Support**
- **DUS Series** touch screens
- **Elo serial** touch screens
- **IGEL Smartcard without locking desktop**
- **VIA Graphics Support**
- **Storage Hotplug devices are not automatically removed anymore**, instead they must be always ejected manually:
  - by panel tray icon
  - by an icon in the **In-Session Control Bar** (configurable at **IGEL Setup > User Interface > Desktop**)
  - by a **Safely Remove Hardware** session (configurable at **IGEL Setup > Accessories**)

The following clients and features are **not available** in this release:

- **Cherry eGK Channel**
- **Open VPN Smartcard Support**
- **NCP Secure Client**
- **Asian Input Methods**
- **Composite Manager**

## Known Issues 10.05.500

### Citrix

- **With activated DRI3 and an amd gpu citrix h264 acceleration plugin could freeze.** Selective H.264 mode (api v2) is not affected from this issue.



- Citrix has known issues with **gstreamer1.0** which describe problems with multimedia redirection of H264, MPEG1 and PEG2. Gstreamer1.0 is used if browser content redirection is active.
- **Browser content redirection does not work with** activated DRI3 and hardware accelerated H.264 deep compression codec.
- **Citrix StoreFront Login with Gemalto smartcard middleware does not detect smartcard correctly** if the card is inserted after start of Login. As a workaround, insert the smartcard before starting StoreFront Login.
- When using **Citrix Workspace App 18.10 in combination with Philips Speech driver**, the session occasionally does not properly terminate at logoff and hangs. As a workaround, usage of **Citrix Receiver 13.10** is recommended when Philips Speech driver is needed.
- **Citrix H264 acceleration plugin does not work with "enabled" server policy "Optimize for 3D graphics workload"** in combination with server policy **Use video codec compression > For the entire screen**.
- When **Expand the session over a self-selected number of monitors** (for "Multi-Monitor full screen mode") is used and setup is restarted, **Restrict full screen session to one monitor** is indicated and the monitor selection is greyed out. **The functionality is available, only the notification in setup is broken.**

#### VMware Horizon

- **External drives** mounted already before connection **do not appear in the remote desktop**. Workaround: map the directory /media as a drive in your desktop. Then the external devices will show up inside the media drive.
- **Client drive mapping** and **USB redirection for storage devices** should **not** be enabled both at the same time.
  - On the one hand, if you want to use USB redirection for your storage devices.

Note that the USB on-insertion feature is only working if the **Client Drive Mapping** is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**.

It is also recommended to disable local **Storage Hotplug**: On page **Devices > Storage Devices > Storage Hotplug**, put number of storage hotplug devices to 0.

- On the other hand, if you use drive mapping instead, it is recommended that you should either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. And because Horizon Client relies on the OS to mount the storage devices itself, please go to setup page: **Devices > Storage Devices > Storage Hotplug** and switch on **Enable dynamic drive mapping** and put **Number of storage hotplug devices** to at least 1.

#### Parallels Client

- **Native USB redirection** does not work with Parallels Client.
- For using the new **FIPS 140-2 compliance mode** it is necessary to connect to the Parallels RAS one time with FIPS support disabled.

#### Base system



- **Display resolution and rotation** could not be changed with nvidia gpu driver via tcsetup.

#### Multimedia

- Multimedia redirection with **gstreamer** could fail with **nouveau gpu driver**.

#### Smartcard

- In some cases, there are instabilities when using **A.E.T. SafeSign smartcards**.

#### Appliance Mode

- **Appliance mode RHEV/Spice**: spice-xpi firefox plugin is no longer supported. The "Console Invocation" has to allow Native client (auto is also possible) and it should start in fullscreen to prevent opening windows.

#### Hardware

- **Suspend on UD10 is disabled**.

#### IGEL Cloud Gateway

- **No support for UMS file transfer status** in ICG protocol.

### New Features 10.05.500

#### Citrix

- Integrated **Citrix Workspace app 18.10**.
  - There is now a registry key to enable **Citrix Workspace App selfservice web UI mode**.  
[More...](#)

|           |                                                      |
|-----------|------------------------------------------------------|
| Parameter | Enable Citrix Workspace app self-service web UI mode |
| Registry  | ica.authman.cwacapableenabled                        |
| Value     | <u>enabled</u> / disabled                            |

- There is now a registry key to make a **Bloomberg v4 keyboard** available across multiple sessions. Additionally USB redirection has to be enabled at least for this device: vid=1188 pid=9545.  
[More...](#)

|           |                                     |
|-----------|-------------------------------------|
| Parameter | Bloomberg v4 keyboard               |
| Registry  | ica.allregions.bloombergredirection |
| Value     | <u>default</u> / true / false       |

- Removed parameter for **Citrix Cloud**. This parameter is not needed anymore.  
[More...](#)

IGEL Setup **Sessions > Citrix > Citrix Global > Options**



|           |                  |
|-----------|------------------|
| Parameter | Connect to cloud |
| Registry  | ica.cloudconnect |

- Citrix client version 13.9.1 was removed.  
Available Citrix client versions: **13.5.0, 13.10, 18.10** (default)
- It is now possible to **span a citrix session over a self-defined number of consecutive monitors**.  
For this, the parameter `ica.wfclient.usexdgfullscreen` must be deactivated and `ica.pnlogin.spanmonitorenable` activated. The selection must be defined in the parameter `ica.pnlogin.spanmonitor`.

[More...](#)

|            |                                                            |
|------------|------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Window</b> |
| Parameter  | Expand the session over a self-selected number of monitors |
| Registry   | <code>ica.pnlogin.spanmonitorenable</code>                 |
| Value      | <code>enabled</code> / <u><a href="#">disabled</a></u>     |

|            |                                                            |
|------------|------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix &gt; Citrix Global &gt; Window</b> |
| Parameter  | Monitor selection                                          |
| Registry   | <code>ica.pnlogin.spanmonitor</code>                       |
| Value      | " "                                                        |

Sample: When using four monitors and expansion of session across monitor 2, 3 and 4 is wanted, insertion should be 2,3,4 or 2,4.

- **Setup renaming**

[More...](#)

| Old Name                               | New Name                          |
|----------------------------------------|-----------------------------------|
| Citrix XenDesktop / XenApp             | Citrix                            |
| Citrix Receiver Selection              | Citrix Workspace Client Selection |
| Citrix Receiver version                | Citrix Client version             |
| HDX / ICA Global                       | Citrix Global                     |
| Legacy ICA Sessions                    | Citrix Legacy ICA Sessions        |
| Citrix Storefront/Webinterface         | Citrix Storefront                 |
| XenApp                                 | Citrix Virtual Apps               |
| XenDesktop                             | Citrix Virtual Desktops           |
| XenApp / XenDesktop                    | Citrix Virtual Apps / Desktops    |
| Server Location: XenApp 6.x or older   | Server Location: Web Interface    |
| Server Location: XenApp/XenDesktop 7.x | Server Location: Storefront       |



| Old Name                                           | New Name                                |
|----------------------------------------------------|-----------------------------------------|
| Server Location: XenApp/XenDesktop 7.x Legacy Mode | Server Location: StoreFront Legacy Mode |

- Updated **deviceTrust** client to version **19.1.100**.

#### UDC3 Installer

- Added **UEFI support in UDC Deployment Appliance 5.0**, downloadable via download section on [www.igel.com](http://www.igel.com)<sup>455</sup>
- Enhanced **UDC3 Converter** by a new option to force **MS-DOS partitioning for EFI installations**.
- Updated "preparestick" tool to version 3.3.0.0 with the following fixes:
  - WMI NullReferenceException
  - dd.exe Processbar asynchronous
    - diskpart->clean failed with access denied
- RDP/IGEL RDP Client 2
  - Updated **deviceTrust** client to version 19.1.100.

#### VMware Horizon

- Updated **Horizon Client** for Linux to **version 4.10.0-11053294**. Added support for the new features:

- H.264 High Color Accuracy**

[More...](#)

|            |                                                                                    |
|------------|------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Server Options</b> |
| Parameter  | High Color Accuracy mode                                                           |
| Registry   | vmware.view.high-color-accuracy-mode                                               |
| Value      | enabled / <a href="#">disabled</a>                                                 |

- Serial port redirection support**

[More...](#)

|            |                                                                                             |
|------------|---------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Serial Port Redirection</b> |
| Parameter  | Serial Port Redirection                                                                     |
| Registry   | vmware.view.high-color-accuracy-mode                                                        |
| Value      | enabled / <a href="#">disabled</a>                                                          |

- High resolution display scaling and DPI synchronisation**

[More...](#)

|           |                 |
|-----------|-----------------|
| Parameter | Display Scaling |
|-----------|-----------------|

<sup>455</sup> <http://www.igel.com>



|          |                                              |
|----------|----------------------------------------------|
| Registry | <code>vmware.view.use-display-scaling</code> |
| Value    | <u>enabled</u> / disabled                    |

- **Relative mouse support**

[More...](#)

|           |                                                |
|-----------|------------------------------------------------|
| Parameter | Relative Mouse Feature for a Remote Desktop    |
| Registry  | <code>vmware.view.enable-relative-mouse</code> |
| Value     | <u>enabled</u> / disabled                      |

- **Automatically hide toolbar**

[More...](#)

|           |                                             |
|-----------|---------------------------------------------|
| Parameter | Auto-hide menu bar (tool bar)               |
| Registry  | <code>vmware.view.menu-bar-auto-hide</code> |
| Value     | <u>enabled</u> / disabled                   |

### Parallels Client

- Updated Parallels Client to **version 16.5.2**
  - Fixed: Remote session closes triggered by audio playback

### IBM\_5250

- Enhanced configuration of **IBM iAccess Client**. The following parameters were added:  
[More...](#)

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | Open new sessions in a new tab                   |
| Registry  | <code>ibm.iaccess.acssm.opensessionintab</code>  |
| Value     | <u>enabled</u> / disabled                        |
| Parameter | Always display the tab bar                       |
| Registry  | <code>ibm.iaccess.acssm.alwaysshowntabbar</code> |
| Value     | <u>enabled</u> / disabled                        |
| Parameter | Switch to new tab when created                   |
| Registry  | <code>ibm.iaccess.acssm.switchtonewtab</code>    |
| Value     | <u>enabled</u> / disabled                        |
| Parameter | Send a warning when closing multiple tabs        |



|           |                                                        |
|-----------|--------------------------------------------------------|
| Registry  | ibm.iaccess.acssm.closemultipletabwarning              |
| Value     | <u>enabled</u> / <u>disabled</u>                       |
| Parameter | Do not start tabbed sessions until the tab is selected |
| Registry  | ibm.iaccess.acssm.tabdelayedstart                      |
| Value     | <u>enabled</u> / <u>disabled</u>                       |
| Parameter | New Tab Action                                         |
| Registry  | ibm.iaccess.acssm.newtabaction                         |
| Range     | [Disable and Hide] [Run the Same] [Run Other...]       |
| Parameter | Tab Placement                                          |
| Registry  | ibm.iaccess.acssm.tabplacement                         |
| Range     | [Top][Bottom] [Left] [Right]                           |
| Parameter | List of visible menu entries                           |
| Registry  | ibm.sessions.iaccess%.options.deletemenus              |
| Value     | list of visible menu entries                           |

#### Firefox

- Updated Mozilla Firefox to **version 60.3.0ESR**  
Fixes for **mfsa2018-27**, also known as: CVE-2018-12392, CVE-2018-12393, CVE-2018-12395, CVE-2018-12396, CVE-2018-12397, CVE-2018-12389, CVE-2018-12390.

#### Cisco JVDI Client

- Updated Cisco JVDI client to **version 12.1**

#### Base system

- Updated **French** and **Dutch** user interface translation.

#### Driver

- Philips Speech Drivers** for Citrix and RDP version 12.6.36  
Support of the new Philips dictation devices **SpeechOne 6000** and **SpeechAir 2000**

#### Audio

- Added support for **Jabra Xpress** mechanism to deploy firmware updates and settings on **Jabra USB headsets**.

[More...](#)

|           |                             |
|-----------|-----------------------------|
| Parameter | File name of Xpress package |
| Registry  | jabra.xpress.package_name   |



|           |                                                       |
|-----------|-------------------------------------------------------|
| Parameter | URL hosting Xpress packages                           |
| Registry  | <code>jabra.xpress.package_url</code>                 |
| Parameter | Login name for access to Xpress package URL           |
| Registry  | <code>jabra.xpress.package_url_login</code>           |
| Parameter | Password for access to Xpress package URL             |
| Registry  | <code>jabra.xpress.package_url_crypt_password</code>  |
| Parameter | Check SSL certificate                                 |
| Registry  | <code>jabra.xpress.package_url_ssl_cert_check</code>  |
| Value     | <u>enabled</u> / disabled                             |
| Parameter | URL of the Audio Device Dashboard server              |
| Registry  | <code>jabra.xpress.device_dashboard.server_url</code> |

- Added suspend on idle for **Jabra wireless headsets**. The headsets are set to offline state after 5 seconds of idle time.

[More...](#)

|           |                                            |
|-----------|--------------------------------------------|
| Parameter | Suspend on idle                            |
| Registry  | <code>devices.jabra.suspend_on_idle</code> |
| Value     | <u>enabled</u> / disabled                  |

- Added parameters to configure the **deferred volume synchronization** in Pulseaudio.

[More...](#)

|           |                                                                              |
|-----------|------------------------------------------------------------------------------|
| Parameter | Enable deferred volume                                                       |
| Registry  | <code>multimedia.pulseaudio.daemon.enable-deferred-volume</code>             |
| Value     | <u>enabled</u> / disabled                                                    |
| Parameter | Safety margin                                                                |
| Registry  | <code>multimedia.pulseaudio.daemon.deferred-volume-safety-margin-usec</code> |
| Value     | <u>8000</u>                                                                  |



|           |                                                               |
|-----------|---------------------------------------------------------------|
| Parameter | Extra delay                                                   |
| Registry  | multimedia.pulseaudio.daemon.deferred-volume-extra-delay-usec |
| Value     | <u>0</u>                                                      |

- Added a parameter to force **configured volumes** for in- and output devices in **Pulseaudio**.  
[More...](#)

|           |                                  |
|-----------|----------------------------------|
| Parameter | Force Volume Settings            |
| Registry  | userinterface.sound.force        |
| Value     | <u>enabled</u> / <u>disabled</u> |

## Hardware

- Added **LG CK 500** to supported hardware.
  - Added **Dell Wyse 5070** to supported hardware.
- Known issues:
- Headset connectors sometimes not recognises a plugged device.
  - USB3.0 ports on back panel sporadic not recognises USB3.0 devices correctly.
  - USB-C front displayport usage is not recommended, connection problems could occur.
  - Wake-up after standby could lead to delay when using multimonitor setup
  - Screen rotation does not work reliable
- Added **ONYX VENUS 223** to supported hardware.
  - Added support for following **Plantronics** devices:
    - Blackwire 5210
    - Voyager Focus UC B825
    - Voyager 8200 UC

## Java

- Updated Oracle Java Runtime Environment to **version 1.8.0 U192**.

## IGEL Cloud Gateway

- Added support for ICG High Availability and ICG load balancing to the **IGEL remote management service**.

## Resolved Issues 10.05.500

### Citrix

- Fixed tool **icacontrol**
- Added: clear error message is returned when a **published desktop is occupied by another user**.
- Added: clear error message is returned when **misconfiguration inhibits start of an application**.

### RDP/IGEL RDP Client 2

- Fixed login error message being displayed in **English** only.



- **Allow server side per user scaling for multimonitor configurations** as well (RDP sessions desktop scaling factor must be set to 100% for this to work):

- Global setting

[More...](#)

|            |                                                      |
|------------|------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; RDP &gt; RDP Global &gt; Window</b> |
| Parameter  | Desktop scale factor                                 |
| Registry   | rdp.winconnect.desktop-scale-factor                  |
| Value      | <u>auto</u> / 100% / 125% / 150%                     |

- Session setting

[More...](#)

|            |                                                                             |
|------------|-----------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; RDP &gt; RDP Sessions &gt; **RDP Session** &gt; Window</b> |
| Parameter  | Desktop scale factor                                                        |
| Registry   | sessions.winconnect%.option.desktop-scale-factor                            |
| Value      | Global setting / auto / 100% / 125% / 150%                                  |

## Evidian

- Fixed **NLA support** in Evidian AuthMgr RDP session type

## Network

- Fixed handling of the following registry keys:

- network.interfaces.wirelesslan.device0.driver.disable\_ht
- network.interfaces.wirelesslan.device0.driver.chain\_num
- network.interfaces.wirelesslan.device0.driver.cfg80211.cfg80211\_disable\_40mhz\_24ghz

The first and the second parameters only affect the driver **rt2800ub** (used e.g. for Ralink RT3372 and RT5572)

- Fixed **iptables IPv6 support** by adding IPv6 netfilter kernel modules.

## WiFi

- Fixed connection to **hidden WiFi networks**

## Cisco JVDI Client

- Fixed: Applications are now startable via **desktop**, start menu and **application launcher**.
- Fixed Webcam support with **32Bit Citrix Receiver** for JVDI.

## Open VPN

- Fixed **desktop folder support** for OpenVPN session.



## Smartcard

- Improved **waiting for smartcard events**.

## Base system

- **IGEL Setup Assistant will no longer start multiple times**, the existing instance will be raised instead.
- Fixed **automatic firmware update** on shutdown.

## Storage Devices

- Fixed potential **hangs on suspend/shutdown** when a **USB memory stick** was in use at that time.

## X11 system

- Fixed **huge icons** in GTK applications when DPI setting was below 96.
- Fixed problems with **Avaya VDI Communicator** and webcams.
- **Disabled SNA sprite X video support as default** because it is unstable and could crash X server.
  - New registry key:  
[More...](#)

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | Use SNA sprite video feature (could be unstable) |
| Registry  | x.drivers.intel.sprite_video                     |
| Value     | enabled / <u>disabled</u>                        |

## Window manager

- Fixed the **custom UI colors for the window manager decoration** that was broken in 10.05.100. The custom UI colors are now applied to the window borders again.

## Audio

- Applied workarounds concerning **USB control requests on Plantronics C510 and 520**.
- Fixed **initialization of sound card** in **Dell Wyse 3040**.
- Fixed blocking mode in compatibility **Pulseaudio PCM plugin for ALSA**. The blocking mode is used by Parallels client to playback sound.

## Media Player (Parole)

- Parole media player now displays a **looping animation** while initiating the connection for **rtmp streams**.
- **Extended integration** of Parole media player configuration in the setup. The following configuration keys are now respected.  
[More...](#)

|            |                                                                        |
|------------|------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Media Player &gt; Media Player Global &gt; Window</b> |
| Parameter  | Automatically resize the player window when a new video is loaded      |



|            |                                                                                                                                                                 |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Registry   | multimedia.mediaplayer.auto_resize                                                                                                                              |
| Value      | enabled / <u>disabled</u>                                                                                                                                       |
| IGEL Setup | <b>Sessions &gt; Media Player &gt; Media Player Global &gt; Window</b>                                                                                          |
| Parameter  | Main window should stay on top                                                                                                                                  |
| Registry   | multimedia.mediaplayer.window_on_top                                                                                                                            |
| Value      | enabled / <u>disabled</u>                                                                                                                                       |
| IGEL Setup | <b>Sessions &gt; Media Player &gt; Media Player Global &gt; Options</b>                                                                                         |
| Parameter  | Network connection speed                                                                                                                                        |
| Registry   | multimedia.mediaplayer.connection_speed                                                                                                                         |
| Range      | [56 kbps Modem/ISDN] [112 kbps Dual ISDN/DSL]<br>[256 kbps DSL/Cable] [384 kbps DSL/Cable]<br>[512 kbps DSL/Cable] [1.5 mbps T1/Intranet/LAN]<br>[Intranet/LAN] |
| Parameter  | Enable debug                                                                                                                                                    |
| Registry   | multimedia.mediaplayer.debug                                                                                                                                    |
| Value      | enabled / <u>disabled</u>                                                                                                                                       |

## Evidian

- Added support to **log out Citrix session type** on tap event.  
**More...**

|           |                                  |
|-----------|----------------------------------|
| Parameter | Logout behavior                  |
| Registry  | evidian.sessiontype.ctx.pnlogout |



|       |                                             |
|-------|---------------------------------------------|
| Value | [Default] [Force disconnect] [Force logoff] |
|-------|---------------------------------------------|

## Hardware

- Fixed problems with **mouse cursor on intel cherryview devices.**

### 7.28.3 IGEL Universal Desktop Converter (UDC3)

Supported Hardware:

<https://kb.igel.com/igelos/en/devices-supported-by-udc3-and-ud-pocket-3117174.html>

- Component Versions 10.05.500(see page 2163)
- New Features 10.05.500(see page 2164)

#### Component Versions 10.05.500

- **Clients**

| Product    | Version   |
|------------|-----------|
| Oracle JRE | 1.8.0_192 |

- **System Components**

|                                         |                              |
|-----------------------------------------|------------------------------|
| OpenSSL                                 | 1.0.2g-1ubuntu4.13           |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5           |
| MESA OpenGL stack                       | 18.2.1-1igel51               |
| Graphics Driver INTEL                   | 2.99.917+git20181113-igel846 |
| Graphics Driver ATI/RADEON              | 18.0.1-1igel831              |
| Graphics Driver ATI/AMDGPU              | 18.0.1-1igel831              |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.15-2igel775              |
| Graphics Driver Vboxvideo               | 5.2.18-dfsg-2igel17          |
| Graphics Driver VMware                  | 13.3.0-2igel812              |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1igel775         |
| Graphics Driver FBDEV                   | 0.5.0-1igel819               |



|                                 |                              |
|---------------------------------|------------------------------|
| Graphics Driver VESA            | 2.3.4-1build2igel639         |
| Input Driver Evdev              | 2.10.5-1ubuntu1igel750       |
| Input Driver Elographics        | 1.4.1-1build5igel633         |
| Input Driver Synaptics          | 1.9.0-1ubuntu1igel748        |
| Input Driver Vmmouse            | 13.1.0-1ubuntu2igel635       |
| Input Driver Wacom              | 0.36.1-0ubuntu1igel813       |
| Kernel                          | 4.18.20 #mainline-udos-r2481 |
| Xorg X11 Server                 | 1.19.6-1ubuntu4igel838       |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1            |
| XFCE4 Windowmanager             | 4.12.3-1ubuntu2igel653       |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel7      |
| Python2                         | 2.7.12                       |
| Python3                         | 3.5.2                        |

## New Features 10.05.500

### UDC3 Installer

- Added **UEFI support in UDC Deployment Appliance 5.0**, downloadable via download section on [www.igel.com](http://www.igel.com)<sup>456</sup>
- Enhanced UDC3 Converter** by a new option to force MS-DOS partitioning for EFI installations.
- Updated "preparestick" tool to version 3.3.0.0 with the following fixes:
  - WMI NullReferenceException
  - dd.exe Processbar asynchronous
  - diskpart->clean failed with access denied

## 7.29 Notes for Release 10.05.100

|                      |            |           |
|----------------------|------------|-----------|
| <b>Software:</b>     | Version    | 10.05.100 |
| <b>Release Date:</b> | 2018-10-25 |           |

<sup>456</sup> <http://www.igel.com>



|                       |            |             |
|-----------------------|------------|-------------|
| <b>Release Notes:</b> | Version    | RN-105100-1 |
| <b>Last update:</b>   | 2018-10-25 |             |

The following formatting is used in this document:

| format type         | example                  | use                                                                                      |
|---------------------|--------------------------|------------------------------------------------------------------------------------------|
| bold and underlined | <u>enable/disable</u>    | the default setting of a value                                                           |
| bold and arrow      | <b>menu &gt; path</b>    | menu path in the IGEL setup                                                              |
| bold                | <b>GUI</b><br>[keyboard] | elements of the graphical user interface or commands that are entered using the keyboard |

- [IGEL Linux Universal Desktop](#)(see page 2165)
- [IGEL Universal Desktop OS3/IGEL UD Pocket](#)(see page 2212)
- [IGEL Universal Desktop Converter \(UDC3\)](#)(see page 2258)

## 7.29.1 IGEL Linux Universal Desktop

### Supported Devices

|                    |                                                  |
|--------------------|--------------------------------------------------|
| Universal Desktop: |                                                  |
| UD2-LX:            | UD2-LX 40                                        |
| UD3-LX:            | UD3-LX 51<br>UD3-LX 50<br>UD3-LX 42<br>UD3-LX 41 |
| UD5-LX:            | UD5-LX 50                                        |
| UD6-LX:            | UD6-LX 51                                        |



|             |                  |
|-------------|------------------|
| UD7-LX:     | UD7-LX 10        |
| UD9-LX:     | UD9-LX Touch 41  |
|             | UD9-LX 40        |
| UD10-LX:    | UD10-LX Touch 10 |
|             | UD10-LX 10       |
| IGEL Zero:  |                  |
| IZ2-RFX     |                  |
| IZ2-HDX     |                  |
| IZ2-HORIZON |                  |
| IZ3-RFX     |                  |
| IZ3-HDX     |                  |
| IZ3-HORIZON |                  |

- Component Versions 10.05.100(see page 2166)
- General Information 10.05.100(see page 2171)
- Security Fixes 10.05.100(see page 2171)
- Known Issues 10.05.100(see page 2176)
- New Features 10.05.100(see page 2177)
- Resolved Issues 10.05.100(see page 2205)

## Component Versions 10.05.100

- **Clients**

| Product                          | Version    |
|----------------------------------|------------|
| Citrix HDX Realtime Media Engine | 2.6.0-2030 |
| Citrix Receiver                  | 13.10.0.20 |



|                                         |                                 |
|-----------------------------------------|---------------------------------|
| Citrix Receiver                         | 13.5.0.10185126                 |
| Citrix Receiver                         | 13.9.1.6                        |
| deviceTRUST Citrix Channel              | 17.2.100.0                      |
| deviceTRUST RDP Channel                 | 17.2.100.0                      |
| Ericom PowerTerm                        | 12.0.1.0.20170219.2-_dev_-34574 |
| Evidian AuthMgr                         | 1.5.6840                        |
| Evince PDF Viewer                       | 3.18.2-1ubuntu4.3               |
| FabulaTech USB for Remote Desktop       | 5.2.29                          |
| Firefox                                 | 60.2.2                          |
| IBM iAccess Client Solutions            | 1.1.5.0                         |
| IGEL RDP Client                         | 2.2                             |
| Imprivata OneSign ProveID Embedded      |                                 |
| Leostream Java Connect                  | 3.3.7.0                         |
| NX Client                               | 5.3.12                          |
| Open VPN                                | 2.3.10-1ubuntu2.1               |
| Oracle JRE                              | 1.8.0_181                       |
| Parallels Client (32 bit)               | 16.5.1.20446                    |
| Parole Media Player                     | 1.0.1-0ubuntu1igel11            |
| Remote Viewer (RedHat Virtualization)   | 7.0-igel47                      |
| Spice GTK (Red Hat Virtualization)      | 0.35                            |
| Spice Protocol (Red Hat Virtualization) | 0.12.14                         |
| Usbredir (Red Hat Virtualization)       | 0.8.0                           |
| Systancia AppliDis                      | 4.0.0.17                        |



|                       |                         |
|-----------------------|-------------------------|
| Thinlinc Client       | 4.9.0-5775              |
| ThinPrint Client      | 7.5.86                  |
| Totem Media Player    | 2.30.2                  |
| VMware Horizon Client | 4.8.0-8518891           |
| VNC Viewer            | 1.8.0+git20180123-igel1 |
| Voip Client Ekiga     | 4.0.1                   |

- **Dictation**

|                                                       |          |
|-------------------------------------------------------|----------|
| Diktamen driver for dictation                         |          |
| Driver for Grundig Business Systems dictation devices |          |
| Nuance Audio Extensions for dictation                 | B048     |
| Olympus driver for dictation                          | 20180621 |
| Philips Speech Driver                                 | 12.5.4   |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.6    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.1.0    |

- **Smartcard**

|                                           |           |
|-------------------------------------------|-----------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101   |
| PKCS#11 Library Athena IDProtect          | 623.07    |
| PKCS#11 Library cryptovision sc/interface | 7.1.9.620 |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0 |
| PKCS#11 Library SecMaker NetID            | 6.7.0.23  |



|                                    |                  |
|------------------------------------|------------------|
| Reader Driver ACS CCID             | 1.1.5            |
| Reader Driver Gemalto eToken       | 10.0.37-0        |
| Reader Driver HID Global Omnikey   | 4.3.3            |
| Reader Driver Identive CCID        | 5.0.35           |
| Reader Driver Identive eHealth200  | 1.0.5            |
| Reader Driver Identive SCRKBC      | 5.0.24           |
| Reader Driver MUSCLE CCID          | 1.4.28           |
| Reader Driver REINER SCT cyberJack | 3.99.5final.SP11 |
| Resource Manager PC/SC Lite        | 1.8.22           |
| Cherry USB2LAN Proxy               | 3.0.0.6          |

- **System Components**

|                            |                                |
|----------------------------|--------------------------------|
| OpenSSL                    | 1.0.2g-1ubuntu4.13             |
| OpenSSH Client             | 7.2p2-4ubuntu2.4               |
| OpenSSH Server             | 7.2p2-4ubuntu2.4               |
| Bluetooth stack (bluez)    | 5.50-0ubuntu1igel5             |
| MESA OpenGL stack          | 18.2.1-1igel51                 |
| VAAPI ABI Version          | 0.40                           |
| VDPAU Library version      | 1.1.1-3ubuntu1                 |
| Graphics Driver INTEL      | 2.99.917+git20180214-igel1830  |
| Graphics Driver ATI/RADEON | 18.0.1-1igel831                |
| Graphics Driver ATI/AMDGPU | 18.0.1-1igel831                |
| Graphics Driver VIA        | 5.76.52.92-009-005f78-20150730 |
| Graphics Driver FBDEV      | 0.5.0-1igel819                 |



|                                 |                            |
|---------------------------------|----------------------------|
| Graphics Driver VESA            | 2.3.4-1build2igel639       |
| Input Driver Evdev              | 2.10.5-1ubuntu1igel750     |
| Input Driver Elographics        | 1.4.1-1build5igel633       |
| Input Driver eGalax             | 2.5.5814                   |
| Input Driver Synaptics          | 1.9.0-1ubuntu1igel748      |
| Input Driver Vmmouse            | 13.1.0-1ubuntu2igel635     |
| Input Driver Wacom              | 0.36.1-0ubuntu1igel813     |
| Kernel                          | 4.18.11 #mainline-ud-r2463 |
| Xorg X11 Server                 | 1.19.6-1ubuntu4igel838     |
| Xorg Xephyr                     | 1.19.6-1ubuntu4igel832     |
| CUPS printing daemon            | 2.1.3-4ubuntu0.5igel20     |
| PrinterLogic                    | 18.2.1.128                 |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1          |
| XFCE4 Windowmanager             | 4.12.3-1ubuntu2igel653     |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel6    |
| NetworkManager                  | 1.6.8-2igel1               |
| ModemManager                    | 1.6.4-1                    |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.1         |
| GStreamer 1.x                   | 1.14.2-1ubuntu1igel192     |

- **Features with Limited IGEL Support**

|                          |
|--------------------------|
| Mobile Device Access USB |
|--------------------------|

|                 |
|-----------------|
| VPN OpenConnect |
|-----------------|

|                 |
|-----------------|
| Scanner support |
|-----------------|

|            |
|------------|
| VirtualBox |
|------------|

- **Features with Limited Functionality**



Cisco JVDI Client

12.0

## General Information 10.05.100

The following clients and features are not supported anymore:

- Citrix Receiver 12.1 and 13.1 - 13.4
- Citrix Access Gateway Standard Plug-in
- Dell vWorkspace Connector for Linux
- Ericom PowerTerm Emulation 9 and 11
- Ericom Webconnect
- IGEL Legacy RDP Client (rdesktop)
- Virtual Bridges VERDE Client
- PPTP VPN Support
- IGEL Upgrade License Tool with IGEL Smartcard Token
- Remote Management by setup.ini file transfer (TFTP)
- Remote Access via RSH
- Legacy Philips Speech Driver
- t-Systems TCOS Smartcard Support
- DUS Series touch screens
- Elo serial touch screens
- IGEL Smartcard without locking desktop
- Video Hardware Acceleration Support is discontinued on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, UD10-LX 10
- H.264 Hardware Acceleration Support is discontinued on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, UD10-LX 10
- Storage Hotplug devices are not automatically removed anymore, instead they must be always ejected manually:
  - by panel tray icon
  - by an icon in the **In-Session Control Bar** (configurable at **IGEL Setup > User Interface > Desktop**)
  - by a **Safely Remove Hardware** session (configurable at **IGEL Setup > Accessories**)

The following clients and features are not available in this release:

- Cherry eGK Channel
- Open VPN Smartcard Support
- NCP Secure Client
- Asian Input Methods
- Composite Manager

## Security Fixes 10.05.100

Firefox



- Updated Mozilla Firefox to version **60.2.2esr**.

[More...](#)

mfsa2018-24: CVE-2018-12386, CVE-2018-12387  
 mfsa2018-23: CVE-2018-12385, CVE-2018-12383  
 mfsa2018-21: CVE-2018-12377, CVE-2018-12378, CVE-2018-12376  
 mfsa2018-16: CVE-2018-12359, CVE-2018-12360, CVE-2018-12361, CVE-2018-12362,  
 CVE-2018-5156, CVE-2018-12363, CVE-2018-12364, CVE-2018-12365,  
 CVE-2018-12371, CVE-2018-12366, CVE-2018-12367, CVE-2018-12369,  
 CVE-2018-5187, CVE-2018-5188  
 mfsa2018-14: CVE-2018-6126  
 mfsa2018-11: CVE-2018-5154, CVE-2018-5155, CVE-2018-5157, CVE-2018-5158,  
 CVE-2018-5159, CVE-2018-5160, CVE-2018-5152, CVE-2018-5153,  
 CVE-2018-5163, CVE-2018-5164, CVE-2018-5166, CVE-2018-5167,  
 CVE-2018-5168, CVE-2018-5169, CVE-2018-5172, CVE-2018-5173,  
 CVE-2018-5175, CVE-2018-5176, CVE-2018-5177, CVE-2018-5165,  
 CVE-2018-5180, CVE-2018-5181, CVE-2018-5182, CVE-2018-5151,  
 CVE-2018-5150.  
 mfsa2018-10: CVE-2018-5148

- Firefox profile partition is now **mounted at /userhome/.mozilla instead of /.ffpro**.
- Firefox could only be started as **user**.
- For security reasons **Java processes could not be started from a browser session now**.
- Added a registry parameter `java.browser.access` to **control java access for all browser sessions**.

[More...](#)

|            |                                                    |
|------------|----------------------------------------------------|
| IGEL Setup | <b>Registry &gt; java &gt; browser &gt; access</b> |
| Parameter  | Allow browser to use java                          |
| Registry   | <code>java.browser.access</code>                   |
| Value      | <u>enabled</u> / <u>disabled</u>                   |

## Network

- **Disabled ICMP redirects.**
- Changed default **LoginGraceTime** from 120 to 30 sec.
- Added new registry keys for a **secure sshd configuration**.

[More...](#)

|           |                                                |
|-----------|------------------------------------------------|
| Parameter | Permit X11 forwarding                          |
| Registry  | <code>network.ssh_server.x11_forwarding</code> |
| Value     | <u>enabled</u> / <u>disabled</u>               |
| Parameter | Show banner                                    |



|           |                                                       |
|-----------|-------------------------------------------------------|
| Registry  | <code>network.ssh_server.show_banner</code>           |
| Value     | <u>enabled</u> / <u>disabled</u>                      |
| Parameter | Permit tcp tunnel forwarding                          |
| Registry  | <code>network.ssh_server.permit_tcp_forwarding</code> |
| Value     | <u>enabled</u> / <u>disabled</u>                      |

- Fixed **SCEP client certificate request file access rights.**

#### Base system

- Added **apparmor** as an additional security layer for components like Firefox, evince, dhclient and cups.

[More...](#)

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Enable apparmor profiles              |
| Registry  | <code>system.security.apparmor</code> |
| Value     | <u>enabled</u> / <u>disabled</u>      |

- For security reasons **graphical terminal sessions** could now only be started by an administrator when an **admin password** is set. Administrator must authenticate before a terminal session is started. This does also affect graphical terminal sessions spawned by applications.

- To **allow users to start a terminal session again** a registry key is defined.

[More...](#)

|           |                                        |
|-----------|----------------------------------------|
| Parameter | User shell terminal                    |
| Registry  | <code>system.security.usershell</code> |
| Value     | <u>enabled</u> / <u>disabled</u>       |

- Fixed **open-vm-tools** security issue CVE-2015-5191.
- Fixed **procps** security issues CVE-2018-1126, CVE-2018-1125, CVE-2018-1124, CVE-2018-1123 and CVE-2018-1122.
- Fixed **imagemagick** security issues.

[More...](#)

CVE-2018-9133, CVE-2018-8960, CVE-2018-8804

CVE-2018-7443, CVE-2018-5248, CVE-2018-11251, CVE-2018-10177, CVE-2017-18273,

CVE-2017-18271, CVE-2017-18252, CVE-2017-18211, CVE-2017-18209,

CVE-2017-17914, CVE-2017-17879, CVE-2017-17682, CVE-2017-17681,

CVE-2017-17504, CVE-2017-16546, CVE-2017-15281, CVE-2017-15277,

CVE-2017-15017, CVE-2017-15016, CVE-2017-15015, CVE-2017-14989,

CVE-2017-14741, CVE-2017-14739, CVE-2017-14682, CVE-2017-14626,

CVE-2017-14625, CVE-2017-14624, CVE-2017-14607, CVE-2017-14532,

CVE-2017-14531, CVE-2017-14505, CVE-2017-14400, CVE-2017-14343,

CVE-2017-14342, CVE-2017-14341, CVE-2017-14325, CVE-2017-14249,

CVE-2017-14224, CVE-2017-14175, CVE-2017-14174, CVE-2017-14173,



CVE-2017-14172, CVE-2017-14060, CVE-2017-13769, CVE-2017-13768,  
CVE-2017-13758, CVE-2017-13145, CVE-2017-13144, CVE-2017-13143,  
CVE-2017-13142, CVE-2017-13139, CVE-2017-13134, CVE-2017-12983,  
CVE-2017-12877, CVE-2017-12875, CVE-2017-12693, CVE-2017-12692,  
CVE-2017-12691, CVE-2017-12674, CVE-2017-12670, CVE-2017-12643,  
CVE-2017-12640, CVE-2017-12587, CVE-2017-12563, CVE-2017-12435,  
CVE-2017-12432, CVE-2017-12431, CVE-2017-12430, CVE-2017-12429,  
CVE-2017-12140, CVE-2017-11640, CVE-2017-11639, CVE-2017-11537,  
CVE-2017-11535, CVE-2017-11533, CVE-2017-11352, CVE-2017-10995,  
CVE-2017-1000476, CVE-2017-1000445, CVE-2018-13153, CVE-2018-12600 and  
CVE-2018-12599.

- Fixed **elfutils** security issues CVE-2017-7613, CVE-2017-7612, CVE-2017-7611, CVE-2017-7610, CVE-2017-7609, CVE-2017-7608, CVE-2017-7607, CVE-2016-10255 and CVE-2016-10254.
- Fixed **ghostscript** security issues CVE-2018-10194, CVE-2016-10317, CVE-2018-16802, CVE-2018-16585, CVE-2018-16543, CVE-2018-16542, CVE-2018-16541, CVE-2018-16540, CVE-2018-16539, CVE-2018-16513, CVE-2018-16511, CVE-2018-16509, CVE-2018-15911, CVE-2018-15910, CVE-2018-15909, CVE-2018-15908, CVE-2018-11645, CVE-2018-1, CVE-2018-17183 and CVE-2018-16510.
- Fixed **icu** security issue CVE-2017-15422.
- Fixed **webkit2gtk** security issues.  
**More...**

CVE-2018-4200, CVE-2018-4165, CVE-2018-4163,  
CVE-2018-4162, CVE-2018-4161, CVE-2018-4146, CVE-2018-4133, CVE-2018-4129,  
CVE-2018-4128, CVE-2018-4127, CVE-2018-4125, CVE-2018-4122, CVE-2018-4120,  
CVE-2018-4119, CVE-2018-4118, CVE-2018-4117, CVE-2018-4114, CVE-2018-4113,  
CVE-2018-4101, CVE-2018-4233, CVE-2018-4232, CVE-2018-4222, CVE-2018-4218,  
CVE-2018-4199, CVE-2018-4190, CVE-2018-12293, CVE-2018-4284, CVE-2018-4278,  
CVE-2018-4273, CVE-2018-4272, CVE-2018-4270, CVE-2018-4267, CVE-2018-4266,  
CVE-2018-4265, CVE-2018-4264, CVE-2018-4263, CVE-2018-4262, CVE-2018-4261,  
CVE-2018-4246 and CVE-2018-12911.

- Fixed **perl** security issues CVE-2018-6913, CVE-2018-6798, CVE-2018-6797, CVE-2017-6512, CVE-2016-6185 and CVE-2018-12015.
- Fixed **poppler** security issues CVE-2017-18267 and CVE-2018-13988.
- Fixed **openssl** security issues CVE-2018-0739, CVE-2018-0737, CVE-2018-0737, CVE-2018-0732 and CVE-2018-0495.
- Fixed **tiff** security issues.  
**More...**

CVE-2018-5784, CVE-2017-9936, CVE-2017-9935,



CVE-2017-9815, CVE-2017-9404, CVE-2017-9403, CVE-2017-9147, CVE-2017-9117, CVE-2017-7602, CVE-2017-7601, CVE-2017-7600, CVE-2017-7599, CVE-2017-7598, CVE-2017-7597, CVE-2017-7596, CVE-2017-7595, CVE-2017-7594, CVE-2017-7593, CVE-2017-7592, CVE-2017-5563, CVE-2017-18013, CVE-2017-17095, CVE-2017-13727, CVE-2017-13726, CVE-2017-12944, CVE-2017-11613, CVE-2017-11335, CVE-2017-10688, CVE-2016-5318, CVE-2016-5102, CVE-2016-3186, CVE-2016-10371, CVE-2016-10269, CVE-2016-10268, CVE-2016-10267 and CVE-2016-10266.

- Fixed **libvncserver** security issue CVE-2018-7225.
- Fixed **libvorbis** security issue CVE-2018-5146.
- Fixed **samba** security issues CVE-2018-1057, CVE-2018-1050, CVE-2018-10919 and CVE-2018-10858.
- Fixed **wget** security issue CVE-2018-0494.
- Fixed **bluez** security issue CVE-2017-1000250.
- Fixed **libgcrypt20** security issue CVE-2018-0495.
- Fixed **file** security issue CVE-2018-10360.
- Fixed **gnupg2** security issue CVE-2018-12020.
- Fixed **isc-dhcp** security issues CVE-2018-5733, CVE-2018-5732, CVE-2018-573, CVE-2017-3144 and CVE-2016-2774.
- Fixed **curl** security issues CVE-2018-1000303, CVE-2018-1000301, CVE-2018-1000300, CVE-2018-1000122, CVE-2018-1000121, CVE-2018-1000120, CVE-2017-8818, CVE-2018-14618 and CVE-2018-0500.
- Fixed **python3.5** security issues CVE-2017-1000158, CVE-2016-5636, CVE-2016-1000110 and CVE-2016-0772.
- Fixed **zlib** security issues CVE-2016-9843, CVE-2016-9842, CVE-2016-9841 and CVE-2016-9840.
- Fixed **libsoup2.4** security issue CVE-2018-12910.
- Fixed **libjpeg-turbo** security issue CVE-2018-1152.
- Fixed **ntp** security issues CVE-2018-7185 and CVE-2018-7183.
- Fixed **libpng1.6** security issue CVE-2018-13785.
- Fixed **cups** security issues CVE-2018-6553, CVE-2018-4181, CVE-2018-4180, CVE-2018-418 and CVE-2017-18248.
- Fixed **libpng** security issue CVE-2016-10087.
- Fixed **policykit-1** security issue CVE-2018-1116.
- Fixed **jansson** security issue CVE-2016-4425.
- Fixed **libmspack** security issues CVE-2018-14682, CVE-2018-14681, CVE-2018-14680 and CVE-2018-14679.
- Fixed **libonig** security issues CVE-2017-9229, CVE-2017-9228, CVE-2017-9227, CVE-2017-9226 and CVE-2017-9224.
- Fixed **libxcursor** security issue CVE-2015-9262.
- Fixed **heimdal** security issue CVE-2017-17439.
- Fixed **libarchive** security issues CVE-2017-14503, CVE-2017-14501, CVE-2017-14166, CVE-2016-10350, CVE-2016-10349 and CVE-2016-10209.
- Fixed **libxml2** security issues CVE-2018-14567, CVE-2018-14404, CVE-2017-18258 and CVE-2016-9318.
- Fixed **confuse** security issue CVE-2018-14447.
- Fixed **libgd2** security issues CVE-2018-5711 and CVE-2018-1000222.



- Fixed **libx11** security issues CVE-2018-14600, CVE-2018-14599, CVE-2018-14598, CVE-2016-7943 and CVE-2016-7942.
- Fixed **mpg123** security issues CVE-2017-10683 and CVE-2016-1000247.
- Fixed **libtirpc** security issues CVE-2018-14622, CVE-2017-8779 and CVE-2016-4429.
- Fixed **jq** security issue CVE-2015-8863.
- Fixed **bind9** security issue CVE-2018-5740.
- Fixed **lcms2** security issue CVE-2018-16435.
- Fixed **xdg-utils** security issue CVE-2017-18266.
- **Restricted access to command su to root and user.**
- Root home is now **/root**.
- **Removed system group (GID 0)** which shadowed root group (GID 0).
- **Stricter folder and file permissions.**

#### X11 system

- Restricted desktop icon creation to administrator only. Therefore, "**/userhome/Desktop**" is **owned by root now**.

#### Known Issues 10.05.100

##### Citrix Receiver 13

- On devices with **AMD/Radeon graphics chipsets** and **activated DRI3 X driver option** the **hardware accelerated Citrix H.264 decoder plugin can hang**. To solve this issue deactivation of DRI3 option is necessary (default setting). Selective H.264 mode (api v2) is not affected from this issue.
- **Citrix StoreFront login with Gemalto smartcard middleware** does not detect smartcard correctly when the card is inserted after start of login. As a workaround, insert the smartcard before starting StoreFront login.
- The Citrix Receiver has known issues with **GStreamer1.x**. This causes **problems with multimedia redirection of H264, MPEG1 and MPEG2**. GStreamer1.x is used if browser content redirection is active.

##### Parallels Client

- **Native USB redirection** does not work with Parallels Client.
- Due to a bug in the Parallels-Client, for using the new **FIPS 140-2 compliance mode** it is necessary to connect to the Parallels RAS one time with FIPS support disabled.

##### VMware Horizon

- VMware Horizon Client for **Linux 4.8.0 supports FIPS Mode on only VMware Horizon server installations up to version 7.5**.
- **External drives are mounted already before connection, do not appear in the remote desktop**. Workaround: mapping the directory /media as a drive on desktop. The external devices will show up within the media drive then.
- **Client drive mapping and USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup



client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.

- On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Enable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.

#### OpenConnect VPN

- VPNs which requires the **OpenConnect client** cannot be used for firmware updates.

#### Appliance Mode

- Appliance mode **RHEV/Spice: spice-xpi Firefox plugin is no longer supported**. The **Console Invocation** has to allow native client (auto is also possible) and it should start in fullscreen to prevent opening windows.

#### Hardware

- Sometimes the **DVI Port on a UD6 is not recognized by the Linux system after booting up**. The only available way to solve the issue is to shut down and disconnect the thin client from power (1-2 minutes) and connect and power up it again.
- **Suspend** is not working on **UD10** so the support for suspend is disabled.

#### Smartcard

- In seldom cases the authentication hung when using A.E.T. SafeSign smartcards.

#### IGEL Cloud Gateway

- **No support for UMS file transfer status** in ICG protocol.

## New Features 10.05.100

#### Citrix Receiver 13

- Integrated **Citrix Receiver 13.10**. Citrix Receiver version 13.7.0 was removed. Citrix Receiver version 13.8.0 was removed. Available Citrix Receiver versions: 13.5.0, 13.9.1, [13.10](#) (default)
    - Enable **Browser content redirection for rendering of whitelisted webpages** on the IGEL Thin Client.
- More...**

|            |                                                                                  |
|------------|----------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix XenDesktop &gt; HDX / ICA Global &gt; HDX Multimedia</b> |
| Parameter  | Browser content redirection                                                      |
| Registry   | ica.module.virtualdriver.webpageredirection                                      |



|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

- Enhanced **Citrix retail logging**.

[More...](#)

|           |                            |
|-----------|----------------------------|
| Parameter | Citrix Logging             |
| Registry  | ica.module.syslogthreshold |
| Value     | <u>0 / 3 / 7</u>           |

> 0 = Disabled

> 3 = Log only errors

> 7 = Log all levels

- Enable **Port forwarding**.

[More...](#)

|           |                                      |
|-----------|--------------------------------------|
| Parameter | Portforward                          |
| Registry  | ica.module.virtualdriver.portforward |
| Value     | <u>enabled / disabled</u>            |

- Workspace configuration parameter for **Citrix Cloud** is now available on setup page.

[More...](#)

|            |                                                                           |
|------------|---------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix XenDesktop &gt; HDX / ICA Global &gt; Options</b> |
| Parameter  | Connect to cloud                                                          |
| Registry   | ica.cloudconnect                                                          |
| Value      | <u>enabled / disabled</u>                                                 |

- Added a registry key to **control the visibility of the Citrix connection bar** for desktop sessions. If activated, the In-Session Control Bar should be disabled at `userinterface.igel_toolbar.enable` and `userinterface.igel_toolbar.show_always`.

This enables the control of the new **Multi-monitor layout persistence** feature.

[More...](#)

|           |                       |
|-----------|-----------------------|
| Parameter | Citrix Connection Bar |
|-----------|-----------------------|



|          |                                                       |
|----------|-------------------------------------------------------|
| Registry | <code>ica.allregions.connectionbar</code>             |
| Value    | <u>factory default</u> / off / on / server determined |

- Added a registry key to control the availability of deprecated cipher suites:
- TLS\_RSA\_AES256\_GCM\_SHA384, TLS\_RSA\_AES128\_GCM\_SHA256,**  
**TLS\_RSA\_AES256\_CBC\_SHA256, TLS\_RSA\_AES256\_CBC\_SHA,**  
**TLS\_RSA\_AES128\_CBC\_SHA,**  
**TLS\_RSA\_3DES\_CBC\_EDE\_SHA.**

|           |                                            |
|-----------|--------------------------------------------|
| Parameter | TLS RSA cipher suites                      |
| Registry  | <code>ica.allregions.enable_tls_rsa</code> |
| Value     | <u>factory default</u> / false / true      |

Factory default: true/enabled. Citrix explicitly remarks: **Important:** Set the flag `enable_tls_rsa` to true to use the other two cipher suites **Enable\_RC4-MD5** and **Enable\_RC4\_128\_SHA**.

- Added a registry key to control the availability of the deprecated cipher suite: **RC4-MD5**.

|           |                                            |
|-----------|--------------------------------------------|
| Parameter | RC4-MD5 cipher suite                       |
| Registry  | <code>ica.allregions.enable_rc4_md5</code> |
| Value     | <u>factory default</u> / false / true      |

Factory default: false/disabled.

- Added a registry key to control the availability of the deprecated cipher suite: **RC4\_128\_SHA**.

|           |                                                |
|-----------|------------------------------------------------|
| Parameter | RC4_128_SHA cipher suite                       |
| Registry  | <code>ica.allregions.enable_rc4_128_sha</code> |
| Value     | <u>factory default</u> / false / true          |

Factory default: false/disabled.

- Added **Selective H.264** (API v2) to the hardware accelerated Citrix deep compression codec. XenDesktop/XenApp server policy: **Use video codec for compression -> For actively changing regions**



- Added **DRI3 acceleration support** to the hardware accelerated Citrix deep compression codec (for INTEL and AMD graphics adapters).
- Enable **debugging to log file `/var/log/user/ctxh264.log`**.

[More...](#)

|           |                                                        |
|-----------|--------------------------------------------------------|
| Parameter | Enable H264 codec debug output                         |
| Registry  | <code>ica.hw-accelerated-h264-codec-debug</code>       |
| Value     | <code>enabled</code> / <a href="#"><u>disabled</u></a> |

- Added **Kerberos Passthrough (domain passthrough) authentication to StoreFront**. Configurable at **Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > StoreFront Logon > Authentication Type**.
- Updated **Citrix HDX RTME** used for optimization of **Skype for Business to 2.6.0-2030**. This new version adds the support for hardware accelerated H.264 en- and decoding on AMD platforms. See <https://support.citrix.com/article/CTX236304> section **Capability Checker for Linux platforms** how to enable hardware decoding with Citrix VDA registry keys `DisableLinuxAMDH264HardwareDecoding` and `SupportedAMDHWAVideoCardList`. The capability check program **RTOP-CapabilityChk-x64** is already installed at path `/services/ica/hdx_rtme/RTOP-CapabilityChk-x64`. The check program must be run with user permissions.
- Added display of **logged on Citrix username in screen lock**, when screen lock password is synchronized with Citrix password.
- Added checkbox to **activate autostart of a single published application/desktop session**.

[More...](#)

|            |                                                                                                 |
|------------|-------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix XenDesktop / XenApp &gt; Citrix StoreFront/Web Interface &gt; Login</b> |
| Parameter  | Start a single published application automatically                                              |
| Registry   | <code>ica.pnlogin.autostart_single_application</code>                                           |
| Value      | <code>enabled</code> / <a href="#"><u>disabled</u></a>                                          |

- Added **Lakeside SysTrack virtual channel in Citrix, RDP and Horizon sessions**. Activation via parameters in Setup.

[More...](#)

|            |                                                                                                    |
|------------|----------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix XenDesktop/XenApp &gt; HDX/ICA Global &gt; Mapping &gt; Device Support</b> |
| Parameter  | Lakeside Systrack channel                                                                          |
| Registry   | <code>ica.module.virtualdriver.lakeside.enable</code>                                              |



|            |                                                                                 |
|------------|---------------------------------------------------------------------------------|
| Value      | enabled / <u>disabled</u>                                                       |
| IGEL Setup | <b>Sessions &gt; RDP &gt; RDP Global &gt; Mapping &gt; Device Support</b>       |
| Parameter  | Lakeside Systrack channel                                                       |
| Registry   | rdp.winconnect.plugins.lakeside.use                                             |
| Value      | enabled / <u>disabled</u>                                                       |
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Performance</b> |
| Parameter  | Lakeside Systrack                                                               |
| Registry   | vmware.view.lakeside_systrack                                                   |
| Value      | enabled / <u>disabled</u>                                                       |

- Updated **Olympus dictation channel for Citrix** to version 20180621.  
[More...](#)

|            |                                                                                                        |
|------------|--------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix XenDesktop / XenApp &gt; HDX / ICA Global &gt; Mapping &gt; Device Support</b> |
| Parameter  | Olympus channel for dictation                                                                          |
| Registry   | ica.module.virtualdriver.olycom.enable                                                                 |
| Value      | enabled / <u>disabled</u>                                                                              |

- Added **CrossMatch / DigitalPersona channel for Citrix** version 0515.  
[More...](#)

|            |                                                                                                       |
|------------|-------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix XenDesktop /XenApp &gt; HDX / ICA Global &gt; Mapping &gt; Device Support</b> |
| Parameter  | Crossmatch DigitalPersona fingerprint channel                                                         |
| Registry   | ica.module.virtualdriver.dpicacnt.enable                                                              |
| Value      | enabled / <u>disabled</u>                                                                             |



## RDP/IGEL RDP Client 2

- Support for new **RDP 10 codec AVC444 (H.264)**, which reduces network bandwidth with Server 2016 and Windows 10 hosts. AMD Radeon graphics is required on the client side. Other graphics hardware (e.g. Intel) as well as other RDP 10 codecs (AVC420 and AVC444V2) will be supported in the future.

[More...](#)

|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; RDP &gt; RDP Global &gt; Performance</b>                     |
| Parameter  | Hardware accelerated codecs AVC420/AVC444 (H.264)                             |
| Registry   | rdp.winconnect.enable-h264                                                    |
| Value      | <u>auto</u> / on / off                                                        |
| IGEL Setup | <b>Sessions &gt; RDP &gt; RDP Sessions &gt; Session Name &gt; Performance</b> |
| Parameter  | Hardware accelerated codecs AVC420/AVC444 (H.264)                             |
| Registry   | sessions.winconnect%.option.enable-h264                                       |
| Value      | <u>Global setting</u> / auto / on / off                                       |

The value "auto" enables supported codecs on supported hardware.

The value "on" enables supported codecs on all hardware.

The value "off" disables H.264 codecs.

- Added new parameter **ignore\_errors** to RDP Session config to **suppress RDP error messages**.

[More...](#)

|          |                                    |
|----------|------------------------------------|
| Registry | sessions.winconnect%.ignore_errors |
| Value    | enabled / <u>disabled</u>          |

- Added **Olympus dictation channel for RDP version 20180621**.

[More...](#)

|            |                                                                           |
|------------|---------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; RDP &gt; RDP Global &gt; Mapping &gt; Device Support</b> |
| Parameter  | Olympus channel for dictation                                             |
| Registry   | rdp.winconnect.plugins.olyvc.use                                          |



|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

## Parallels Client

- Updated **Parallels client to version 16.5.1.20446 (32-Bit)**
  - Added support for **FIPS 140-2 compliance**.
- More...**

|            |                                           |
|------------|-------------------------------------------|
| IGEL Setup | <b>System &gt; Registry</b>               |
| Parameter  | Enable support for FIPS 140-2 compliance  |
| Registry   | sessions.twox%.connection.fips_compliance |
| Value      | <u>enabled / disabled</u>                 |

## VMware Horizon

- Updated **Horizon client to version 4.8.0-8518891**.

## ThinLinc

- Updated **ThinLinc client to version 4.9.0**.
  - Shadowing notification is now more reliable and interactive, allowing end users more control of their sessions.
  - More than 80 minor enhancements and fixes. See <https://www.cendio.com/thinlinc/docs/relnotes/4.9.0>.

## RedHat Enterprise Virtualization client

- **Updated spice components** (virt-viewer 7.0, spice-gtk 0.35).
- **Removed support for spice-xpi plugin**.

## X session (Xephyr)

- Added support for X sessions configurable at `IGEL Setup > Sessions > X Sessions`. The available XDMCP connection types: indirect via localhost, indirect, direct and broadcast. With the additional connection type "local display", a command can be specified that will be displayed inside the X session window.

**More...**

|            |                                                                                 |
|------------|---------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; X Sessions &gt; X Session &gt; Server</b>                      |
| Parameter  | Connection type                                                                 |
| Registry   | sessions.xnest<NR>.server.connectiontype                                        |
| Range      | <u>[Indirect via localhost] [Indirect] [Direct] [Broadcast] [Local display]</u> |


**IGEL Setup Sessions > X Sessions > X Session > Server**

Parameter Command to be displayed

Registry sessions.xnest&lt;NR&gt;.server.runcommand

## Firefox

- Updated Mozilla Firefox to **version 60.2.2 ESR**.
- The **initial page** displayed by firefox with default settings is now **<https://kb.igel.com>** instead of the older **<https://edocs.igel.com>**.
- Updated **Adobe Flash Player** download URL to **version 31.0.0.122**.
- **Removed the webapp specific options**, this feature was removed from Firefox and is not relevant anymore.
- Moved **Browser Certificate** configuration to page **Sessions > Browser > Browser Global > Certificates**.
- Moved **Browser Security Device** configuration to page **Sessions > Browser > Browser Global > Smartcard Middleware**.
- Added **Fluendo FFmpeg GStreamer** proxy: Provides ffmpeg-libavcodec-compatible library, which is needed for H.264 playback in firefox. Instead decoding by standard ffmpeg libraries, the video stream is redirected to GStreamer framework.

## Network

- **SCEP**: Added subject alternative name type **DNS Name as UPN (auto)**. This is similar to **DNS Name (auto)**. In the CSR the result is a Microsoft User Principal Name (UPN) that consists of the hostname.
- **NetworkManager** updated to version **1.2.6**.

## Cisco JVDI Client

- Integrated new **Cisco Jabber Softphone for VDI** (Cisco JVDI client) **version 12.0.0** as feature with limited functionality. See product documentation for details -> <https://kb.igel.com/cisco-jvdi/en>. Activation of this feature at: **System > Firmware Customization > Features > Cisco JVDI client**. Only Citrix Receiver 13.9.1 is supported.

[More...](#)

Parameter Log Level

Registry multimedia.ciscovxme.log\_level

Range [Info] [Warning] [Error] [Fatal] [Debug] [Trace]

IGEL Setup

**Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Unified Communications > Cisco JVDI Client**

Parameter

Cisco JVDI Client



|          |                                                      |
|----------|------------------------------------------------------|
| Registry | <code>ica.module.virtualdriver.vdcisco.enable</code> |
| Value    | <u>enabled</u> / <u>disabled</u>                     |

Registry path for Common JVDI options: `multimedia.ciscovxme.\*\*` The Cisco JVDI Client configuration is only displayed if the Multimedia Codec Pack (MMC) is present.

## Java

- Updated **Oracle Java Runtime Environment to version 1.8.0 U181**.

## Smartcard

- Updated **SecMaker Net iD to version 6.7.0.23**.
- Updated **HID Global Omnikey smartcard reader driver to version 4.3.3**.
- Updated **cryptovision sc/interface to version 7.1.9**. Changelog since version 7.0.5:
  - Fixed **an error during certificate registration** using the MS Minidriver for MS VSC. Compatible with sc/interface cache version 1.2 or higher.
  - Fixed an error where **writing a certificate using the Minidriver for MS VSC corrupted the Container-ID**. As a result, the key could not be used using CNG/CAPI.
  - Fixed an error during **certificate registration using the Minidriver for MS VSC where some Container-ID's could not be used by CNG/CAPI**.
  - General Bug Fixes.
  - Fixed **error during profile creation on JCOP3 with ePasslet-Suite 3.0**.
  - Added support for **additional BWI card profiles based on CardOS-5.x**. Versions **1.7, 1.8, 1.9, 4.2, 4.3 and 4.4**. Support **4k RSA for 1.9 and 4.4**.
  - Fixed support for **remote logon in sc/interface cache**.
  - Fixed **Free after use** in ReadOnly Minidriver.
  - PKCS#11 Fixed **MS VSC (GIDSv2) support**.
  - PKCS#11 Fixed **CardOS-4.x "non sc/interface card profile" support**.
  - **MS VSC (GIDSv2)** Support for PKCS#11 - Maximum CKA\_ID length reduced to 25 bytes!
  - Support for **JCOP3 and Infineon JTOP - DolphinV2**.
  - Support for **cryptovision's ePasslet-Suite-3.0**.
  - New **ePKIAppllet-2.129 for JCOP3, SCE7 and JTOP (DolphinV2)** with up to 4096 bits RSA and 512 bits
  - **EC** support, **PACE** optional.
  - **RegisterTool plugins now available in Setup**. Removed from "support\RegisterTool\_Plugins".
  - **New sc/interface Minidriver support for MS VSC** (instead of the MS Minidriver) to allow extended PIN cache configuration.
  - Added support for **sc/interface cache version 1.0** for Minidriver/ReadOnly Minidriver and PKCS#11.
  - **Cross-application PIN cache for Windows 8.1** and later.
  - **WARNING: No longer compatible with Credential Cache (CSP)**. When there are any questions, [support@cryptovision.com](mailto:support@cryptovision.com)<sup>457</sup> should be contacted.

---

<sup>457</sup> mailto:support@cryptovision.com



- Added **macOS CTK Token Driver for 10.12 and later**. Unfortunately, after the installation, a shell script must be executed to enable the full functionality.
- **Removed macOS tokend support** beginning with version 10.12, installation of 10.10 can be used if needed.
- **WARNING: macOS tokend support will discontinue, usage of new CTK Token Driver is necessary.**
- Re-Added **cvSimpleCardProv for Windows** (based on 6.4.2) to enabled the default login selection, see "support\CredentialProvider".
- Updated **OpenSC library to version 0.19.0**. Improved handling of PIV and CAC ALT token.

#### Base system

- Updated to **kernel version 4.18.11**.
- Added new **GStreamer 1.x support version 1.14.2**.

There will only ever be GStreamer in version 1.0 or version 0.10. By default, clients run with the version they have best support for. The provided registry key can be used to override the automatic detection/setting and pin a single version if required.

[More...](#)

|           |                                   |
|-----------|-----------------------------------|
| Parameter | Fluendo GStreamer Codec Version   |
| Registry  | multimedia.gstreamer.version      |
| Value     | [1.x] [0.10] [ <u>automatic</u> ] |

- With **GStreamer 1.x the new Parole player is used** for media player sessions. When there occur problems with the new player, a switch back to totem/GStreamer 0.10 media player is possible by **Fluendo GStreamer Codec Version** parameter.
- Added **optional logoff button in taskbar** when the screenlock is active.

[More...](#)

| IGEL Setup <b>Security &gt; Logon &gt; Taskbar</b> |                                                          |
|----------------------------------------------------|----------------------------------------------------------|
| Parameter                                          | Show logoff button                                       |
| Registry                                           | userinterface.screenlock_taskbar_logged_in.logoff_button |
| Value                                              | enabled / <u>disabled</u>                                |

- **Mobile broadband configuration dialog now provides a simple mode**, that displays 3 dropdown boxes to select country, provider and access point (plan). The former version is available via an **Expert Mode** button.
- **IGEL Setup Assistant enhancements:**
  - displaying page for **mobile broadband configuration** when any mobile broadband modem is detected.
  - displaying page to **show broken network connectivity**
  - **desktop icon** will now be displayed **when the assistant was not yet finished**.



- **the assistant is now always started on devices without IGEL license**, that are not registered at UMS
  - new **icon design**
  - Added support for **Chinese, Japanese, Korean** and **Thai** fonts.
  - **KVM kernel modules added**.
  - Added **USB power off on shutdown in IGEL UD7 (H850C) and IGEL UD3 (M340C)**. The feature can be configured by the parameter: (default: deactivated).
- More...**

|           |                               |
|-----------|-------------------------------|
| Parameter | Power off on shutdown         |
| Registry  | devices.usb.poweroff_shutdown |
| Value     | enabled / <u>disabled</u>     |

- Added **policykit-1-gnome session agent** to get a GUI interface for actions which requires root authentication.
- Added **remote (network attached) logging via rsyslog**.

| IGEL Setup <b>System -&gt; Remote Syslog</b> |                                  |
|----------------------------------------------|----------------------------------|
| Parameter                                    | Remote mode                      |
| Registry                                     | system.syslog.remote_mode        |
| Range                                        | [Server] [Client] [ <u>Off</u> ] |
| Parameter                                    | Custom client config entries     |
| Registry                                     | system.syslog.client_custom      |

- **Server mode** is possible, though limited and intended for short-term debugging.
- More...**

| IGEL Setup <b>System -&gt; Remote Syslog</b> |                               |
|----------------------------------------------|-------------------------------|
| Parameter                                    | Template for log file storage |
| Registry                                     | system.syslog.template        |
| Value                                        | /var/log/%HOSTNAME%/messages  |
| Parameter                                    | Local port                    |
| Registry                                     | system.syslog.input%.port     |



|           |                                    |
|-----------|------------------------------------|
| Value     | <u>514</u>                         |
| Parameter | Transport protocol                 |
| Registry  | system.syslog.input%.transport     |
| Value     | [TCP] [UDP]                        |
| Parameter | Local Address                      |
| Registry  | system.syslog.input%.local_address |
| Parameter | Name                               |
| Registry  | system.syslog.input%.name          |

- **Client mode** allows to filter and send commands to multiple remotes.  
[More...](#)

|                                              |                                                                               |
|----------------------------------------------|-------------------------------------------------------------------------------|
| <b>IGEL Setup System -&gt; Remote Syslog</b> |                                                                               |
| Parameter                                    | Remote port                                                                   |
| Registry                                     | system.syslog.output%.port                                                    |
| Value                                        | <u>514</u>                                                                    |
| Parameter                                    | Transport protocol                                                            |
| Registry                                     | system.syslog.output%.transport                                               |
| Value                                        | [TCP] [UDP]                                                                   |
| Parameter                                    | Remote address                                                                |
| Registry                                     | system.syslog.output%.address                                                 |
| Parameter                                    | Syslog facility                                                               |
| Registry                                     | system.syslog.output%.facility                                                |
| Range                                        | [Any] [AUTH] [CRON] [DAEMON] [FTP] [KERN] [LPR] [MAIL] [NEWS] [USER]<br>UUCP] |



|           |                                                                      |
|-----------|----------------------------------------------------------------------|
| Parameter | Syslog level                                                         |
| Registry  | system.syslog.output%.level                                          |
| Range     | [Any] [EMERG] [ALERT] [CRIT] [ERR] [WARNING] [NOTICE] [INFO] [DEBUG] |

- **Shutdown or suspend by inactivity.**

[More...](#)

IGEL Setup **System > Power Options > System**

Parameter System action on inactivity

Registry system.power\_management.system\_standby.ac\_action

Value Suspend / Shutdown

- Enhanced **Change Password** utility to be able changing the following items of the logged on user:

- **Password of local user** (screen lock password).
- **PIN of IGEL smartcard**.
- **PIN of PKCS#11 smartcard**.

#### CUPS Printing

- Added **PrinterLogic support, Version 18.2.1.128**.

[More...](#)

IGEL Setup **Devices > Printer > PrinterLogic**

Parameter Manage printers by Printer Installer Client

Registry printerlogic.active

Value enabled / disabled

Parameter HomeURL Protocol

Registry printerlogic.homeurl.protocol

Value http:// / https://

Parameter HomeURL Hostname

Registry printerlogic.homeurl.hostname



|           |                                                 |
|-----------|-------------------------------------------------|
| Value     | <u>.printercloud.com</u>                        |
| Parameter | Authorization Code                              |
| Registry  | printerlogic.auth.crypt_password                |
| Parameter | (Mapping in sessions) ICA Sessions              |
| Registry  | printerlogic.map_ica                            |
| Value     | <u>enabled</u> / disabled                       |
| Parameter | (Mapping in sessions) RDP Sessions              |
| Registry  | printerlogic.map_rdp                            |
| Value     | <u>enabled</u> / disabled                       |
| Parameter | (Mapping in sessions) NX Sessions               |
| Registry  | printerlogic.map_nxclient                       |
| Value     | <u>enabled</u> / <u>disabled</u>                |
| Parameter | (Mapping in sessions) Parallels Client Sessions |
| Registry  | printerlogic.map_twox                           |
| Value     | <u>enabled</u> / <u>disabled</u>                |

## Driver

- Added **Kofax virtual channel for signature pads in Citrix sessions.**  
[More...](#)

|            |                                                                                                    |
|------------|----------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix XenDesktop/XenApp &gt; HDX/ICA Global &gt; Mapping &gt; Device Support</b> |
| Parameter  | Kofax SPVC Signature Pad Channel                                                                   |
| Registry   | ica.module.virtualdriver.spvc.enable                                                               |
| Value      | <u>enabled</u> / <u>disabled</u>                                                                   |



- Added configuration to change the **dynamic power management settings for ATI graphics driver.**

[More...](#)

|           |                                     |
|-----------|-------------------------------------|
| Parameter | ATI dynamic power management        |
| Registry  | x.drivers.ati.dpm                   |
| Value     | <u>default</u> / enabled / disabled |

- Added the possibility to change the **dynamic power management settings for graphics AMDGPU driver.**

[More...](#)

|           |                                     |
|-----------|-------------------------------------|
| Parameter | AMDGPU dynamic power management     |
| Registry  | x.drivers.amdgpu.dpm                |
| Value     | <u>default</u> / enabled / disabled |

- Added possibility to use **generic modesetting graphics driver** instead of the hardware specific one.

[More...](#)

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | Use generic modesetting driver for ATI hardware. |
| Registry  | x.drivers.ati.use_modesetting                    |
| Value     | enabled / <u>disabled</u>                        |

|           |                                                     |
|-----------|-----------------------------------------------------|
| Parameter | Use generic modesetting driver for AMDGPU hardware. |
| Registry  | x.drivers.amdgpu.use_modesetting                    |
| Value     | enabled / <u>disabled</u>                           |

|           |                                                     |
|-----------|-----------------------------------------------------|
| Parameter | Use generic modesetting driver for NVIDIA hardware. |
| Registry  | x.drivers.nouveau.use_modesetting                   |
| Value     | enabled / <u>disabled</u>                           |

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | Use generic modesetting driver for VIA hardware. |
| Registry  | x.drivers.via.use_modesetting                    |



|          |                               |
|----------|-------------------------------|
| Registry | x.drivers.via.use_modesetting |
| Value    | enabled / <u>disabled</u>     |

## Bluetooth

- Added new **Bluetooth Autopairing Wizard** for IGEL OS installations without keyboard or mouse available, but with unpaired bluetooth keyboard/mouse. The **Autopairing Wizard** is started together with **IGEL Setup Assistant**.

## Appliance Mode

- The wireless manager can now be invoked from the In-Session control bar.** Furthermore, it will be automatically started when no network connection can be established.  
**Prerequisites:** A WiFi device is available and the following registry keys are set to true.  
[More...](#)

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Activate Wireless Interface                   |
| Registry  | network.interfaces.wirelesslan.device0.active |
| Value     | enabled / <u>disabled</u>                     |

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | Enable wireless manager                          |
| Registry  | network.applet.wireless.enable_connection_editor |
| Value     | enabled / <u>disabled</u>                        |

- It is possible to use **Accessories**, **VPN connections** and **other session types** in **Appliance Mode** now. The access to those session types must be explicitly enabled by a new parameter **Appliance Mode Access**. Possible starting methods:

- XDMCP Appliance mode:** Hotkey
- All other Appliance modes:** Desktop icon, Desktop Context Menu, Application Launcher (+ System tab), Hotkey, Autostart.  
[More...](#)

|                                                          |                                               |
|----------------------------------------------------------|-----------------------------------------------|
| <b>IGEL Setup Accessories &gt; ICA Connection Center</b> |                                               |
| Parameter                                                | Application Mode Access                       |
| Registry                                                 | sessions.icaconncenter0.appliance_mode_access |
| Value                                                    | enabled / <u>disabled</u>                     |

|                                                 |  |
|-------------------------------------------------|--|
| <b>IGEL Setup Accessories &gt; Task Manager</b> |  |
|-------------------------------------------------|--|



|                                   |                                             |
|-----------------------------------|---------------------------------------------|
| Parameter Application Mode Access |                                             |
| Registry                          | sessions.taskmanager0.appliance_mode_access |
| Value                             | enabled / <u>disabled</u>                   |

|            |                                                 |
|------------|-------------------------------------------------|
| IGEL Setup | <b>Accessories &gt; Application Launcher</b>    |
| Parameter  | Application Mode Access                         |
| Registry   | sessions.launcher0.appliance_mode_access        |
| Value      | enabled / <u>disabled</u>                       |
| IGEL Setup | <b>Accessories &gt; Firmware Update</b>         |
| Parameter  | Application Mode Access                         |
| Registry   | sessions.firmware_update0.appliance_mode_access |
| Value      | enabled / <u>disabled</u>                       |
| IGEL Setup | <b>Accessories &gt; Quick Settings</b>          |
| Parameter  | Application Mode Access                         |
| Registry   | sessions.usersetup0.appliance_mode_access       |
| Value      | enabled / <u>disabled</u>                       |
| IGEL Setup | <b>Accessories &gt; Sound Preferences</b>       |
| Parameter  | Application Mode Access                         |
| Registry   | sessions.mixer0.appliance_mode_access           |
| Value      | enabled / <u>disabled</u>                       |
| IGEL Setup | <b>Accessories &gt; Disk Removal</b>            |
| Parameter  | Application Mode Access                         |
| Registry   | sessions.storage_dcdm0.appliance_mode_access    |
| Value      | enabled / <u>disabled</u>                       |
| IGEL Setup | <b>Accessories &gt; Disk Utility</b>            |



|            |                                                                                                                                    |
|------------|------------------------------------------------------------------------------------------------------------------------------------|
| Parameter  | Application Mode Access                                                                                                            |
| Registry   | <code>sessions.storage_info0.appliance_mode_access</code>                                                                          |
| Value      | <code>enabled</code> / <code>disabled</code>                                                                                       |
| IGEL Setup | <b>Accessories &gt; Commands User Interface &gt; Hotkeys &gt; Commands</b>                                                         |
| Parameter  | Application Mode Access                                                                                                            |
| Registry   | <code>sessions.commands&lt;NR&gt;.appliance_mode_access</code><br><code>sessions.wmcommands&lt;NR&gt;.appliance_mode_access</code> |
| Value      | <code>enabled</code> / <code>disabled</code>                                                                                       |
| IGEL Setup | <b>Accessories &gt; Webcam Information</b>                                                                                         |
| Parameter  | Application Mode Access                                                                                                            |
| Registry   | <code>sessions.webcaminfo0.appliance_mode_access</code>                                                                            |
| Value      | <code>enabled</code> / <code>disabled</code>                                                                                       |
| IGEL Setup | <b>Accessories &gt; Touchscreen Calibration</b>                                                                                    |
| Parameter  | Application Mode Access                                                                                                            |
| Registry   | <code>sessions.touchcalib0.appliance_mode_access</code>                                                                            |
| Value      | <code>enabled</code> / <code>disabled</code>                                                                                       |
| IGEL Setup | <b>User Interface &gt; Screenlock / Screensaver</b>                                                                                |
| Parameter  | Application Mode Access                                                                                                            |
| Registry   | <code>sessions.xlock0.appliance_mode_access</code>                                                                                 |
| Value      | <code>enabled</code> / <code>disabled</code>                                                                                       |
| IGEL Setup | <b>Accessories &gt; Monitor Calibration</b>                                                                                        |
| Parameter  | Application Mode Access                                                                                                            |
| Registry   | <code>sessions.xpattern0.appliance_mode_access</code>                                                                              |



|            |                                                |
|------------|------------------------------------------------|
| Value      | enabled / <u>disabled</u>                      |
| IGEL Setup | <b>Accessories &gt; Network Tools</b>          |
| Parameter  | Application Mode Access                        |
| Registry   | sessions.gnome-nettool0.appliance_mode_access  |
| Value      | enabled / <u>disabled</u>                      |
| IGEL Setup | <b>Accessories &gt; Screenshot Tool</b>        |
| Parameter  | Application Mode Access                        |
| Registry   | sessions.screenshooter0.appliance_mode_access  |
| Value      | enabled / <u>disabled</u>                      |
| IGEL Setup | <b>Accessories &gt; System Information</b>     |
| Parameter  | Application Mode Access                        |
| Registry   | sessions.device_manager0.appliance_mode_access |
| Value      | enabled / <u>disabled</u>                      |
| IGEL Setup | <b>Accessories &gt; Bluetooth Tool</b>         |
| Parameter  | Application Mode Access                        |
| Registry   | sessions.bluetooth0.appliance_mode_access      |
| Value      | enabled / <u>disabled</u>                      |
| IGEL Setup | <b>Accessories &gt; Display Switch</b>         |
| Parameter  | Application Mode Access                        |
| Registry   | sessions.user_display.appliance_mode_access    |
| Value      | enabled / <u>disabled</u>                      |
| IGEL Setup | <b>Accessories &gt; Identify Monitors</b>      |
| Parameter  | Application Mode Access                        |
| Registry   | sessions.screenid0.appliance_mode_access       |



|            |                                                                                             |
|------------|---------------------------------------------------------------------------------------------|
| Value      | enabled / <u>disabled</u>                                                                   |
| IGEL Setup | <b>Accessories &gt; System Log Viewer (&gt; Options)</b>                                    |
| Parameter  | Application Mode Access                                                                     |
| Registry   | sessions.systemviewer0.appliance_mode_access                                                |
| Value      | enabled / <u>disabled</u>                                                                   |
| Registry   | sessions.setup.displaynames.add_layout.appliance_mode_access                                |
| Value      | enabled / <u>disabled</u>                                                                   |
| IGEL Setup | <b>Accessories &gt; Terminals &gt; Local Terminal</b>                                       |
| Parameter  | Application Mode Access                                                                     |
| Registry   | sessions.xterm<NR>.appliance_mode_access                                                    |
| Value      | enabled / <u>disabled</u>                                                                   |
| IGEL Setup | <b>Sessions &gt; SSH &gt; SSH Session</b>                                                   |
| Parameter  | Application Mode Access                                                                     |
| Registry   | sessions.ssh<NR>.appliance_mode_access                                                      |
| Value      | enabled / <u>disabled</u>                                                                   |
| IGEL Setup | <b>System &gt; Firmware Customization -&gt; Custom Application -&gt; Custom Application</b> |
| Parameter  | Application Mode Access                                                                     |
| Registry   | sessions.custom_application<NR>.appliance_mode_access                                       |
| Value      | enabled / <u>disabled</u>                                                                   |
| IGEL Setup | <b>Accessories &gt; Mobile Device Access</b>                                                |
| Parameter  | Application Mode Access                                                                     |
| Registry   | sessions.mtp-devices0.appliance_mode_access                                                 |



|            |                                                                                                   |
|------------|---------------------------------------------------------------------------------------------------|
| Value      | <u>enabled / disabled</u>                                                                         |
| IGEL Setup | <b>Network &gt; VPN &gt; OpenConnect VPN (&gt; OpenVPN Connection (&gt; Desktop Integration))</b> |
| Parameter  | Application Mode Access                                                                           |
| Registry   | sessions.openvpn<NR>.appliance_mode_access                                                        |
| Value      | <u>enabled / disabled</u>                                                                         |
| IGEL Setup | <b>Network &gt; VPN &gt; OpenConnect VPN (&gt; VPN OpenConnection (&gt; Desktop Integration))</b> |
| Parameter  | Application Mode Access                                                                           |
| Registry   | sessions.openconnect<NR>.appliance_mode_access                                                    |
| Value      | <u>enabled / disabled</u>                                                                         |
| IGEL Setup | <b>Network &gt; VPN &gt; genucard (&gt; Desktop Integration)</b>                                  |
| Parameter  | Application Mode Access                                                                           |
| Registry   | sessions.genucard_vpn_connection0.appliance_mode_access                                           |
| Value      | <u>enabled / disabled</u>                                                                         |

#### X11 system

- Set of **User Interface > Display > Options > Monitor DPI** now automatically affects the size of the **mouse cursor**, the **panel height**, the **desktop icons**, the **application launcher**, the **size of the start menu** and the **window manager decorations**.

#### VirtualBox

- Added VirtualBox as **feature with limited support**. Activation of the feature at: **System > Firmware Customization > Features > VirtualBox**. Added new registry keys under `virtualbox` and `sessions.virtualbox<NR>`.

#### Audio

- Updated **Pulseaudio to version 12.0-1**.
- The resample method in Pulseaudio can now be configured by the newly introduced parameter **resample-method**.  
**More...**

|           |                 |
|-----------|-----------------|
| Parameter | Resample method |
|-----------|-----------------|



|          |                                                                                                             |
|----------|-------------------------------------------------------------------------------------------------------------|
| Registry | <code>multimedia.pulseaudio.daemon.resample-method</code>                                                   |
| Range    | [soxr-vhq] [soxr-hq] [soxr-mq] [speex-float-10] [speex-float-5] [speex-float-3]<br>[ <u>speex-float-1</u> ] |

## Media Player (Parole/Totem)

- Added new **Parole Media Player 1.0.1-0ubuntu1**. It is used for media player sessions **by default** now. When there occur problems with the new player, switch back to totem/GStreamer 0.10 media player is possible by setting **Fluendo GStreamer Codec Version** parameter to 0.10.

[More...](#)

|           |                                           |
|-----------|-------------------------------------------|
| Parameter | Fluendo GStreamer Codec Version           |
| Registry  | <code>multimedia.gstreamer.version</code> |
| Range     | [1.x] [0.10] [ <u>automatic</u> ]         |

- Added **RTSP/RTMP** support to parole media player / gstreamer 1.x.
- The following parameters are only functional with **Totem media player/GStreamer 0.10** and not for Parole media player.

[More...](#)

|            |                                                                        |
|------------|------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Media Player &gt; Media Player Global &gt; Window</b> |
| Parameter  | Automatically resize the player window when a new video is loaded      |
| Registry   | <code>multimedia.mediaplayer.auto_resize</code>                        |
| Value      | enabled / <u>disabled</u>                                              |

|            |                                                                        |
|------------|------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Media Player &gt; Media Player Global &gt; Window</b> |
| Parameter  | Main window should stay on top                                         |
| Registry   | <code>multimedia.mediaplayer.window_on_top</code>                      |
| Value      | enabled / <u>disabled</u>                                              |

|            |                                                                          |
|------------|--------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Media Player &gt; Media Player Global &gt; Playback</b> |
| Parameter  | Visualization size                                                       |
| Registry   | <code>multimedia.mediaplayer.visual_quality</code>                       |
| Range      | [ <u>Small</u> ] [Normal] [Large] [Extra Large]                          |



|            |                                                                                                                                                              |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Media Player &gt; Media Player Global &gt; Options</b>                                                                                      |
| Parameter  | Network connection speed                                                                                                                                     |
| Registry   | multimedia.mediaplayer.connection_speed                                                                                                                      |
| Range      | [56 kbps Modem/ISDN] [112 kbps Dual ISDN/DSL] [256 kbps DSL/Cable]<br>[384 kbps DSL/Cable] [512 kbps DSL/Cable] [1.5 mbps T1/Intranet/LAN]<br>[Intranet/LAN] |
| Parameter  | Enable deinterlacing                                                                                                                                         |
| Registry   | multimedia.mediaplayer.deinterlace                                                                                                                           |
| Value      | enabled / <u>disabled</u>                                                                                                                                    |
| Parameter  | Enable debug                                                                                                                                                 |
| Registry   | multimedia.mediaplayer.debug                                                                                                                                 |
| Value      | enabled / <u>disabled</u>                                                                                                                                    |
| Parameter  | Network buffering threshold                                                                                                                                  |
| Registry   | multimedia.mediaplayer.network_buffer_threshold                                                                                                              |
| Value      | 2                                                                                                                                                            |

- As the **Media Player Browser Plugin** is not supported with **Firefox 60 ESR**, the following parameters are not available anymore.

[More...](#)

|            |                                                                                |
|------------|--------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Media Player &gt; Media Player Global &gt; Browser Plugin</b> |
| Parameter  | Video output                                                                   |
| Registry   | multimedia.mediaplayer.browser_plugin.video_sink                               |
| Range      | [Default] [Auto] [Hardware Accelerated] [X Video Extension] [X Window System]  |
| IGEL Setup | <b>Sessions &gt; Media Player &gt; Media Player Global &gt; Browser Plugin</b> |
| Parameter  | Aspect ratio                                                                   |
| Registry   | multimedia.mediaplayer.browser_plugin.aspect_ratio                             |



|       |                                                                                                                                                                         |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Range | <a href="#">[Default]</a> <a href="#">[Auto]</a> <a href="#">[Square]</a> <a href="#">[4:3 (TV)]</a> <a href="#">[16:9 (Widescreen)]</a> <a href="#">[2.11:1 (DVB)]</a> |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Evidian

- Integrated **Evidian AuthMgr version 1.5.6840.**
  - Evidian AuthMgr sessions can be configured at **IGEL Setup > Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions** (registry keys: sessions.rsuserauth%).
  - Evidian AuthMgr global settings can be configured at **IGEL Setup > Sessions > Evidian AuthMgr > Evidian AuthMgr Global** (registry keys: evidian).
- Added support for **Custom catalog of messages.**  
[More...](#)

|            |                                                                                                                                                                           |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Evidian AuthMgr &gt; Evidian AuthMgr Sessions &gt; Evidian AuthMgr Session &gt; Options</b>                                                              |
| Parameter  | Language selection                                                                                                                                                        |
| Registry   | sessions.rsuserauth<NR>.parameters.message_catalog                                                                                                                        |
| Range      | <a href="#">[Automatic]</a> <a href="#">[English (UK)]</a> <a href="#">[English (US)]</a> <a href="#">[German]</a> <a href="#">[French]</a> <a href="#">[Custom]</a>      |
| IGEL Setup | <b>Sessions &gt; Evidian AuthMgr &gt; Evidian AuthMgr Global &gt; Options</b>                                                                                             |
| Parameter  | Language selection                                                                                                                                                        |
| Registry   | evidian.message_catalog                                                                                                                                                   |
| Range      | <a href="#">[Global setting]</a> <a href="#">[English (UK)]</a> <a href="#">[English (US)]</a> <a href="#">[German]</a> <a href="#">[French]</a> <a href="#">[Custom]</a> |
| IGEL Setup | <b>Sessions &gt; Evidian AuthMgr &gt; Evidian AuthMgr Global &gt; Options</b>                                                                                             |
| Parameter  | Custom catalog of messages                                                                                                                                                |
| Registry   | evidian.custom_message_catalog                                                                                                                                            |
| Value      | <a href="#">/services/evidian/share/locale/en/rsUserAuth.cat</a>                                                                                                          |

- Added support for **Evidian Data Partition.**

[More...](#)

|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Evidian AuthMgr &gt; Evidian AuthMgr Global &gt; Options</b> |
| Parameter  | Evidian AuthMgr Data Partition                                                |
| Registry   | evidian.datapart.enabled                                                      |
| Value      | <a href="#">enabled</a> / <a href="#">disabled</a>                            |


**IGEL Setup Sessions > Evidian AuthMgr > Evidian AuthMgr Global > Options**

|           |                       |
|-----------|-----------------------|
| Parameter | Size                  |
| Registry  | evidian.datapart.size |
| Value     | <u>10</u>             |

- Added support for **Password Authentication**.

[More...](#)

**IGEL Setup Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions > Evidian AuthMgr Session > Options**

|           |                               |
|-----------|-------------------------------|
| Parameter | Allow password authentication |
|-----------|-------------------------------|

|          |                                                            |
|----------|------------------------------------------------------------|
| Registry | sessions.rsuserauth<NR>.parameters.password_authentication |
|----------|------------------------------------------------------------|

|       |                           |
|-------|---------------------------|
| Value | enabled / <u>disabled</u> |
|-------|---------------------------|

**IGEL Setup Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions > Evidian AuthMgr Session > Options**

|           |                          |
|-----------|--------------------------|
| Parameter | Allow password forgotten |
|-----------|--------------------------|

|          |                                                       |
|----------|-------------------------------------------------------|
| Registry | sessions.rsuserauth<NR>.parameters.password_forgotten |
|----------|-------------------------------------------------------|

|       |                           |
|-------|---------------------------|
| Value | enabled / <u>disabled</u> |
|-------|---------------------------|

**IGEL Setup Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions > Evidian AuthMgr Session > Options**

|           |                                                 |
|-----------|-------------------------------------------------|
| Parameter | Default domain name for password authentication |
|-----------|-------------------------------------------------|

|          |                                                            |
|----------|------------------------------------------------------------|
| Registry | sessions.rsuserauth<NR>.parameters.password_default_domain |
|----------|------------------------------------------------------------|

|       |  |
|-------|--|
| Value |  |
|-------|--|

## Misc

- Added support for **local scanning as feature with limited support**. Activate the feature at: **System > Firmware Customization > Features > Scanner support**. This has been tested with a Canon LiDE 120 scanner.
- [More...](#)



|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| Parameter                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Scanner support                                                |
| Registry                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <code>product.partitions41.enabled</code>                      |
| Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <code>enabled</code> / <code>disabled</code>                   |
| This must be enabled for the feature to become active and the remaining keys to be valid.                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                |
| Parameter                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Enable scanner daemon                                          |
| Registry                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <code>devices.scanner.daemon</code>                            |
| Range                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <code>[none]</code> <code>[scanbd]</code> <code>[saned]</code> |
| The key determines the daemon to be started. <code>scanbd</code> is necessary for handling buttons on the scanner. It runs <code>saned</code> when necessary (and the scanner is available). <code>saned</code> alone provides scanning functionality to local and remote applications ( <code>xsane</code> , <code>scanimate</code> , ..). If <code>none</code> is selected the system can still be used as a client for remote scanner servers (using <code>xsane</code> or <code>scanimate</code> ). |                                                                |
| Parameter                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Allowed remote clients                                         |
| Registry                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <code>devices.scanner.allowed_clients</code>                   |
| The key may contain a space-separated list of hosts and networks (CIDR > notation) that are allowed to connect to a local server.                                                                                                                                                                                                                                                                                                                                                                       |                                                                |
| Parameter                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Remote scanners                                                |
| Registry                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <code>devices.scannerclient.remote</code>                      |
| This may contain a space-separated list of remote scanner servers to be used by local applications ( <code>xsane</code> , <code>scanimate</code> ). It is only relevant if no local server is configured.                                                                                                                                                                                                                                                                                               |                                                                |

- **The remaining keys influence scanner button handling.** For each button there is an instance of the `devices.scanner.scanbd.action%` template.
- In order to keep scanner button handling flexible **the default handling may be replaced by custom scripts.** Details of the default handling are listed at the end of this section.

[More...](#)

|                                                                                                                                                                                                                                                                                           |                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| Parameter                                                                                                                                                                                                                                                                                 | Scanner button name                                |
| Registry                                                                                                                                                                                                                                                                                  | <code>devices.scanner.scanbd.action%.button</code> |
| This contains the (symbolic) name of the button. There are currently four predefined instances of the template where the value is 'file', 'scan', 'copy', and 'email' respectively. (These refer to the buttons on a Canon LiDE 120 from left to right where 'file' may be labeled 'PDF') |                                                    |



|                                                                                                                                                                                                                                                                                         |                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| Parameter                                                                                                                                                                                                                                                                               | Allow while nobody is logged in                           |
| Registry                                                                                                                                                                                                                                                                                | devices.scanner.scanbd.action%.allow_lockpanel_logged_out |
| Value                                                                                                                                                                                                                                                                                   | <u>enabled / disabled</u>                                 |
| If this is set to false, the button is ignored when nobody is logged in (only > relevant when local logon is configured)                                                                                                                                                                |                                                           |
| Parameter                                                                                                                                                                                                                                                                               | Allow while screen is locked                              |
| Registry                                                                                                                                                                                                                                                                                | devices.scanner.scanbd.action%.allow_lockpanel_logged_in  |
| Value                                                                                                                                                                                                                                                                                   | <u>enabled / disabled</u>                                 |
| When this is set to false, the button is ignored while the screen is locked.                                                                                                                                                                                                            |                                                           |
| Parameter                                                                                                                                                                                                                                                                               | scanbd custom action                                      |
| Registry                                                                                                                                                                                                                                                                                | devices.scanner.scanbd.action%.custom_cmd                 |
| This may contain a custom button handling command. The value is empty by default. If it is not, the value will be passed to "bash -c .." and the default button handling will not be effective. The consequence is that entering some space characters results in disabling the button. |                                                           |
| Parameter                                                                                                                                                                                                                                                                               | Directory                                                 |
| Registry                                                                                                                                                                                                                                                                                | devices.scanner.scanbd.action%.directory                  |
| Value                                                                                                                                                                                                                                                                                   | <u>/tmp</u>                                               |
| Set the target directory for scan results.                                                                                                                                                                                                                                              |                                                           |
| Parameter                                                                                                                                                                                                                                                                               | Format                                                    |
| Registry                                                                                                                                                                                                                                                                                | devices.scanner.scanbd.action%.format                     |
| Range                                                                                                                                                                                                                                                                                   | [pnm] [tiff] [png] [ <u>jpeg</u> ]                        |
| Determines the image format (passed as argument to scanimage).                                                                                                                                                                                                                          |                                                           |
| Parameter                                                                                                                                                                                                                                                                               | Color mode                                                |
| Registry                                                                                                                                                                                                                                                                                | devices.scanner.scanbd.action%.mode                       |
| Value                                                                                                                                                                                                                                                                                   | [Color] [ <u>Gray</u> ] [Lineart]                         |
| Determines the color mode (passed as argument to scanimage).                                                                                                                                                                                                                            |                                                           |
| Parameter                                                                                                                                                                                                                                                                               | Resolution in dpi                                         |



|                                                              |                                                   |
|--------------------------------------------------------------|---------------------------------------------------|
| Registry                                                     | devices.scanner.scanbd.action%.resolution         |
| Range                                                        | [75] [100] [150] [300] [600] [1200] [2400] [4800] |
| Determines the resolution (passed as argument to scanimage). |                                                   |
| Parameter                                                    | Brightness                                        |
| Registry                                                     | devices.scanner.scanbd.action%.brightness         |
| Value                                                        | 0                                                 |
| Determines the brightness (passed as argument to scanimage). |                                                   |

- **Default button handling script:** There is a default button handling script /etc/scanbd/scripts/action. It might be used as a potential starting point for custom button handling. The script handles the four buttons of a **Canon LiDE 120** in the following ways:
  - **file** results in a PDF document that contains a series of pages where each page contains a scan result acquired with scanimage according to the settings. This needs user interaction on the local machine's desktop.
  - **scan** results in an image file that is silently created and stored according to the settings.
  - **copy** makes the script use scanimage according to the settings, convert the resulting image to PDF and send it to the default printer. This obviously requires that a printer is configured.
  - **email** just results in xsane being started. The following settings are not respected in this case:
    - devices.scanner.scanbd.action%.directory
    - devices.scanner.scanbd.action%.format
    - devices.scanner.scanbd.action%.mode
    - devices.scanner.scanbd.action%.resolution
    - devices.scanner.scanbd.action%.brightness

#### TC Setup (Java)

- Updated **TC Setup to version 5.9.11**.
- Added an **additional local administrator access** to IGEL setup. The local administrator password is configurable at **Security > Password** setup page. The page permissions are configurable at **Accessories > Setup > Setup Administrator Permissions** setup page.
- Reworked **Accessories > Commands** and **User Interface > Hotkeys > Commands** setup pages.
- Reworked **Storage Hotplug** setup page.

#### Remote Management

- Added support for **UMS File Transfer Status**.
  - Added a new configuration to **prevent a user from canceling UMS actions like firmware update, reboot, shutdown, etc.** through the UMS notification dialog.
- More...**

|           |                                          |
|-----------|------------------------------------------|
| Parameter | Allow user to cancel UMS actions         |
| Registry  | userinterface.rmagent.cancel_usermessage |



|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

## Fabulatech

- **FabulaTech USB for Remote Desktop** updated to **versions 5.2.29; FabulaTech FTPlugin** updated to **version 3.4.0**.
- Support for some specific devices has been improved.

## Resolved Issues 10.05.100

## Citrix Receiver 13

- Fixed: Now **applications may be displayed in application launcher** independently from startmenu.
- Fixed **Citrix Azure Cloud** login window.
- Added a **new window manager tweak** to automatically unmap unwanted Citrix fragment windows when seamless apps are used.

[More...](#)

|           |                                                                |
|-----------|----------------------------------------------------------------|
| Parameter | Auto-close unwanted Wfica windows                              |
| Registry  | windowmanager.tweaks.suppress_wfica_window_in_seamless_session |
| Value     | <u>enabled / disabled</u>                                      |

- Fixed **native USB redirection with Citrix receiver 13.10**.
- Fixed **black rectangle around 32-bit mouse icons**.
- Fixed **sound playback over Nuance channel**.
- Fixed stopping of the **Pulseaudio PCM I/O plugin** which is used by Citrix Receiver for sound output and recording.
- When using the **Citrix login method the system language is used now**.
- Fixed a problem with the parameter `ica.pnlogin.suppressconnectiondialog`, **connection messages are suppressed** as desired.

## RDP/IGEL RDP Client 2

- Fixed **locking in smartcard transactions**.
- Fixed **audio recording in RDP sessions**.
- Fixed **\$HOSTNAME** to work for RDP login when variable substitution is enabled.

[More...](#)

|            |                                                                      |
|------------|----------------------------------------------------------------------|
| IGEL Setup | <b>System &gt; Firmware Customization &gt; Environment Variables</b> |
| Parameter  | Enable variable substitution in session                              |
| Registry   | system.environment_variables.enable_application_variables            |



|                      |                                                                              |
|----------------------|------------------------------------------------------------------------------|
| Value                | <u>enabled</u> / disabled                                                    |
| IGEL Setup Parameter | <b>Sessions &gt; RDP &gt; RDP Global &gt; Local Logon</b>                    |
| Registry             | rdp.login.saveusertype                                                       |
| Value                | Set user/domain from session setup / <u>Set user/ domain from last login</u> |

- Added **Arabic (101) keyboard layout** to RDP client.
- Added **MultiPointServer 2016** to supported servers for **RDP MultiPoint Server** appliance.

#### RD Web Access

- Fixed **wrong RDP Remote Application icon** when opening a application twice.
- Fixed unexpected behavior when maximizing/minimizing **RDP Remote Applications**.

#### VMware Horizon

- Added possibility to **make certificate verification mandatory**.  
**More...**

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Allow change of certificate verification mode |
| Registry  | vmware.view.ssl-verify-mode-change-allow      |
| Value     | <u>enabled</u> / disabled                     |

- Fixed **H.264 hardware decoding** for Horizon.

#### PowerTerm

- Fixed **printing to CUPS printers in PowerTerm**.
- Added **TLS-1.2 in list of SSL Versions for PowerTerm** on page **Sessions > PowerTerm Terminal Emulation > PowerTerm Sessions > session name > Connection**.

#### Parallels Client

- Fixed: **Authentication fails with Gemalto smartcards**.
- Fixed: Sometimes **remote session windows remain on screen after one was logged off from the remote session**.
- Fixed: **Remote session closes unexpectedly**.
- Fixed: Combination of **CTRL-C** doesn't work in remote session.
- Improved: **Use of multiple monitors**.
- Fixed: **Client might hang while watching YouTube videos**.
- Fixed: **Multiple USB drives might not be auto-mapped to a remote session**.
- Fixed: **Logoff from a remote session blocks Linux desktop with a black screen**.

#### Firefox



- Fixed **occasional loss of trusted certificates** in Firefox. Certificates transmitted via UMS filetransfer were not reinstalled when Firefox profile was rebuilt.
- Fixed **PDF Plugin** in Firefox browser.
- Removed the browser plugin option from **RHEV/Spice** as it is no longer supported.
- Removed the browser plugin option from **SecMaker** as it is no longer supported.

## Network

- Fixed **failing Wake-on-LAN configuration after update on shutdown**. Particularly UD2-LX40 devices were affected.
- Fixed bug in the **GetCA operation for SCEP**: An intermediate certificate in addition to the root certificate and any RA certificates resulted in confusion.
- **sscep version is now 0.6.1**
- **CA certificate fingerprint is now mandatory for SCEP**. So far it could be left empty for debugging purposes.
- Added **parameter to specify whether a slash (/) is appended to SCEP URL**. The slash is needed e.g. with Microsoft servers, but not with Nexus servers.

[More...](#)

|           |                                             |
|-----------|---------------------------------------------|
| Parameter | Append slash (/) to SCEP server URL         |
| Registry  | network.scepclient.cert0.scepurlappendslash |
| Value     | <u>enabled</u> / disabled                   |

- Fixed **generating certificate request** if challenge password or other fields include **special characters like \$, #, quotes or spaces** in SCEP.
- Reaction to **Ethernet 802.1X reauthentication failure** is now configurable.

[More...](#)

|           |                                                                         |
|-----------|-------------------------------------------------------------------------|
| Parameter | Restart on reauthentication failure                                     |
| Registry  | network.interfaces.ethernet.device%.ieee8021x.restart_on_reauth_failure |
| Value     | <u>enabled</u> / disabled                                               |

The default value preserves the traditional behaviour. If the registry key is set to enabled the network connection will get restarted when a reauthentication failure occurs. This way the system might switch to a guest VLAN where authentication is not required.

- Added **support for SFTP protocol** (enabled as default) configurable with new registry key.

[More...](#)

|           |                    |
|-----------|--------------------|
| Parameter | Enable SFTP server |
|-----------|--------------------|



|          |                                       |
|----------|---------------------------------------|
| Registry | network.ssh_server.enable_sftp_server |
| Value    | <u>enabled</u> / disabled             |

- Improved **general security** in regards of SCEP

#### WiFi

- Fixed non working **Mediatek MT7630e WiFi driver**.
- Added several **WiFi drivers** (Realtek 8188eu, 8822be, 8150, 8187, 8192ce, 8192de, 8192ee, 8723ae, 8821ae....) to the firmware.
- Re-enforce configuration after **IGEL Setup Assistant** exits to ensure consistent state between configuration and system.
- Added drivers for **Realtek rtl8723de** and **rtl8822be WiFi** devices.
- Added support for **StarTech USB300WN2X2C Wireless-N WiFi adapter**.

#### Smartcard

- Updated **OpenSC library to version 0.19.0**. Improved handling of PIV and CAC ALT token and other improvements.
- Fixed problem with **ActivClient smartcards in VMware Horizon sessions**. Before this fix, smartcard access inside the session was blocked.

**More...**

|           |                                             |
|-----------|---------------------------------------------|
| Parameter | Smartcard SCardConnect in non-blocking mode |
| Registry  | vmware.view.pcsc-connect-nonblocking        |
| Value     | <u>enabled</u> / disabled                   |

- Improved **PC/SC lite daemon** to handle attributes SCARD\_ATTR\_DEVICE\_FRIENDLY\_NAME\_W and SCARD\_ATTR\_DEVICE\_SYSTEM\_NAME\_W.
- Updated **Cherry USB2LAN Proxy to version 3.0.0.6**.
  - Fixed an issue where the **SICCT listener was not restarted** when a SICCT connection has been closed by the EGK device (ORS-880).
  - Fixed **TLS errors** resulting from re-using channels before the EGK device confirmed the disconnection of the previous connection (ORS-735).
  - **Increase connection handshake timeout from 1 second to 20 seconds**. This is necessary as the EGK device (G87-1505, firmware 2.108.3) does not process the handshake immediately in all situations. (ORS-735).
  - Added **timestamp** to log output.
- Fixed **AD/Kerberos log on with smartcard** and **Smartcard Removal Action: Lock Thin Client**.
- Fixed custom **PKCS#11 module for VMware Horizon logon**. Before this fix, the parameters did not get effective.

**More...**

|           |                                          |
|-----------|------------------------------------------|
| Parameter | Horizon logon with custom PKCS#11 module |
|-----------|------------------------------------------|



|           |                                |
|-----------|--------------------------------|
| Registry  | vmware.view.pkcs11.use_custom  |
| Value     | enabled / <u>disabled</u>      |
| Parameter | Path to the library            |
| Registry  | vmware.view.pkcs11.custom_path |
| Value     |                                |

- Fixed **error in IGEL Smartcard which prevented login with personalized cards** when certain card holder names contained **non-ASCII characters**.

#### HID

- Added support for **Wacom HID 483C touchscreens** (HP Pro x2 612 g2).
- Fixed non working **Lenovo KBRFBU71 wireless keyboard**.
- Fixed **mouse button mapping**.

#### CUPS Printing

- Fixed **HPLIP related printer drivers**.
- Added missing **LaserJet 200 color MFP M276 Postscript to Printer Names** for manufacturer HP in the TC Setup under **Devices > Printer > CUPS > Printers**.

#### Application Launcher

- Fixed **display order** of DNS servers in **Application Launcher** and **About** dialog.

#### OpenVPN

- Fixed **no retry** in case the client **key passphrase** was entered incorrectly.

#### Base system

- **IGEL Setup Assistant** fixes:
  - Fixed **startup on first boot**.
  - **Retain network configuration** if exited via cancel.
  - Fixed **graphical glitches**
  - Fixed **WiFi configuration**
  - **Prevent startup if an administrator passphrase is set** (e.g. from a IGEL System 5 migration).
- Fixed **System suspend on inactivity** showing the suspend dialog directly after system resume.
- Fixed the **custom bootsplashscaling when multiple monitors are configured**. Necessary to force a re-installation of the custom bootsplash for this fix to take effect. To force a re-installation:
  - Trigger the **Update desktop customization** command via UMS or
  - Press the **Bootsplash update** button at **IGEL Setup > System > Firmware Customization > Corporate Design > Custom Bootsplash**.



- Fixed sporadic problems with **custom bootsplash and wallpaper installation**.
- Fixed the **buddy update server** so that UD Pocket devices can also update from buddy update servers.
- Fixed handling of **custom environment variables**. If values contained white spaces the variables could not be set.
- Fixed **reboot/shutdown** when triggered from the lock screen panel.
- Improved **support for IGEL UD7 with additional graphic card**.
- Removed **maximize button from on-screen keyboard window**.
- Fixed **deletion of debuglog partition content** when booted in emergency boot.
- Fixed **handling of optional partitions which are not active as default** while booting in emergency mode.
- Fixed instability in **authentication module pam\_igelsession.so** in some special cases.
- Fixed **ECDSA/ECDH support in HEIMDAL libraries**.
- Fixed **black screen issues** if hostname contains other characters as 'A-Z a-z 0-9 . \_ - '.
- Improved **debuglog partition based login**.
- **Restricted access to command \*\*su\*\* to root and user**.
- **Root home** is now `/root`.
- Removed **system** group (GID 0) which shadowed **root** group (GID 0).
- **Stricter folder and file permissions**.
- Prevent **flickering problems on 4k 60Hz screens**.

#### Storage Devices

- Fixed **mount issue of PTP devices** (Mobile Device Access USB feature must be enabled).
- Fixed **double detection of MTP and PTP**. MTP is preferred over PTP now (Mobile Device Access USB feature must be enabled).

#### Appliance Mode

- Fixed **configuration of post session commands via UMS profile**: There is no second reboot required anymore to apply the settings properly in Appliance Mode.

#### X11 system

- Fixed **automatic order selection of screens for IGEL UD7**.
- Fixed **order of desktop wallpapers for IGEL UD7** when the additional graphics card is installed.
- Fixed **screen stays black problem on UD3-LX**.
- Fixed **non loading DRM/KMS driver on Spectra Nise 106**.
- Added possibility to **change the framebuffer compression for AMDGPU driver**.

**More...**

|           |                                       |
|-----------|---------------------------------------|
| Parameter | AMDGPU framebuffer compression.       |
| Registry  | <code>x.drivers.amdgpu.use_fbc</code> |
| Range     | [default][enable][disable]            |

- Fixed `sessions.user_display0.options.lid_events` work for **eDP** also.
- Fixed **VESA only boot with UEFI system**.
- **AMDGPU stability** fixes applied.



- Fixed issue with **screen configuration for certain cases**.
- Fixed **screen configuration** getting in **endless loop** with multi monitor setups.
- Fixed **memleak in igel\_drm\_daemon**.
- Fixed **DRI2 memleak with AMDGPU driver**.
- Changed `x.xserver0.force_reconfig` registry key (former bool now range).

**More...**

|           |                                                            |
|-----------|------------------------------------------------------------|
| Parameter | Force a display reconfiguration                            |
| Registry  | <code>x.xserver0.force_reconfig</code>                     |
| Range     | <u>default</u> [only on Xorg start/restart][always][never] |

- Usage of **only on Xorg start/restart** as new default for **AMDGPU based devices**.
- Removed `x.xserver0.composite` registry key to prevent problems with **AMD/ATI devices**.
- Fixed **screen remains black when Monitor Probing (DDC)** option is "Off", configurable at setup page **User Interface > Display > Options**.
- Added possibility to configure **graphic displays only if DPMS state is not OFF**.

**More...**

|           |                                                      |
|-----------|------------------------------------------------------|
| Parameter | Do not reconfigure if monitors are in DPMS off state |
| Registry  | <code>x.xserver0.config_on_dpms_on</code>            |
| Value     | <u>enabled</u> / disabled                            |

## Window Manager

- **On-Screen Keyboard will keep aspect ratio** when resized via double click on edge.

## Shadowing/VNC

- Fixed instability of **Secure Shadowing** connector.

## Audio

- Added a workaround for **button handling of Sennheiser USB headsets**.
- Fixed saving and restoring of **volume controls in Pulseaudio and ALSA**.
- Improved consistency while **storing of changed volume values**.
- Fixed **missing audio output over DVI to HDMI/DP in IGEL UD2 (D220)**.
- Fixed configuration of the **default sound output or input on hardware** when presence detection in jack connector is missing.

## Hardware

- Fixed non working **StarTech.com USB2DVIPRO2 DisplayLink** graphics adapter.
- Fixed freezes of **Intel Baytrail** devices.
- Fixed non working **DisplayLink USB** graphics adapter after reboot.

## Remote Management



- Fixed **zero touch deployment** by adding a timeout to the Setup Assistant abort message.
- Fixed **computation of Unit ID**. The Unit ID is the identification key of the thin client in UMS, and also thin client licenses will be bound to the Unid ID. Now the Unit ID is computed once and persistently saved. It consists of the serial number of UD Pocket or the MAC address of a network interface. When multiple network interfaces are present, the interface is selected taking following attributes into account:  
If a license bound to the interface exists, how it is connected (PCI, SDIO, USB or other) and if it is wireless or wired.  
It is best practice not to connect external network interfaces when a freshly installed thin client device is booted for the first time, so that the Unit ID will consist of a MAC address of a network interface which cannot be removed from the thin client device.
- Fixed **monitor serial numbers** not shown in UMS.
- Fixed **Bluetooth Asset Inventory** zombie when bluetooth dongle is removed.
- Fixed **UMS filetransfer** - now filetransfer action is triggered also if only the file classification was changed.
- Fixed **Update on shutdown** UMS job which could be stucked if update is failed once for some reasons.

## 7.29.2 IGEL Universal Desktop OS3/IGEL UD Pocket

Supported Hardware:

<https://kb.igel.com/igelos/en/devices-supported-by-udc3-and-ud-pocket-3117174.html>

- Versions 10.05.100(see page 2212)
- General Information 10.05.100(see page 2217)
- Security Fixes 10.05.100(see page 2217)
- Known Issues 10.05.100(see page 2222)
- New Features 10.05.100(see page 2223)
- Resolved Issues 10.05.100(see page 2251)

### Versions 10.05.100

- **Clients**

| Product                          | Version         |
|----------------------------------|-----------------|
| Citrix HDX Realtime Media Engine | 2.6.0-2030      |
| Citrix Receiver                  | 13.10.0.20      |
| Citrix Receiver                  | 13.5.0.10185126 |
| Citrix Receiver                  | 13.9.1.6        |



|                                         |                                 |
|-----------------------------------------|---------------------------------|
| deviceTRUST Citrix Channel              | 17.2.100.0                      |
| deviceTRUST RDP Channel                 | 17.2.100.0                      |
| Ericom PowerTerm                        | 12.0.1.0.20170219.2-_dev_-34574 |
| Evidian AuthMgr                         | 1.5.6840                        |
| Evince PDF Viewer                       | 3.18.2-1ubuntu4.3               |
| FabulaTech USB for Remote Desktop       | 5.2.29                          |
| Firefox                                 | 60.2.2                          |
| IBM iAccess Client Solutions            | 1.1.5.0                         |
| IGEL RDP Client                         | 2.2                             |
| Imprivata OneSign ProveID Embedded      |                                 |
| Leostream Java Connect                  | 3.3.7.0                         |
| NX Client                               | 5.3.12                          |
| Open VPN                                | 2.3.10-1ubuntu2.1               |
| Oracle JRE                              | 1.8.0_181                       |
| Parallels Client (32 bit)               | 16.5.1.20446                    |
| Parole Media Player                     | 1.0.1-0ubuntu1igel11            |
| Remote Viewer (RedHat Virtualization)   | 7.0-igel47                      |
| Spice GTK (Red Hat Virtualization)      | 0.35                            |
| Spice Protocol (Red Hat Virtualization) | 0.12.14                         |
| Usbredir (Red Hat Virtualization)       | 0.8.0                           |
| Systancia AppliDis                      | 4.0.0.17                        |
| Thinlinc Client                         | 4.9.0-5775                      |
| ThinPrint Client                        | 7.5.86                          |



|                       |                         |
|-----------------------|-------------------------|
| Totem Media Player    | 2.30.2                  |
| VMware Horizon Client | 4.8.0-8518891           |
| VNC Viewer            | 1.8.0+git20180123-igel1 |
| Voip Client Ekiga     | 4.0.1                   |

Permalink:<https://kb.igel.com/display/ENLITEOS/Versions+OS3+10.05>

- **Dictation**

|                                                       |          |
|-------------------------------------------------------|----------|
| Diktamen driver for dictation                         |          |
| Driver for Grundig Business Systems dictation devices |          |
| Nuance Audio Extensions for dictation                 | B048     |
| Olympus driver for dictation                          | 20180621 |
| Philips Speech Driver                                 | 12.5.4   |

- **Signature**

|                           |          |
|---------------------------|----------|
| Kofax SPVC Citrix Channel | 3.1.41.0 |
| signotec Citrix Channel   | 8.0.6    |
| signotec VCOM Daemon      | 2.0.0    |
| StepOver TCP Client       | 2.1.0    |

- **Smartcard**

|                                           |           |
|-------------------------------------------|-----------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101   |
| PKCS#11 Library Athena IDProtect          | 623.07    |
| PKCS#11 Library cryptovision sc/interface | 7.1.9.620 |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0 |
| PKCS#11 Library SecMaker NetID            | 6.7.0.23  |
| Reader Driver ACS CCID                    | 1.1.5     |



|                                    |                  |
|------------------------------------|------------------|
| Reader Driver Gemalto eToken       | 10.0.37-0        |
| Reader Driver HID Global Omnikey   | 4.3.3            |
| Reader Driver Identive CCID        | 5.0.35           |
| Reader Driver Identive eHealth200  | 1.0.5            |
| Reader Driver Identive SCRKBC      | 5.0.24           |
| Reader Driver MUSCLE CCID          | 1.4.28           |
| Reader Driver REINER SCT cyberJack | 3.99.5final.SP11 |
| Resource Manager PC/SC Lite        | 1.8.22           |
| Cherry USB2LAN Proxy               | 3.0.0.6          |

- **System Components**

|                                         |                               |
|-----------------------------------------|-------------------------------|
| OpenSSL                                 | 1.0.2g-1ubuntu4.13            |
| OpenSSH Client                          | 7.2p2-4ubuntu2.4              |
| OpenSSH Server                          | 7.2p2-4ubuntu2.4              |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5            |
| MESA OpenGL stack                       | 18.2.1-1igel51                |
| VAAPI ABI Version                       | 0.40                          |
| VDPAU Library version                   | 1.1.1-3ubuntu1                |
| Graphics Driver INTEL                   | 2.99.917+git20180214-igel1830 |
| Graphics Driver ATI/RADEON              | 18.0.1-1igel831               |
| Graphics Driver ATI/AMDGPU              | 18.0.1-1igel831               |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.15-2igel775               |
| Graphics Driver Nvidia                  | 390.87-0ubuntu1               |
| Graphics Driver Vboxvideo               | 5.2.18-dfsg-2igel17           |
| Graphics Driver VMware                  | 13.3.0-2igel812               |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1igel775          |



|                                 |                              |
|---------------------------------|------------------------------|
| Graphics Driver FBDEV           | 0.5.0-1igel819               |
| Graphics Driver VESA            | 2.3.4-1build2igel639         |
| Input Driver Evdev              | 2.10.5-1ubuntu1igel750       |
| Input Driver Elographics        | 1.4.1-1build5igel633         |
| Input Driver eGalax             | 2.5.5814                     |
| Input Driver Synaptics          | 1.9.0-1ubuntu1igel748        |
| Input Driver Vmmouse            | 13.1.0-1ubuntu2igel635       |
| Input Driver Wacom              | 0.36.1-0ubuntu1igel813       |
| Kernel                          | 4.18.11 #mainline-udos-r2463 |
| Xorg X11 Server                 | 1.19.6-1ubuntu4igel838       |
| Xorg Xephyr                     | 1.19.6-1ubuntu4igel832       |
| CUPS printing daemon            | 2.1.3-4ubuntu0.5igel20       |
| PrinterLogic                    | 18.2.1.128                   |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1            |
| XFCE4 Windowmanager             | 4.12.3-1ubuntu2igel653       |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.10igel6      |
| NetworkManager                  | 1.2.6-0ubuntu0.16.04.2igel58 |
| ModemManager                    | 1.6.8-2igel1                 |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.1           |
| GStreamer 1.x                   | 1.14.2-1ubuntu1igel192       |

- **Features with Limited IGEL Support**

|                          |
|--------------------------|
| Mobile Device Access USB |
|--------------------------|

|                 |
|-----------------|
| VPN OpenConnect |
|-----------------|

|                        |
|------------------------|
| Scanner support / SANE |
|------------------------|



### VirtualBox

- **Features with Limited Functionality**

|                   |      |
|-------------------|------|
| Cisco JVDI Client | 12.0 |
|-------------------|------|

## General Information 10.05.100

The following clients and features are not supported anymore:

- Citrix Receiver 12.1 and 13.1 - 13.4
- Citrix Access Gateway Standard Plug-in
- Dell vWorkspace Connector for Linux
- Ericom PowerTerm Emulation 9 and 11
- Ericom Webconnect
- IGEL Legacy RDP Client (rdesktop)
- Virtual Bridges VERDE Client
- PPTP VPN Support
- IGEL Upgrade License Tool with IGEL Smartcard Token
- Remote Management by setup.ini file transfer (TFTP)
- Remote Access via RSH
- Legacy Philips Speech Driver
- t-Systems TCOS Smartcard Support
- DUS Series touch screens
- Elo serial touch screens
- IGEL Smartcard without locking desktop
- VIA Graphic Support
- Storage Hotplug devices are not automatically removed anymore, instead they must be always ejected manually:
  - by panel tray icon
  - by an icon in the **In-Session Control Bar** (configurable at **IGEL Setup > User Interface > Desktop**)
  - by a **Safely Remove Hardware** session (configurable at **IGEL Setup > Accessories**)

The following clients and features are not available in this release:

- Cherry eGK Channel
- Open VPN Smartcard Support
- NCP Secure Client
- Asian Input Methods
- Composite Manager

## Security Fixes 10.05.100

Firefox

- Updated Mozilla Firefox to version **60.2.2esr**.

**More...**

mfsa2018-24: CVE-2018-12386, CVE-2018-12387  
 mfsa2018-23: CVE-2018-12385, CVE-2018-12383  
 mfsa2018-21: CVE-2018-12377, CVE-2018-12378, CVE-2018-12376  
 mfsa2018-16: CVE-2018-12359, CVE-2018-12360, CVE-2018-12361, CVE-2018-12362,  
 CVE-2018-5156, CVE-2018-12363, CVE-2018-12364, CVE-2018-12365,  
 CVE-2018-12371, CVE-2018-12366, CVE-2018-12367, CVE-2018-12369,  
 CVE-2018-5187, CVE-2018-5188  
 mfsa2018-14: CVE-2018-6126  
 mfsa2018-11: CVE-2018-5154, CVE-2018-5155, CVE-2018-5157, CVE-2018-5158,  
 CVE-2018-5159, CVE-2018-5160, CVE-2018-5152, CVE-2018-5153,  
 CVE-2018-5163, CVE-2018-5164, CVE-2018-5166, CVE-2018-5167,  
 CVE-2018-5168, CVE-2018-5169, CVE-2018-5172, CVE-2018-5173,  
 CVE-2018-5175, CVE-2018-5176, CVE-2018-5177, CVE-2018-5165,  
 CVE-2018-5180, CVE-2018-5181, CVE-2018-5182, CVE-2018-5151,  
 CVE-2018-5150.  
 mfsa2018-10: CVE-2018-5148

- Firefox profile partition is now **mounted at /userhome/.mozilla instead of /.ffpro**.
- Firefox could only be started as **user**.
- For security reasons **Java processes could not be started from a browser session now**.
- Added a registry parameter `java.browser.access` to **control java access for all browser sessions**.

**More...**

|           |                                  |
|-----------|----------------------------------|
| Parameter | Allow browser to use java        |
| Registry  | <code>java.browser.access</code> |
| Value     | <u>enabled</u> / <u>disabled</u> |

## Network

- **Disabled ICMP redirects.**
- Changed default **LoginGraceTime** from 120 to 30 sec.
- Added new registry keys for a **secure sshd configuration**.

**More...**

|           |                                                |
|-----------|------------------------------------------------|
| Parameter | Permit X11 forwarding                          |
| Registry  | <code>network.ssh_server.x11_forwarding</code> |
| Value     | <u>enabled</u> / <u>disabled</u>               |
| Parameter | Show banner                                    |
| Registry  | <code>network.ssh_server.show_banner</code>    |



|           |                                          |
|-----------|------------------------------------------|
| Value     | <u>enabled / disabled</u>                |
| Parameter | Permit tcp tunnel forwarding             |
| Registry  | network.ssh_server.permit_tcp_forwarding |
| Value     | <u>enabled / disabled</u>                |

- Fixed **SCEP client certificate request file access rights.**

#### Base system

- Added **apparmor** as an additional security layer for components like Firefox, evince, dhclient and cups.

[More...](#)

|           |                           |
|-----------|---------------------------|
| Parameter | Enable apparmor profiles  |
| Registry  | system.security.apparmor  |
| Value     | <u>enabled / disabled</u> |

- For security reasons **graphical terminal sessions** could now only be started by an administrator when an **admin password** is set. Administrator must authenticate before a terminal session is started. This does also affect graphical terminal sessions spawned by applications.
- To **allow users to start a terminal session again** a registry key is defined.

[More...](#)

|           |                           |
|-----------|---------------------------|
| Parameter | User shell terminal       |
| Registry  | system.security.usershell |
| Value     | <u>enabled / disabled</u> |

- Fixed **open-vm-tools** security issue CVE-2015-5191.
- Fixed **procps** security issues CVE-2018-1126, CVE-2018-1125, CVE-2018-1124, CVE-2018-1123 and CVE-2018-1122.
- Fixed **imagemagick** security issues.

[More...](#)

CVE-2018-9133, CVE-2018-8960, CVE-2018-8804

CVE-2018-7443, CVE-2018-5248, CVE-2018-11251, CVE-2018-10177, CVE-2017-18273,

CVE-2017-18271, CVE-2017-18252, CVE-2017-18211, CVE-2017-18209,

CVE-2017-17914, CVE-2017-17879, CVE-2017-17682, CVE-2017-17681,

CVE-2017-17504, CVE-2017-16546, CVE-2017-15281, CVE-2017-15277,

CVE-2017-15017, CVE-2017-15016, CVE-2017-15015, CVE-2017-14989,

CVE-2017-14741, CVE-2017-14739, CVE-2017-14682, CVE-2017-14626,

CVE-2017-14625, CVE-2017-14624, CVE-2017-14607, CVE-2017-14532,

CVE-2017-14531, CVE-2017-14505, CVE-2017-14400, CVE-2017-14343,

CVE-2017-14342, CVE-2017-14341, CVE-2017-14325, CVE-2017-14249,

CVE-2017-14224, CVE-2017-14175, CVE-2017-14174, CVE-2017-14173,

CVE-2017-14172, CVE-2017-14060, CVE-2017-13769, CVE-2017-13768,



CVE-2017-13758, CVE-2017-13145, CVE-2017-13144, CVE-2017-13143, CVE-2017-13142, CVE-2017-13139, CVE-2017-13134, CVE-2017-12983, CVE-2017-12877, CVE-2017-12875, CVE-2017-12693, CVE-2017-12692, CVE-2017-12691, CVE-2017-12674, CVE-2017-12670, CVE-2017-12643, CVE-2017-12640, CVE-2017-12587, CVE-2017-12563, CVE-2017-12435, CVE-2017-12432, CVE-2017-12431, CVE-2017-12430, CVE-2017-12429, CVE-2017-12140, CVE-2017-11640, CVE-2017-11639, CVE-2017-11537, CVE-2017-11535, CVE-2017-11533, CVE-2017-11352, CVE-2017-10995, CVE-2017-1000476, CVE-2017-1000445, CVE-2018-13153, CVE-2018-12600 and CVE-2018-12599.

- Fixed **elfutils** security issues CVE-2017-7613, CVE-2017-7612, CVE-2017-7611, CVE-2017-7610, CVE-2017-7609, CVE-2017-7608, CVE-2017-7607, CVE-2016-10255 and CVE-2016-10254.
- Fixed **ghostscript** security issues CVE-2018-10194, CVE-2016-10317, CVE-2018-16802, CVE-2018-16585, CVE-2018-16543, CVE-2018-16542, CVE-2018-16541, CVE-2018-16540, CVE-2018-16539, CVE-2018-16513, CVE-2018-16511, CVE-2018-16509, CVE-2018-15911, CVE-2018-15910, CVE-2018-15909, CVE-2018-15908, CVE-2018-11645, CVE-2018-1, CVE-2018-17183 and CVE-2018-16510.
- Fixed **icu** security issue CVE-2017-15422.
- Fixed **webkit2gtk** security issues.

**More...**

CVE-2018-4200, CVE-2018-4165, CVE-2018-4163, CVE-2018-4162, CVE-2018-4161, CVE-2018-4146, CVE-2018-4133, CVE-2018-4129, CVE-2018-4128, CVE-2018-4127, CVE-2018-4125, CVE-2018-4122, CVE-2018-4120, CVE-2018-4119, CVE-2018-4118, CVE-2018-4117, CVE-2018-4114, CVE-2018-4113, CVE-2018-4101, CVE-2018-4233, CVE-2018-4232, CVE-2018-4222, CVE-2018-4218, CVE-2018-4199, CVE-2018-4190, CVE-2018-12293, CVE-2018-4284, CVE-2018-4278, CVE-2018-4273, CVE-2018-4272, CVE-2018-4270, CVE-2018-4267, CVE-2018-4266, CVE-2018-4265, CVE-2018-4264, CVE-2018-4263, CVE-2018-4262, CVE-2018-4261, CVE-2018-4246 and CVE-2018-12911.

- Fixed **perl** security issues CVE-2018-6913, CVE-2018-6798, CVE-2018-6797, CVE-2017-6512, CVE-2016-6185 and CVE-2018-12015.
- Fixed **poppler** security issues CVE-2017-18267 and CVE-2018-13988.
- Fixed **openssl** security issues CVE-2018-0739, CVE-2018-0737, CVE-2018-0737, CVE-2018-0732 and CVE-2018-0495.
- Fixed **tiff** security issues.

**More...**

CVE-2018-5784, CVE-2017-9936, CVE-2017-9935, CVE-2017-9815, CVE-2017-9404, CVE-2017-9403, CVE-2017-9147, CVE-2017-9117,



CVE-2017-7602, CVE-2017-7601, CVE-2017-7600, CVE-2017-7599, CVE-2017-7598,  
CVE-2017-7597, CVE-2017-7596, CVE-2017-7595, CVE-2017-7594, CVE-2017-7593,  
CVE-2017-7592, CVE-2017-5563, CVE-2017-18013, CVE-2017-17095, CVE-2017-13727,  
CVE-2017-13726, CVE-2017-12944, CVE-2017-11613, CVE-2017-11335,  
CVE-2017-10688, CVE-2016-5318, CVE-2016-5102, CVE-2016-3186, CVE-2016-10371,  
CVE-2016-10269, CVE-2016-10268, CVE-2016-10267 and CVE-2016-10266.

- Fixed **libvncserver** security issue CVE-2018-7225.
- Fixed **libvorbis** security issue CVE-2018-5146.
- Fixed **samba** security issues CVE-2018-1057, CVE-2018-1050, CVE-2018-10919 and CVE-2018-10858.
- Fixed **wget** security issue CVE-2018-0494.
- Fixed **bluez** security issue CVE-2017-1000250.
- Fixed **libgcrypt20** security issue CVE-2018-0495.
- Fixed **file** security issue CVE-2018-10360.
- Fixed **gnupg2** security issue CVE-2018-12020.
- Fixed **isc-dhcp** security issues CVE-2018-5733, CVE-2018-5732, CVE-2018-573, CVE-2017-3144 and CVE-2016-2774.
- Fixed **curl** security issues CVE-2018-1000303, CVE-2018-1000301, CVE-2018-1000300, CVE-2018-1000122, CVE-2018-1000121, CVE-2018-1000120, CVE-2017-8818, CVE-2018-14618 and CVE-2018-0500.
- Fixed **python3.5** security issues CVE-2017-1000158, CVE-2016-5636, CVE-2016-1000110 and CVE-2016-0772.
- Fixed **zlib** security issues CVE-2016-9843, CVE-2016-9842, CVE-2016-9841 and CVE-2016-9840.
- Fixed **libsoup2.4** security issue CVE-2018-12910.
- Fixed **libjpeg-turbo** security issue CVE-2018-1152.
- Fixed **ntp** security issues CVE-2018-7185 and CVE-2018-7183.
- Fixed **libpng1.6** security issue CVE-2018-13785.
- Fixed **cups** security issues CVE-2018-6553, CVE-2018-4181, CVE-2018-4180, CVE-2018-418 and CVE-2017-18248.
- Fixed **libpng** security issue CVE-2016-10087.
- Fixed **policykit-1** security issue CVE-2018-1116.
- Fixed **jansson** security issue CVE-2016-4425.
- Fixed **libmspack** security issues CVE-2018-14682, CVE-2018-14681, CVE-2018-14680 and CVE-2018-14679.
- Fixed **libonig** security issues CVE-2017-9229, CVE-2017-9228, CVE-2017-9227, CVE-2017-9226 and CVE-2017-9224.
- Fixed **libxcursor** security issue CVE-2015-9262.
- Fixed **heimdal** security issue CVE-2017-17439.
- Fixed **libarchive** security issues CVE-2017-14503, CVE-2017-14501, CVE-2017-14166, CVE-2016-10350, CVE-2016-10349 and CVE-2016-10209.
- Fixed **libxml2** security issues CVE-2018-14567, CVE-2018-14404, CVE-2017-18258 and CVE-2016-9318.
- Fixed **confuse** security issue CVE-2018-14447.
- Fixed **libgd2** security issues CVE-2018-5711 and CVE-2018-1000222.



- Fixed **libx11** security issues CVE-2018-14600, CVE-2018-14599, CVE-2018-14598, CVE-2016-7943 and CVE-2016-7942.
- Fixed **mpg123** security issues CVE-2017-10683 and CVE-2016-1000247.
- Fixed **libtirpc** security issues CVE-2018-14622, CVE-2017-8779 and CVE-2016-4429.
- Fixed **jq** security issue CVE-2015-8863.
- Fixed **bind9** security issue CVE-2018-5740.
- Fixed **lcms2** security issue CVE-2018-16435.
- Fixed **xdg-utils** security issue CVE-2017-18266.
- Root home is now **/root**.
- **Removed system group (GID 0)** which shadowed root group (GID 0).
- **Stricter folder and file permissions**.

#### X11 system

- Restricted desktop icon creation to administrator only. Therefore, "**/userhome/Desktop**" is **owned by root now**.

#### Known Issues 10.05.100

##### Citrix Receiver 13

- On devices with **AMD/Radeon graphics chipsets** and **activated DRI3 X driver option** the **hardware accelerated Citrix H.264 decoder plugin can hang**. To solve this issue deactivation of DRI3 option is necessary (default setting). Selective H.264 mode (api v2) is not affected from this issue.
- **Citrix StoreFront login with Gemalto smartcard middleware** does not detect smartcard correctly when the card is inserted after start of login. As a workaround, insert the smartcard before starting StoreFront login.
- The Citrix Receiver has known issues with **GStreamer1.x**. This causes **problems with multimedia redirection of H264, MPEG1 and MPEG2**. GStreamer1.x is used if browser content redirection is active.

##### Parallels Client

- **Native USB redirection** does not work with Parallels Client.
- Due to a bug in the Parallels-Client, for using the new **FIPS 140-2 compliance mode** it is necessary to connect to the Parallels RAS one time with FIPS support disabled.

##### VMware Horizon

- VMware Horizon Client for Linux **4.8.0 supports FIPS Mode on only VMware Horizon server installations up to version 7.5**.
- **External drives are mounted already before connection, do not appear in the remote desktop**. Workaround: mapping the directory /media as a drive on desktop. The external devices will show up within the media drive then.
- **Client drive mapping and USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global >**



**Drive Mapping > Enable Drive Mapping.** It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.

- On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Enable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.

#### OpenConnect VPN

- VPNs that require the **OpenConnect client** cannot be used for firmware updates.

#### Appliance Mode

- Appliance mode **RHEV/Spice: spice-xpi Firefox plugin is no longer supported.** The **Console Invocation** has to allow native client (auto is also possible) and it should start in fullscreen to prevent opening windows.

#### Smartcard

- In seldom cases, the authentication hung when using A.E.T. SafeSign smartcards.

#### IGEL Cloud Gateway

- **No support for UMS file transfer status** in ICG protocol.

## New Features 10.05.100

#### Citrix Receiver 13

- Integrated **Citrix Receiver 13.10.** Citrix Receiver version 13.7.0 was removed. Citrix Receiver version 13.8.0 was removed. Available Citrix Receiver versions: 13.5.0, 13.9.1, 13.10 (default)
  - Enable **Browser content redirection for rendering of whitelisted webpages** on the IGEL Thin Client.  
[More...](#)

|            |                                                                                  |
|------------|----------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix XenDesktop &gt; HDX / ICA Global &gt; HDX Multimedia</b> |
| Parameter  | Browser content redirection                                                      |
| Registry   | ica.module.virtualdriver.webpageredirection                                      |
| Value      | enabled / <u>disabled</u>                                                        |

- Enhanced **Citrix retail logging.**

[More...](#)

|           |                            |
|-----------|----------------------------|
| Parameter | Citrix Logging             |
| Registry  | ica.module.syslogthreshold |



|                                                             |           |
|-------------------------------------------------------------|-----------|
| Value                                                       | 0 / 3 / 7 |
| > 0 = Disabled; > 3 = Log only errors; > 7 = Log all levels |           |

- Enable **Port forwarding**.

[More...](#)

|           |                                      |
|-----------|--------------------------------------|
| Parameter | Portforward                          |
| Registry  | ica.module.virtualdriver.portforward |
| Value     | enabled / <u>disabled</u>            |

- **Workspace configuration parameter for Citrix Cloud** is now available on setup page.

[More...](#)

|            |                                                           |
|------------|-----------------------------------------------------------|
| IGEL Setup | Sessions > Citrix XenDesktop > HDX / ICA Global > Options |
| Parameter  | Connect to cloud                                          |
| Registry   | ica.cloudconnect                                          |
| Value      | enabled / <u>disabled</u>                                 |

- Added a registry key to **control the visibility of the Citrix connection bar** for desktop sessions. If activated, the In-Session Control Bar should be disabled at `userinterface.igel_toolbar.enable`

and `userinterface.igel_toolbar.show_always`.

This enables the control of the new **Multi-monitor layout persistence** feature.

[More...](#)

|           |                                                       |
|-----------|-------------------------------------------------------|
| Parameter | Citrix Connection Bar                                 |
| Registry  | ica.allregions.connectionbar                          |
| Value     | <u>factory default</u> / off / on / server determined |

- Added a registry key to control the availability of deprecated cipher suites:

**TLS\_RSA\_AES256\_GCM\_SHA384, TLS\_RSA\_AES128\_GCM\_SHA256,**

**TLS\_RSA\_AES256\_CBC\_SHA256, TLS\_RSA\_AES256\_CBC\_SHA,**

**TLS\_RSA\_AES128\_CBC\_SHA,**

**TLS\_RSA\_3DES\_CBC\_EDE\_SHA.**

[More...](#)

|           |                       |
|-----------|-----------------------|
| Parameter | TLS RSA cipher suites |
|-----------|-----------------------|



|                                                                                                                                                                                                                       |                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| Registry                                                                                                                                                                                                              | <code>ica.allregions.enable_tls_rsa</code> |
| Value                                                                                                                                                                                                                 | <u>factory default</u> / false / true      |
| Factory default: true/enabled. Citrix explicitly remarks: <b>Important:</b> Set the flag <code>enable_tls_rsa</code> to true to use the other two cipher suites <b>Enable_RC4-MD5</b> and <b>Enable_RC4_128_SHA</b> . |                                            |

- Added a registry key to control the availability of the deprecated cipher suite: **RC4-MD5**.  
**More...**

|                                  |                                            |
|----------------------------------|--------------------------------------------|
| Parameter                        | RC4-MD5 cipher suite                       |
| Registry                         | <code>ica.allregions.enable_rc4_md5</code> |
| Value                            | <u>factory default</u> / false / true      |
| Factory default: false/disabled. |                                            |

- Added a registry key to control the availability of the deprecated cipher suite: **RC4\_128\_SHA**.  
**More...**

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| Parameter                        | RC4_128_SHA cipher suite                       |
| Registry                         | <code>ica.allregions.enable_rc4_128_sha</code> |
| Value                            | <u>factory default</u> / false / true          |
| Factory default: false/disabled. |                                                |

- Added **Selective H.264** (API v2) to the hardware accelerated Citrix deep compression codec. XenDesktop/XenApp server policy: **Use video codec for compression -> For actively changing regions**
- Added **DRI3 acceleration support** to the hardware accelerated Citrix deep compression codec (for INTEL and AMD graphics adapters).
- Enable **debugging to log file** `/var/log/user/ctxh264.log`.  
**More...**

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | Enable H264 codec debug output                   |
| Registry  | <code>ica.hw-accelerated-h264-codec-debug</code> |
| Value     | enabled / <u>disabled</u>                        |

- Added **Kerberos Passthrough (domain passthrough) authentication to StoreFront**. Configurable at **Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > StoreFront Logon > Authentication Type**.



- Updated **Citrix HDX RTME** used for optimization of **Skype for Business** to **2.6.0-2030**. This new version adds the support for hardware accelerated H.264 en- and decoding on AMD platforms. See <https://support.citrix.com/article/CTX236304> section **Capability Checker for Linux platforms** how to enable hardware decoding with Citrix VDA registry keys `DisableLinuxAMDH264HardwareDecoding` and `SupportedAMDHWAVideoCardList`. The capability check program **RTOP-CapabilityChk-x64** is already installed at path `/services/ica/hdx_rtme/RTOP-CapabilityChk-x64`. The check program must be run with user permissions.
- Added display of **logged on Citrix username in screen lock**, when screen lock password is synchronized with Citrix password.
- Added checkbox to **activate autostart of a single published application/desktop session**.

[More...](#)

|            |                                                                                                 |
|------------|-------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix XenDesktop / XenApp &gt; Citrix StoreFront/Web Interface &gt; Login</b> |
| Parameter  | Start a single published application automatically                                              |
| Registry   | <code>ica.pnlogin.autostart_single_application</code>                                           |
| Value      | enabled / <u>disabled</u>                                                                       |

- Added **Lakeside SysTrack virtual channel in Citrix, RDP and Horizon sessions**. Activation via parameters in Setup.

[More...](#)

|            |                                                                                                    |
|------------|----------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix XenDesktop/XenApp &gt; HDX/ICA Global &gt; Mapping &gt; Device Support</b> |
| Parameter  | Lakeside Systrack channel                                                                          |
| Registry   | <code>ica.module.virtualdriver.lakeside.enable</code>                                              |
| Value      | enabled / <u>disabled</u>                                                                          |
| IGEL Setup | <b>Sessions &gt; RDP &gt; RDP Global &gt; Mapping &gt; Device Support</b>                          |
| Parameter  | Lakeside Systrack channel                                                                          |
| Registry   | <code>rdp.winconnect.plugins.lakeside.use</code>                                                   |
| Value      | enabled / <u>disabled</u>                                                                          |



|            |                                                                                 |
|------------|---------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Performance</b> |
| Parameter  | Lakeside Systrack                                                               |
| Registry   | vmware.view.lakeside_systrack                                                   |
| Value      | enabled / <u>disabled</u>                                                       |

- Updated **Olympus dictation channel for Citrix to version 20180621.**

[More...](#)

|            |                                                                                                        |
|------------|--------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix XenDesktop / XenApp &gt; HDX / ICA Global &gt; Mapping &gt; Device Support</b> |
| Parameter  | Olympus channel for dictation                                                                          |
| Registry   | ica.module.virtualdriver.olycom.enable                                                                 |
| Value      | enabled / <u>disabled</u>                                                                              |

- Added **CrossMatch / DigitalPersona channel for Citrix version 0515.**

[More...](#)

|            |                                                                                                        |
|------------|--------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix XenDesktop / XenApp &gt; HDX / ICA Global &gt; Mapping &gt; Device Support</b> |
| Parameter  | Crossmatch DigitalPersona fingerprint channel                                                          |
| Registry   | ica.module.virtualdriver.dpicacnt.enable                                                               |
| Value      | enabled / <u>disabled</u>                                                                              |

#### RDP/IGEL RDP Client 2

- Support for new **RDP 10 codec AVC444 (H.264)**, which reduces network bandwidth with Server 2016 and Windows 10 hosts. AMD Radeon graphics is required on the client side. Other graphics hardware (e.g. Intel) as well as other RDP 10 codecs (AVC420 and AVC444V2) will be supported in the future.

[More...](#)

|            |                                                           |
|------------|-----------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; RDP &gt; RDP Global &gt; Performance</b> |
| Parameter  | Hardware accelerated codecs AVC420/AVC444 (H.264)         |



|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| Registry   | <code>rdp.winconnect.enable-h264</code>                                       |
| Value      | <u>auto</u> / on / off                                                        |
| IGEL Setup | <b>Sessions &gt; RDP &gt; RDP Sessions &gt; Session Name &gt; Performance</b> |
| Parameter  | Hardware accelerated codecs AVC420/AVC444 (H.264)                             |
| Registry   | <code>sessions.winconnect%.option.enable-h264</code>                          |
| Value      | <u>Global setting</u> / auto / on / off                                       |

The value "auto" enables supported codecs on supported hardware.

The value "on" enables supported codecs on all hardware.

The value "off" disables H.264 codecs.

- Added new parameter **ignore\_errors** to RDP Session config to **suppress RDP error messages**.  
[More...](#)

|          |                                                 |
|----------|-------------------------------------------------|
| Registry | <code>sessions.winconnect%.ignore_errors</code> |
| Value    | <u>enabled</u> / <u>disabled</u>                |

- Added **Olympus dictation channel for RDP version 20180621**.

[More...](#)

|            |                                                                           |
|------------|---------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; RDP &gt; RDP Global &gt; Mapping &gt; Device Support</b> |
| Parameter  | Olympus channel for dictation                                             |
| Registry   | <code>rdp.winconnect.plugins.olyvc.use</code>                             |
| Value      | <u>enabled</u> / <u>disabled</u>                                          |

#### UD Pocket

- UD Pocket demo license registration dialog** will now show an option to **set up proxy servers when IGEL servers cannot be reached**.
- Updated the page displayed for the **UD Pocket demo registration**. It can be chosen now whether a partner or the customer is setting up the device, before displaying the form asking for customer information.

#### Parallels Client



- Updated **Parallels client to version 16.5.1.20446 (32-Bit)**
- Added support for **FIPS 140-2 compliance**.

[More...](#)

|            |                                           |
|------------|-------------------------------------------|
| IGEL Setup | <b>System &gt; Registry</b>               |
| Parameter  | Enable support for FIPS 140-2 compliance  |
| Registry   | sessions.twox%.connection.fips_compliance |
| Value      | enabled / <u>disabled</u>                 |

#### VMware Horizon

- Updated **Horizon client to version 4.8.0-8518891**.

#### ThinLinc

- Updated **ThinLinc client to version 4.9.0**.
  - Shadowing notification is now more reliable and interactive, allowing end users more control of their sessions.
  - More than 80 minor enhancements and fixes. See <https://www.cendio.com/thinlinc/docs/relnotes/4.9.0>.

#### RedHat Enterprise Virtualization client

- **Updated spice components** (virt-viewer 7.0, spice-gtk 0.35).
- **Removed support for spice-xpi plugin**.

#### X session (Xephyr)

- Added support for X sessions configurable at `IGEL Setup > Sessions > X Sessions`. The available XDMCP connection types: indirect via localhost, indirect, direct and broadcast. With the additional connection type "local display" a command can be specified, that will be displayed inside the X session window.

[More...](#)

|            |                                                                          |
|------------|--------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; X Sessions &gt; X Session &gt; Server</b>               |
| Parameter  | Connection type                                                          |
| Registry   | sessions.xnest<NR>.server.connectiontype                                 |
| Range      | [Indirect via localhost] [Indirect] [Direct] [Broadcast] [Local display] |

#### IGEL Setup **Sessions > X Sessions > X Session > Server**

|           |                         |
|-----------|-------------------------|
| Parameter | Command to be displayed |
|-----------|-------------------------|



|          |                                      |
|----------|--------------------------------------|
| Registry | sessions.xnest<NR>.server.runcommand |
|----------|--------------------------------------|

## Firefox

- Updated Mozilla Firefox to **version 60.2.2 ESR**.
- The **initial page** displayed by firefox with default settings is now <https://kb.igel.com/> instead of the older <https://edocs.igel.com/>.
- Updated **Adobe Flash Player** download URL to **version 31.0.0.122**.
- **Removed the webapp specific options**, this feature was removed from Firefox and is not relevant anymore.
- Moved **Browser Certificate** configuration to page **Sessions > Browser > Browser Global > Certificates**.
- Moved **Browser Security Device** configuration to page **Sessions > Browser > Browser Global > Smartcard Middleware**.
- Added **Fluendo FFmpeg GStreamer** proxy: Provides ffmpeg-libavcodec-compatible library, which is needed for H.264 playback in firefox. Instead decoding by standard ffmpeg libraries, the video stream is redirected to GStreamer framework.

## Network

- **SCEP**: Added subject alternative name type **DNS Name as UPN (auto)**. This is similar to **DNS Name (auto)**. In the CSR the result is a Microsoft User Principal Name (UPN) that consists of the hostname.
- **NetworkManager** updated to version **1.2.6**.

## Cisco JVDI Client

- Integrated new **Cisco Jabber Softphone for VDI** (Cisco JVDI client) **version 12.0.0** as feature with limited functionality. See product documentation for details -> <https://kb.igel.com/cisco-jvdi/en>. Activation of this feature at: **System > Firmware Customization > Features > Cisco JVDI client**. Only Citrix Receiver 13.9.1 is supported.

[More...](#)

|            |                                                                                                                      |
|------------|----------------------------------------------------------------------------------------------------------------------|
| Parameter  | Log Level                                                                                                            |
| Registry   | multimedia.ciscovxme.log_level                                                                                       |
| Range      | [Info] [Warning] [Error] [Fatal] [ <u>Debug</u> ] [Trace]                                                            |
| IGEL Setup | <b>Sessions &gt; Citrix XenDesktop/XenApp &gt; HDX/ICA Global &gt; Unified Communications &gt; Cisco JVDI Client</b> |
| Parameter  | Cisco JVDI Client                                                                                                    |
| Registry   | ica.module.virtualdriver.vdcisco.enable                                                                              |
| Value      | enabled / <u>disabled</u>                                                                                            |



Registry path for Common JVDI options: ` multimedia.ciscovxme.\*\*` The Cisco JVDI Client configuration is only displayed if the Multimedia Codec Pack (MMC) is present.

## Java

- Updated **Oracle Java Runtime Environment to version 1.8.0 U181.**

## Smartcard

- Updated **SecMaker Net iD to version 6.7.0.23.**
- Updated **HID Global Omnikey smartcard reader driver to version 4.3.3.**
- Updated **cryptovision sc/interface to version 7.1.9.** Changelog since version 7.0.5:
  - Fixed **an error during certificate registration** using the MS Minidriver for MS VSC. Compatible with sc/interface cache version 1.2 or higher.
  - Fixed an error where **writing a certificate using the Minidriver for MS VSC corrupted the Container-ID.** As a result the key could not be used using CNG/CAPI.
  - Fixed an error during **certificate registration using the Minidriver for MS VSC where some Container-ID's could not be used by CNG/CAPI.**
  - General Bug Fixes.
  - Fixed **error during profile creation on JCOP3 with ePasslet-Suite 3.0**
  - Added support for **additional BWI card profiles based on CardOS-5.x.** Versions **1.7, 1.8, 1.9, 4.2, 4.3 and 4.4.** Support **4k RSA for 1.9 and 4.4.**
  - Fixed support for **remote logon in sc/interface cache.**
  - Fixed **Free after use** in ReadOnly Minidriver.
  - PKCS#11 Fixed **MS VSC (GIDSv2) support.**
  - PKCS#11 Fixed **CardOS-4.x "non sc/interface card profile" support.**
  - **MS VSC (GIDSv2)** Support for PKCS#11 - Maximum CKA\_ID length reduced to 25 bytes!
  - Support for **JCOP3 and Infineon JTOP - DolphinV2.**
  - Support for **cryptovision's ePasslet-Suite-3.0.**
  - New **ePKIApplet-2.129 for JCOP3, SCE7 and JTOP (DolphinV2)** with up to 4096 bits RSA and 512 bits
  - **EC** support, **PACE** optional.
  - **RegisterTool plugins now available in Setup.** Removed from "support\RegisterTool\_Plugins".
  - **New sc/interface Minidriver support for MS VSC** (instead of the MS Minidriver) to allow extended PIN cache configuration.
  - Added support for **sc/interface cache version 1.0** for Minidriver/ReadOnly Minidriver and PKCS#11.
  - **Cross-application PIN cache for Windows 8.1** and later.
  - **WARNING: No longer compatible with Credential Cache (CSP).** When there are any questions, [support@cryptovision.com<sup>458</sup>](mailto:support@cryptovision.com) should be contacted.
  - Added **macOS CTK Token Driver for 10.12 and later.** Unfortunately, after the installation, a shell script must be executed to enable the full functionality.
  - **Removed macOS tokend support** beginning with version 10.12, installation of 10.10 can be used if needed.

---

<sup>458</sup> mailto:support@cryptovision.com



- **WARNING: macOS tokend support will discontinue, usage of new CTK Token Driver is necessary.**
- Re-Added **cvSimpleCardProv for Windows** (based on 6.4.2) to enable the default login selection, see "support\CredentialProvider".
- Updated **OpenSC library to version 0.19.0**. Improved handling of PIV and CAC ALT token.

#### Base system

- Updated to **kernel version 4.18.11**.
- Added new **GStreamer 1.x support version 1.14.2**.

There will only ever be GStreamer in version 1.0 or version 0.10. By default, clients run with the version they have best support for. The provided registry key can be used to override the automatic detection/setting and pin a single version if required.

**More...**

|           |                                   |
|-----------|-----------------------------------|
| Parameter | Fluendo GStreamer Codec Version   |
| Registry  | multimedia.gstreamer.version      |
| Value     | [1.x] [0.10] [ <u>automatic</u> ] |

- With **GStreamer 1.x the new Parole player is used** for media player sessions. When there occur problems with the new player, a switch back to totem/GStreamer 0.10 media player is possible by **Fluendo GStreamer Codec Version** parameter.
- Added **optional logoff button in taskbar** when the screenlock is active.

**More...**

|            |                                                          |
|------------|----------------------------------------------------------|
| IGEL Setup | <b>Security &gt; Logon &gt; Taskbar</b>                  |
| Parameter  | Show logoff button                                       |
| Registry   | userinterface.screenlock_taskbar_logged_in.logoff_button |
| Value      | enabled / <u>disabled</u>                                |

- **Mobile broadband configuration dialog now provides a simple mode**, that displays 3 dropdown boxes to select country, provider and access point (plan). The former version is available via an **Expert Mode** button.
- **IGEL Setup Assistant enhancements:**
  - displaying page for **mobile broadband configuration** when any mobile broadband modem is detected.
  - displaying page to **show broken network connectivity**
  - **desktop icon** will now be displayed **when the assistant was not yet finished**.
  - **the assistant is now always started on devices without IGEL license**, that are not registered at UMS
  - new **icon design**
- Added support for **chinese, japanese, korean** and **thai** fonts.



- **KVM kernel modules added.**
  - Added **policykit-1-gnome session agent** to get a gui interface for actions which requires root authentication.
  - Added **remote (network attached) logging via rsyslog**.
- [More...](#)

| IGEL Setup <b>System -&gt; Remote Syslog</b> |                                  |
|----------------------------------------------|----------------------------------|
| Parameter                                    | Remote mode                      |
| Registry                                     | system.syslog.remote_mode        |
| Range                                        | [Server] [Client] [ <u>Off</u> ] |
| Parameter                                    | Custom client config entries     |
| Registry                                     | system.syslog.client_custom      |

- **Server mode** is possible, though limited and intended for short-term debugging.
- [More...](#)

| IGEL Setup <b>System -&gt; Remote Syslog</b> |                                    |
|----------------------------------------------|------------------------------------|
| Parameter                                    | Template for log file storage      |
| Registry                                     | system.syslog.template             |
| Value                                        | /var/log/%HOSTNAME%/messages       |
| Parameter                                    | Local port                         |
| Registry                                     | system.syslog.input%.port          |
| Value                                        | <u>514</u>                         |
| Parameter                                    | Transport protocol                 |
| Registry                                     | system.syslog.input%.transport     |
| Value                                        | [TCP] [UDP]                        |
| Parameter                                    | Local Address                      |
| Registry                                     | system.syslog.input%.local_address |



|               |                           |
|---------------|---------------------------|
| ParameterName |                           |
| Registry      | system.syslog.input%.name |

- **Client mode** allows to filter and send commands to multiple remotes.  
[More...](#)

#### IGEL Setup **System -> Remote Syslog**

Parameter Remote port

|          |                            |
|----------|----------------------------|
| Registry | system.syslog.output%.port |
|----------|----------------------------|

|       |            |
|-------|------------|
| Value | <u>514</u> |
|-------|------------|

Parameter Transport protocol

|          |                                 |
|----------|---------------------------------|
| Registry | system.syslog.output%.transport |
|----------|---------------------------------|

|       |             |
|-------|-------------|
| Value | [TCP] [UDP] |
|-------|-------------|

Parameter Remote address

|          |                               |
|----------|-------------------------------|
| Registry | system.syslog.output%.address |
|----------|-------------------------------|

Parameter Syslog facility

|          |                                |
|----------|--------------------------------|
| Registry | system.syslog.output%.facility |
|----------|--------------------------------|

|       |                                                                             |
|-------|-----------------------------------------------------------------------------|
| Range | [Any] [AUTH] [CRON] [DAEMON] [FTP] [KERN] [LPR] [MAIL] [NEWS] [USER] [UUCP] |
|-------|-----------------------------------------------------------------------------|

Parameter Syslog level

|          |                             |
|----------|-----------------------------|
| Registry | system.syslog.output%.level |
|----------|-----------------------------|

|       |                                                                      |
|-------|----------------------------------------------------------------------|
| Range | [Any] [EMERG] [ALERT] [CRIT] [ERR] [WARNING] [NOTICE] [INFO] [DEBUG] |
|-------|----------------------------------------------------------------------|

- **Shutdown or suspend by inactivity.**  
[More...](#)

#### IGEL Setup **System > Power Options > System**



|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | System action on inactivity                      |
| Registry  | system.power_management.system_standby.ac_action |
| Value     | <u>Suspend</u> / Shutdown                        |

- Enhanced **Change Password** utility to be able changing the following items of the logged on user:
  - Password of local user** (screen lock password).
  - PIN of IGEL smartcard**.
  - PIN of PKCS#11 smartcard**.

## CUPS Printing

- Added **PrinterLogic support, Version 18.2.1.128**.
- [More...](#)

|            |                                               |
|------------|-----------------------------------------------|
| IGEL Setup | <b>Devices &gt; Printer &gt; PrinterLogic</b> |
| Parameter  | Manage printers by Printer Installer Client   |
| Registry   | printerlogic.active                           |
| Value      | enabled / <u>disabled</u>                     |
| Parameter  | HomeURL Protocol                              |
| Registry   | printerlogic.homeurl.protocol                 |
| Value      | http:// / <u>https://</u>                     |
| Parameter  | HomeURL Hostname                              |
| Registry   | printerlogic.homeurl.hostname                 |
| Value      | <u>.printercloud.com</u> <sup>459</sup>       |
| Parameter  | Authorization Code                            |
| Registry   | printerlogic.auth.crypt_password              |
| Parameter  | (Mapping in sessions) ICA Sessions            |
| Registry   | printerlogic.map_ica                          |

<sup>459</sup> <http://printercloud.com>



|           |                                                 |
|-----------|-------------------------------------------------|
| Value     | <u>enabled</u> / disabled                       |
| Parameter | (Mapping in sessions) RDP Sessions              |
| Registry  | printerlogic.map_rdp                            |
| Value     | <u>enabled</u> / disabled                       |
| Parameter | (Mapping in sessions) NX Sessions               |
| Registry  | printerlogic.map_nxclient                       |
| Value     | <u>enabled</u> / <u>disabled</u>                |
| Parameter | (Mapping in sessions) Parallels Client Sessions |
| Registry  | printerlogic.map_twox                           |
| Value     | <u>enabled</u> / <u>disabled</u>                |

## Driver

- Added **Kofax virtual channel for signature pads in Citrix sessions.**  
[More...](#)

|            |                                                                                                    |
|------------|----------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Citrix XenDesktop/XenApp &gt; HDX/ICA Global &gt; Mapping &gt; Device Support</b> |
| Parameter  | Kofax SPVC Signature Pad Channel                                                                   |
| Registry   | ica.module.virtualdriver.spvc.enable                                                               |
| Value      | <u>enabled</u> / <u>disabled</u>                                                                   |

- Improved support for **FIBOCOM L830-EB LTE module in Lenovo Thinpad L480.**
- Added configuration to change the **dynamic power management settings for ATI graphics driver.**  
[More...](#)

|           |                              |
|-----------|------------------------------|
| Parameter | ATI dynamic power management |
| Registry  | x.drivers.ati.dpm            |



|       |                                     |
|-------|-------------------------------------|
| Value | <u>default</u> / enabled / disabled |
|-------|-------------------------------------|

- Added the possibility to change the **dynamic power management settings for graphics AMDGPU driver.**

[More...](#)

|           |                                 |
|-----------|---------------------------------|
| Parameter | AMDGPU dynamic power management |
|-----------|---------------------------------|

|          |                      |
|----------|----------------------|
| Registry | x.drivers.amdgpu.dpm |
|----------|----------------------|

|       |                                     |
|-------|-------------------------------------|
| Value | <u>default</u> / enabled / disabled |
|-------|-------------------------------------|

- Added possibility to use **generic modesetting graphics driver** instead of the hardware specific one.

[More...](#)

|           |                                                  |
|-----------|--------------------------------------------------|
| Parameter | Use generic modesetting driver for ATI hardware. |
|-----------|--------------------------------------------------|

|          |                               |
|----------|-------------------------------|
| Registry | x.drivers.ati.use_modesetting |
|----------|-------------------------------|

|       |                           |
|-------|---------------------------|
| Value | enabled / <u>disabled</u> |
|-------|---------------------------|

|           |                                                     |
|-----------|-----------------------------------------------------|
| Parameter | Use generic modesetting driver for AMDGPU hardware. |
|-----------|-----------------------------------------------------|

|          |                                  |
|----------|----------------------------------|
| Registry | x.drivers.amdgpu.use_modesetting |
|----------|----------------------------------|

|       |                           |
|-------|---------------------------|
| Value | enabled / <u>disabled</u> |
|-------|---------------------------|

|           |                                                     |
|-----------|-----------------------------------------------------|
| Parameter | Use generic modesetting driver for NVIDIA hardware. |
|-----------|-----------------------------------------------------|

|          |                                   |
|----------|-----------------------------------|
| Registry | x.drivers.nouveau.use_modesetting |
|----------|-----------------------------------|

|       |                           |
|-------|---------------------------|
| Value | enabled / <u>disabled</u> |
|-------|---------------------------|

## Bluetooth

- Added new **Bluetooth Autopairing Wizard** for IGEL OS installations without keyboard or mouse available, but with unpaired bluetooth keyboard/mouse. The **Autopairing Wizard** is started together with **IGEL Setup Assistant**.

## Appliance Mode

- The wireless manager can now be invoked from the In-Session control bar. Furthermore, it will be automatically started when no network connection can be established.

**Prerequisites:** A WiFi device is available and the following registry keys are set to true.

[More...](#)



|           |                             |
|-----------|-----------------------------|
| Parameter | Activate Wireless Interface |
|-----------|-----------------------------|

|          |                                               |
|----------|-----------------------------------------------|
| Registry | network.interfaces.wirelesslan.device0.active |
|----------|-----------------------------------------------|

|       |                           |
|-------|---------------------------|
| Value | enabled / <u>disabled</u> |
|-------|---------------------------|

|           |                         |
|-----------|-------------------------|
| Parameter | Enable wireless manager |
|-----------|-------------------------|

|          |                                                  |
|----------|--------------------------------------------------|
| Registry | network.applet.wireless.enable_connection_editor |
|----------|--------------------------------------------------|

|       |                           |
|-------|---------------------------|
| Value | enabled / <u>disabled</u> |
|-------|---------------------------|

- It is possible to use **Accessories**, **VPN connections** and **other session types** in **Appliance Mode** now. The access to those session types must be explicitly enabled by a new parameter **Appliance Mode Access**. The possible starting methods:

- XDMCP Appliance mode:** Hotkey
  - All other Appliance modes:** Desktop icon, Desktop Context Menu, Application Launcher (+ System tab), Hotkey, Autostart.
- [More...](#)

|            |                                               |
|------------|-----------------------------------------------|
| IGEL Setup | <b>Accessories &gt; ICA Connection Center</b> |
|------------|-----------------------------------------------|

|           |                         |
|-----------|-------------------------|
| Parameter | Application Mode Access |
|-----------|-------------------------|

|          |                                               |
|----------|-----------------------------------------------|
| Registry | sessions.icaconncenter0.appliance_mode_access |
|----------|-----------------------------------------------|

|       |                           |
|-------|---------------------------|
| Value | enabled / <u>disabled</u> |
|-------|---------------------------|

|            |                                      |
|------------|--------------------------------------|
| IGEL Setup | <b>Accessories &gt; Task Manager</b> |
|------------|--------------------------------------|

|           |                         |
|-----------|-------------------------|
| Parameter | Application Mode Access |
|-----------|-------------------------|

|          |                                             |
|----------|---------------------------------------------|
| Registry | sessions.taskmanager0.appliance_mode_access |
|----------|---------------------------------------------|

|       |                           |
|-------|---------------------------|
| Value | enabled / <u>disabled</u> |
|-------|---------------------------|

|            |                                              |
|------------|----------------------------------------------|
| IGEL Setup | <b>Accessories &gt; Application Launcher</b> |
|------------|----------------------------------------------|

|           |                         |
|-----------|-------------------------|
| Parameter | Application Mode Access |
|-----------|-------------------------|

|          |                                          |
|----------|------------------------------------------|
| Registry | sessions.launcher0.appliance_mode_access |
|----------|------------------------------------------|

|       |                           |
|-------|---------------------------|
| Value | enabled / <u>disabled</u> |
|-------|---------------------------|

|            |                                         |
|------------|-----------------------------------------|
| IGEL Setup | <b>Accessories &gt; Firmware Update</b> |
|------------|-----------------------------------------|



|           |                                                 |
|-----------|-------------------------------------------------|
| Parameter | Application Mode Access                         |
| Registry  | sessions.firmware_update0.appliance_mode_access |
| Value     | enabled / <u>disabled</u>                       |

|            |                                           |
|------------|-------------------------------------------|
| IGEL Setup | <b>Accessories &gt; Quick Settings</b>    |
| Parameter  | Application Mode Access                   |
| Registry   | sessions.usersetup0.appliance_mode_access |
| Value      | enabled / <u>disabled</u>                 |

|            |                                           |
|------------|-------------------------------------------|
| IGEL Setup | <b>Accessories &gt; Sound Preferences</b> |
| Parameter  | Application Mode Access                   |
| Registry   | sessions.mixer0.appliance_mode_access     |
| Value      | enabled / <u>disabled</u>                 |

|            |                                              |
|------------|----------------------------------------------|
| IGEL Setup | <b>Accessories &gt; Disk Removal</b>         |
| Parameter  | Application Mode Access                      |
| Registry   | sessions.storage_dcdm0.appliance_mode_access |
| Value      | enabled / <u>disabled</u>                    |

|            |                                              |
|------------|----------------------------------------------|
| IGEL Setup | <b>Accessories &gt; Disk Utility</b>         |
| Parameter  | Application Mode Access                      |
| Registry   | sessions.storage_info0.appliance_mode_access |
| Value      | enabled / <u>disabled</u>                    |

|            |                                                                                              |
|------------|----------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Accessories &gt; Commands User Interface &gt; Hotkeys &gt; Commands</b>                   |
| Parameter  | Application Mode Access                                                                      |
| Registry   | sessions.commands<NR>.appliance_mode_access<br>sessions.wmcommands<NR>.appliance_mode_access |



|                                                                |                                               |
|----------------------------------------------------------------|-----------------------------------------------|
| Value                                                          | <u>enabled / disabled</u>                     |
| <b>IGEL Setup Accessories &gt; Webcam Information</b>          |                                               |
| Parameter                                                      | Application Mode Access                       |
| Registry                                                       | sessions.webcaminfo0.appliance_mode_access    |
| Value                                                          | <u>enabled / disabled</u>                     |
| <b>IGEL Setup Accessories &gt; Touchscreen Calibration</b>     |                                               |
| Parameter                                                      | Application Mode Access                       |
| Registry                                                       | sessions.touchcalib0.appliance_mode_access    |
| Value                                                          | <u>enabled / disabled</u>                     |
| <b>IGEL Setup User Interface &gt; Screenlock / Screensaver</b> |                                               |
| Parameter                                                      | Application Mode Access                       |
| Registry                                                       | sessions.xlock0.appliance_mode_access         |
| Value                                                          | <u>enabled / disabled</u>                     |
| <b>IGEL Setup Accessories &gt; Monitor Calibration</b>         |                                               |
| Parameter                                                      | Application Mode Access                       |
| Registry                                                       | sessions.xpattern0.appliance_mode_access      |
| Value                                                          | <u>enabled / disabled</u>                     |
| <b>IGEL Setup Accessories &gt; Network Tools</b>               |                                               |
| Parameter                                                      | Application Mode Access                       |
| Registry                                                       | sessions.gnome-nettool0.appliance_mode_access |
| Value                                                          | <u>enabled / disabled</u>                     |
| <b>IGEL Setup Accessories &gt; Screenshot Tool</b>             |                                               |
| Parameter                                                      | Application Mode Access                       |
| Registry                                                       | sessions.screenshooter0.appliance_mode_access |



|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

**IGEL Setup Accessories > System Information**

Parameter Application Mode Access

|          |                                                |
|----------|------------------------------------------------|
| Registry | sessions.device_manager0.appliance_mode_access |
|----------|------------------------------------------------|

|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

**IGEL Setup Accessories > Bluetooth Tool**

Parameter Application Mode Access

|          |                                           |
|----------|-------------------------------------------|
| Registry | sessions.bluetooth0.appliance_mode_access |
|----------|-------------------------------------------|

|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

**IGEL Setup Accessories > Display Switch**

Parameter Application Mode Access

|          |                                             |
|----------|---------------------------------------------|
| Registry | sessions.user_display.appliance_mode_access |
|----------|---------------------------------------------|

|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

**IGEL Setup Accessories > Identify Monitors**

Parameter Application Mode Access

|          |                                          |
|----------|------------------------------------------|
| Registry | sessions.screenid0.appliance_mode_access |
|----------|------------------------------------------|

|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

**IGEL Setup Accessories > System Log Viewer (> Options)**

Parameter Application Mode Access

|          |                                              |
|----------|----------------------------------------------|
| Registry | sessions.systemviewer0.appliance_mode_access |
|----------|----------------------------------------------|

|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

|          |                                                              |
|----------|--------------------------------------------------------------|
| Registry | sessions.setup.displaynames.add_layout.appliance_mode_access |
|----------|--------------------------------------------------------------|

|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|


**IGEL Setup Accessories > Terminals > Local Terminal**

Parameter Application Mode Access

Registry sessions.xterm&lt;NR&gt;.appliance\_mode\_access

 Value enabled / disabled
**IGEL Setup Sessions > SSH > SSH Session**

Parameter Application Mode Access

Registry sessions.ssh&lt;NR&gt;.appliance\_mode\_access

 Value enabled / disabled
**IGEL Setup System > Firmware Customization -> Custom Application -> Custom Application**

Parameter Application Mode Access

Registry sessions.custom\_application&lt;NR&gt;.appliance\_mode\_access

 Value enabled / disabled
**IGEL Setup Accessories > Mobile Device Access**

Parameter Application Mode Access

Registry sessions.mtp-devices0.appliance\_mode\_access

 Value enabled / disabled
**IGEL Setup Network > VPN > OpenConnect VPN (> OpenVPN Connection (> Desktop Integration))**

Parameter Application Mode Access

Registry sessions.openvpn&lt;NR&gt;.appliance\_mode\_access

 Value enabled / disabled
**IGEL Setup Network > VPN > OpenConnect VPN (> VPN OpenConnection (> Desktop Integration))**



|            |                                                                  |
|------------|------------------------------------------------------------------|
| Parameter  | Application Mode Access                                          |
| Registry   | sessions.openconnect<NR>.appliance_mode_access                   |
| Value      | enabled / <u>disabled</u>                                        |
| IGEL Setup | <b>Network &gt; VPN &gt; genucard (&gt; Desktop Integration)</b> |
| Parameter  | Application Mode Access                                          |
| Registry   | sessions.genucard_vpn_connection0.appliance_mode_access          |
| Value      | enabled / <u>disabled</u>                                        |

#### X11 system

- Set of **User Interface > Display > Options > Monitor DPI** now automatically affects the size of the **mouse cursor**, the **panel height**, the **desktop icons**, the **application launcher**, the **size of the start menu** and the **window manager decorations**.

#### VirtualBox

- Added VirtualBox as **feature with limited support**. Activation of the feature at: **System > Firmware Customization > Features > VirtualBox**. Added new registry keys under `virtualbox` and `sessions.virtualbox<NR>`.

#### Audio

- Updated **Pulseaudio to version 12.0-1**.
  - The resample method in Pulseaudio can now be configured by the newly introduced parameter **resample-method**.
- More...**

|           |                                                                                                          |
|-----------|----------------------------------------------------------------------------------------------------------|
| Parameter | Resample method                                                                                          |
| Registry  | multimedia.pulseaudio.daemon.resample-method                                                             |
| Range     | [soxr-vhq] [soxr-hq] [soxr-mq] [speex-float-10] [speex-float-5] [speex-float-3] [ <u>speex-float-1</u> ] |

#### Media Player (Parole/Totem)

- Added new **Parole Media Player 1.0.1-0ubuntu1**. It is used for media player sessions **by default** now. When there occur problems with the new player, switch back to totem/GStreamer 0.10 media player is possible by setting **Fluendo GStreamer Codec Version** parameter to 0.10.
- More...**



|           |                                   |
|-----------|-----------------------------------|
| Parameter | Fluendo GStreamer Codec Version   |
| Registry  | multimedia.gstreamer.version      |
| Range     | [1.x] [0.10] [ <u>automatic</u> ] |

- Added **RTSP/RTMP** support to parole media player / gstreamer 1.x.
- The following parameters are only functional with **Totem media player/GStreamer 0.10** and not for Parole media player.

[More...](#)

|            |                                                                        |
|------------|------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Media Player &gt; Media Player Global &gt; Window</b> |
| Parameter  | Automatically resize the player window when a new video is loaded      |
| Registry   | multimedia.mediaplayer.auto_resize                                     |
| Value      | enabled / <u>disabled</u>                                              |

|            |                                                                        |
|------------|------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Media Player &gt; Media Player Global &gt; Window</b> |
| Parameter  | Main window should stay on top                                         |
| Registry   | multimedia.mediaplayer.window_on_top                                   |
| Value      | enabled / <u>disabled</u>                                              |

|            |                                                                          |
|------------|--------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Media Player &gt; Media Player Global &gt; Playback</b> |
| Parameter  | Visualization size                                                       |
| Registry   | multimedia.mediaplayer.visual_quality                                    |
| Range      | [Small] [Normal] [Large] [Extra Large]                                   |

|            |                                                                                                                                                                 |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Media Player &gt; Media Player Global &gt; Options</b>                                                                                         |
| Parameter  | Network connection speed                                                                                                                                        |
| Registry   | multimedia.mediaplayer.connection_speed                                                                                                                         |
| Range      | [56 kbps Modem/ISDN] [112 kbps Dual ISDN/DSL] [256 kbps DSL/Cable] [384 kbps DSL/Cable] [512 kbps DSL/Cable] [1.5 mbps T1/Intranet/LAN] [ <u>Intranet/LAN</u> ] |



|           |                                    |
|-----------|------------------------------------|
| Parameter | Enable deinterlacing               |
| Registry  | multimedia.mediaplayer.deinterlace |
| Value     | enabled / <u>disabled</u>          |

|           |                              |
|-----------|------------------------------|
| Parameter | Enable debug                 |
| Registry  | multimedia.mediaplayer.debug |
| Value     | enabled / <u>disabled</u>    |

|           |                                                 |
|-----------|-------------------------------------------------|
| Parameter | Network buffering threshold                     |
| Registry  | multimedia.mediaplayer.network_buffer_threshold |
| Value     | <u>2</u>                                        |

- As the **Media Player Browser Plugin** is not supported with **Firefox 60 ESR**, the following parameters are not available anymore.

[More...](#)

#### IGEL Setup **Sessions > Media Player > Media Player Global > Browser Plugin**

Parameter Video output

Registry multimedia.mediaplayer.browser\_plugin.video\_sink

Range [Default] [Auto] [Hardware Accelerated] [X Video Extension] [X Window System]

#### IGEL Setup **Sessions > Media Player > Media Player Global > Browser Plugin**

Parameter Aspect ratio

Registry multimedia.mediaplayer.browser\_plugin.aspect\_ratio

Range [Default] [Auto] [Square] [4:3 (TV)] [16:9 (Widescreen)] [2.11:1 (DVB)]

## Evidian

- Integrated **Evidian AuthMgr version 1.5.6840**.
  - Evidian AuthMgr sessions can be configured at **IGEL Setup > Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions** (registry keys: sessions.rususerauth%).
  - Evidian AuthMgr global settings can be configured at **IGEL Setup > Sessions > Evidian AuthMgr > Evidian AuthMgr Global** (registry keys: evidian).
- Added support for **Custom catalog of messages**.



[More...](#)

|            |                                                                                                              |
|------------|--------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Evidian AuthMgr &gt; Evidian AuthMgr Sessions &gt; Evidian AuthMgr Session &gt; Options</b> |
| Parameter  | Language selection                                                                                           |
| Registry   | sessions.rsuserauth<NR>.parameters.message_catalog                                                           |
| Range      | [Automatic] [English (UK)] [English (US)] [German] [French] [Custom]                                         |
| IGEL Setup | <b>Sessions &gt; Evidian AuthMgr &gt; Evidian AuthMgr Global &gt; Options</b>                                |
| Parameter  | Language selection                                                                                           |
| Registry   | evidian.message_catalog                                                                                      |
| Range      | [Global setting] [English (UK)] [English (US)] [German] [French] [Custom]                                    |
| IGEL Setup | <b>Sessions &gt; Evidian AuthMgr &gt; Evidian AuthMgr Global &gt; Options</b>                                |
| Parameter  | Custom catalog of messages                                                                                   |
| Registry   | evidian.custom_message_catalog                                                                               |
| Value      | <u>/services/evidian/share/locale/en/rsUserAuth.cat</u>                                                      |

- Added support for **Evidian Data Partition**.

[More...](#)

|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Evidian AuthMgr &gt; Evidian AuthMgr Global &gt; Options</b> |
| Parameter  | Evidian AuthMgr Data Partition                                                |
| Registry   | evidian.datapart.enabled                                                      |
| Value      | enabled / <u>disabled</u>                                                     |
| IGEL Setup | <b>Sessions &gt; Evidian AuthMgr &gt; Evidian AuthMgr Global &gt; Options</b> |
| Parameter  | Size                                                                          |
| Registry   | evidian.datapart.size                                                         |
| Value      | <u>10</u>                                                                     |

- Added support for **Password Authentication**.

[More...](#)



|            |                                                                                                              |
|------------|--------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Evidian AuthMgr &gt; Evidian AuthMgr Sessions &gt; Evidian AuthMgr Session &gt; Options</b> |
| Parameter  | Allow password authentication                                                                                |
| Registry   | sessions.rsuserauth<NR>.parameters.password_authentication                                                   |
| Value      | enabled / <u>disabled</u>                                                                                    |
| IGEL Setup | <b>Sessions &gt; Evidian AuthMgr &gt; Evidian AuthMgr Sessions &gt; Evidian AuthMgr Session &gt; Options</b> |
| Parameter  | Allow password forgotten                                                                                     |
| Registry   | sessions.rsuserauth<NR>.parameters.password_forgotten                                                        |
| Value      | enabled / <u>disabled</u>                                                                                    |
| IGEL Setup | <b>Sessions &gt; Evidian AuthMgr &gt; Evidian AuthMgr Sessions &gt; Evidian AuthMgr Session &gt; Options</b> |
| Parameter  | Default domain name for password authentication                                                              |
| Registry   | sessions.rsuserauth<NR>.parameters.password_default_domain                                                   |
| Value      |                                                                                                              |

## Misc

- Added support for **local scanning as feature with limited support**. Activate the feature at: **System > Firmware Customization > Features > Scanner support**. This has been tested with a Canon LiDE 120 scanner.

[More...](#)

|                                                                                           |                              |
|-------------------------------------------------------------------------------------------|------------------------------|
| Parameter                                                                                 | Scanner support              |
| Registry                                                                                  | product.partitions41.enabled |
| Value                                                                                     | enabled / <u>disabled</u>    |
| This must be enabled for the feature to become active and the remaining keys to be valid. |                              |
| Parameter                                                                                 | Enable scanner daemon        |



|                                                                                                                                                                                                                                                                                                                                                                                             |                                              |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| Registry                                                                                                                                                                                                                                                                                                                                                                                    | <code>devices.scanner.daemon</code>          |
| Range                                                                                                                                                                                                                                                                                                                                                                                       | [none] [scanbd] [saned]                      |
| The key determines the daemon to be started. scanbd is necessary for handling buttons on the scanner. It runs saned when necessary (and the scanner is available). saned alone provides scanning functionality to local and remote applications (xsane, scanimage, ..). If none is selected the system can still be used as a client for remote scanner servers (using xsane or scanimage). |                                              |
| Parameter                                                                                                                                                                                                                                                                                                                                                                                   | Allowed remote clients                       |
| Registry                                                                                                                                                                                                                                                                                                                                                                                    | <code>devices.scanner.allowed_clients</code> |
| The key may contain a space-separated list of hosts and networks (CIDR > notation) that are allowed to connect to a local server.                                                                                                                                                                                                                                                           |                                              |
| Parameter                                                                                                                                                                                                                                                                                                                                                                                   | Remote scanners                              |
| Registry                                                                                                                                                                                                                                                                                                                                                                                    | <code>devices.scannerclient.remote</code>    |
| This may contain a space-separated list of remote scanner servers to be used by local applications (xsane, scanimage). It is only relevant if no local server is configured.                                                                                                                                                                                                                |                                              |

- **The remaining keys influence scanner button handling.** For each button there is an instance of the `devices.scanner.scanbd.action%` template.
- In order to keep scanner button handling flexible **the default handling may be replaced by custom scripts.** Details of the default handling are listed at the end of this section.

[More...](#)

|                                                                                                                                                                                                                                                                                           |                                                                        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| Parameter                                                                                                                                                                                                                                                                                 | Scanner button name                                                    |
| Registry                                                                                                                                                                                                                                                                                  | <code>devices.scanner.scanbd.action%.button</code>                     |
| This contains the (symbolic) name of the button. There are currently four predefined instances of the template where the value is 'file', 'scan', 'copy', and 'email' respectively. (These refer to the buttons on a Canon LiDE 120 from left to right where 'file' may be labeled 'PDF') |                                                                        |
| Parameter                                                                                                                                                                                                                                                                                 | Allow while nobody is logged in                                        |
| Registry                                                                                                                                                                                                                                                                                  | <code>devices.scanner.scanbd.action%.allow_lockpanel_logged_out</code> |
| Value                                                                                                                                                                                                                                                                                     | <u>enabled</u> / <u>disabled</u>                                       |
| If this is set to false, the button is ignored when nobody is logged in (only > relevant when local logon is configured)                                                                                                                                                                  |                                                                        |



|           |                                                          |
|-----------|----------------------------------------------------------|
| Parameter | Allow while screen is locked                             |
| Registry  | devices.scanner.scanbd.action%.allow_lockpanel_logged_in |
| Value     | <u>enabled</u> / <u>disabled</u>                         |

When this is set to false, the button is ignored while the screen is locked.

|                                                                                                                                                                                                                                                                                         |                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| Parameter                                                                                                                                                                                                                                                                               | scanbd custom action                          |
| Registry                                                                                                                                                                                                                                                                                | devices.scanner.scanbd.action%.custom_cm<br>d |
| This may contain a custom button handling command. The value is empty by default. If it is not, the value will be passed to "bash -c .." and the default button handling will not be effective. The consequence is that entering some space characters results in disabling the button. |                                               |

|           |                                          |
|-----------|------------------------------------------|
| Parameter | Directory                                |
| Registry  | devices.scanner.scanbd.action%.directory |
| Value     | <u>/tmp</u>                              |

Set the target directory for scan results.

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Format                                |
| Registry  | devices.scanner.scanbd.action%.format |
| Range     | [pnm] [tiff] [png] [jpeg]             |

Determines the image format (passed as argument to scanimage).

|           |                                     |
|-----------|-------------------------------------|
| Parameter | Color mode                          |
| Registry  | devices.scanner.scanbd.action%.mode |
| Value     | [Color] [Gray] [Lineart]            |

Determines the color mode (passed as argument to scanimage).

|           |                                                   |
|-----------|---------------------------------------------------|
| Parameter | Resolution in dpi                                 |
| Registry  | devices.scanner.scanbd.action%.resolution         |
| Range     | [75] [100] [150] [300] [600] [1200] [2400] [4800] |

Determines the resolution (passed as argument to scanimage).

|           |            |
|-----------|------------|
| Parameter | Brightness |
|-----------|------------|



|          |                                           |
|----------|-------------------------------------------|
| Registry | devices.scanner.scanbd.action%.brightness |
| Value    | 0                                         |

Determines the brightness (passed as argument to scanimage).

- **Default button handling script:** There is a default button handling script /etc/scanbd/scripts/action. It might be used as a potential starting point for custom button handling. The script handles the four buttons of a **Canon LiDE 120** in the following ways:

- **file** results in a PDF document that contains a series of pages where each page contains a scan result acquired with scanimage according to the settings. This needs user interaction on the local machine's desktop.
- **scan** results in an image file that is silently created and stored according to the settings.
- **copy** makes the script use scanimage according to the settings, convert the resulting image to PDF and send it to the default printer. This obviously requires that a printer is configured.
- **email** just results in xsane being started. The following settings are not respected in this case:
  - devices.scanner.scanbd.action%.directory
  - devices.scanner.scanbd.action%.format
  - devices.scanner.scanbd.action%.mode
  - devices.scanner.scanbd.action%.resolution
  - devices.scanner.scanbd.action%.brightness

## Hardware

- Added official support for **HP T630**.
- Added official support for **Intel NUC 6CAYH and 5i5MYHE**.
- Added official support for **Dell/Wyse 3040**.
- Added official support for **Toshiba Tecra C50-B1503**.
- Added official support for **Toshiba R50**.
- Added official support for **Dell/Wyse AIO 5212**.
- Added official support for **LG 24CK550W AiO Thin Client**.

## TC Setup (Java)

- Updated **TC Setup to version 5.9.11**.
- Added an **additional local administrator access** to IGEL setup. The local administrator password is configurable at **Security > Password** setup page. The page permissions are configurable at **Accessories > Setup > Setup Administrator Permissions** setup page.
- Reworked **Accessories > Commands** and **User Interface > Hotkeys > Commands** setup pages.
- Reworked **Storage Hotplug** setup page.

## Remote Management

- Added support for **UMS File Transfer Status**.
- Added a new configuration to **prevent a user from canceling UMS actions like firmware update, reboot, shutdown, etc.** through the UMS notification dialog.  
**More...**

|           |                                  |
|-----------|----------------------------------|
| Parameter | Allow user to cancel UMS actions |
|-----------|----------------------------------|



|          |                                                       |
|----------|-------------------------------------------------------|
| Registry | <code>userinterface.rmagent.cancel_usermessage</code> |
| Value    | <u>enabled</u> / disabled                             |

## Fabulatech

- **FabulaTech USB for Remote Desktop** updated to **versions 5.2.29; FabulaTech FTPPlugin** updated to **version 3.4.0**.
- Support for some specific devices has been improved.

## Resolved Issues 10.05.100

## Citrix Receiver 13

- Fixed: Now **applications may be displayed in application launcher** independently from startmenu.
- Fixed **Citrix Azure Cloud** login window.
- Added a **new window manager tweak** to automatically unmap unwanted Citrix fragment windows when seamless apps are used.

**More...**

|           |                                                                             |
|-----------|-----------------------------------------------------------------------------|
| Parameter | Auto-close unwanted Wfica windows                                           |
| Registry  | <code>windowmanager.tweaks.suppress_wfica_window_in_seamless_session</code> |
| Value     | <u>enabled</u> / disabled                                                   |

- Fixed **native USB redirection with Citrix receiver 13.10**.
- Fixed **black rectangle around 32-bit mouse icons**.
- Fixed **sound playback over Nuance channel**.
- Fixed stopping of the **Pulseaudio PCM I/O plugin** which is used by Citrix Receiver for sound output and recording.
- When using the **Citrix login method the system language is used now**.
- Fixed a problem with the parameter `ica.pnlogin.suppressconnectiondialog`, **connection messages are suppressed** as desired.

## RDP/IGEL RDP Client 2

- Fixed **locking in smartcard transactions**.
- Fixed **audio recording in RDP sessions**.
- Fixed **\$HOSTNAME** to work for RDP login when variable substitution is enabled.

**More...**

|            |                                                                      |
|------------|----------------------------------------------------------------------|
| IGEL Setup | <b>System &gt; Firmware Customization &gt; Environment Variables</b> |
| Parameter  | Enable variable substitution in session                              |



|                      |                                                                             |
|----------------------|-----------------------------------------------------------------------------|
| Registry             | system.environment_variables.enable_application_variables                   |
| Value                | <u>enabled</u> / disabled                                                   |
| IGEL Setup Parameter | <b>Sessions &gt; RDP &gt; RDP Global &gt; Local Logon</b>                   |
| Registry             | rdp.login.saveusertype                                                      |
| Value                | Set user/domain from session setup / <u>Set user/domain from last login</u> |

- Added **Arabic (101) keyboard layout** to RDP client.
- Added **MultiPointServer 2016** to supported servers for **RDP MultiPoint Server** appliance.

#### RD Web Access

- Fixed **wrong RDP Remote Application icon** when opening a application twice.
- Fixed unexpected behavior when maximizing/minimizing **RDP Remote Applications**.

#### UD Pocket

- Fixes for **UD Pocket demo license registration** dialog:
  - Fixed **german translation**.
  - The **toolbar context menu** is not available anymore (it could hide the toolbar without a way to restore it).
  - The javascript confirm **popup from igel.com is hidden now**.

#### VMware Horizon

- Added possibility to **make certificate verification mandatory**.  
**More...**

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Allow change of certificate verification mode |
| Registry  | vmware.view.ssl-verify-mode-change-allow      |
| Value     | <u>enabled</u> / disabled                     |

- Fixed **H.264 hardware decoding** for Horizon.

#### PowerTerm

- Fixed **printing to CUPS printers in PowerTerm**.
- Added **TLS-1.2 in list of SSL Versions for PowerTerm** on page **Sessions > PowerTerm Terminal Emulation > PowerTerm Sessions > session name > Connection**.

#### Parallels Client



- Fixed: **Authentication fails with Gemalto smartcards.**
- Fixed: Sometimes **remote session windows remain on screen after one was logged off from the remote session.**
- Fixed: **Remote session closes unexpectedly.**
- Fixed: Combination of **CTRL-C** doesn't work in remote session.
- Improved: **Use of multiple monitors.**
- Fixed: **Client might hang while watching YouTube videos.**
- Fixed: **Multiple USB drives might not be auto-mapped to a remote session.**
- Fixed: **Logoff from a remote session blocks Linux desktop with a black screen.**

#### Firefox

- Fixed **occasional loss of trusted certificates** in Firefox. Certificates transmitted via UMS filetransfer were not reinstalled when Firefox profile was rebuilt.
- Fixed **PDF Plugin** in Firefox browser.
- Removed the browser plugin option from **RHEV/Spice** as it is no longer supported.
- Removed the browser plugin option from **SecMaker** as it is no longer supported.

#### Network

- Fixed **failing Wake-on-LAN configuration after update on shutdown.** Particularly UD2-LX40 devices were affected.
- Fixed bug in the **GetCA operation for SCEP**: An intermediate certificate in addition to the root certificate and any RA certificates resulted in confusion.
- **sscep version is now 0.6.1**
- **CA certificate fingerprint is now mandatory for SCEP.** So far it could be left empty for debugging purposes.
- Added **parameter to specify whether a slash (/) is appended to SCEP URL.** The slash is needed e.g. with Microsoft servers, but not with Nexus servers.

**More...**

|           |                                             |
|-----------|---------------------------------------------|
| Parameter | Append slash (/) to SCEP server URL         |
| Registry  | network.scepclient.cert0.scepurlappendslash |
| Value     | <u>enabled</u> / disabled                   |

- Fixed **generating certificate request** if challenge password or other fields include **special characters like \$, #, quotes or spaces** in SCEP.
- Reaction to **Ethernet 802.1X reauthentication failure** is now configurable.

**More...**

|           |                                                                         |
|-----------|-------------------------------------------------------------------------|
| Parameter | Restart on reauthentication failure                                     |
| Registry  | network.interfaces.ethernet.device%.ieee8021x.restart_on_reauth_failure |
| Value     | <u>enabled</u> / disabled                                               |



The default value preserves the traditional behaviour. If the registry key is set to enabled the network connection will get restarted when a reauthentication failure occurs. This way the system might switch to a guest VLAN where authentication is not required.

- Added **support for SFTP protocol** (enabled as default) configurable with new registry key.  
[More...](#)

|           |                                       |
|-----------|---------------------------------------|
| Parameter | Enable SFTP server                    |
| Registry  | network.ssh_server.enable_sftp_server |
| Value     | <u>enabled</u> / disabled             |

- Improved **general security** in regards of SCEP

#### WiFi

- Fixed non working **Mediatek MT7630e WiFi driver**.
- Added several **WiFi drivers** (Realtek 8188eu, 8822be, 8150, 8187, 8192ce, 8192de, 8192ee, 8723ae, 8821ae....) to the firmware.
- Re-enforce configuration after **IGEL Setup Assistant** exits to ensure consistent state between configuration and system.
- Added drivers for **Realtek rtl8723de** and **rtl8822be WiFi devices**.
- Added support for **StarTech USB300WN2X2C Wireless-N WiFi adapter**.

#### Smartcard

- Updated **OpenSC library to version 0.19.0**. Improved handling of PIV and CAC ALT token and other improvements.
- Fixed problem with **ActivClient smartcards in VMware Horizon sessions**. Before this fix, smartcard access inside the session was blocked.

[More...](#)

|           |                                             |
|-----------|---------------------------------------------|
| Parameter | Smartcard SCardConnect in non-blocking mode |
| Registry  | vmware.view.pcsc-connect-nonblocking        |
| Value     | <u>enabled</u> / disabled                   |

- Improved **PC/SC lite daemon** to handle attributes SCARD\_ATTR\_DEVICE\_FRIENDLY\_NAME\_W and SCARD\_ATTR\_DEVICE\_SYSTEM\_NAME\_W.
- Updated **Cherry USB2LAN Proxy to version 3.0.0.6**.
  - Fixed an issue where the **SICCT listener was not restarted** when a SICCT connection has been closed by the EGK device (ORS-880).
  - Fixed **TLS errors** resulting from re-using channels before the EGK device confirmed the disconnection of the previous connection (ORS-735).



- **Increase connection handshake timeout from 1 second to 20 seconds.** This is necessary as the EGK device (G87-1505, firmware 2.108.3) does not process the handshake immediately in all situations. (ORS-735).
- Added **timestamp** to log output.
- Fixed **AD/Kerberos log on with smartcard** and **Smartcard Removal Action: Lock Thin Client**.
- Fixed custom **PKCS#11 module for VMware Horizon logon**. Before this fix, the parameters did not get effective.

[More...](#)

|           |                                          |
|-----------|------------------------------------------|
| Parameter | Horizon logon with custom PKCS#11 module |
| Registry  | vmware.view.pkcs11.use_custom            |
| Value     | enabled / <u>disabled</u>                |
| Parameter | Path to the library                      |
| Registry  | vmware.view.pkcs11.custom_path           |
| Value     |                                          |

- Fixed **error in IGEL Smartcard which prevented login with personalized cards** when certain card holder names contained **non-ASCII characters**.

#### HID

- Added support for **Wacom HID 483C touchscreens** (HP Pro x2 612 g2).
- Fixed non working **Lenovo KBRFBU71 wireless keyboard**.
- Fixed **mouse button mapping**.

#### CUPS Printing

- Fixed **HPLIP related printer drivers**.
- Added missing **LaserJet 200 color MFP M276 Postscript to Printer Names** for manufacturer HP in the TC Setup under **Devices > Printer > CUPS > Printers**.

#### Application Launcher

- Fixed **display order** of DNS servers in **Application Launcher** and **About** dialog.

#### Base system

- **IGEL Setup Assistant** fixes:
  - Fixed **startup on first boot**.
  - **Retain network configuration** if exited via cancel.
  - Fixed **graphical glitches**
  - Fixed **WiFi configuration**
  - **Prevent startup if an administrator passphrase is set** (e.g. from a IGEL System 5 migration).
- Fixed **System suspend on inactivity** showing the suspend dialog directly after system resume.



- Fixed the **custom bootsplash scaling when multiple monitors are configured**. Necessary to force a re-installation of the custom bootsplash for this fix to take effect. To force a re-installation:
  - Trigger the **Update desktop customization** command via UMS or
  - Press the **Bootsplash update** button at **IGEL Setup > System > Firmware Customization > Corporate Design > Custom Bootsplash**.
- Fixed sporadic problems with **custom bootsplash and wallpaper installation**.
- Fixed the **buddy update server** so that UD Pocket devices can also update from buddy update servers.
- Fixed handling of **custom environment variables**. If values contained white spaces the variables could not be set.
- Fixed **reboot/shutdown** when triggered from the lock screen panel.
- Removed **maximize button from on-screen keyboard window**.
- Fixed **deletion of debuglog partition content** when booted in emergency boot.
- Fixed **handling of optional partitions which are not active as default** while booting in emergency mode.
- Fixed instability in **authentication module pam\_igelsession.so** in some special cases.
- Fixed **ECDSA/ECDH support in HEIMDAL libraries**.
- Fixed **black screen issues** if hostname contains other characters as 'A-Z a-z 0-9 . \_ - '.
- Improved **debuglog partition based login**.
- **Restricted access to command \*\*su\*\* to root and user**.
- **Root home** is now **/root**.
- Removed **system** group (GID 0) which shadowed **root** group (GID 0).
- **Stricter folder and file permissions**.
- Prevent **flickering problems on 4k 60Hz screens**.

#### Storage Devices

- Fixed **mount issue of PTP devices** (Mobile Device Access USB feature must be enabled).
- Fixed **double detection of MTP and PTP**. MTP is preferred over PTP now (Mobile Device Access USB feature must be enabled).

#### Appliance Mode

- Fixed **configuration of post session commands via UMS profile**: There is no second reboot required anymore to apply the settings properly in Appliance Mode.

#### X11 system

- Fixed graphic card support for **HP EliteBook 745 G5** (disabled AMDGPU framebuffer compression as default).
  - Fixed **non loading DRM/KMS driver on Spectra Nise 106**.
  - Added possibility to **change the framebuffer compression for AMDGPU driver**.
- More...**

|           |                                 |
|-----------|---------------------------------|
| Parameter | AMDGPU framebuffer compression. |
| Registry  | x.drivers.amdgpu.use_fbc        |
| Range     | [default][enable][disable]      |



- Fixed **DP MST handling** (fixes Dell XPS Notebook Dock Station monitor issues).
  - Fixed sessions.user\_display0.options.lid\_events work for **eDP** also.
  - Fixed **VESA** only boot with **UEFI system**.
  - **AMDGPU stability** fixes applied.
  - Fixed issue with **screen configuration for certain cases**.
  - Fixed **screen configuration** getting in **endless loop** with multi monitor setups.
  - Fixed **memleak in igel\_drm\_daemon**.
  - Fixed **DRI2 memleak with AMDGPU driver**.
  - Changed x.xserver0.force\_reconfig registry key (former bool now range).
- More...**

|           |                                                      |
|-----------|------------------------------------------------------|
| Parameter | Force a display reconfiguration                      |
| Registry  | x.xserver0.force_reconfig                            |
| Range     | [default][only on Xorg start/restart][always][never] |

- Usage of **only on Xorg start/restart** as new default for **AMDGPU based devices**.
  - Removed x.xserver0.composite registry key to prevent problems with **AMD/ATI devices**.
  - Fixed **screen remains black when Monitor Probing (DDC)** option is "Off", configurable at setup page **User Interface > Display > Options**.
  - Fixed wrong detected **DisplayPort (eDP instead of DP) for Dell Wyse 5070**.
  - Added possibility to configure **graphic displays only if DPMS state is not OFF**.
- More...**

|           |                                                      |
|-----------|------------------------------------------------------|
| Parameter | Do not reconfigure if monitors are in DPMS off state |
| Registry  | x.xserver0.config_on_dpms_on                         |
| Value     | <u>enabled</u> / disabled                            |

## Window Manager

- **On-Screen Keyboard will keep aspect ratio** when resized via double click on edge.

## Shadowing/VNC

- Fixed instability of **Secure Shadowing** connector.

## Audio

- Added a workaround for **button handling of Sennheiser USB headsets**.
- Fixed saving and restoring of **volume controls in Pulseaudio and ALSA**.
- Fixed **volume control** of the internal speaker in **Wyse ZX0D**.
- Improved consistency while **storing of changed volume values**.
- Fixed configuration of the **default sound output or input on hardware** when presence detection in jack connector is missing.

## Hardware



- Fixed shutdown problems for **Dell Wyse Thin Client AIO 5212** (use legacy boot instead of EFI).
- Fixed support for **four screens with Nvidia Quadro graphic cards** (all current cards which are able to drive four outputs).
- Fixed graphic issues for **HP ProBook 455 G5**.
- Fixed non working **StarTech.com USB2DVIPRO2 DisplayLink** graphics adapter.
- Fixed freezes of Intel **Baytrail devices**.
- Fixed **VDPAU** hardware accelerated video support for **NVIDIA graphics cards**.
- Fixed non working **DisplayLink USB graphics adapter** after reboot.

#### Remote Management

- Fixed **zero touch deployment** by adding a timeout to the Setup Assistant abort message.
- Fixed **computation of Unit ID**. The Unit ID is the identification key of the thin client in UMS, and also thin client licenses will be bound to the Unid ID. Now the Unit ID is computed once and persistently saved. It consists of the serial number of UD Pocket or the MAC address of a network interface. When multiple network interfaces are present, the interface is selected taking following attributes into account:  
If a license bound to the interface exists, how it is connected (PCI, SDIO, USB or other) and if it is wireless or wired.  
It is best practice not to connect external network interfaces when a freshly installed thin client device is booted for the first time, so that the Unit ID will consist of a MAC address of a network interface which cannot be removed from the thin client device.
- Fixed **monitor serial numbers** not shown in UMS.
- Fixed **Bluetooth Asset Inventory** zombie when bluetooth dongle is removed.
- Fixed **UMS filetransfer** - now filetransfer action is triggered also if only the file classification was changed.
- Fixed **Update on shutdown** UMS job which could be stucked if update is failed once for some reasons.

### 7.29.3 IGEL Universal Desktop Converter (UDC3)

#### Supported Hardware:

<https://kb.igel.com/igelos/en/devices-supported-by-udc3-and-ud-pocket-3117174.html>

- Versions 10.05.100(see page 2258)
- New Features 10.05.100(see page 2260)

#### Versions 10.05.100

- **Clients**

| Product    | Version   |
|------------|-----------|
| Oracle JRE | 1.8.0_181 |



- **System Components**

|                                         |                               |
|-----------------------------------------|-------------------------------|
| OpenSSL                                 | 1.0.2g-1ubuntu4.13            |
| Bluetooth stack (bluez)                 | 5.50-0ubuntu1igel5            |
| MESA OpenGL stack                       | 18.2.1-1igel51                |
| Graphics Driver INTEL                   | 2.99.917+git20180214-igel1830 |
| Graphics Driver ATI/RADEON              | 18.0.1-1igel831               |
| Graphics Driver ATI/AMDGPU              | 18.0.1-1igel831               |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.15-2igel775               |
| Graphics Driver Vboxvideo               | 5.2.18-dfsg-2igel17           |
| Graphics Driver VMware                  | 13.3.0-2igel812               |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1igel775          |
| Graphics Driver FBDEV                   | 0.5.0-1igel819                |
| Graphics Driver VESA                    | 2.3.4-1build2igel639          |
| Input Driver Evdev                      | 2.10.5-1ubuntu1igel750        |
| Input Driver Elographics                | 1.4.1-1build5igel633          |
| Input Driver eGalax                     | 2.5.5814                      |
| Input Driver Synaptics                  | 1.9.0-1ubuntu1igel748         |
| Input Driver Vmmouse                    | 13.1.0-1ubuntu2igel635        |
| Input Driver Wacom                      | 0.36.1-0ubuntu1igel813        |
| Kernel                                  | 4.18.11 #mainline-udos-r2463  |
| Xorg X11 Server                         | 1.19.6-1ubuntu4igel838        |
| Lightdm graphical login manager         | 1.18.3-0ubuntu1.1             |
| XFCE4 Windowmanager                     | 4.12.3-1ubuntu2igel653        |
| ISC DHCP Client                         | 4.3.3-5ubuntu12.10igel6       |



## New Features 10.05.100

### Hardware

- Added official support for **HP T630**.
- Added official support for **Intel NUC 6CAYH and 5i5MYHE**.
- Added official support for **Dell/Wyse 3040**.
- Added official support for **Toshiba Tecra C50-B1503**.
- Added official support for **Toshiba R50**.
- Added official support for **Dell/Wyse AIO 5212**.
- Added official support for **LG 24CK550W AiO Thin Client**.

## 7.30 Notes for Release 10.04.100

|                |            |             |
|----------------|------------|-------------|
| Software:      | Version    | 10.04.100   |
| Release Date:  | 2018-04-12 |             |
| Release Notes: | Version    | RN-104100-1 |
| Last update:   | 2018-04-12 |             |

The following formatting is used in this document:

| format type         | example                  | use                                                                                      |
|---------------------|--------------------------|------------------------------------------------------------------------------------------|
| bold and underlined | <u>enable/disable</u>    | the default setting of a value                                                           |
| bold and arrow      | <b>menu &gt; path</b>    | menu path in the IGEL setup                                                              |
| bold                | <b>GUI</b><br>[keyboard] | elements of the graphical user interface or commands that are entered using the keyboard |

- [IGEL Linux Universal Desktop 10.04.100](#)(see page 2261)
- [IGEL Universal Desktop OS3/IGEL UD Pocket 10.04.100](#)(see page 2286)
- [IGEL Universal Desktop Converter \(UDC3\) 10.04.100](#)(see page 2310)



## 7.30.1 IGEL Linux Universal Desktop 10.04.100

### Supported Devices

|                    |                                                  |
|--------------------|--------------------------------------------------|
| Universal Desktop: |                                                  |
| UD2-LX:            | UD2-LX 40                                        |
| UD3-LX:            | UD3-LX 51<br>UD3-LX 50<br>UD3-LX 42<br>UD3-LX 41 |
| UD5-LX:            | UD5-LX 50<br>UD5-LX 40                           |
| UD6-LX:            | UD6-LX 51                                        |
| UD7-LX:            | UD7-LX 10                                        |
| UD9-LX:            | UD9-LX Touch 41<br>UD9-LX 40                     |
| UD10-LX:           | UD10-LX Touch 10<br>UD10-LX 10                   |
| IGEL Zero:         |                                                  |
| IZ2-RFX            |                                                  |
| IZ2-HDX            |                                                  |
| IZ2-HORIZON        |                                                  |
| IZ3-RFX            |                                                  |



IZ3-HDX

IZ3-HORIZON

- [Versions for Release 10.04.100\(see page 2262\)](#)
- [General Information 10.04.100\(see page 2266\)](#)
- [Security Fixes 10.04.100\(see page 2267\)](#)
- [Known Issues 10.04.100\(see page 2270\)](#)
- [New Features 10.04.100\(see page 2271\)](#)
- [Resolved Issues 10.04.100\(see page 2283\)](#)

## Versions for Release 10.04.100

### • Clients

| Product                           | Version                         |
|-----------------------------------|---------------------------------|
| Citrix HDX Realtime Media Engine  | 2.4.0-1233                      |
| Citrix Receiver                   | 13.3.2.366713                   |
| Citrix Receiver                   | 13.4.2.10146724                 |
| Citrix Receiver                   | 13.7.0.10276927                 |
| Citrix Receiver                   | 13.8.0.10299729                 |
| deviceTRUST Citrix Channel        | 17.2.100.0                      |
| deviceTRUST RDP Channel           | 17.2.100.0                      |
| Ericom PowerTerm                  | 12.0.1.0.20170219.2-_dev_-34574 |
| Evidian AuthMgr                   | 1.5.6362                        |
| Evince PDF Viewer                 | 3.18.2-1ubuntu4.3               |
| FabulaTech USB for Remote Desktop | 5.2.23                          |
| Firefox                           | 52.7.2                          |
| IBM iAccess Client Solutions      | 1.1.5.0                         |



|                                                       |                   |
|-------------------------------------------------------|-------------------|
| IGEL RDP Client                                       | 2.2               |
| Imprivata OneSign ProvID Embedded                     |                   |
| Leostream Java Connect                                | 3.3.7.0           |
| NX Client                                             | 5.3.12            |
| Open VPN                                              | 2.3.10-1ubuntu2.1 |
| Oracle JRE                                            | 1.8.0_162         |
| Parallels Client (64 bit)                             | 16.2.0.19039      |
| Remote Viewer (RedHat Virtualization)                 | 7.0               |
| Systancia AppliDis                                    | 4.0.0.17          |
| Thinlinc Client                                       | 4.8.0-5456        |
| ThinPrint Client                                      | 7.5.83            |
| Totem Media Player                                    | 2.30.2            |
| VMware Horizon Client                                 | 4.7.0-7395152     |
| Voip Client Ekiga                                     | 4.0.1             |
| <b>• Dictation</b>                                    |                   |
| Diktamen driver for dictation                         |                   |
| Driver for Grundig Business Systems dictation devices |                   |
| Nuance Audio Extensions for dictation                 | B048              |
| Olympus driver for dictation                          | 20161103          |
| Philips Speech Driver                                 | 12.5.4            |
| <b>• Signature</b>                                    |                   |
| signotec Citrix Channel                               | 8.0.6             |



|                      |       |
|----------------------|-------|
| signotec VCOM Daemon | 2.0.0 |
| StepOver TCP Client  | 2.1.0 |

- **Smartcard**

|                                           |                  |
|-------------------------------------------|------------------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101          |
| PKCS#11 Library Athena IDProtect          | 623.07           |
| PKCS#11 Library cryptovision sc/interface | 7.0.5.592        |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0        |
| PKCS#11 Library SecMaker NetID            | 6.6.0.30         |
| Reader Driver ACS CCID                    | 1.1.5            |
| Reader Driver Gemalto eToken              | 10.0.37-0        |
| Reader Driver HID Global Omnikey          | 4.2.4            |
| Reader Driver Identive CCID               | 5.0.35           |
| Reader Driver Identive eHealth200         | 1.0.5            |
| Reader Driver Identive SCRKBC             | 5.0.24           |
| Reader Driver MUSCLE CCID                 | 1.4.28           |
| Reader Driver REINER SCT cyberJack        | 3.99.5final.SP11 |
| Resource Manager PC/SC Lite               | 1.8.22           |
| Cherry USB2LAN Proxy                      | 3.0.0.4          |

- **System Components**

|                         |               |
|-------------------------|---------------|
| Bluetooth stack (bluez) | 5.46-0ubuntu3 |
| MESA OpenGL stack       | 17.2.8-0igel3 |
| VAAPI ABI Version       | 0.40          |



|                                         |                            |
|-----------------------------------------|----------------------------|
| VDPAU Library version                   | 1.1.1-3ubuntu1             |
| Graphics Driver INTEL                   | 2.99.917+git20180214-igel1 |
| Graphics Driver ATI/RADEON              | 7.10.0-2igel3              |
| Graphics Driver ATI/AMDGPU              | 1.4.0-2igel3               |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.15-2                   |
| Graphics Driver Nvidia                  | 384.111-0ubuntu0.16.04.1   |
| Graphics Driver Vboxvideo               | 5.2.6-dfsg-2               |
| Graphics Driver VMware                  | 13.2.1-1build1             |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1              |
| Graphics Driver FBDEV                   | 0.4.4-1build5              |
| Graphics Driver VESA                    | 2.3.4-1build2              |
| Input Driver Evdev                      | 2.10.5-1ubuntu1            |
| Input Driver Elographics                | 1.4.1-1build5              |
| Input Driver eGalax                     | 2.5.5814                   |
| Input Driver Synaptics                  | 1.9.0-1ubuntu1             |
| Input Driver Vmmouse                    | 13.1.0-1ubuntu2            |
| Input Driver Wacom                      | 0.34.0-0ubuntu2            |
| Kernel                                  | 4.15.15 #mainline-ud-r2141 |
| Xorg X11 Server                         | 1.19.6-2igel1              |
| CUPS printing daemon                    | 2.1.3-4ubuntu0.4           |
| Lightdm graphical login manager         | 1.18.3-0ubuntu1.1          |



|                     |                        |
|---------------------|------------------------|
| XFCE4 Windowmanager | 4.12.3-1ubuntu2        |
| ISC DHCP Client     | 4.3.3-5ubuntu12.7      |
| NetworkManager      | 1.2.2-0ubuntu0.16.04.4 |
| ModemManager        | 1.6.4-1                |
| GStreamer 0.10      | 0.10.36-2ubuntu0.1     |

- **Features with Limited IGEL Support**

|                          |  |
|--------------------------|--|
| Mobile Device Access USB |  |
| VPN OpenConnect          |  |

## General Information 10.04.100

The following clients and features are not supported anymore in version 10.04.100:

- Citrix Receiver 12.1 and 13.1
- Citrix Access Gateway Standard Plug-in
- Dell vWorkspace Connector for Linux
- Ericom PowerTerm Emulation 9 and 11
- Ericom Webconnect
- IGEL Legacy RDP Client (rdesktop)
- Virtual Bridges VERDE Client
- PPTP VPN Support
- IGEL Upgrade License Tool with IGEL Smartcard Token
- Remote Management by setup.ini file transfer (TFTP)
- Remote Access via RSH
- Legacy Philips Speech Driver
- Digital Persona Support
- Sane Scanner Support
- Softpro/Kofax Citrix Virtual Channel
- t-Systems TCOS Smartcard Support
- DUS Series touch screens
- Elo serial touch screens
- IGEL Smartcard without locking desktop
- Video Hardware Acceleration Support is discontinued on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, D10-LX 10
- H.264 Hardware Acceleration Support is discontinued on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, UD10-LX 10
- Storage Hotplug devices are not automatically removed anymore, instead they must always be ejected manually:



- by panel tray icon
- by an icon in the 'In-Session Control Bar' (configurable at **IGEL Setup > User Interface > Desktop**)
- by a 'Safely Remove Hardware' session (configurable at **IGEL Setup > Accessories**)

The following clients and features are not available in release 10.04.100:

- X session (Xorg Xephyr)
- Cherry eGK Channel
- Open VPN Smartcard Support
- NCP Secure Client
- Asian Input Methods
- Composite Manager
- Softpro/Kofax Citrix Virtual Channel

## Security Fixes 10.04.100

### Firefox

- Fixes for **mfsa2018-08**, also known as CVE-2018-5146, CVE-2018-5147.
- Fixes for **mfsa2018-07**, also known as CVE-2018-5127, CVE-2018-5129, CVE-2018-5130, CVE-2018-5131, CVE-2018-5144, CVE-2018-5125, CVE-2018-5145.

### Base System

- Added support for UEFI Secure Boot.

When booted with Secure Boot the downgrade to a firmware version older than 10.04.100 is locked.

- When booted with Secure Boot the downgrade to a firmware version older than 10.04.100 is locked.
- Fixed evince security issue CVE-2017-1000159.
- Fixed bind9 security issue CVE-2017-3145.
- Fixed glibc security issues CVE-2018-1000001, CVE-2017-16997, CVE-2017-15804, CVE-2017-15670, CVE-2017-1000409 and CVE-2017-1000408.
- Fixed gdk-pixbuf security issues CVE-2017-6314, CVE-2017-6313, CVE-2017-6312 and CVE-2017-1000422.
- Fixed webkit2gtk security issues CVE-2017-7156, CVE-2017-5753, CVE-2017-5715, CVE-2017-13870, CVE-2017-13866, CVE-2017-13856, CVE-2018-4096, CVE-2018-4088, CVE-2017-7165, CVE-2017-7161, CVE-2017-7160, CVE-2017-7153, CVE-2017-13885 and CVE-2017-13884.
- Fixed poppler security issues CVE-2017-14976 and CVE-2017-1000456.
- Fixed openssl security issues CVE-2017-3738 and CVE-2017-3737.
- Fixed libxml2 security issues CVE-2017-16932 and CVE-2017-15412.
- Fixed nvidia-graphics-drivers-384 security issue CVE-2017-5753.
- Fixed openssh security issues CVE-2017-15906, CVE-2016-10012, CVE-2016-10011, CVE-2016-10010 and CVE-2016-10009.
- Fixed libtasn1-6 security issues CVE-2018-6003 and CVE-2017-10790.
- Fixed curl security issues CVE-2018-1000005 and CVE-2018-1000007.



- Fixed libvorbis security issues CVE-2017-14633 and CVE-2017-14632.
- Fixed wavpack security issue CVE-2016-10169.
- Fixed cups security issue CVE-2017-18190.
- Fixed sensible-utils security issue CVE-2017-17512.
- Removed terminal start function from task manager menu bar.
- Updated kernel to version 4.15.15
  - Fixed Meltdown (CVE-2017-5754) by PTI (page table isolation)
  - Fixed Spectre Variant 1 (CVE-2017-5753) by \_\_user pointer sanitization
  - Fixed Spectre Variant 2 (CVE-2017-5715) by full generic retrampoline
- Fixed beep security issue CVE-2018-0492.
- Added Intel Processor Microcode Updates to provide IBRS/IBPB/STIBP microcode support for Spectre Variant 2 (CVE-2017-5715) mitigation.

| Product Name                                                                   | CPU ID | Platform ID | Microcode Revision |
|--------------------------------------------------------------------------------|--------|-------------|--------------------|
| IGEL UD9-LX Touch 41, IGEL UD9-LX 40, IGEL UD6-LX 51, IGEL UD5-LX 50 Bay Trail | 30678  | 0C          | 0x836              |
| IGEL UD2-LX 40 Bay Trail                                                       | 30679  | 0F          | 0x90A              |
| IGEL UD5-LX 40 Sandy Bridge                                                    | 206A7  | 12          | 0x2D               |

## Network

- Disabled **weak message authentication codes** for SSH server and client as default. If problems occur change the default setting.

### More

|           |                                           |
|-----------|-------------------------------------------|
| Parameter | Disable weak message authentication codes |
| Registry  | network.ssh_client.disable_weak_macs      |
| Value     | <u>enabled</u> / disabled                 |

|           |                                           |
|-----------|-------------------------------------------|
| Parameter | Disable weak message authentication codes |
| Registry  | network.ssh_server.disable_weak_macs      |
| Value     | <u>enabled</u> / disabled                 |



- Disabled **weak key exchange algorithms** for SSH server and client as default. If problems occur, change the default setting.

**More**

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Disable weak key exchange algorithms          |
| Registry  | network.ssh_client.disable_weak_kexalgorithms |
| Value     | <u>enabled</u> / disabled                     |
| Parameter | Disable weak key exchange algorithms          |
| Registry  | network.ssh_server.disable_weak_kexalgorithms |
| Value     | <u>enabled</u> / disabled                     |

- Disabled **weak hostkeys** (server) and **hostkey algorithms** (client) for SSH server and client as default. If problems occur, change the default setting.

**More**

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Disable weak Hostkey algorithms               |
| Registry  | network.ssh_client.disable_weak_hostkey_algos |
| Value     | <u>enabled</u> / disabled                     |
| Parameter | Disable weak Hostkeys                         |
| Registry  | network.ssh_server.disable_weak_hostkeys      |
| Value     | <u>enabled</u> / disabled                     |

- Changed **SMB protocol version default** v1.0 to **v2.0** for mounting windows shares to improve security.
- Added the possibility to change the **SMB protocol** version for windows shares. The windows shares are configurable at **IGEL Setup > Network > Network Drives > Windows Drive**.

**More**

|           |                      |
|-----------|----------------------|
| Parameter | SMB protocol version |
|-----------|----------------------|



|          |                                           |
|----------|-------------------------------------------|
| Registry | <code>network.smbmount.smb_version</code> |
| Range    | 1.0 / <u>2.0</u> / 2.1 / 3.0              |

When using a very old Windows file server, the change to version 1.0 is necessary.

#### RDP / IGEL RDP Client 2

- Fixed RDP: CVE-2018-0886.

#### Java

- Fixed in **Oracle JRE 1.8U162** : CVE-2018-2638, CVE-2018-2639, CVE-2018-2633, CVE-2018-2627, CVE-2018-2637, CVE-2018-2634, CVE-2018-2582, CVE-2018-2641, CVE-2018-2618, CVE-2018-2629, CVE-2018-2603, CVE-2018-2657, CVE-2018-2599, CVE-2018-2581, CVE-2018-2602, CVE-2018-2677, CVE-2018-2678, CVE-2018-2588, CVE-2018-2663, CVE-2018-2675, CVE-2018-2579

#### Known Issues 10.04.100

##### Citrix Receiver 13

- On devices with AMD/Radeon graphics chipsets and activated DRI3 X driver option **the hardware accelerated Citrix H.264 decoder plugin can hang**. To solve this issue deactivation of DRI3 option is necessary (default setting).

[More](#)

|           |                                                                                   |
|-----------|-----------------------------------------------------------------------------------|
| Parameter | Use DRI3                                                                          |
| Registry  | <code>x.drivers.use_dri3</code>                                                   |
| Value     | enabled / <u>disabled</u>                                                         |
| Parameter | Force usage of DRI3                                                               |
| Registry  | <code>x.drivers.amdgpu.force_dri3</code><br><code>x.drivers.ati.force_dri3</code> |
| Value     | enabled / <u>disabled</u>                                                         |

- Citrix StoreFront login with **Gemalto smartcard middleware** does not detect smartcard correctly when the card is inserted after start of login. As a workaround, insert the smartcard before starting StoreFront login.
- **No smooth playback** over **Nuance** channel if the dictation device isn't attached.

##### VMware Horizon



- **External drives** mounted already before connection do not appear in the remote desktop.  
**Workaround:** mapping the directory /media as a drive on desktop.  
 Then the external devices will show up inside the media drive.
- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local Storage Hotplug: On page **Devices > Storage Devices > Storage Hotplug**, put number of storage hotplug devices to 0.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Change on the following setup page is required: **Devices > Storage Devices > Storage Hotplug**.  
 Activate **Enable dynamic drive mapping** and set **Number of storage hotplug devices** to at least 1.

#### Firefox

- Because the **support for the gstreamer framework** was dropped by recent Firefox versions, support for H264 decoding in the browser is not possible anymore due to licensing restrictions.

#### OpenConnect VPN

- **VPNs which need the OpenConnect** client cannot be used for firmware updates.

#### Evidian

- Active Directory users with a **password containing special characters** may have problems to authenticate with the configured session.  
 Known special characters which result in errors are:
  - ˋ (grave accent, ASCII code 96)
  - ˊ (acute accent, ASCII code 239)

#### New Features 10.04.100

##### Citrix Receiver 13

- Integrated **Citrix Receiver 13.8.0**.  
**More**

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Use Citrix Cloud with receiver 13.8 or newer |
| Registry  | ica.cloudconnect                             |
| Value     | enabled / <u>disabled</u>                    |

- Support for **Azure** Active Directory (Azure AD) authentication



- Support for **Workspace** configuration from Citrix Cloud
- Integrated **Citrix Receiver 13.4.2**. Citrix Receiver version 13.5.0 was removed. Available Citrix Receiver versions: 13.3.2, 13.4.2, 13.7.0, 13.8.0 (default)
- Updated **Citrix HDX RTME** used for optimization of Skype for Business to 2.4.0.

#### RDP / IGEL RDP Client 2

- Added possibility to use **RDP local logon** for smartcard login. This can be activated in the setup.  
[More](#)

|           |                                          |
|-----------|------------------------------------------|
| Parameter | Enable smartcard support for local logon |
| Registry  | rdp.login.smartcard-local-logon          |
| Value     | enabled / <u>disabled</u>                |

By enabling this parameter local logon can be used for smartcard authentication. If **Username** is left empty the connection to the RDP server will be made without sending credentials, so you can choose **Smartcard** as login method in the microsoft login window . However this will not work with **NLA**.

- Added support for CredSSP up to version 6.

#### VMware Horizon

- Updated **VMware Horizon Client** to version **4.7.0-7395152**.
- Added key to enable **seamless window mode** in each application session.  
[More](#)

|           |                                                    |
|-----------|----------------------------------------------------|
| Parameter | Seamless Application Windows                       |
| Registry  | sessions.vdm_client.options.enable_seamless_window |
| Value     | enabled / <u>disabled</u>                          |

- Added possibility to use **Fabulatech USB Redirection** in a Horizon Client PCoIP session.  
[More](#)

|            |                                                                                                |
|------------|------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Fabulatech USB Redirection</b> |
| Parameter  | Enable Fabulatech USB Redirection                                                              |
| Registry   | vmware.view.usb.enable-fabulatech-usb                                                          |
| Value      | enabled / <u>disabled</u>                                                                      |

#### Parallels Client



- Integrated **Parallels Client** version **16.2.0 (19039)**
- Added support for USB Redirection, configurable at new IGEL Setup page **Sessions > Parallels Client > Parallels Client Global > USB Redirection.**  
[More](#)

|            |                                                                                         |
|------------|-----------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Parallels Client &gt; Parallels Client Global &gt; USB Redirection</b> |
| Parameter  | Enable USB Redirection                                                                  |
| Registry   | twox.usb_redirection.usb_enable                                                         |
| Value      | <u>enabled</u> / <u>disabled</u>                                                        |
| Parameter  | Product ID                                                                              |
| Registry   | twox.usb_redirection.devicepolicy.product_rule.product                                  |
| Parameter  | Vendor ID                                                                               |
| Registry   | twox.usb_redirection.devicepolicy.product_rule.vendor                                   |
| Parameter  | Rule                                                                                    |
| Registry   | twox.usb_redirection.devicepolicy.product_rule.rule                                     |
| Value      | <u>Deny</u> / <u>Allow</u>                                                              |
| Parameter  | Name                                                                                    |
| Registry   | twox.usb_redirection.devicepolicy.product_rule.name                                     |
| Value      | Policy Rule                                                                             |
| Parameter  | Automatically redirect all USB devices                                                  |
| Registry   | twox.usb_redirection.devicepolicy.redirect_all                                          |
| Value      | <u>enabled</u> / <u>disabled</u>                                                        |

- Added support for **PTP/MTP** Redirection.  
[More](#)

|            |                                                                                         |
|------------|-----------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Parallels Client &gt; Parallels Client Global &gt; USB Redirection</b> |
|------------|-----------------------------------------------------------------------------------------|



|           |                                                        |
|-----------|--------------------------------------------------------|
| Parameter | Enable PTP/MTP Redirection                             |
| Registry  | twox.mtp_redirection.mtp_enable                        |
| Value     | enabled / <u>disabled</u>                              |
| Parameter | Product ID                                             |
| Registry  | twox.mtp_redirection.devicepolicy.product_rule.product |
| Parameter | Vendor ID                                              |
| Registry  | twox.mtp_redirection.devicepolicy.product_rule.vendor  |
| Parameter | Rule                                                   |
| Registry  | twox.mtp_redirection.devicepolicy.product_rule.rule    |
| Value     | <u>Deny</u> / Allow                                    |
| Parameter | Name                                                   |
| Registry  | twox.mtp_redirection.devicepolicy.product_rule.name    |
| Value     | Policy Rule                                            |
| Parameter | Automatically redirect all PTP/MTP devices             |
| Registry  | twox.mtp_redirection.devicepolicy.redirect_all         |
| Value     | enabled / <u>disabled</u>                              |

- Added support for **Clipboard** Redirection.

[More](#)

|            |                                                                                                                         |
|------------|-------------------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Parallels Client &gt; Parallels Client Sessions &gt; Parallels Client Session &gt; Local Resources</b> |
| Parameter  | Connect clipboard                                                                                                       |
| Registry   | sessions.twox.local_resources.connect_clipboard                                                                         |



|       |                           |
|-------|---------------------------|
| Value | <u>enabled</u> / disabled |
|-------|---------------------------|

## VoIP

- Added **VoIP client Ekiga 4.0.1**.

## Firefox

- Updated **Firefox** to version **52.7.2 ESR**.
- Updated **Adobe Flash Player** download URL to version 29.0.0.113.

## Network

- Added **TTLS/PAP** and **TTLS/MSCHAPv2** to possible 802.1x authentication methods.
- Improved support for **Sierra EM7305 LTE** device (e.g. in Toshiba Portégé and Fujitsu LIFEBOOK E Series).

The EM7305 comes in various variants, e.g. one with ProductId 9041 and another one with ProductId 9063. The latter comes at least with one or with two USB configuration options. A device with only one configuration option has been observed on a Toshiba Tecra Z-50-D-115 notebook. It only works in MBIM mode and with IGEL firmware, when the device has successfully connected before with the same settings (particularly APN), e.g. under Microsoft Windows 10.

- Added support for **Sierra EM7455 WWAN module**.
- Added support for running the **Huawei E3531i WWAN** device in modem mode (in addition to HiLink mode).
- Added possibility to adopt the **hostname from a DHCP lease** as **permanent** terminal name. The purpose is to use the name received as part of a DHCP lease in future interactions with the DHCP server.

**More**

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Adopt permanent Terminal Name from DHCP lease |
| Registry  | network.dns.hostname_adopt_from_dhcp          |
| Value     | <u>enabled</u> / disabled                     |

- NetworkManager** updated to version **1.2.2**
- ModemManager** updated to version **1.6.4**
- usb\_modeswitch** updated to version **2.5.1**

## Open VPN

- Added **Huawei HiLink Mobile Broadband USB** device as possible uplink to OpenVPN sessions.

## OpenConnect VPN

- Added **OpenConnect** client version **7.08** to connect to **Cisco AnyConnect** and **Juniper VPN**. The feature must be enabled.

**More**



|            |                                                                                                  |
|------------|--------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>System &gt; Firmware Customization &gt; Features</b>                                          |
| Parameter  | VPN OpenConnect (Limited support - functionality "as is", see product documentation for details) |
| Registry   | services.unsupported02.enabled                                                                   |
| Value      | enabled / <u>disabled</u>                                                                        |

- The OpenConnect VPN configuration is available at IGEL Setup page **Network > VPN > OpenConnect VPN**.

[More](#)

|            |                                                                                |
|------------|--------------------------------------------------------------------------------|
| IGEL Setup | <b>Network &gt; VPN &gt; OpenConnect VPN &gt; VPN OpenConnect &gt; Session</b> |
| Parameter  | Gateway                                                                        |
| Registry   | sessions.openconnect.vpnopts.gateway                                           |
| Parameter  | Enable Name/Password Authentication                                            |
| Registry   | sessions.openconnect.vpnopts.enable-name-pwd                                   |
| Value      | enabled / <u>disabled</u>                                                      |
| Parameter  | User Name                                                                      |
| Registry   | sessions.openconnect.vpnopts.username                                          |
| Parameter  | Password                                                                       |
| Registry   | sessions.openconnect.vpnopts.crypt_password                                    |
| Parameter  | CA Certificate                                                                 |
| Registry   | sessions.openconnect.vpnopts.ca-cert                                           |
| Parameter  | User Certificate                                                               |
| Registry   | sessions.openconnect.vpnopts.user-cert                                         |
| Parameter  | Private Key                                                                    |



|           |                                                                       |
|-----------|-----------------------------------------------------------------------|
| Registry  | <code>sessions.openconnect.vpnopts.priv-key</code>                    |
| Parameter | Private Key password                                                  |
| Registry  | <code>sessions.openconnect.vpnopts.priv-key-pwd.crypt_password</code> |
| Parameter | Connect to Juniper Networks VPN                                       |
| Registry  | <code>sessions.openconnect%.vpnopts.is-juniper</code>                 |
| Value     | enabled / <u>disabled</u>                                             |

Tray icon is placed in the panel to disconnect from a running OpenConnect VPN connection.

## Smartcard

- Added **CoolKey PKCS#11** library for access to **Common Access Card (CAC)** smartcards.  
[More](#)

|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Browser &gt; Browser Global &gt; Encryption</b>              |
| Parameter  | Coolkey Security Device                                                       |
| Registry   | <code>browserglobal.security_device.coolkey</code>                            |
| Value      | enabled / <u>disabled</u>                                                     |
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Smartcard</b> |
| Parameter  | Horizon logon with smartcards supported by Coolkey library                    |
| Registry   | <code>vmware.view.pkcs11.use_coolkey</code>                                   |
| Value      | enabled / <u>disabled</u>                                                     |
| IGEL Setup | <b>Security &gt; Smartcard &gt; Middleware</b>                                |
| Parameter  | Coolkey                                                                       |
| Registry   | <code>scard.pkcs11.use_coolkey</code>                                         |



|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

- Updated **Gemalto SafeNet PKCS#11** library to version **10.0.37-0**. This package replaces **Gemalto/SafeNet eToken** and **Gemalto IDPrime** libraries.  
**Gemalto SafeNet** (formerly **Gemalto/SafeNet eToken**) now handles Gemalto cards and tokens including eToken and IDPrime.  
**Gemalto IDPrime** now handles IDPrime cards and tokens, preferred Common Criteria (CC) cards and tokens in Unlinked Mode.
- Added full integration of **OpenSC PKCS#11** library for access to smartcards.  
[More](#)

|            |                                                                  |
|------------|------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Browser &gt; Browser Global &gt; Encryption</b> |
|------------|------------------------------------------------------------------|

|           |                        |
|-----------|------------------------|
| Parameter | OpenSC Security Device |
|-----------|------------------------|

|          |                                      |
|----------|--------------------------------------|
| Registry | browserglobal.security_device.opensc |
|----------|--------------------------------------|

|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Smartcard</b> |
|------------|-------------------------------------------------------------------------------|

|           |                                                           |
|-----------|-----------------------------------------------------------|
| Parameter | Horizon logon with smartcards supported by OpenSC library |
|-----------|-----------------------------------------------------------|

|          |                               |
|----------|-------------------------------|
| Registry | vmware.view.pkcs11.use_opensc |
|----------|-------------------------------|

|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

|            |                                                |
|------------|------------------------------------------------|
| IGEL Setup | <b>Security &gt; Smartcard &gt; Middleware</b> |
|------------|------------------------------------------------|

|           |        |
|-----------|--------|
| Parameter | OpenSC |
|-----------|--------|

|          |                         |
|----------|-------------------------|
| Registry | scard.pkcs11.use_opensc |
|----------|-------------------------|

|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

- Updated **MUSCLE CCID** smartcard reader driver to version **1.4.28**.
- Updated **ACS CCID** smartcard reader driver to version **1.1.5**.
- Updated **REINER SCT cyberJack** smartcard reader driver to version **3.99.5final.sp11**.
- Added parameter to disable **Identive CCID** smartcard reader driver. If this driver is disabled, some of the readers are handled by the MUSCLE CCID driver. This can help when problems with Identive reader driver occur.

[More](#)

|           |                                        |
|-----------|----------------------------------------|
| Parameter | Identive driver for smart card readers |
|-----------|----------------------------------------|



|          |                                         |
|----------|-----------------------------------------|
| Registry | <code>scard.pcscd.identiv_enable</code> |
| Value    | <u>enabled</u> / disabled               |

- Updated **cryptovision sc/interface PKCS#11** library to version **7.0.5.592**.
- New smartcard reader driver for **Fujitsu KB SCR eSIG** version **5.0.24**.

## HID

- Added **layout toggle** feature to on-screen keyboard.

**More**

|            |                                                                   |
|------------|-------------------------------------------------------------------|
| IGEL Setup | <b>Accessories &gt; On-Screen Keyboard &gt; Appearance</b>        |
| Parameter  | Enable switching to alternative layout                            |
| Registry   | <code>userinterface.softkeyboard.enable_alternative_layout</code> |
| Value      | <u>enabled</u> / <u>disabled</u>                                  |

If this is enabled there is a key on the on-screen keyboard for toggling between the normal layout and a reduced layout, that saves space on the screen and has more or less the same features as the number block of an ordinary keyboard with some extensions.

## Base System

- Added support for **UEFI Secure Boot**.

When booted with Secure Boot the downgrade to a firmware version older than 10.04.100 is locked.

- Updated **kernel to version 4.15.15**
- **Boot time optimization** (up to 25% faster)
- **Switch power off on USB ports on shutdown and reboot**. The feature can be enabled in IGEL Setup. At the moment only IGEL H830C is supported.

**More**

|            |                                            |
|------------|--------------------------------------------|
| IGEL Setup | <b>System &gt; Registry</b>                |
| Parameter  | Power off on shutdown                      |
| Registry   | <code>devices.usb.poweroff_shutdown</code> |
| Value      | <u>enabled</u> / <u>disabled</u>           |

- Added Unit ID in Application Launcher **About > Hardware** section.
- Showing **number of CPU cores** in Application Launcher **About > Hardware** section now.



## Storage Devices

- Added support for **Mobile Device Access** feature in **Appliance Mode**. The Mobile Device Access tool can be opened via a new icon in the **In-session control bar**. The Mobile Device Access tool can also be started automatically.

**More**

|           |                                 |
|-----------|---------------------------------|
| Parameter | Autostart                       |
| Registry  | sessions.mtp-devices0.autostart |
| Value     | enabled / <u>disabled</u>       |

Mobile Device Access must be enabled at **IGEL Setup > System > Firmware Customization > Features**. Appliance Mode must be enabled at **IGEL Setup > Sessions > Appliance Mode**.

- The **Mobile Device Access tool** is now configurable at **IGEL Setup > Accessories > Mobile Device Access**.
- The **Mobile Device Access tray icon** respects the current theme now.

## X11 System

- Added support for **XDMCP Appliance Mode**. The XDMCP connection is configurable.

**More**

|            |                                                               |
|------------|---------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b>                           |
| Parameter  | XDMCP for this Display                                        |
| Registry   | x.xdmcp0.enabled                                              |
| Value      | enabled / <u>disabled</u>                                     |
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b>                           |
| Parameter  | Connection Type                                               |
| Registry   | x.xdmcp0.server.connectiontype                                |
| Range      | <b>indirect via localhost</b> / indirect / direct / broadcast |
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b>                           |
| Parameter  | Name or IP of server                                          |
| Registry   | x.xdmcp0.server.servername                                    |



|            |                                     |
|------------|-------------------------------------|
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b> |
| Parameter  | Enable hotkeys for XDMCP Display    |
| Registry   | x.xdmcp0.hotkeys.enabled            |
| Value      | <u>enabled</u> / <u>disabled</u>    |

The default hotkey to open IGEL Setup is: CTRL + ALT + F2. The setup page **User Interface > Display > XDMCP** was removed.

- Added **XC Font Service** support.

[More](#)

|            |                                                               |
|------------|---------------------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
| Parameter  | Enable XC Font Service                                        |
| Registry   | x.xc_fontservice.enabled                                      |
| Value      | <u>enabled</u> / <u>disabled</u>                              |
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
| Parameter  | XC Font Server                                                |
| Registry   | x.xc_fontservice.fontserver                                   |
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
| Parameter  | Port Number                                                   |
| Registry   | x.xc_fontservice.port                                         |
| Value      | <u>7100</u>                                                   |
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
| Parameter  | Prefer Local Fonts                                            |
| Registry   | x.xc_fontservice.prefer_localfonts                            |
| Value      | <u>enabled</u> / <u>disabled</u>                              |



- Added **auto detection of monitor refresh rate**. This can be controlled with new parameters.  
**More**

|            |                                                  |
|------------|--------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Display &gt; Advanced</b> |
| Parameter  | Detect refresh rate automatically                |
| Registry   | x.xserver0.auto_frequency                        |
| Value      | <u>enabled</u> / disabled                        |

|            |                                                  |
|------------|--------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Display &gt; Advanced</b> |
| Parameter  | Detect refresh rate automatically                |
| Registry   | x.xserver0.screen.auto_frequency                 |
| Value      | <u>enabled</u> / disabled                        |

- Added xorg debug script **/etc/igel/igel\_debug\_tools/xorg-debug.sh** to make collecting Xorg debug data easier (a /tmp/xorg-debug.log file is generated).

## Window Manager

- Added possibility to
  - a) **change the preferred placement mode** and
  - b) **modify the threshold value** up to which window size this placement mode should be chosen (otherwise window placement defaults to so called smart mode which tries to minimize overlapping).

**More**

|           |                                                                        |
|-----------|------------------------------------------------------------------------|
| Parameter | Preferred Placement                                                    |
| Registry  | windowmanager.wm0.variables.placement_mode                             |
| Value     | At mouse position / <u>Centered</u>                                    |
| Parameter | Maximum window size for which the preferred placement should apply     |
| Registry  | windowmanager.wm0.variables.placement_ratio                            |
| Value     | 0% / 10% / <u>20%</u> / 30% / 40% / 50% / 60% / 70% / 80% / 90% / 100% |



## Audio

- **Volume** of audio output and input can now be configured up to 150% at **IGEL Setup page Accessories > Sound Preferences > Options**.
- Added a parameter for log level configuration of **Pulseaudio** service.  
[More](#)

| Parameter | Log level                                      |
|-----------|------------------------------------------------|
| Registry  | multimedia.pulseaudio.daemon.log-level         |
| Range     | debug / info / <u>notice</u> / warning / error |

## Misc

- An EULA must be accepted now in IGEL setup assistant before finalizing it and using the IGEL OS.

## Java

- Updated **Oracle JRE to 1.8U162**.

## Remote Management

- Added **new log file transfer mechanism** for UMS feature **Save TC files for support** (UMS 5.08.110 or higher required). By default, it collects all log files visible in system log viewer, system configuration files group.ini, setup.ini and dhclient lease files. More files can be specified at **IGEL Setup > Accessories > System Log Viewer > Options**. The resulting zip file has now a folder structure.

## IGEL Cloud Gateway

- Added **UMS structure tag** handling for usage with **ICG agent**.

## Hardware

- Added support for **IGEL UD7-LX 10**.

## Resolved Issues 10.04.100

### Citrix

- Fixed sporadic crashes of the **Citrix USB Daemon**.

### RDP / IGEL RDP Client 2

- Fixed passing **Ctrl+Alt+C keyboard shortcut** to RDP session.
- Fixed **smartcard redirection**: after session reconnection readers and cards were not connected any more in some cases.
- Fixed the **rdpdebugger** to work again (was broken in the previous release).
- Fixed misleading **RDP error message `Authentication failed`** on wakeup from suspend mode
- Fixed **TCP timeout value** to get more stable **RDP connections** under certain circumstances.

### VMware Horizon

- Fixed bug which prevented **microphone redirection** in Horizon Client RDP sessions.

**More**

|            |                                                                  |
|------------|------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; RDP &gt; RDP Global &gt; Mapping &gt; Audio</b> |
| Parameter  | Audio recording                                                  |
| Registry   | rdp.winconnect.rdppeai.enable                                    |
| Value      | enabled / <u>disabled</u>                                        |

RedHat Enterprise Virtualization Client

- Fixed **display corruption** with Windows connections.

Firefox

- Fixed possibility to **download files in the browser** if needed. The parameter to enable/disable file download is available here.

**More**

|            |                                                                |
|------------|----------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Browser &gt; Browser Sessions &gt; Window</b> |
| Parameter  | Hide local filesystem                                          |
| Registry   | sessions.browser.app.filepicker_dialog_hidden                  |
| Value      | enabled / <u>disabled</u>                                      |

If enabled, the user is not allowed to download or use any save-as functionality from menu, context or keyboard shortcut.

- Fixed bug which **prevented the download using the file dialog** (in the case you open a link to a file of unknown type).
- Fixed **unmounting of the Firefox profile partition during shutdown** - now it is unmounted in a determinate manner after Custom Partition.

Network

- Fixed bug: **Network tray icons** sometimes didn't reappear after network restart.
- Fixed bug: **tcpdump debug tool** terminated immediately during boot.
- Fixed issue with **naming of USB ethernet devices**.
- Fixed wrong **LinkMode (10baseT/Half)** with autonegotiation and some USB ethernet devices.

AppliDis

- Changed default value of **PasswordMode** from **cmdline** to **prompt** as suggested by Systancia.

Smartcard

- Fixed driver for **Elatec RFID readers**. Before this fix the readers sometimes were not available after boot.
- Fixed VMware Horizon logon with OpenSC smartcards.



## CUPS Printing

- Fixed bug where the **user for printjobs** was not set to the **domain user**.

## Base System

- Fixed **Kerberos password change** to work also with transport protocol **TCP**. To force protocol TCP, prepend Domain Controllers with prefix "tcp/", e.g. "tcp/dc.example.com".
- Fixed **occasional desktop hang** in the local login or the network login mask after successful authentication.
- Fixed **password expiry notification** showing negative expiry period.
- Fixed **update to connect to SFTP** servers with very restrictive key exchange settings.
- Fixed input of the **reset key in reset to defaults boot**, if the administrator password is not available anymore. If more than 255 characters were entered in the 1st try, it was not possible to enter the reset key for a 2nd or 3rd time.
- Fixed **Active Directory logon with smartcard**: If the smartcard contains logon certificates for multiple users, it is possible to switch between these certificates and log on with the chosen certificate now.
- Fixed missing names for some **partitions** in update notification when having a user interface **language other than English**.
- Fixed problems with **never ending bootcode** update with some EFI BIOS variants.
- Fixed **ssh server port** configuration.
- Fixed **signotec signature pad** channel for Citrix.
- Increased stability of **signotec VCOM Daemon**.
- Remove residual information belonging to a **removed content from a custom partition**.
- Fixed **crash of xfce4-power-manager** after adding or removing input devices.

## Custom Partition

- Fixed **automatic update of custom partition** - if download source isn't accessible then the content of the custom partition got lost.

## Appliance Mode

- Fixed post session command **Logoff** in Appliance Mode.

## X11 System

- Fixed **Elo-USB Touchscreen functionality** after reboot.
- Fixed **DisplayLink USB Support on UD3 LX50**.
- Fixed issue with **two monitors connected via DVI-D to HDMI adapter on a UD3 M330 (VIA)**. Added registry key to disable the new HDMI autodetection.

**More**

|           |                                             |
|-----------|---------------------------------------------|
| Parameter | Autodetect if DVI to HDMI adapter is in use |
| Registry  | x.drivers.via.autodetect_hdmi_output        |
| Value     | <u>enabled</u> / disabled                   |

- Fixed **wrong automatic resolution detection** if monitor does not have a preferred mode.
- Fixed **sporadic display corruptions** after monitors leaving the power saving mode.



- Improved handling of more than 2 screens.

#### Shadowing/VNC

- Fixed **sporadic VNC server crash**.

#### Audio

- Fixed **volume control of internal speaker in HP T610**.
- Fixed **automatic switch to output** over analog headphones.
- Not existing **S/PDIF inputs and outputs in Plantronics and Jabra USB headsets** are now ignored by audio subsystem (Pulseaudio).
- Added workaround in the kernel USB audio driver for **volume control on Sennheiser USB headsets**.

#### Remote Management

- Fixed **calculation of Unit ID for UMS management**. In some cases, it could happen that the MAC address of wrong network interface was chosen.
- Fixed **IGEL Setup Assistant** to get stopped when settings were received from UMS.

## 7.30.2 IGEL Universal Desktop OS3/IGEL UD Pocket 10.04.100

#### Supported Hardware:

[Third-Party Devices Supported by IGEL OS 10<sup>460</sup>](#)

- Versions for Release 10.04.100(see page 2286)
- General Information 10.04.100(see page 2290)
- Security Fixes 10.04.100(see page 2291)
- Known Issues 10.04.100(see page 2294)
- New Features 10.04.100(see page 2296)
- Resolved Issues 10.04.100(see page 2308)

#### Versions for Release 10.04.100

##### • Clients

| Product                          | Version         |
|----------------------------------|-----------------|
| Citrix HDX Realtime Media Engine | 2.4.0-1233      |
| Citrix Receiver                  | 13.3.2.366713   |
| Citrix Receiver                  | 13.4.2.10146724 |

<sup>460</sup> <https://kb.igel.com/display/hardware/Third+Party+Devices+Supported+by+IGEL+OS+10>



|                                       |                                 |
|---------------------------------------|---------------------------------|
| Citrix Receiver                       | 13.7.0.10276927                 |
| Citrix Receiver                       | 13.8.0.10299729                 |
| deviceTRUST Citrix Channel            | 17.2.100.0                      |
| deviceTRUST RDP Channel               | 17.2.100.0                      |
| Ericom PowerTerm                      | 12.0.1.0.20170219.2-_dev_-34574 |
| Evidian AuthMgr                       | 1.5.6362                        |
| Evince PDF Viewer                     | 3.18.2-1ubuntu4.3               |
| FabulaTech USB for Remote Desktop     | 5.2.23                          |
| Firefox                               | 52.7.2                          |
| IBM iAccess Client Solutions          | 1.1.5.0                         |
| IGEL RDP Client                       | 2.2                             |
| Imprivata OneSign ProveID Embedded    |                                 |
| Leostream Java Connect                | 3.3.7.0                         |
| NX Client                             | 5.3.12                          |
| Open VPN                              | 2.3.10-1ubuntu2.1               |
| Oracle JRE                            | 1.8.0_162                       |
| Parallels Client (64 bit)             | 16.2.0.19039                    |
| Remote Viewer (RedHat Virtualization) | 7.0                             |
| Systancia AppliDis                    | 4.0.0.17                        |
| Thinlinc Client                       | 4.8.0-5456                      |
| ThinPrint Client                      | 7.5.83                          |



|                       |               |
|-----------------------|---------------|
| Totem Media Player    | 2.30.2        |
| VMware Horizon Client | 4.7.0-7395152 |
| Voip Client Ekiga     | 4.0.1         |

- **Dictation**

|                                                       |          |
|-------------------------------------------------------|----------|
| Diktamen driver for dictation                         |          |
| Driver for Grundig Business Systems dictation devices |          |
| Nuance Audio Extensions for dictation                 | B048     |
| Olympus driver for dictation                          | 20161103 |
| Philips Speech Driver                                 | 12.5.4   |

- **Signature**

|                         |       |
|-------------------------|-------|
| signotec Citrix Channel | 8.0.6 |
| signotec VCOM Daemon    | 2.0.0 |
| StepOver TCP Client     | 2.1.0 |

- **Smartcard**

|                                           |           |
|-------------------------------------------|-----------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101   |
| PKCS#11 Library Athena IDProtect          | 623.07    |
| PKCS#11 Library cryptovision sc/interface | 7.0.5.592 |
| PKCS#11 Library Gemalto SafeNet           | 10.0.37-0 |
| PKCS#11 Library SecMaker NetID            | 6.6.0.30  |
| Reader Driver ACS CCID                    | 1.1.5     |
| Reader Driver Gemalto eToken              | 10.0.37-0 |
| Reader Driver HID Global Omnikey          | 4.2.4     |



|                                    |                  |
|------------------------------------|------------------|
| Reader Driver Identive CCID        | 5.0.35           |
| Reader Driver Identive eHealth200  | 1.0.5            |
| Reader Driver Identive SCRKBC      | 5.0.24           |
| Reader Driver MUSCLE CCID          | 1.4.28           |
| Reader Driver REINER SCT cyberJack | 3.99.5final.SP11 |
| Resource Manager PC/SC Lite        | 1.8.22           |
| Cherry USB2LAN Proxy               | 3.0.0.4          |

- **System Components**

|                                         |                            |
|-----------------------------------------|----------------------------|
| Bluetooth stack (bluez)                 | 5.46-0ubuntu3              |
| MESA OpenGL stack                       | 17.2.8-0igel3              |
| VAAPI ABI Version                       | 0.40                       |
| VDPAU Library version                   | 1.1.1-3ubuntu1             |
| Graphics Driver INTEL                   | 2.99.917+git20180214-igel1 |
| Graphics Driver ATI/RADEON              | 7.10.0-2igel3              |
| Graphics Driver ATI/AMDGPU              | 1.4.0-2igel3               |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.15-2                   |
| Graphics Driver Nvidia                  | 384.111-0ubuntu0.16.04.1   |
| Graphics Driver Vboxvideo               | 5.2.6-dfsg-2               |
| Graphics Driver VMware                  | 13.2.1-1build1             |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1              |
| Graphics Driver FBDEV                   | 0.4.4-1build5              |



|                                 |                              |
|---------------------------------|------------------------------|
| Graphics Driver VESA            | 2.3.4-1build2                |
| Input Driver Evdev              | 2.10.5-1ubuntu1              |
| Input Driver Elographics        | 1.4.1-1build5                |
| Input Driver eGalax             | 2.5.5814                     |
| Input Driver Synaptics          | 1.9.0-1ubuntu1               |
| Input Driver Vmmouse            | 13.1.0-1ubuntu2              |
| Input Driver Wacom              | 0.34.0-0ubuntu2              |
| Kernel                          | 4.15.15 #mainline-udos-r2141 |
| Xorg X11 Server                 | 1.19.6-2igel1                |
| CUPS printing daemon            | 2.1.3-4ubuntu0.4             |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1            |
| XFCE4 Windowmanager             | 4.12.3-1ubuntu2              |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.7            |
| NetworkManager                  | 1.2.2-0ubuntu0.16.04.4       |
| ModemManager                    | 1.6.4-1                      |
| GStreamer 0.10                  | 0.10.36-2ubuntu0.1           |

- **Features with Limited IGEL Support**

|                          |  |
|--------------------------|--|
| Mobile Device Access USB |  |
| VPN OpenConnect          |  |

## General Information 10.04.100

The following clients and features are not supported anymore in version 10.04.100:

- Citrix Receiver 12.1 and 13.1
- Citrix Access Gateway Standard Plug-in



- Dell vWorkspace Connector for Linux
- Ericom PowerTerm Emulation 9 and 11
- Ericom Webconnect
- IGEL Legacy RDP Client (rdesktop)
- Virtual Bridges VERDE Client
- PPTP VPN Support
- IGEL Upgrade License Tool with IGEL Smartcard Token
- Remote Management by setup.ini file transfer (TFTP)
- Remote Access via RSH
- Legacy Philips Speech Driver
- Digital Persona Support
- Sane Scanner Support
- t-Systems TCOS Smartcard Support
- DUS Series touch screens
- Elo serial touch screens
- IGEL Smartcard without locking desktop
- VIA Graphics Support
- Storage Hotplug devices are not automatically removed anymore, instead they must be always ejected manually:
  - by panel tray icon
  - by an icon in the **In-Session Control Bar** (configurable at **IGEL Setup > User Interface > Desktop**)
  - by a **Safely Remove Hardware** session (configurable at **IGEL Setup > Accessories**)

The following clients and features are not available in release 10.04.100:

- X session (Xorg Xephyr)
- Cherry eGK Channel
- Softpro/Kofax Citrix Virtual Channel
- Open VPN Smartcard Support
- NCP Secure Client
- Asian Input Methods
- Composite Manager

## Security Fixes 10.04.100

### Firefox

- Fixes for **mfsa2018-08**, also known as CVE-2018-5146, CVE-2018-5147.
- Fixes for **mfsa2018-07**, also known as CVE-2018-5127, CVE-2018-5129, CVE-2018-5130, CVE-2018-5131, CVE-2018-5144, CVE-2018-5125, CVE-2018-5145.

### Base System

- Added support for UEFI Secure Boot.

When booted with Secure Boot the downgrade to a firmware version older than 10.04.100 is locked.



- When booted with Secure Boot the downgrade to a firmware version older than 10.04.100 is locked.
- Fixed evince security issue CVE-2017-1000159.
- Fixed bind9 security issue CVE-2017-3145.
- Fixed glibc security issues CVE-2018-1000001, CVE-2017-16997, CVE-2017-15804, CVE-2017-15670, CVE-2017-1000409 and CVE-2017-1000408.
- Fixed gdk-pixbuf security issues CVE-2017-6314, CVE-2017-6313, CVE-2017-6312 and CVE-2017-1000422.
- Fixed webkit2gtk security issues CVE-2017-7156, CVE-2017-5753, CVE-2017-5715, CVE-2017-13870, CVE-2017-13866, CVE-2017-13856, CVE-2018-4096, CVE-2018-4088, CVE-2017-7165, CVE-2017-7161, CVE-2017-7160, CVE-2017-7153, CVE-2017-13885 and CVE-2017-13884.
- Fixed poppler security issues CVE-2017-14976 and CVE-2017-1000456.
- Fixed openssl security issues CVE-2017-3738 and CVE-2017-3737.
- Fixed libxml2 security issues CVE-2017-16932 and CVE-2017-15412.
- Fixed nvidia-graphics-drivers-384 security issue CVE-2017-5753.
- Fixed openssh security issues CVE-2017-15906, CVE-2016-10012, CVE-2016-10011, CVE-2016-10010 and CVE-2016-10009.
- Fixed libtasn1-6 security issues CVE-2018-6003 and CVE-2017-10790.
- Fixed curl security issues CVE-2018-1000005 and CVE-2018-1000007.
- Fixed libvorbis security issues CVE-2017-14633 and CVE-2017-14632.
- Fixed wavpack security issue CVE-2016-10169.
- Fixed cups security issue CVE-2017-18190.
- Fixed sensible-utils security issue CVE-2017-17512.
- Removed terminal start function from task manager menu bar.
- Updated kernel to version 4.15.15
  - Fixed Meltdown (CVE-2017-5754) by PTI (page table isolation)
  - Fixed Spectre Variant 1 (CVE-2017-5753) by \_\_user pointer sanitization
  - Fixed Spectre Variant 2 (CVE-2017-5715) by full generic retpoline
- Fixed beep security issue CVE-2018-0492.
- Added Intel Processor Microcode Updates to provide IBRS/IBPB/STIBP microcode support for Spectre Variant 2 (CVE-2017-5715) mitigation.

| <b>Product Name</b>                                                            | <b>CPU ID</b> | <b>Platform ID</b> | <b>Microcode Revision</b> |
|--------------------------------------------------------------------------------|---------------|--------------------|---------------------------|
| IGEL UD9-LX Touch 41, IGEL UD9-LX 40, IGEL UD6-LX 51, IGEL UD5-LX 50 Bay Trail | 30678         | 0C                 | 0x836                     |
| IGEL UD2-LX 40 Bay Trail                                                       | 30679         | 0F                 | 0x90A                     |
| IGEL UD5-LX 40 Sandy Bridge                                                    | 206A7         | 12                 | 0x2D                      |

Network



- Disabled **weak message authentication codes** for SSH server and client as default. If problems occur change the default setting.

**More**

|           |                                           |
|-----------|-------------------------------------------|
| Parameter | Disable weak message authentication codes |
| Registry  | network.ssh_client.disable_weak_macs      |
| Value     | <u>enabled</u> / disabled                 |

|           |                                           |
|-----------|-------------------------------------------|
| Parameter | Disable weak message authentication codes |
| Registry  | network.ssh_server.disable_weak_macs      |
| Value     | <u>enabled</u> / disabled                 |

- Disabled **weak key exchange algorithms** for SSH server and client as default. If problems occur, change the default setting.

**More**

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Disable weak key exchange algorithms          |
| Registry  | network.ssh_client.disable_weak_kexalgorithms |
| Value     | <u>enabled</u> / disabled                     |
| Parameter | Disable weak key exchange algorithms          |
| Registry  | network.ssh_server.disable_weak_kexalgorithms |
| Value     | <u>enabled</u> / disabled                     |

- Disabled **weak hostkeys** (server) and **hostkey algorithms** (client) for SSH server and client as default. If problems occur, change the default setting.

**More**

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Disable weak Hostkey algorithms               |
| Registry  | network.ssh_client.disable_weak_hostkey_algos |



|           |                                          |
|-----------|------------------------------------------|
| Value     | <u>enabled</u> / disabled                |
| Parameter | Disable weak Hostkeys                    |
| Registry  | network.ssh_server.disable_weak_hostkeys |
| Value     | <u>enabled</u> / disabled                |

- Changed **SMB protocol version default** v1.0 to **v2.0** for mounting windows shares to improve security.
- Added the possibility to change the **SMB protocol** version for windows shares. The windows shares are configurable at **IGEL Setup > Network > Network Drives > Windows Drive**.

**More**

|           |                              |
|-----------|------------------------------|
| Parameter | SMB protocol version         |
| Registry  | network.smbmount.smb_version |
| Range     | 1.0 / <u>2.0</u> / 2.1 / 3.0 |

When using a very old Windows file server, the change to version 1.0 is necessary.

#### RDP / IGEL RDP Client 2

- Fixed RDP: CVE-2018-0886.

#### Java

- Fixed in **Oracle JRE 1.8U162** : CVE-2018-2638, CVE-2018-2639, CVE-2018-2633, CVE-2018-2627, CVE-2018-2637, CVE-2018-2634, CVE-2018-2582, CVE-2018-2641, CVE-2018-2618, CVE-2018-2629, CVE-2018-2603, CVE-2018-2657, CVE-2018-2599, CVE-2018-2581, CVE-2018-2602, CVE-2018-2677, CVE-2018-2678, CVE-2018-2588, CVE-2018-2663, CVE-2018-2675, CVE-2018-2579

#### Known Issues 10.04.100

##### Citrix Receiver 13

- On devices with AMD/Radeon graphics chipsets and activated DRI3 X driver option **the hardware accelerated Citrix H.264 decoder plugin can hang**. To solve this issue deactivation of DRI3 option is necessary (default setting).

**More**

|           |                           |
|-----------|---------------------------|
| Parameter | Use DRI3                  |
| Registry  | x.drivers.use_dri3        |
| Value     | <u>enabled</u> / disabled |



|           |                                                         |
|-----------|---------------------------------------------------------|
| Parameter | Force usage of DRI3                                     |
| Registry  | x.drivers.amdgpu.force_dri3<br>x.drivers.ati.force_dri3 |
| Value     | enabled / <u>disabled</u>                               |

- Citrix StoreFront login with **Gemalto smartcard middleware** does not detect smartcard correctly when the card is inserted after start of login. As a workaround, insert the smartcard before starting StoreFront login.
- **No smooth playback** over **Nuance** channel if the dictation device isn't attached.

#### VMware Horizon

- **External drives** mounted already before connection do not appear in the remote desktop.  
**Workaround:** mapping the directory /media as a drive on desktop.  
Then the external devices will show up inside the media drive.
  - **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
    - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local Storage Hotplug: On page **Devices > Storage Devices > Storage Hotplug**, put number of storage hotplug devices to 0.
    - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Change on the following setup page is required: **Devices > Storage Devices > Storage Hotplug**.
- Activate **Enable dynamic drive mapping** and set **Number of storage hotplug devices** to at least 1.

#### Firefox

- Because the **support for the gstreamer framework** was dropped by recent Firefox versions, support for H264 decoding in the browser is not possible anymore due to licensing restrictions.

#### OpenConnect VPN

- **VPNs which need the OpenConnect** client cannot be used for firmware updates.

#### Evidian

- Active Directory users with a **password containing special characters** may have problems to authenticate with the configured session.  
Known special characters which result in errors are:
  - (grave accent, ASCII code 96)
  - (acute accent, ASCII code 239)



## New Features 10.04.100

### Citrix Receiver 13

- Integrated **Citrix Receiver 13.8.0**.

**More**

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Use Citrix Cloud with receiver 13.8 or newer |
| Registry  | ica.cloudconnect                             |
| Value     | enabled / <u>disabled</u>                    |

- Support for **Azure Active Directory (Azure AD)** authentication
- Support for **Workspace** configuration from Citrix Cloud
- Integrated **Citrix Receiver 13.4.2**. Citrix Receiver version 13.5.0 was removed. Available Citrix Receiver versions: 13.3.2, 13.4.2, 13.7.0, 13.8.0 (default)
- Updated **Citrix HDX RTME** used for optimization of Skype for Business to 2.4.0.

### RDP / IGEL RDP Client 2

- Added possibility to use **RDP local logon** for smartcard login. This can be activated in the setup.

**More**

|           |                                          |
|-----------|------------------------------------------|
| Parameter | Enable smartcard support for local logon |
| Registry  | rdp.login.smartcard-local-logon          |
| Value     | enabled / <u>disabled</u>                |

By enabling this parameter local logon can be used for smartcard authentication. If **Username** is left empty the connection to the RDP server will be made without sending credentials, so you can choose **Smartcard** as login method in the microsoft login window . However this will not work with **NLA**.

- Added support for CredSSP up to version 6.

### VMware Horizon

- Updated **VMware Horizon Client** to version **4.7.0-7395152**.
- Added key to enable **seamless window mode** in each application session.

**More**

|           |                                                    |
|-----------|----------------------------------------------------|
| Parameter | Seamless Application Windows                       |
| Registry  | sessions.vdm_client.options.enable_seamless_window |
| Value     | enabled / <u>disabled</u>                          |



- Added possibility to use **Fabulatech USB Redirection** in a Horizon Client PCoIP session.

[More](#)

|            |                                                                                                |
|------------|------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Fabulatech USB Redirection</b> |
| Parameter  | Enable Fabulatech USB Redirection                                                              |
| Registry   | vmware.view.usb.enable-fabulatech-usb                                                          |
| Value      | enabled / <u>disabled</u>                                                                      |

#### Parallels Client

- Integrated **Parallels Client** version **16.2.0 (19039)**
- Added support for USB Redirection, configurable at new IGEL Setup page **Sessions > Parallels Client > Parallels Client Global > USB Redirection**.

[More](#)

|            |                                                                                         |
|------------|-----------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Parallels Client &gt; Parallels Client Global &gt; USB Redirection</b> |
| Parameter  | Enable USB Redirection                                                                  |
| Registry   | twox.usb_redirection.usb_enable                                                         |
| Value      | enabled / <u>disabled</u>                                                               |
| Parameter  | Product ID                                                                              |
| Registry   | twox.usb_redirection.devicepolicy.product_rule.product                                  |
| Parameter  | Vendor ID                                                                               |
| Registry   | twox.usb_redirection.devicepolicy.product_rule.vendor                                   |
| Parameter  | Rule                                                                                    |
| Registry   | twox.usb_redirection.devicepolicy.product_rule.rule                                     |
| Value      | <u>Deny</u> / Allow                                                                     |
| Parameter  | Name                                                                                    |
| Registry   | twox.usb_redirection.devicepolicy.product_rule.name                                     |



| Value     | Policy Rule                                    |
|-----------|------------------------------------------------|
| Parameter | Automatically redirect all USB devices         |
| Registry  | twox.usb_redirection.devicepolicy.redirect_all |
| Value     | <u>enabled / disabled</u>                      |

- Added support for **PTP/MTP** Redirection.

[More](#)

|            |                                                                                         |
|------------|-----------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Parallels Client &gt; Parallels Client Global &gt; USB Redirection</b> |
| Parameter  | Enable PTP/MTP Redirection                                                              |
| Registry   | twox.mtp_redirection.mtp_enable                                                         |
| Value      | <u>enabled / disabled</u>                                                               |
| Parameter  | Product ID                                                                              |
| Registry   | twox.mtp_redirection.devicepolicy.product_rule.product                                  |
| Parameter  | Vendor ID                                                                               |
| Registry   | twox.mtp_redirection.devicepolicy.product_rule.vendor                                   |
| Parameter  | Rule                                                                                    |
| Registry   | twox.mtp_redirection.devicepolicy.product_rule.rule                                     |
| Value      | <u>Deny / Allow</u>                                                                     |
| Parameter  | Name                                                                                    |
| Registry   | twox.mtp_redirection.devicepolicy.product_rule.name                                     |
| Value      | Policy Rule                                                                             |
| Parameter  | Automatically redirect all PTP/MTP devices                                              |
| Registry   | twox.mtp_redirection.devicepolicy.redirect_all                                          |



|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

- Added support for **Clipboard** Redirection.

**More**

|            |                                                                                                                         |
|------------|-------------------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Parallels Client &gt; Parallels Client Sessions &gt; Parallels Client Session &gt; Local Resources</b> |
| Parameter  | Connect clipboard                                                                                                       |
| Registry   | sessions.twox.local_resources.connect_clipboard                                                                         |
| Value      | <u>enabled / disabled</u>                                                                                               |

#### VoIP

- Added **VoIP client Ekiga 4.0.1**.

#### Firefox

- Updated **Firefox** to version **52.7.2 ESR**.
- Updated **Adobe Flash Player** download URL to version 29.0.0.113.

#### Network

- Added **TTLS/PAP** and **TTLS/MSCHAPv2** to possible 802.1x authentication methods.
- Improved support for **Sierra EM7305 LTE** device (e.g. in Toshiba Portégé and Fujitsu LIFEBOOK E Series).

The EM7305 comes in various variants, e.g. one with ProductId 9041 and another one with ProductId 9063. The latter comes at least with one or with two USB configuration options. A device with only one configuration option has been observed on a Toshiba Tecra Z-50-D-115 notebook. It only works in MBIM mode and with IGEL firmware, when the device has successfully connected before with the same settings (particularly APN), e.g. under Microsoft Windows 10.

- Added support for **Sierra EM7455 WWAN module**.
- Added support for running the **Huawei E3531i WWAN** device in modem mode (in addition to HiLink mode).
- Added possibility to adopt the **hostname from a DHCP lease** as **permanent** terminal name. The purpose is to use the name received as part of a DHCP lease in future interactions with the DHCP server.

**More**

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Adopt permanent Terminal Name from DHCP lease |
| Registry  | network.dns.hostname_adopt_from_dhcp          |



|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

- **NetworkManager** updated to version **1.2.2**
- **ModemManager** updated to version **1.6.4**
- **usb\_modeswitch** updated to version **2.5.1**

## Open VPN

- Added **Huawei HiLink Mobile Broadband USB** device as possible uplink to OpenVPN sessions.

## OpenConnect VPN

- Added **OpenConnect** client version **7.08** to connect to **Cisco AnyConnect** and **Juniper VPN**. The feature must be enabled.

**More**

|            |                                                                                                  |
|------------|--------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>System &gt; Firmware Customization &gt; Features</b>                                          |
| Parameter  | VPN OpenConnect (Limited support - functionality "as is", see product documentation for details) |
| Registry   | services.unsupported02.enabled                                                                   |
| Value      | <u>enabled / disabled</u>                                                                        |

- The OpenConnect VPN configuration is available at IGEL Setup page **Network > VPN > OpenConnect VPN**.

**More**

|            |                                                                                |
|------------|--------------------------------------------------------------------------------|
| IGEL Setup | <b>Network &gt; VPN &gt; OpenConnect VPN &gt; VPN OpenConnect &gt; Session</b> |
| Parameter  | Gateway                                                                        |
| Registry   | sessions.openconnect.vpnopts.gateway                                           |
| Parameter  | Enable Name/Password Authentication                                            |
| Registry   | sessions.openconnect.vpnopts.enable-name-pwd                                   |
| Value      | <u>enabled / disabled</u>                                                      |
| Parameter  | User Name                                                                      |
| Registry   | sessions.openconnect.vpnopts.username                                          |
| Parameter  | Password                                                                       |



|           |                                                                       |
|-----------|-----------------------------------------------------------------------|
| Registry  | <code>sessions.openconnect.vpnopts.crypt_password</code>              |
| Parameter | CA Certificate                                                        |
| Registry  | <code>sessions.openconnect.vpnopts.ca-cert</code>                     |
| Parameter | User Certificate                                                      |
| Registry  | <code>sessions.openconnect.vpnopts.user-cert</code>                   |
| Parameter | Private Key                                                           |
| Registry  | <code>sessions.openconnect.vpnopts.priv-key</code>                    |
| Parameter | Private Key password                                                  |
| Registry  | <code>sessions.openconnect.vpnopts.priv-key-pwd.crypt_password</code> |
| Parameter | Connect to Juniper Networks VPN                                       |
| Registry  | <code>sessions.openconnect%.vpnopts.is-juniper</code>                 |
| Value     | <u>enabled / disabled</u>                                             |

Tray icon is placed in the panel to disconnect from a running OpenConnect VPN connection.

## Smartcard

- Added **CoolKey PKCS#11** library for access to **Common Access Card (CAC)** smartcards.  
[More](#)

|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Browser &gt; Browser Global &gt; Encryption</b>              |
| Parameter  | Coolkey Security Device                                                       |
| Registry   | <code>browserglobal.security_device.coolkey</code>                            |
| Value      | <u>enabled / disabled</u>                                                     |
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Smartcard</b> |



|            |                                                            |
|------------|------------------------------------------------------------|
| Parameter  | Horizon logon with smartcards supported by Coolkey library |
| Registry   | vmware.view.pkcs11.use_coolkey                             |
| Value      | enabled / <u>disabled</u>                                  |
| IGEL Setup | <b>Security &gt; Smartcard &gt; Middleware</b>             |
| Parameter  | Coolkey                                                    |
| Registry   | scard.pkcs11.use_coolkey                                   |
| Value      | enabled / <u>disabled</u>                                  |

- Updated **Gemalto SafeNet PKCS#11** library to version **10.0.37-0**. This package replaces **Gemalto/ SafeNet eToken** and **Gemalto IDPrime** libraries.  
**Gemalto SafeNet** (formerly **Gemalto/SafeNet eToken**) now handles Gemalto cards and tokens including eToken and IDPrime.  
**Gemalto IDPrime** now handles IDPrime cards and tokens, preferred Common Criteria (CC) cards and tokens in Unlinked Mode.
- Added full integration of **OpenSC PKCS#11** library for access to smartcards.  
[More](#)

|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Browser &gt; Browser Global &gt; Encryption</b>              |
| Parameter  | OpenSC Security Device                                                        |
| Registry   | browserglobal.security_device.opensc                                          |
| Value      | enabled / <u>disabled</u>                                                     |
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Smartcard</b> |
| Parameter  | Horizon logon with smartcards supported by OpenSC library                     |
| Registry   | vmware.view.pkcs11.use_opensc                                                 |
| Value      | enabled / <u>disabled</u>                                                     |
| IGEL Setup | <b>Security &gt; Smartcard &gt; Middleware</b>                                |
| Parameter  | OpenSC                                                                        |



|          |                                      |
|----------|--------------------------------------|
| Registry | <code>scard.pkcs11.use_opensc</code> |
| Value    | <u>enabled</u> / <u>disabled</u>     |

- Updated **MUSCLE CCID** smartcard reader driver to version **1.4.28**.
- Updated **ACS CCID** smartcard reader driver to version **1.1.5**.
- Updated **REINER SCT cyberJack** smartcard reader driver to version **3.99.5final.sp11**.
- Added parameter to disable **Identive CCID** smartcard reader driver. If this driver is disabled, some of the readers are handled by the MUSCLE CCID driver. This can help when problems with Identive reader driver occur.

**More**

|           |                                         |
|-----------|-----------------------------------------|
| Parameter | Identive driver for smart card readers  |
| Registry  | <code>scard.pcscd.identiv_enable</code> |
| Value     | <u>enabled</u> / <u>disabled</u>        |

- Updated **cryptovision sc/interface PKCS#11** library to version **7.0.5.592**.
- New smartcard reader driver for **Fujitsu KB SCR eSIG** version **5.0.24**.

## HID

- Added **layout toggle** feature to on-screen keyboard.

**More**

|            |                                                                   |
|------------|-------------------------------------------------------------------|
| IGEL Setup | <b>Accessories &gt; On-Screen Keyboard &gt; Appearance</b>        |
| Parameter  | Enable switching to alternative layout                            |
| Registry   | <code>userinterface.softkeyboard.enable_alternative_layout</code> |
| Value      | <u>enabled</u> / <u>disabled</u>                                  |

If this is enabled there is a key on the on-screen keyboard for toggling between the normal layout and a reduced layout, that saves space on the screen and has more or less the same features as the number block of an ordinary keyboard with some extensions.

## Base System

- Added support for **UEFI Secure Boot**.

When booted with Secure Boot the downgrade to a firmware version older than 10.04.100 is locked.

- Updated **kernel to version 4.15.15**
- Boot time optimization** (up to 25% faster)



- **Switch power off on USB ports on shutdown and reboot.** The feature can be enabled in IGEL Setup. At the moment only IGEL H830C is supported.

**More**

|            |                               |
|------------|-------------------------------|
| IGEL Setup | <b>System &gt; Registry</b>   |
| Parameter  | Power off on shutdown         |
| Registry   | devices.usb.poweroff_shutdown |
| Value      | enabled / <u>disabled</u>     |

- Added Unit ID in Application Launcher **About > Hardware** section.
- Showing **number of CPU cores** in Application Launcher **About > Hardware** section now.

#### Storage Devices

- Added support for **Mobile Device Access** feature in **Appliance Mode**. The Mobile Device Access tool can be opened via a new icon in the **In-session control bar**. The Mobile Device Access tool can also be started automatically.

**More**

|           |                                 |
|-----------|---------------------------------|
| Parameter | Autostart                       |
| Registry  | sessions.mtp-devices0.autostart |
| Value     | enabled / <u>disabled</u>       |

Mobile Device Access must be enabled at **IGEL Setup > System > Firmware Customization > Features**. Appliance Mode must be enabled at **IGEL Setup > Sessions > Appliance Mode**.

- The **Mobile Device Access tool** is now configurable at **IGEL Setup > Accessories > Mobile Device Access**.
- The **Mobile Device Access tray icon** respects the current theme now.

#### X11 System

- Added support for **XDMCP Appliance Mode**. The XDMCP connection is configurable.

**More**

|            |                                     |
|------------|-------------------------------------|
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b> |
| Parameter  | XDMCP for this Display              |
| Registry   | x.xdmcp0.enabled                    |
| Value      | enabled / <u>disabled</u>           |



|            |                                                               |
|------------|---------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b>                           |
| Parameter  | Connection Type                                               |
| Registry   | x.xdmcp0.server.connectiontype                                |
| Range      | <b>indirect via localhost</b> / indirect / direct / broadcast |
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b>                           |
| Parameter  | Name or IP of server                                          |
| Registry   | x.xdmcp0.server.servername                                    |
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b>                           |
| Parameter  | Enable hotkeys for XDMCP Display                              |
| Registry   | x.xdmcp0.hotkeys.enabled                                      |
| Value      | <u>enabled</u> / disabled                                     |

The default hotkey to open IGEL Setup is: CTRL + ALT + F2. The setup page **User Interface > Display > XDMCP** was removed.

- Added **XC Font Service** support.

#### **More**

|            |                                                               |
|------------|---------------------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
| Parameter  | Enable XC Font Service                                        |
| Registry   | x.xc_fontservice.enabled                                      |
| Value      | enabled / <u>disabled</u>                                     |
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
| Parameter  | XC Font Server                                                |
| Registry   | x.xc_fontservice.fontserver                                   |
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |



|            |                                                               |
|------------|---------------------------------------------------------------|
| Parameter  | Port Number                                                   |
| Registry   | x.xc_fontservice.port                                         |
| Value      | <u>7100</u>                                                   |
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
| Parameter  | Prefer Local Fonts                                            |
| Registry   | x.xc_fontservice.prefer_localfonts                            |
| Value      | <u>enabled / disabled</u>                                     |

- Added **auto detection of monitor refresh rate**. This can be controlled with new parameters.  
[More](#)

|            |                                                  |
|------------|--------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Display &gt; Advanced</b> |
| Parameter  | Detect refresh rate automatically                |
| Registry   | x.xserver0.auto_frequency                        |
| Value      | <u>enabled / disabled</u>                        |

|            |                                                  |
|------------|--------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Display &gt; Advanced</b> |
| Parameter  | Detect refresh rate automatically                |
| Registry   | x.xserver0.screen.auto_frequency                 |
| Value      | <u>enabled / disabled</u>                        |

- Added xorg debug script **/etc/igel/igel\_debug\_tools/xorg-debug.sh** to make collecting Xorg debug data easier (a /tmp/xorg-debug.log file is generated).

## Window Manager

- Added possibility to
  - a) **change the preferred placement mode** and



- b) **modify the threshold value** up to which window size this placement mode should be chosen (otherwise window placement defaults to so called smart mode which tries to minimize overlapping).

#### **More**

|           |                                                                        |
|-----------|------------------------------------------------------------------------|
| Parameter | Preferred Placement                                                    |
| Registry  | windowmanager.wm0.variables.placement_mode                             |
| Value     | At mouse position / <u>Centered</u>                                    |
| Parameter | Maximum window size for which the preferred placement should apply     |
| Registry  | windowmanager.wm0.variables.placement_ratio                            |
| Value     | 0% / 10% / <u>20%</u> / 30% / 40% / 50% / 60% / 70% / 80% / 90% / 100% |

#### Audio

- **Volume** of audio output and input can now be configured up to 150% at **IGEL Setup page Accessories > Sound Preferences > Options**.
- Added a parameter for log level configuration of **Pulseaudio** service.

#### **More**

|           |                                                |
|-----------|------------------------------------------------|
| Parameter | Log level                                      |
| Registry  | multimedia.pulseaudio.daemon.log-level         |
| Range     | debug / info / <u>notice</u> / warning / error |

#### Misc

- An EULA must be accepted now in IGEL setup assistant before finalizing it and using the IGEL OS.

#### Java

- Updated **Oracle JRE to 1.8U162**.

#### Remote Management

- Added **new log file transfer mechanism** for UMS feature **Save TC files for support** (UMS 5.08.110 or higher required). By default, it collects all log files visible in system log viewer, system configuration files group.ini, setup.ini and dhclient lease files. More files can be specified at **IGEL Setup > Accessories > System Log Viewer > Options**. The resulting zip file has now a folder structure.

#### IGEL Cloud Gateway

- Added **UMS structure tag** handling for usage with **ICG agent**.



## Hardware

- Added support for **IGEL UD7-LX 10**.

## Resolved Issues 10.04.100

## Citrix

- Fixed sporadic crashes of the **Citrix USB Daemon**.

## RDP / IGEL RDP Client 2

- Fixed passing **Ctrl+Alt+C keyboard shortcut** to RDP session.
- Fixed **smartcard redirection**: after session reconnection readers and cards were not connected any more in some cases.
- Fixed the **rdpdebugger** to work again (was broken in the previous release).
- Fixed misleading **RDP error message 'Authentication failed'** on wakeup from suspend mode
- Fixed **TCP timeout value** to get more stable **RDP connections** under certain circumstances.

## VMware Horizon

- Fixed bug which prevented **microphone redirection** in Horizon Client RDP sessions.

**More**

| IGEL Setup | <b>Sessions &gt; RDP &gt; RDP Global &gt; Mapping &gt; Audio</b> |
|------------|------------------------------------------------------------------|
| Parameter  | Audio recording                                                  |
| Registry   | rdp.winconnect.rdpai.enable                                      |
| Value      | enabled / <u>disabled</u>                                        |

## RedHat Enterprise Virtualization Client

- Fixed **display corruption** with Windows connections.

## Firefox

- Fixed possibility to **download files in the browser** if needed. The parameter to enable/disable file download is available here.

**More**

| IGEL Setup | <b>Sessions &gt; Browser &gt; Browser Sessions &gt; Window</b> |
|------------|----------------------------------------------------------------|
| Parameter  | Hide local filesystem                                          |
| Registry   | sessions.browser.app.filepicker_dialog_hidden                  |
| Value      | enabled / <u>disabled</u>                                      |



If enabled, the user is not allowed to download or use any save-as functionality from menu, context or keyboard shortcut.

- Fixed bug which **prevented the download using the file dialog** (in the case you open a link to a file of unknown type).
- Fixed **unmounting of the Firefox profile partition during shutdown** - now it is unmounted in a determinate manner after Custom Partition.

#### Network

- Fixed bug: **Network tray icons** sometimes didn't reappear after network restart.
- Fixed bug: **tcpdump debug tool** terminated immediately during boot.
- Fixed issue with **naming of USB ethernet devices**.
- Fixed wrong **LinkMode (10baseT/Half)** with autonegotiation and some USB ethernet devices.

#### AppliDis

- Changed default value of **PasswordMode** from **cmdline** to **prompt** as suggested by Systancia.

#### Smartcard

- Fixed driver for **Elatec RFID readers**. Before this fix the readers sometimes were not available after boot.
- Fixed VMware Horizon logon with OpenSC smartcards.

#### CUPS Printing

- Fixed bug where the **user for printjobs** was not set to the **domain user**.

#### Base System

- Fixed **Kerberos password change** to work also with transport protocol **TCP**. To force protocol TCP, prepend Domain Controllers with prefix "tcp/", e.g. "tcp/dc.example.com".
- Fixed **occasional desktop hang** in the local login or the network login mask after successful authentication.
- Fixed **password expiry notification** showing negative expiry period.
- Fixed **update to connect to SFTP** servers with very restrictive key exchange settings.
- Fixed input of the **reset key in reset to defaults boot**, if the administrator password is not available anymore. If more than 255 characters were entered in the 1st try, it was not possible to enter the reset key for a 2nd or 3rd time.
- Fixed **Active Directory logon with smartcard**: If the smartcard contains logon certificates for multiple users, it is possible to switch between these certificates and log on with the chosen certificate now.
- Fixed missing names for some **partitions** in update notification when having a user interface **language other than English**.
- Fixed problems with **never ending bootcode** update with some EFI BIOS variants.
- Fixed **ssh server port** configuration.
- Fixed **signotec signature pad** channel for Citrix.
- Increased stability of **signotec VCOM Daemon**.
- Remove residual information belonging to a **removed content from a custom partition**.
- Fixed **crash of xfce4-power-manager** after adding or removing input devices.

#### Custom Partition



- Fixed **automatic update of custom partition** - if download source isn't accessible then the content of the custom partition got lost.

#### Appliance Mode

- Fixed post session command **Logoff** in Appliance Mode.

#### X11 System

- Fixed **Elo-USB Touchscreen functionality** after reboot.
- Fixed **DisplayLink USB Support on UD3 LX50**.
- Fixed issue with **two monitors connected via DVI-D to HDMI adapter on a UD3 M330 (VIA)**.  
Added registry key to disable the new HDMI autodetection.

##### **More**

|           |                                             |
|-----------|---------------------------------------------|
| Parameter | Autodetect if DVI to HDMI adapter is in use |
| Registry  | x.drivers.via.autodetect_hdmi_output        |
| Value     | <u>enabled</u> / disabled                   |

- Fixed **wrong automatic resolution detection** if monitor does not have a preferred mode.
- Fixed **sporadic display corruptions** after monitors leaving the power saving mode.
- Improved handling of more than 2 screens.

#### Shadowing/VNC

- Fixed **sporadic VNC server crash**.

#### Audio

- Fixed **volume control of internal speaker in HP T610**.
- Fixed **automatic switch to output** over analog headphones.
- Non existing **S/PDIF inputs and outputs in Plantronics and Jabra USB headsets** are now ignored by audio subsystem (Pulseaudio).
- Added workaround in the kernel USB audio driver for **volume control on Sennheiser USB headsets**.

#### Remote Management

- Fixed **calculation of Unit ID for UMS management**. In some cases, it could happen that the MAC address of wrong network interface was chosen.
- Fixed **IGEL Setup Assistant** to get stopped when settings were received from UMS.

### 7.30.3 IGEL Universal Desktop Converter (UDC3) 10.04.100

#### Supported Hardware:

[Third-Party Devices Supported by IGEL OS 10<sup>461</sup>](#)

---

<sup>461</sup> <https://kb.igel.com/display/hardware/Third+Party+Devices+Supported+by+IGEL+OS+10>



- Versions for Release 10.04.100(see page 2311)
- New Features 10.04.100(see page 2312)

## Versions for Release 10.04.100

### • Clients

| Product    | Version   |
|------------|-----------|
| Oracle JRE | 1.8.0_162 |

### • System Components

|                                         |                            |
|-----------------------------------------|----------------------------|
| Bluetooth stack (bluez)                 | 5.46-0ubuntu3              |
| MESA OpenGL stack                       | 17.2.8-0igel3              |
| VAAPI ABI Version                       | 0.40                       |
| Graphics Driver INTEL                   | 2.99.917+git20180214-igel1 |
| Graphics Driver ATI/RADEON              | 7.10.0-2igel3              |
| Graphics Driver ATI/AMDGPU              | 1.4.0-2igel3               |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.15-2                   |
| Graphics Driver Vboxvideo               | 5.2.6-dfsg-2               |
| Graphics Driver VMware                  | 13.2.1-1build1             |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1              |
| Graphics Driver FBDEV                   | 0.4.4-1build5              |
| Graphics Driver VESA                    | 2.3.4-1build2              |
| Input Driver Evdev                      | 2.10.5-1ubuntu1            |
| Input Driver Elographics                | 1.4.1-1build5              |
| Input Driver Synaptics                  | 1.9.0-1ubuntu1             |



|                                 |                              |
|---------------------------------|------------------------------|
| Input Driver Vmmouse            | 13.1.0-1ubuntu2              |
| Input Driver Wacom              | 0.34.0-0ubuntu2              |
| Kernel                          | 4.15.15 #mainline-udos-r2141 |
| Xorg X11 Server                 | 1.19.6-2igel1                |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1            |
| XFCE4 Windowmanager             | 4.12.3-1ubuntu2              |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.7            |

#### Security Fixes

- Added support for UEFI Secure Boot.

When booted with Secure Boot the downgrade to a firmware version older than 10.04.100 is locked.

#### New Features 10.04.100

##### Citrix Receiver 13

- Integrated **Citrix Receiver 13.8.0**.  
**More**

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Use Citrix Cloud with receiver 13.8 or newer |
| Registry  | ica.cloudconnect                             |
| Value     | enabled / <u>disabled</u>                    |

- Support for **Azure** Active Directory (Azure AD) authentication
- Support for **Workspace** configuration from Citrix Cloud
- Integrated **Citrix Receiver 13.4.2**. Citrix Receiver version 13.5.0 was removed. Available Citrix Receiver versions: 13.3.2, 13.4.2, 13.7.0, 13.8.0 (default)
- Updated **Citrix HDX RTME** used for optimization of Skype for Business to 2.4.0.

##### RDP / IGEL RDP Client 2

- Added possibility to use **RDP local logon** for smartcard login. This can be activated in the setup.  
**More**



|           |                                          |
|-----------|------------------------------------------|
| Parameter | Enable smartcard support for local logon |
| Registry  | rdp.login.smartcard-local-logon          |
| Value     | enabled / <u>disabled</u>                |

By enabling this parameter local logon can be used for smartcard authentication. If **Username** is left empty the connection to the RDP server will be made without sending credentials, so you can choose **Smartcard** as login method in the microsoft login window . However this will not work with **NLA**.

- Added support for CredSSP up to version 6.

#### VMware Horizon

- Updated **VMware Horizon Client** to version **4.7.0-7395152**.
- Added key to enable **seamless window mode** in each application session.

**More**

|           |                                                    |
|-----------|----------------------------------------------------|
| Parameter | Seamless Application Windows                       |
| Registry  | sessions.vdm_client.options.enable_seamless_window |
| Value     | enabled / <u>disabled</u>                          |

- Added possibility to use **Fabulatech USB Redirection** in a Horizon Client PCoIP session.

**More**

|            |                                                                                                |
|------------|------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Fabulatech USB Redirection</b> |
| Parameter  | Enable Fabulatech USB Redirection                                                              |
| Registry   | vmware.view.usb.enable-fabulatech-usb                                                          |
| Value      | enabled / <u>disabled</u>                                                                      |

#### Parallels Client

- Integrated **Parallels Client** version **16.2.0 (19039)**
- Added support for USB Redirection, configurable at new IGEL Setup page **Sessions > Parallels Client > Parallels Client Global > USB Redirection**.

**More**

|            |                                                                                         |
|------------|-----------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Parallels Client &gt; Parallels Client Global &gt; USB Redirection</b> |
| Parameter  | Enable USB Redirection                                                                  |



|           |                                                                     |
|-----------|---------------------------------------------------------------------|
| Registry  | <code>twox.usb_redirection.usb_enable</code>                        |
| Value     | <u>enabled</u> / <u>disabled</u>                                    |
| Parameter | Product ID                                                          |
| Registry  | <code>twox.usb_redirection.devicepolicy.product_rule.product</code> |
| Parameter | Vendor ID                                                           |
| Registry  | <code>twox.usb_redirection.devicepolicy.product_rule.vendor</code>  |
| Parameter | Rule                                                                |
| Registry  | <code>twox.usb_redirection.devicepolicy.product_rule.rule</code>    |
| Value     | <u>Deny</u> / <u>Allow</u>                                          |
| Parameter | Name                                                                |
| Registry  | <code>twox.usb_redirection.devicepolicy.product_rule.name</code>    |
| Value     | Policy Rule                                                         |
| Parameter | Automatically redirect all USB devices                              |
| Registry  | <code>twox.usb_redirection.devicepolicy.redirect_all</code>         |
| Value     | <u>enabled</u> / <u>disabled</u>                                    |

- Added support for **PTP/MTP** Redirection.

**More**

|            |                                                                                         |
|------------|-----------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Parallels Client &gt; Parallels Client Global &gt; USB Redirection</b> |
| Parameter  | Enable PTP/MTP Redirection                                                              |
| Registry   | <code>twox.mtp_redirection.mtp_enable</code>                                            |
| Value      | <u>enabled</u> / <u>disabled</u>                                                        |
| Parameter  | Product ID                                                                              |



|           |                                                                     |
|-----------|---------------------------------------------------------------------|
| Registry  | <code>twox.mtp_redirection.devicepolicy.product_rule.product</code> |
| Parameter | Vendor ID                                                           |
| Registry  | <code>twox.mtp_redirection.devicepolicy.product_rule.vendor</code>  |
| Parameter | Rule                                                                |
| Registry  | <code>twox.mtp_redirection.devicepolicy.product_rule.rule</code>    |
| Value     | <u>Deny / Allow</u>                                                 |
| Parameter | Name                                                                |
| Registry  | <code>twox.mtp_redirection.devicepolicy.product_rule.name</code>    |
| Value     | Policy Rule                                                         |
| Parameter | Automatically redirect all PTP/MTP devices                          |
| Registry  | <code>twox.mtp_redirection.devicepolicy.redirect_all</code>         |
| Value     | <u>enabled / disabled</u>                                           |

- Added support for **Clipboard** Redirection.

**More**

|            |                                                                                                                         |
|------------|-------------------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Parallels Client &gt; Parallels Client Sessions &gt; Parallels Client Session &gt; Local Resources</b> |
| Parameter  | Connect clipboard                                                                                                       |
| Registry   | <code>sessions.twox.local_resources.connect_clipboard</code>                                                            |
| Value      | <u>enabled / disabled</u>                                                                                               |

## VoIP

- Added **VoIP client Ekiga 4.0.1**.

## Firefox

- Updated **Firefox** to version **52.7.2 ESR**.
- Updated **Adobe Flash Player** download URL to version 29.0.0.113.

## Network



- Added **TTLS/PAP** and **TTLS/MSCHAPv2** to possible 802.1x authentication methods.
- Improved support for **Sierra EM7305 LTE** device (e.g. in Toshiba Portégé and Fujitsu LIFEBOOK E Series).

The EM7305 comes in various variants, e.g. one with ProductId 9041 and another one with ProductId 9063. The latter comes at least with one or with two USB configuration options. A device with only one configuration option has been observed on a Toshiba Tecra Z-50-D-115 notebook. It only works in MBIM mode and with IGEL firmware, when the device has successfully connected before with the same settings (particularly APN), e.g. under Microsoft Windows 10.

- Added support for **Sierra EM7455 WWAN module**.
- Added support for running the **Huawei E3531i WWAN** device in modem mode (in addition to HiLink mode).
- Added possibility to adopt the **hostname from a DHCP lease** as **permanent** terminal name. The purpose is to use the name received as part of a DHCP lease in future interactions with the DHCP server.

#### More

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Adopt permanent Terminal Name from DHCP lease |
| Registry  | network.dns.hostname_adopt_from_dhcp          |
| Value     | enabled / <u>disabled</u>                     |

- NetworkManager** updated to version **1.2.2**
- ModemManager** updated to version **1.6.4**
- usb\_modeswitch** updated to version **2.5.1**

#### Open VPN

- Added **Huawei HiLink Mobile Broadband USB** device as possible uplink to OpenVPN sessions.

#### OpenConnect VPN

- Added **OpenConnect** client version **7.08** to connect to **Cisco AnyConnect** and **Juniper VPN**. The feature must be enabled.

#### More

|            |                                                                                                  |
|------------|--------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>System &gt; Firmware Customization &gt; Features</b>                                          |
| Parameter  | VPN OpenConnect (Limited support - functionality "as is", see product documentation for details) |
| Registry   | services.unsupported02.enabled                                                                   |
| Value      | enabled / <u>disabled</u>                                                                        |



- The OpenConnect VPN configuration is available at IGEL Setup page **Network > VPN > OpenConnect VPN**.

[More](#)

| IGEL Setup | <b>Network &gt; VPN &gt; OpenConnect VPN &gt; VPN OpenConnect &gt; Session</b> |
|------------|--------------------------------------------------------------------------------|
| Parameter  | Gateway                                                                        |
| Registry   | sessions.openconnect.vpnopts.gateway                                           |
| Parameter  | Enable Name/Password Authentication                                            |
| Registry   | sessions.openconnect.vpnopts.enable-name-pwd                                   |
| Value      | enabled / <u>disabled</u>                                                      |
| Parameter  | User Name                                                                      |
| Registry   | sessions.openconnect.vpnopts.username                                          |
| Parameter  | Password                                                                       |
| Registry   | sessions.openconnect.vpnopts.crypt_password                                    |
| Parameter  | CA Certificate                                                                 |
| Registry   | sessions.openconnect.vpnopts.ca-cert                                           |
| Parameter  | User Certificate                                                               |
| Registry   | sessions.openconnect.vpnopts.user-cert                                         |
| Parameter  | Private Key                                                                    |
| Registry   | sessions.openconnect.vpnopts.priv-key                                          |
| Parameter  | Private Key password                                                           |
| Registry   | sessions.openconnect.vpnopts.priv-key-pwd.crypt_password                       |
| Parameter  | Connect to Juniper Networks VPN                                                |



|          |                                                       |
|----------|-------------------------------------------------------|
| Registry | <code>sessions.openconnect%.vpnopts.is-juniper</code> |
| Value    | enabled / <u>disabled</u>                             |

Tray icon is placed in the panel to disconnect from a running OpenConnect VPN connection.

## Smartcard

- Added **CoolKey PKCS#11** library for access to **Common Access Card (CAC)** smartcards.  
[More](#)

|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Browser &gt; Browser Global &gt; Encryption</b>              |
| Parameter  | Coolkey Security Device                                                       |
| Registry   | <code>browserglobal.security_device.coolkey</code>                            |
| Value      | enabled / <u>disabled</u>                                                     |
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Smartcard</b> |
| Parameter  | Horizon logon with smartcards supported by Coolkey library                    |
| Registry   | <code>vmware.view.pkcs11.use_coolkey</code>                                   |
| Value      | enabled / <u>disabled</u>                                                     |
| IGEL Setup | <b>Security &gt; Smartcard &gt; Middleware</b>                                |
| Parameter  | Coolkey                                                                       |
| Registry   | <code>scard.pkcs11.use_coolkey</code>                                         |
| Value      | enabled / <u>disabled</u>                                                     |

- Updated **Gemalto SafeNet PKCS#11** library to version **10.0.37-0**. This package replaces **Gemalto/ SafeNet eToken** and **Gemalto IDPrime** libraries.  
**Gemalto SafeNet** (formerly **Gemalto/SafeNet eToken**) now handles Gemalto cards and tokens including eToken and IDPrime.  
**Gemalto IDPrime** now handles IDPrime cards and tokens, preferred Common Criteria (CC) cards and tokens in Unlinked Mode.
- Added full integration of **OpenSC PKCS#11** library for access to smartcards.

**More**

|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Browser &gt; Browser Global &gt; Encryption</b>              |
| Parameter  | OpenSC Security Device                                                        |
| Registry   | browserglobal.security_device.opensc                                          |
| Value      | enabled / <u>disabled</u>                                                     |
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Smartcard</b> |
| Parameter  | Horizon logon with smartcards supported by OpenSC library                     |
| Registry   | vmware.view.pkcs11.use_opensc                                                 |
| Value      | enabled / <u>disabled</u>                                                     |
| IGEL Setup | <b>Security &gt; Smartcard &gt; Middleware</b>                                |
| Parameter  | OpenSC                                                                        |
| Registry   | scard.pkcs11.use_opensc                                                       |
| Value      | enabled / <u>disabled</u>                                                     |

- Updated **MUSCLE CCID** smartcard reader driver to version **1.4.28**.
- Updated **ACS CCID** smartcard reader driver to version **1.1.5**.
- Updated **REINER SCT cyberJack** smartcard reader driver to version **3.99.5final.sp11**.
- Added parameter to disable **Identive CCID** smartcard reader driver. If this driver is disabled, some of the readers are handled by the MUSCLE CCID driver. This can help when problems with Identive reader driver occur.

**More**

|           |                                        |
|-----------|----------------------------------------|
| Parameter | Identive driver for smart card readers |
| Registry  | scard.pcscd.identiv_enable             |
| Value     | <u>enabled</u> / disabled              |

- Updated **cryptovision sc/interface PKCS#11** library to version **7.0.5.592**.
- New smartcard reader driver for **Fujitsu KB SCR eSIG** version **5.0.24**.



- Added **layout toggle** feature to on-screen keyboard.

[More](#)

|            |                                                            |
|------------|------------------------------------------------------------|
| IGEL Setup | <b>Accessories &gt; On-Screen Keyboard &gt; Appearance</b> |
| Parameter  | Enable switching to alternative layout                     |
| Registry   | userinterface.softkeyboard.enable_alternative_layout       |
| Value      | <u>enabled</u> / <u>disabled</u>                           |

If this is enabled there is a key on the on-screen keyboard for toggling between the normal layout and a reduced layout, that saves space on the screen and has more or less the same features as the number block of an ordinary keyboard with some extensions.

## Base System

- Added support for **UEFI Secure Boot**.

When booted with Secure Boot the downgrade to a firmware version older than 10.04.100 is locked.

- Updated **kernel to version 4.15.15**
- Boot time optimization** (up to 25% faster)
- Switch power off on USB ports on shutdown and reboot**. The feature can be enabled in IGEL Setup. At the moment only IGEL H830C is supported.

[More](#)

|            |                                  |
|------------|----------------------------------|
| IGEL Setup | <b>System &gt; Registry</b>      |
| Parameter  | Power off on shutdown            |
| Registry   | devices.usb.poweroff_shutdown    |
| Value      | <u>enabled</u> / <u>disabled</u> |

- Added Unit ID in Application Launcher **About > Hardware** section.
- Showing **number of CPU cores** in Application Launcher **About > Hardware** section now.

## Storage Devices

- Added support for **Mobile Device Access** feature in **Appliance Mode**. The Mobile Device Access tool can be opened via a new icon in the **In-session control bar**. The Mobile Device Access tool can also be started automatically.

[More](#)

|           |           |
|-----------|-----------|
| Parameter | Autostart |
|-----------|-----------|



|          |                                              |
|----------|----------------------------------------------|
| Registry | <code>sessions.mtp-devices0.autostart</code> |
| Value    | enabled / <u>disabled</u>                    |

Mobile Device Access must be enabled at **IGEL Setup > System > Firmware Customization > Features**. Appliance Mode must be enabled at **IGEL Setup > Sessions > Appliance Mode**.

- The **Mobile Device Access tool** is now configurable at **IGEL Setup > Accessories > Mobile Device Access**.
- The **Mobile Device Access tray icon** respects the current theme now.

#### X11 System

- Added support for **XDMCP Appliance Mode**. The XDMCP connection is configurable.  
[More](#)

|            |                                                               |
|------------|---------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b>                           |
| Parameter  | XDMCP for this Display                                        |
| Registry   | <code>x.xdmcp0.enabled</code>                                 |
| Value      | enabled / <u>disabled</u>                                     |
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b>                           |
| Parameter  | Connection Type                                               |
| Registry   | <code>x.xdmcp0.server.connectiontype</code>                   |
| Range      | <b>indirect via localhost</b> / indirect / direct / broadcast |
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b>                           |
| Parameter  | Name or IP of server                                          |
| Registry   | <code>x.xdmcp0.server.servername</code>                       |
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b>                           |
| Parameter  | Enable hotkeys for XDMCP Display                              |
| Registry   | <code>x.xdmcp0.hotkeys.enabled</code>                         |



|       |                           |
|-------|---------------------------|
| Value | <u>enabled</u> / disabled |
|-------|---------------------------|

The default hotkey to open IGEL Setup is: CTRL + ALT + F2. The setup page **User Interface > Display > XDMCP** was removed.

- Added **XC Font Service** support.

[More](#)

|            |                                                               |
|------------|---------------------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
|------------|---------------------------------------------------------------|

|           |                        |
|-----------|------------------------|
| Parameter | Enable XC Font Service |
|-----------|------------------------|

|          |                          |
|----------|--------------------------|
| Registry | x.xc_fontservice.enabled |
|----------|--------------------------|

|       |                                  |
|-------|----------------------------------|
| Value | <u>enabled</u> / <u>disabled</u> |
|-------|----------------------------------|

|            |                                                               |
|------------|---------------------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
|------------|---------------------------------------------------------------|

|           |                |
|-----------|----------------|
| Parameter | XC Font Server |
|-----------|----------------|

|          |                             |
|----------|-----------------------------|
| Registry | x.xc_fontservice.fontserver |
|----------|-----------------------------|

|            |                                                               |
|------------|---------------------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
|------------|---------------------------------------------------------------|

|           |             |
|-----------|-------------|
| Parameter | Port Number |
|-----------|-------------|

|          |                       |
|----------|-----------------------|
| Registry | x.xc_fontservice.port |
|----------|-----------------------|

|       |             |
|-------|-------------|
| Value | <u>7100</u> |
|-------|-------------|

|            |                                                               |
|------------|---------------------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
|------------|---------------------------------------------------------------|

|           |                    |
|-----------|--------------------|
| Parameter | Prefer Local Fonts |
|-----------|--------------------|

|          |                                    |
|----------|------------------------------------|
| Registry | x.xc_fontservice.prefer_localfonts |
|----------|------------------------------------|

|       |                                  |
|-------|----------------------------------|
| Value | <u>enabled</u> / <u>disabled</u> |
|-------|----------------------------------|

- Added **auto detection of monitor refresh rate**. This can be controlled with new parameters.

[More](#)

|            |                                                  |
|------------|--------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Display &gt; Advanced</b> |
|------------|--------------------------------------------------|

|           |                                   |
|-----------|-----------------------------------|
| Parameter | Detect refresh rate automatically |
|-----------|-----------------------------------|



|          |                           |
|----------|---------------------------|
| Registry | x.xserver0.auto_frequency |
| Value    | <u>enabled</u> / disabled |

|            |                                                  |
|------------|--------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Display &gt; Advanced</b> |
| Parameter  | Detect refresh rate automatically                |
| Registry   | x.xserver0.screen.auto_frequency                 |
| Value      | <u>enabled</u> / disabled                        |

- Added xorg debug script **/etc/igel/igel\_debug\_tools/xorg-debug.sh** to make collecting Xorg debug data easier (a /tmp/xorg-debug.log file is generated).

#### Window Manager

- Added possibility to
  - a) **change the preferred placement mode** and
  - b) **modify the threshold value** up to which window size this placement mode should be chosen (otherwise window placement defaults to so called smart mode which tries to minimize overlapping).

#### More

|           |                                                                        |
|-----------|------------------------------------------------------------------------|
| Parameter | Preferred Placement                                                    |
| Registry  | windowmanager.wm0.variables.placement_mode                             |
| Value     | At mouse position / <u>Centered</u>                                    |
| Parameter | Maximum window size for which the preferred placement should apply     |
| Registry  | windowmanager.wm0.variables.placement_ratio                            |
| Value     | 0% / 10% / <u>20%</u> / 30% / 40% / 50% / 60% / 70% / 80% / 90% / 100% |

#### Audio

- Volume** of audio output and input can now be configured up to 150% at **IGEL Setup page Accessories > Sound Preferences > Options**.
- Added a parameter for log level configuration of **Pulseaudio** service.

#### More



|           |                                                |
|-----------|------------------------------------------------|
| Parameter | Log level                                      |
| Registry  | multimedia.pulseaudio.daemon.log-level         |
| Range     | debug / info / <u>notice</u> / warning / error |

## Misc

- An EULA must be accepted now in IGEL setup assistant before finalizing it and using the IGEL OS.

## Java

- Updated **Oracle JRE to 1.8U162**.

## Remote Management

- Added **new log file transfer mechanism** for UMS feature **Save TC files for support** (UMS 5.08.110 or higher required). By default, it collects all log files visible in system log viewer, system configuration files group.ini, setup.ini and dhclient lease files. More files can be specified at **IGEL Setup > Accessories > System Log Viewer > Options**. The resulting zip file has now a folder structure.

## IGEL Cloud Gateway

- Added **UMS structure tag** handling for usage with **ICG agent**.

## Hardware

- Added support for **IGEL UD7-LX 10**.

## 7.31 Notes for Release 10.03.570

|                |            |              |
|----------------|------------|--------------|
| Software:      | Version    | 10.03.570    |
| Release Date:  | 2018-02-01 |              |
| Release Notes: | Version    | RN-1003570-1 |
| Last update:   | 2018-02-05 |              |

- 
- IGEL Universal Desktop LX / IGEL Zero 10.03.570(see page 2325)
  - IGEL Universal Desktop OS 3 / IGEL UD Pocket 10.03.570(see page 2332)



### 7.31.1 IGEL Universal Desktop LX / IGEL Zero 10.03.570

#### Supported Devices

##### Universal Desktop:

|          |                                                  |
|----------|--------------------------------------------------|
| UD2-LX:  | UD2-LX 40                                        |
| UD3-LX:  | UD3-LX 50<br>UD3-LX 42<br>UD3-LX 41<br>UD3-LX 40 |
| UD5-LX:  | UD5-LX 50<br>UD5-LX 40                           |
| UD6-LX:  | UD6-LX 51                                        |
| UD9-LX:  | UD9-LX Touch 41<br>UD9-LX 40                     |
| UD10-LX: | UD10-LX Touch 10<br>UD10-LX 10                   |

##### IGEL Zero:

|             |
|-------------|
| IZ2-RFX     |
| IZ2-HDX     |
| IZ2-HORIZON |
| IZ3-RFX     |
| IZ3-HDX     |



## IZ3-HORIZON

- [Versions for Release 10.03.570](#)(see page 2326)
- [Security Fixes 10.03.570](#)(see page 2329)
- [General Information 10.03.570](#)(see page 2330)
- [Known Issues 10.03.570](#)(see page 2331)

## Versions for Release 10.03.570

• **Clients**

| <b>Product</b>                     | <b>Version</b>                |
|------------------------------------|-------------------------------|
| Citrix HDX Realtime Media Engine   | 2.3.0-1075                    |
| Citrix Receiver                    | 13.3.2.366713                 |
| Citrix Receiver                    | 13.5.0.10185126               |
| Citrix Receiver                    | 13.7.0.10276927               |
| deviceTRUST Citrix Channel         | 17.2.100.0                    |
| deviceTRUST RDP Channel            | 17.2.100.0                    |
| Ericom PowerTerm                   | 12.0.1.0.20170219.2-dev-34574 |
| Evidian AuthMgr                    | 1.5.6362                      |
| Evince PDF Viewer                  | 3.18.2-1ubuntu4.2             |
| FabulaTech USB for Remote Desktop  | 5.2.23                        |
| Firefox                            | 52.5.0                        |
| IBM iAccess Client Solutions       | 1.1.5.0                       |
| IGEL RDP Client                    | 2.2                           |
| Imprivata OneSign ProveID Embedded |                               |
| Leostream Java Connect             | 3.3.7.0                       |



|                                                             |                   |
|-------------------------------------------------------------|-------------------|
| NX Client                                                   | 5.3.12            |
| Open VPN                                                    | 2.3.10-1ubuntu2.1 |
| Oracle JRE                                                  | 1.8.0_152         |
| Parallels 2X Client                                         | 16.2.0.19039      |
| Remote Viewer for RedHat Enterprise Virtualization Desktops | 7.0               |
| Systancia AppliDis                                          | 4.0.0.17          |
| Thinlinc Client                                             | 4.8.0-5456        |
| ThinPrint Client                                            | 7.5.83            |
| Totem Media Player                                          | 2.30.2            |
| VMware Horizon Client                                       | 4.6.0-6617224     |

- **Dictation**

|                                                       |          |
|-------------------------------------------------------|----------|
| Diktamen driver for dictation                         |          |
| Driver for Grundig Business Systems dictation devices |          |
| Nuance Audio Extensions for dictation                 | B048     |
| Olympus driver for dictation                          | 20161103 |
| Philips Speech Driver                                 | 12.5.4   |

- **Signature**

|                         |       |
|-------------------------|-------|
| signotec Citrix Channel | 8.0.6 |
| signotec VCOM Daemon    | 2.0.0 |
| StepOver TCP Client     | 2.1.0 |

- **Smartcard**

|                                |         |
|--------------------------------|---------|
| PKCS#11 Library A.E.T SafeSign | 3.0.101 |
|--------------------------------|---------|



|                                               |                  |
|-----------------------------------------------|------------------|
| PKCS#11 Library Athena IDProtect              | 623.07           |
| PKCS#11 Library cryptovision sc/interface     | 6.6.3.502        |
| PKCS#11 Library Gemalto IDPrime               | 1.2.3            |
| PKCS#11 Library SecMaker NetID                | 6.6.0.30         |
| Reader Driver ACS CCID                        | 1.1.3            |
| Reader Driver Gemalto eToken                  | 9.0.43           |
| Reader Driver HID Global Omnikey CCID         | 4.2.4            |
| Reader Driver Identiv / SCM Microsystems CCID | 5.0.35           |
| Reader Driver Identiv eHealth200              | 1.0.5            |
| Reader Driver MUSCLE CCID                     | 1.4.27           |
| Reader Driver REINER SCT cyberJack            | 3.99.5final.SP09 |
| Resource Manager PC/SC Lite                   | 1.8.22           |
| Cherry USB2LAN Proxy                          | 3.0.0.4          |

- **System Components**

|                            |                                |
|----------------------------|--------------------------------|
| Bluetooth stack (bluez)    | 5.46-0ubuntu3                  |
| MESA OpenGL stack          | 17.2.2-0ubuntu1                |
| VAAPI ABI Version          | 0.40                           |
| VDPAU Library version      | 1.1.1-3ubuntu1                 |
| Graphics Driver INTEL      | 2.99.917+git20171109-igel      |
| Graphics Driver ATI/RADEON | 7.10.0-1                       |
| Graphics Driver ATI/AMDGPU | 1.4.0-1                        |
| Graphics Driver VIA        | 5.76.52.92-009-005f78-20150730 |



|                                 |                         |
|---------------------------------|-------------------------|
| Graphics Driver FBDEV           | 0.4.4-1build5           |
| Graphics Driver VESA            | 2.3.4-1build2           |
| Input Driver Evdev              | 2.10.5-1ubuntu1         |
| Input Driver Elographics        | 1.4.1-1build5           |
| Input Driver eGalax             | 2.5.5814                |
| Input Driver Synaptics          | 1.9.0-1ubuntu1          |
| Input Driver Vmmouse            | 13.1.0-1ubuntu2         |
| Input Driver Wacom              | 0.34.0-0ubuntu2         |
| Kernel                          | 4.10.17 #43.47-ud-r1949 |
| Xorg X11 Server                 | 1.19.5-0ubuntu2         |
| CUPS printing daemon            | 2.1.3-4ubuntu0.3        |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1       |
| XFCE4 Windowmanager             | 4.12.3-1ubuntu2         |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.7       |
| NetworkManager                  | 1.2.0-0ubuntu0.16.04.3  |
| ModemManager                    | 1.4.12-1ubuntu1         |
| GStreamer                       | 0.10.36-2ubuntu0.1      |

- **Features with Limited IGEL Support**

|                          |  |
|--------------------------|--|
| Mobile Device Access USB |  |
|--------------------------|--|

## Security Fixes 10.03.570

- Fixed kernel security issues CVE-2017-16939, CVE-2017-12192, CVE-2017-1000370, CVE-2017-1000371, CVE-2017-12190, CVE-2017-15274, CVE-2017-14156, CVE-2017-14140,



CVE-2017-15115, CVE-2017-14489, CVE-2017-12153, CVE-2017-16525, CVE-2017-7542 and CVE-2017-8824.

- Removed Intel Spectre microcode updates due to various issues with them. (Intel officially withdrew the microcode updates.)
- Fixed kernel security issues CVE-2017-1000405 (aka Huge Dirty Cow).
- Fixed Intel meltdown problem CVE-2017-5754 with Kernel Page Table Isolation (KPTI) Patch

## General Information 10.03.570

The following clients and features are not supported anymore in version 10.03.570:

- Citrix Receiver 12.1 and 13.1
- Citrix Access Gateway Standard Plug-in
- Dell vWorkspace Connector for Linux
- Ericom PowerTerm Emulation 9 and 11
- Ericom Webconnect
- IGEL Legacy RDP Client (rdesktop)
- Virtual Bridges VERDE Client
- PPTP VPN Support
- IGEL Upgrade License Tool with IGEL Smartcard Token
- Remote Management by setup.ini file transfer (TFTP)
- XC Font Service
- Remote Access via RSH
- Legacy Philips Speech Driver
- Digital Persona Support
- Sane Scanner Support
- Softpro/Kofax Citrix Virtual Channel
- t-Systems TCOS Smartcard Support
- DUS Series touch screens
- Elo serial touch screens
- IGEL Smartcard without locking desktop
- Video Hardware Acceleration Support is discontinued on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, UD10-LX 10
- H.264 Hardware Acceleration Support is discontinued on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, UD10-LX 10
- Storage Hotplug devices are not automatically removed anymore, instead they must be always ejected manually:
  - by panel tray icon
  - by an icon in the 'In-Session Control Bar' (configurable at IGEL Setup > User Interface > Desktop )
  - by a 'Safely Remove Hardware' session (configurable at IGEL Setup > Accessories )

The following clients and features are not available in release 10.03.570:

- Voip Client Ekiga



- X session (Xorg Xephyr)
- XDMCP
- Cherry eGK Channel
- Open VPN Smartcard Support
- NCP Secure Client
- Asian Input Methods
- Composite Manager

## Known Issues 10.03.570

### Citrix Receiver 13

- With Citrix Receiver 13.5 print problems in legacy sessions can occur.

### VMware Horizon

- External drives mounted already before connection, do not appear in the remote desktop.  
Workaround: map the directory /media as a drive in your desktop. Then the external devices will show up inside the media drive.
- Client drive mapping and USB redirection for storage devices should not be enabled both at the same time.
  - On the one hand, if you want to use USB redirection for your storage devices: Note that the USB on-insertion feature is only working if the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in:  
Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping  
. It is also recommended to disable local Storage Hotplug: On page Devices > Storage Devices > Storage Hotplug , put number of storage hotplug devices to 0.
  - On the other hand, if you use drive mapping instead, it is recommended that you should either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. And because Horizon Client relies on the OS to mount the storage devices itself, please go to setup page:  
Devices > Storage Devices > Storage Hotplug and switch on 'Enable dynamic drive mapping' and put 'Number of storage hotplug devices' to at least 1.

### Firefox

- Support for the gstreamer framework was dropped by recent Firefox versions. Therefore support for H264 decoding in the browser is not possible anymore, due to licensing restrictions.
- After firmware update, a fullscreen browser session starts onetime in window mode. Afterwards the fullscreen mode is functional again.

### Audio

- Headphone jack detection doesn't properly work on IGEL UD3 (M330C and M340C). The audio controlling system is unable to notice status change of the audio jack.



## 7.31.2 IGEL Universal Desktop OS 3 / IGEL UD Pocket 10.03.570

- [Versions for Release 10.03.570](#)(see page 2332)
- [Security Fixes 10.03.570](#)(see page 2336)
- [General Information 10.03.570](#)(see page 2336)
- [Known Issues 10.03.570](#)(see page 2337)

### Versions for Release 10.03.570

- **Clients**

| <b>Product</b>                     | <b>Version</b>                |
|------------------------------------|-------------------------------|
| Citrix HDX Realtime Media Engine   | 2.3.0-1075                    |
| Citrix Receiver                    | 13.3.2.366713                 |
| Citrix Receiver                    | 13.5.0.10185126               |
| Citrix Receiver                    | 13.7.0.10276927               |
| deviceTRUST Citrix Channel         | 17.2.100.0                    |
| deviceTRUST RDP Channel            | 17.2.100.0                    |
| Ericom PowerTerm                   | 12.0.1.0.20170219.2-dev-34574 |
| Evidian AuthMgr                    | 1.5.6362                      |
| Evince PDF Viewer                  | 3.18.2-1ubuntu4.2             |
| FabulaTech USB for Remote Desktop  | 5.2.23                        |
| Firefox                            | 52.5.0                        |
| IBM iAccess Client Solutions       | 1.1.5.0                       |
| IGEL RDP Client                    | 2.2                           |
| Imprivata OneSign ProveID Embedded |                               |
| Leostream Java Connect             | 3.3.7.0                       |



|                                                             |                   |
|-------------------------------------------------------------|-------------------|
| NX Client                                                   | 5.3.12            |
| Open VPN                                                    | 2.3.10-1ubuntu2.1 |
| Oracle JRE                                                  | 1.8.0_152         |
| Parallels 2X Client                                         | 16.2.0.19039      |
| Remote Viewer for RedHat Enterprise Virtualization Desktops | 7.0               |
| Systancia AppliDis                                          | 4.0.0.17          |
| Thinlinc Client                                             | 4.8.0-5456        |
| ThinPrint Client                                            | 7.5.83            |
| Totem Media Player                                          | 2.30.2            |
| VMware Horizon Client                                       | 4.6.0-6617224     |

- **Dictation**

|                                                       |          |
|-------------------------------------------------------|----------|
| Diktamen driver for dictation                         |          |
| Driver for Grundig Business Systems dictation devices |          |
| Nuance Audio Extensions for dictation                 | B048     |
| Olympus driver for dictation                          | 20161103 |
| Philips Speech Driver                                 | 12.5.4   |

- **Signature**

|                         |       |
|-------------------------|-------|
| signotec Citrix Channel | 8.0.6 |
| signotec VCOM Daemon    | 2.0.0 |
| StepOver TCP Client     | 2.1.0 |

- **Smartcard**

|                                |         |
|--------------------------------|---------|
| PKCS#11 Library A.E.T SafeSign | 3.0.101 |
|--------------------------------|---------|



|                                               |                  |
|-----------------------------------------------|------------------|
| PKCS#11 Library Athena IDProtect              | 623.07           |
| PKCS#11 Library cryptovision sc/interface     | 6.6.3.502        |
| PKCS#11 Library Gemalto IDPrime               | 1.2.3            |
| PKCS#11 Library SecMaker NetID                | 6.6.0.30         |
| Reader Driver ACS CCID                        | 1.1.3            |
| Reader Driver Gemalto eToken                  | 9.0.43           |
| Reader Driver HID Global Omnikey CCID         | 4.2.4            |
| Reader Driver Identiv / SCM Microsystems CCID | 5.0.35           |
| Reader Driver Identiv eHealth200              | 1.0.5            |
| Reader Driver MUSCLE CCID                     | 1.4.27           |
| Reader Driver REINER SCT cyberJack            | 3.99.5final.SP09 |
| Resource Manager PC/SC Lite                   | 1.8.22           |
| Cherry USB2LAN Proxy                          | 3.0.0.4          |

- **System Components**

|                                         |                           |
|-----------------------------------------|---------------------------|
| Bluetooth stack (bluez)                 | 5.46-0ubuntu3             |
| MESA OpenGL stack                       | 17.2.2-0ubuntu1           |
| VAAPI ABI Version                       | 0.40                      |
| VDPAU Library version                   | 1.1.1-3ubuntu1            |
| Graphics Driver INTEL                   | 2.99.917+git20171109-igel |
| Graphics Driver ATI/RADEON              | 7.10.0-1                  |
| Graphics Driver ATI/AMDGPU              | 1.4.0-1                   |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.15-2                  |



|                                 |                           |
|---------------------------------|---------------------------|
| Graphics Driver Nvidia          | 384.90-0ubuntu0.16.04.2   |
| Graphics Driver Vboxvideo       | 5.1.30-dfsg-1             |
| Graphics Driver VMware          | 13.2.1-1build1            |
| Graphics Driver QXL (Spice)     | 0.1.5-2build1             |
| Graphics Driver FBDEV           | 0.4.4-1build5             |
| Graphics Driver VESA            | 2.3.4-1build2             |
| Input Driver Evdev              | 2.10.5-1ubuntu1           |
| Input Driver Elographics        | 1.4.1-1build5             |
| Input Driver eGalax             | 2.5.5814                  |
| Input Driver Synaptics          | 1.9.0-1ubuntu1            |
| Input Driver Vmmouse            | 13.1.0-1ubuntu2           |
| Input Driver Wacom              | 0.34.0-0ubuntu2           |
| Kernel                          | 4.10.17 #43.47-udos-r1949 |
| Xorg X11 Server                 | 1.19.5-0ubuntu2           |
| CUPS printing daemon            | 2.1.3-4ubuntu0.3          |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1         |
| XFCE4 Windowmanager             | 4.12.3-1ubuntu2           |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.7         |
| NetworkManager                  | 1.2.0-0ubuntu0.16.04.3    |
| ModemManager                    | 1.4.12-1ubuntu1           |
| GStreamer                       | 0.10.36-2ubuntu0.1        |

- **Features with Limited IGEL Support**



## Mobile Device Access USB

### Security Fixes 10.03.570

- Fixed kernel security issues CVE-2017-16939, CVE-2017-12192, CVE-2017-1000370, CVE-2017-1000371, CVE-2017-12190, CVE-2017-15274, CVE-2017-14156, CVE-2017-14140, CVE-2017-15115, CVE-2017-14489, CVE-2017-12153, CVE-2017-16525, CVE-2017-7542 and CVE-2017-8824.
- Partially addressed CVE-2017-5715 (Spectre Branch Target Injection) with Intel microcode updates version 20180108. CPU Models with updated microcode:
  - IVT C0
  - SKL-U/Y D0 and SKL-H/S R0
  - BDW-U/Y E/F and BDW-H E/G
  - HSW-ULT Cx/Dx and HSW Cx/Dx
  - Crystalwell Cx
  - HSX-EX E0 and HSX C0
  - BDX-DE V0/V1 and BDX-DE V2
  - KBL-U/Y H0, KBL Y0 / CFL D0 and KBL-H/S B0
  - CFL U0 and CFL B0
  - SKX H0
  - GLK B0
- Fixed kernel security issues CVE-2017-1000405 (aka Huge Dirty Cow).
- Fixed Intel meltdown problem CVE-2017-5754 with Kernel Page Table Isolation (KPTI) Patch

### General Information 10.03.570

The following clients and features are not supported anymore in version 10.03.570:

- Citrix Receiver 12.1 and 13.1
- Citrix Access Gateway Standard Plug-in
- Dell vWorkspace Connector for Linux
- Ericom PowerTerm Emulation 9 and 11
- Ericom Webconnect
- IGEL Legacy RDP Client (rdesktop)
- Virtual Bridges VERDE Client
- PPTP VPN Support
- IGEL Upgrade License Tool with IGEL Smartcard Token
- Remote Management by setup.ini file transfer (TFTP)
- XC Font Service
- Remote Access via RSH
- Legacy Philips Speech Driver
- Digital Persona Support
- Sane Scanner Support
- Softpro/Kofax Citrix Virtual Channel
- t-Systems TCOS Smartcard Support



- DUS Series touch screens
- Elo serial touch screens
- IGEL Smartcard without locking desktop
- Video Hardware Acceleration Support is discontinued on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, UD10-LX 10
- H.264 Hardware Acceleration Support is discontinued on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, UD10-LX 10
- Storage Hotplug devices are not automatically removed anymore, instead they must be always ejected manually:
  - by panel tray icon
  - by an icon in the 'In-Session Control Bar' (configurable at IGEL Setup > User Interface > Desktop )
  - by a 'Safely Remove Hardware' session (configurable at IGEL Setup > Accessories )

The following clients and features are not available in release 10.03.570:

- Voip Client Ekiga
- X session (Xorg Xephyr)
- XDMCP
- Cherry eGK Channel
- Open VPN Smartcard Support
- NCP Secure Client
- Asian Input Methods
- Composite Manager

## Known Issues 10.03.570

### Citrix Receiver 13

- With Citrix Receiver 13.5 print problems in legacy sessions can occur.

### VMware Horizon

- External drives mounted already before connection, do not appear in the remote desktop. Workaround: map the directory /media as a drive in your desktop. Then the external devices will show up inside the media drive.
- Client drive mapping and USB redirection for storage devices should not be enabled both at the same time.
  - On the one hand, if you want to use USB redirection for your storage devices: Note that the USB on-insertion feature is only working if the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in:  
Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping . It is also recommended to disable local Storage Hotplug: On page Devices > Storage Devices > Storage Hotplug , put number of storage hotplug devices to 0.



- On the other hand, if you use drive mapping instead, it is recommended that you should either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. And because Horizon Client relies on the OS to mount the storage devices itself, please go to setup page:  
Devices > Storage Devices > Storage Hotplug  
and switch on 'Enable dynamic drive mapping' and put 'Number of storage hotplug devices' to at least 1.

#### Firefox

- Support for the gstreamer framework was dropped by recent Firefox versions. Therefore support for H264 decoding in the browser is not possible anymore, due to licensing restrictions.
- After firmware update, a fullscreen browser session starts onetime in window mode. Afterwards the fullscreen mode is functional again.

#### Audio

- Headphone jack detection doesn't properly work on IGEL UD3 (M330C and M340C). The audio controlling system is unable to notice status change of the audio jack.

## 7.32 Notes for Release 10.03.550

|                |            |              |
|----------------|------------|--------------|
| Software:      | Version    | 10.03.550    |
| Release Date:  | 2018-01-12 |              |
| Release Notes: | Version    | RN-1003550-1 |
| Last update:   | 2018-01-12 |              |

- [IGEL Universal Desktop / IGEL Zero 10.03.550\(see page 2338\)](#)
- [IGEL Universal Desktop OS 3 / IGEL UD Pocket 10.03.550\(see page 2346\)](#)

### 7.32.1 IGEL Universal Desktop / IGEL Zero 10.03.550

#### Supported Devices

|                    |           |
|--------------------|-----------|
| Universal Desktop: |           |
| UD2-LX:            | UD2-LX 40 |



|             |                                                  |
|-------------|--------------------------------------------------|
| UD3-LX:     | UD3-LX 50<br>UD3-LX 42<br>UD3-LX 41<br>UD3-LX 40 |
| UD5-LX:     | UD5-LX 50<br>UD5-LX 40                           |
| UD6-LX:     | UD6-LX 51                                        |
| UD9-LX:     | UD9-LX Touch 41<br>UD9-LX 40                     |
| UD10-LX:    | UD10-LX Touch 10<br>UD10-LX 10                   |
| IGEL Zero:  |                                                  |
| IZ2-RFX     |                                                  |
| IZ2-HDX     |                                                  |
| IZ2-HORIZON |                                                  |
| IZ3-RFX     |                                                  |
| IZ3-HDX     |                                                  |
| IZ3-HORIZON |                                                  |

- Versions for Release 10.03.550(see page 2340)
- Security Fixes 10.03.550(see page 2343)
- General Information 10.03.550(see page 2343)
- Known Issues 10.03.550(see page 2344)
- New Features 10.03.550(see page 2345)
- Resolved Issues 10.03.550(see page 2345)



## Versions for Release 10.03.550

• **Clients**

| <b>Product</b>                     | <b>Version</b>                |
|------------------------------------|-------------------------------|
| Citrix HDX Realtime Media Engine   | 2.3.0-1075                    |
| Citrix Receiver                    | 13.3.2.366713                 |
| Citrix Receiver                    | 13.5.0.10185126               |
| Citrix Receiver                    | 13.7.0.10276927               |
| deviceTRUST Citrix Channel         | 17.2.100.0                    |
| deviceTRUST RDP Channel            | 17.2.100.0                    |
| Ericom PowerTerm                   | 12.0.1.0.20170219.2-dev-34574 |
| Evidian AuthMgr                    | 1.5.6362                      |
| FabulaTech USB for Remote Desktop  | 5.2.23                        |
| Firefox                            | 52.5.0                        |
| IBM iAccess Client Solutions       | 1.1.5.0                       |
| IGEL RDP Client                    | 2.2                           |
| Imprivata OneSign ProveID Embedded |                               |
| Leostream Java Connect             | 3.3.7.0                       |
| NX Client                          | 5.3.12                        |
| Open VPN                           | 2.3.10-1ubuntu2.1             |
| Oracle JRE                         | 1.8.0_152                     |
| Parallels 2X Client                | 16.2.0.19039                  |



|                                                             |               |
|-------------------------------------------------------------|---------------|
| Remote Viewer for RedHat Enterprise Virtualization Desktops | 7.0           |
| Systancia AppliDis                                          | 4.0.0.17      |
| Thinlinc Client                                             | 4.8.0-5456    |
| ThinPrint Client                                            | 7.5.83        |
| Totem Media Player                                          | 2.30.2        |
| VMware Horizon Client                                       | 4.6.0-6617224 |

- **Dictation**

|                                                       |          |
|-------------------------------------------------------|----------|
| Diktamen driver for dictation                         |          |
| Driver for Grundig Business Systems dictation devices |          |
| Nuance Audio Extensions for dictation                 | B048     |
| Olympus driver for dictation                          | 20161103 |
| Philips Speech Driver                                 | 12.5.4   |

- **Signature**

|                         |       |
|-------------------------|-------|
| signotec Citrix Channel | 8.0.6 |
| signotec VCOM Daemon    | 2.0.0 |
| StepOver TCP Client     | 2.1.0 |

- **Smartcard**

|                                           |           |
|-------------------------------------------|-----------|
| PKCS#11 Library A.E.T SafeSign            | 3.0.101   |
| PKCS#11 Library Athena IDProtect          | 623.07    |
| PKCS#11 Library cryptovision sc/interface | 6.6.3.502 |
| PKCS#11 Library Gemalto IDPrime           | 1.2.3     |
| PKCS#11 Library SecMaker NetID            | 6.6.0.30  |



|                                               |                  |
|-----------------------------------------------|------------------|
| Reader Driver ACS CCID                        | 1.1.3            |
| Reader Driver Gemalto eToken                  | 9.0.43           |
| Reader Driver HID Global Omnikey CCID         | 4.2.4            |
| Reader Driver Identiv / SCM Microsystems CCID | 5.0.35           |
| Reader Driver Identiv eHealth200              | 1.0.5            |
| Reader Driver MUSCLE CCID                     | 1.4.27           |
| Reader Driver REINER SCT cyberJack            | 3.99.5final.SP09 |
| Resource Manager PC/SC Lite                   | 1.8.22           |
| Cherry USB2LAN Proxy                          | 3.0.0.4          |

- **System Components**

|                            |                                |
|----------------------------|--------------------------------|
| Bluetooth stack (bluez)    | 5.46-0ubuntu3                  |
| MESA OpenGL stack          | 17.2.2-0ubuntu1                |
| VAAPI ABI Version          | 0.40                           |
| VDPAU Library version      | 1.1.1-3ubuntu1                 |
| Graphics Driver INTEL      | 2.99.917+git20171109-igel      |
| Graphics Driver ATI/RADEON | 7.10.0-1                       |
| Graphics Driver ATI/AMDGPU | 1.4.0-1                        |
| Graphics Driver VIA        | 5.76.52.92-009-005f78-20150730 |
| Graphics Driver FBDEV      | 0.4.4-1build5                  |
| Graphics Driver VESA       | 2.3.4-1build2                  |
| Input Driver Evdev         | 2.10.5-1ubuntu1                |
| Input Driver Elographics   | 1.4.1-1build5                  |



|                                 |                         |
|---------------------------------|-------------------------|
| Input Driver eGalax             | 2.5.5814                |
| Input Driver Synaptics          | 1.9.0-1ubuntu1          |
| Input Driver Vmmouse            | 13.1.0-1ubuntu2         |
| Input Driver Wacom              | 0.34.0-0ubuntu2         |
| Kernel                          | 4.10.17 #43.47-ud-r1949 |
| Xorg X11 Server                 | 1.19.5-0ubuntu2         |
| CUPS printing daemon            | 2.1.3-4ubuntu0.3        |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1       |
| XFCE4 Windowmanager             | 4.12.3-1ubuntu2         |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.7       |
| NetworkManager                  | 1.2.0-0ubuntu0.16.04.3  |
| ModemManager                    | 1.4.12-1ubuntu1         |
| GStreamer                       | 0.10.36-2ubuntu0.1      |

- **Features with Limited IGEL Support**

|                          |  |
|--------------------------|--|
| Mobile Device Access USB |  |
|--------------------------|--|

## Security Fixes 10.03.550

- Fixed **kernel security issues** CVE-2017-16939, CVE-2017-12192, CVE-2017-1000370, CVE-2017-1000371, CVE-2017-12190, CVE-2017-15274, CVE-2017-14156, CVE-2017-14140, CVE-2017-15115, CVE-2017-14489, CVE-2017-12153, CVE-2017-16525, CVE-2017-7542 and CVE-2017-8824.
- Fixed **kernel security issues** CVE-2017-1000405 (aka Huge Dirty Cow).
- Fixed **Intel meltdown problem** CVE-2017-5754 with Kernel Page Table Isolation (KPTI) Patch.

## General Information 10.03.550

The following clients and features are not supported anymore:

- Citrix Receiver 12.1 and 13.1



- Citrix Access Gateway Standard Plug-in
- Dell vWorkspace Connector for Linux
- Ericom PowerTerm Emulation 9 and 11
- Ericom Webconnect
- IGEL Legacy RDP Client (rdesktop)
- Virtual Bridges VERDE Client
- PPTP VPN Support
- IGEL Upgrade License Tool with IGEL Smartcard Token
- Remote Management by setup.ini file transfer (TFTP)
- XC Font Service
- Remote Access via RSH
- Legacy Philips Speech Driver
- Digital Persona Support
- Sane Scanner Support
- Softpro/Kofax Citrix Virtual Channel
- t-Systems TCOS Smartcard Support
- DUS Series touch screens
- Elo serial touch screens
- IGEL Smartcard without locking desktop
- Video Hardware Acceleration Support is discontinued on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, UD10-LX 10
- H.264 Hardware Acceleration Support is discontinued on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, UD10-LX 10
- Storage Hotplug devices are not automatically removed anymore, instead they must be always ejected manually:
  - by panel tray icon
  - by an icon in the 'In-Session Control Bar' (configurable at **IGEL Setup > User Interface > Desktop**)
  - by a 'Safely Remove Hardware' session (configurable at **IGEL Setup > Accessories**)

The following clients and features are not available in this release:

- Voip Client Ekiga
- X session (Xorg Xephyr)
- XDMCP
- Cherry eGK Channel
- Open VPN Smartcard Support
- NCP Secure Client
- Asian Input Methods
- Composite Manager

## Known Issues 10.03.550

### Citrix Receiver 13

- With Citrix Receiver 13.5 **print problems** in legacy sessions can occur.

### VMware Horizon



- External drives mounted already before connection, do not appear in the remote desktop.  
Workaround: map the directory /media as a drive in your desktop. Then the external devices will show up inside the media drive.
- Client drive mapping and USB redirection for storage devices should not be enabled both at the same time.
  - On the one hand, if you want to use USB redirection for your storage devices: Note that the USB on-insertion feature is only working if the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping. It is also recommended to disable local Storage Hotplug: On page Devices > Storage Devices > Storage Hotplug, put number of storage hotplug devices to 0.
  - On the other hand, if you use drive mapping instead, it is recommended that you should either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. And because Horizon Client relies on the OS to mount the storage devices itself, please go to setup page: Devices > Storage Devices > Storage Hotplug and switch on 'Enable dynamic drive mapping' and put 'Number of storage hotplug devices' to at least 1.

#### Firefox

- Because the support for the gstreamer framework was dropped by recent Firefox versions, support for H264 decoding in the browser is not possible anymore due to licensing restrictions.
- After firmware update, a fullscreen browser session starts onetime in window mode. Afterwards the fullscreen mode is functional again.

#### Audio

- Headphone jack detection doesn't properly work on IGEL UD3 (M330C and M340C). The audio controlling system is unable to notice status change of the audio jack.

## New Features 10.03.550

### Parallels Client

- Integrated Parallels Client version 16.2.0 (19039) 64 bit.

## Resolved Issues 10.03.550

### RDP/IGEL RDP Client 2

- Fixed the rdpdebugger to work again (was broken in the previous release).
- Fixed smartcard redirection: after session reconnection readers and cards were not connected anymore in some cases.

### Parallels Client

- Fixed crash after closing one session if started 2 same sessions before

### Smartcard

- Fixed driver for Elatec RFID readers. Before this fix the readers sometimes were not available after boot.



## Base System

- Updated kernel to Ubuntu-hwe-4.10.0-43.47\_16.04.1.
- Fixed kernel security issues CVE-2017-16939, CVE-2017-12192, CVE-2017-1000370, CVE-2017-1000371, CVE-2017-12190, CVE-2017-15274, CVE-2017-14156, CVE-2017-14140, CVE-2017-15115, CVE-2017-14489, CVE-2017-12153, CVE-2017-16525, CVE-2017-7542 and CVE-2017-8824.
- Fixed kernel security issues CVE-2017-1000405 (aka Huge Dirty Cow).
- Fixed Intel meltdown problem CVE-2017-5754 with Kernel Page Table Isolation (KPTI) Patch.

## 7.32.2 IGEL Universal Desktop OS 3 / IGEL UD Pocket 10.03.550

Supported Hardware:

[Third-Party Devices Supported by IGEL OS 10<sup>462</sup>](#)

- Versions for Release 10.03.550(see page 2346)
- Security Fixes 10.03.550(see page 2350)
- General Information 10.03.550(see page 2351)
- Known Issues 10.03.550(see page 2351)
- New Features 10.03.550(see page 2352)
- Resolved Issues 10.03.550(see page 2352)

## Versions for Release 10.03.550

## • Clients

| Product                          | Version                       |
|----------------------------------|-------------------------------|
| Citrix HDX Realtime Media Engine | 2.3.0-1075                    |
| Citrix Receiver                  | 13.3.2.366713                 |
| Citrix Receiver                  | 13.5.0.10185126               |
| Citrix Receiver                  | 13.7.0.10276927               |
| deviceTRUST Citrix Channel       | 17.2.100.0                    |
| deviceTRUST RDP Channel          | 17.2.100.0                    |
| Ericom PowerTerm                 | 12.0.1.0.20170219.2-dev-34574 |

<sup>462</sup> <https://kb.igel.com/display/hardware/Third+Party+Devices+Supported+by+IGEL+OS+10>



|                                                             |                   |
|-------------------------------------------------------------|-------------------|
| Evidian AuthMgr                                             | 1.5.6362          |
| Evince PDF Viewer                                           | 3.18.2-1ubuntu4.2 |
| FabulaTech USB for Remote Desktop                           | 5.2.23            |
| Firefox                                                     | 52.5.0            |
| IBM iAccess Client Solutions                                | 1.1.5.0           |
| IGEL RDP Client                                             | 2.2               |
| Imprivata OneSign ProveID Embedded                          |                   |
| Leostream Java Connect                                      | 3.3.7.0           |
| NX Client                                                   | 5.3.12            |
| Open VPN                                                    | 2.3.10-1ubuntu2.1 |
| Oracle JRE                                                  | 1.8.0_152         |
| Parallels 2X Client                                         | 16.2.0.19039      |
| Remote Viewer for RedHat Enterprise Virtualization Desktops | 7.0               |
| Systancia AppliDis                                          | 4.0.0.17          |
| Thinlinc Client                                             | 4.8.0-5456        |
| ThinPrint Client                                            | 7.5.83            |
| Totem Media Player                                          | 2.30.2            |
| VMware Horizon Client                                       | 4.6.0-6617224     |

- **Dictation**

|                                                       |  |
|-------------------------------------------------------|--|
| Diktamen driver for dictation                         |  |
| Driver for Grundig Business Systems dictation devices |  |



|                                       |          |
|---------------------------------------|----------|
| Nuance Audio Extensions for dictation | B048     |
| Olympus driver for dictation          | 20161103 |
| Philips Speech Driver                 | 12.5.4   |

- **Signature**

|                         |       |
|-------------------------|-------|
| signotec Citrix Channel | 8.0.6 |
| signotec VCOM Daemon    | 2.0.0 |
| StepOver TCP Client     | 2.1.0 |

- **Smartcard**

|                                               |                  |
|-----------------------------------------------|------------------|
| PKCS#11 Library A.E.T SafeSign                | 3.0.101          |
| PKCS#11 Library Athena IDProtect              | 623.07           |
| PKCS#11 Library cryptovision sc/interface     | 6.6.3.502        |
| PKCS#11 Library Gemalto IDPrime               | 1.2.3            |
| PKCS#11 Library SecMaker NetID                | 6.6.0.30         |
| Reader Driver ACS CCID                        | 1.1.3            |
| Reader Driver Gemalto eToken                  | 9.0.43           |
| Reader Driver HID Global Omnikey CCID         | 4.2.4            |
| Reader Driver Identiv / SCM Microsystems CCID | 5.0.35           |
| Reader Driver Identiv eHealth200              | 1.0.5            |
| Reader Driver MUSCLE CCID                     | 1.4.27           |
| Reader Driver REINER SCT cyberJack            | 3.99.5final.SP09 |
| Resource Manager PC/SC Lite                   | 1.8.22           |
| Cherry USB2LAN Proxy                          | 3.0.0.4          |

- **System Components**



|                                         |                           |
|-----------------------------------------|---------------------------|
| Bluetooth stack (bluez)                 | 5.46-0ubuntu3             |
| MESA OpenGL stack                       | 17.2.2-0ubuntu1           |
| VAAPI ABI Version                       | 0.40                      |
| VDPAU Library version                   | 1.1.1-3ubuntu1            |
| Graphics Driver INTEL                   | 2.99.917+git20171109-igel |
| Graphics Driver ATI/Radeon              | 7.10.0-1                  |
| Graphics Driver ATI/AMDGPU              | 1.4.0-1                   |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.15-2                  |
| Graphics Driver Nvidia                  | 384.90-0ubuntu0.16.04.2   |
| Graphics Driver Vboxvideo               | 5.1.30-dfsg-1             |
| Graphics Driver VMware                  | 13.2.1-1build1            |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1             |
| Graphics Driver FBDEV                   | 0.4.4-1build5             |
| Graphics Driver VESA                    | 2.3.4-1build2             |
| Input Driver Evdev                      | 2.10.5-1ubuntu1           |
| Input Driver Elographics                | 1.4.1-1build5             |
| Input Driver eGalax                     | 2.5.5814                  |
| Input Driver Synaptics                  | 1.9.0-1ubuntu1            |
| Input Driver Vmmouse                    | 13.1.0-1ubuntu2           |
| Input Driver Wacom                      | 0.34.0-0ubuntu2           |
| Kernel                                  | 4.10.17 #43.47-udos-r1949 |



|                                             |                        |
|---------------------------------------------|------------------------|
| Xorg X11 Server                             | 1.19.5-0ubuntu2        |
| CUPS printing daemon                        | 2.1.3-4ubuntu0.3       |
| Lightdm graphical login manager             | 1.18.3-0ubuntu1.1      |
| XFCE4 Windowmanager                         | 4.12.3-1ubuntu2        |
| ISC DHCP Client                             | 4.3.3-5ubuntu12.7      |
| NetworkManager                              | 1.2.0-0ubuntu0.16.04.3 |
| ModemManager                                | 1.4.12-1ubuntu1        |
| GStreamer                                   | 0.10.36-2ubuntu0.1     |
| <b>• Features with Limited IGEL Support</b> |                        |
| Mobile Device Access USB                    |                        |

## Security Fixes 10.03.550

- Fixed kernel security issues CVE-2017-16939, CVE-2017-12192, CVE-2017-1000370, CVE-2017-1000371, CVE-2017-12190, CVE-2017-15274, CVE-2017-14156, CVE-2017-14140, CVE-2017-15115, CVE-2017-14489, CVE-2017-12153, CVE-2017-16525, CVE-2017-7542 and CVE-2017-8824.
- Partially addressed CVE-2017-5715 (Spectre Branch Target Injection) with Intel microcode updates version 20180108. CPU Models with updated microcode:
  - IVT C0
  - SKL-U/Y D0 and SKL-H/S R0
  - BDW-U/Y E/F and BDW-H E/G
  - HSW-ULT Cx/Dx and HSW Cx/Dx
  - Crystalwell Cx
  - HSX-EX E0 and HSX C0
  - BDX-DE V0/V1 and BDX-DE V2
  - KBL-U/Y H0, KBL Y0 / CFL D0 and KBL-H/S B0
  - CFL U0 and CFL B0
  - SKX H0
  - GLK B0
- Fixed kernel security issues CVE-2017-1000405 (aka Huge Dirty Cow).
- Fixed Intel meltdown problem CVE-2017-5754 with Kernel Page Table Isolation (KPTI) Patch.



## General Information 10.03.550

The following clients and features are not supported anymore in version 10.03.550:

- Citrix Receiver 12.1 and 13.1
- Citrix Access Gateway Standard Plug-in
- Dell vWorkspace Connector for Linux
- Ericom PowerTerm Emulation 9 and 11
- Ericom Webconnect
- IGEL Legacy RDP Client (rdesktop)
- Virtual Bridges VERDE Client
- PPTP VPN Support
- IGEL Upgrade License Tool with IGEL Smartcard Token
- Remote Management by setup.ini file transfer (TFTP)
- XC Font Service
- Remote Access via RSH
- Legacy Philips Speech Driver
- Digital Persona Support
- Sane Scanner Support
- Softpro/Kofax Citrix Virtual Channel
- t-Systems TCOS Smartcard Support
- DUS Series touch screens
- Elo serial touch screens
- IGEL Smartcard without locking desktop
- VIA Graphics Support
- Storage Hotplug devices are not automatically removed anymore, instead they must be always ejected manually:
  - by panel tray icon
  - by an icon in the 'In-Session Control Bar' (configurable at **IGEL Setup > User Interface > Desktop**)
  - by a 'Safely Remove Hardware' session (configurable at **IGEL Setup > Accessories**)

The following clients and features are not available in release 10.03.550:

- Voip Client Ekiga
- X session (Xorg Xephyr)
- XDMCP
- Cherry eGK Channel
- Open VPN Smartcard Support
- NCP Secure Client
- Asian Input Methods
- Composite Manager

## Known Issues 10.03.550

### Citrix Receiver 13

- With Citrix Receiver 13.5 print problems in legacy sessions can occur.



## VMware Horizon

- External drives mounted already before connection, do not appear in the remote desktop.  
Workaround: map the directory /media as a drive in your desktop. Then the external devices will show up inside the media drive.
- Client drive mapping and USB redirection for storage devices should not be enabled both at the same time.
  - On the one hand, if you want to use USB redirection for your storage devices: Note that the USB on-insertion feature is only working if the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping. It is also recommended to disable local Storage Hotplug: On page Devices > Storage Devices > Storage Hotplug, put number of storage hotplug devices to 0.
  - On the other hand, if you use drive mapping instead, it is recommended that you should either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. And because Horizon Client relies on the OS to mount the storage devices itself, please go to setup page: Devices > Storage Devices > Storage Hotplug and switch on 'Enable dynamic drive mapping' and put 'Number of storage hotplug devices' to at least 1.

## Firefox

- Because the support for the gstreamer framework was dropped by recent Firefox versions, support for H264 decoding in the browser is not possible anymore due to licensing restrictions.
- After firmware update, a fullscreen browser session starts onetime in window mode. Afterwards the fullscreen mode is functional again.

## Hardware

- The TrackPoint and TrackPoint keys of the Toshiba Portege X30-D laptop are not working.

## New Features 10.03.550

### Parallels Client

- Integrated Parallels Client version 16.2.0 (19039) 64 bit.

## Resolved Issues 10.03.550

### RDP/IGEL RDP Client 2

- Fixed the rdpdebugger to work again (was broken in the previous release).
- Fixed smartcard redirection: after session reconnection readers and cards were not connected anymore in some cases.

### Parallels Client

- Fixed crash after closing one session if started 2 same sessions before

### Smartcard



- Fixed driver for Elatec RFID readers. Before this fix the readers sometimes were not available after boot.

#### Base System

- Updated kernel to Ubuntu-hwe-4.10.0-43.47\_16.04.1.
- Fixed kernel security issues CVE-2017-16939, CVE-2017-12192, CVE-2017-1000370, CVE-2017-1000371, CVE-2017-12190, CVE-2017-15274, CVE-2017-14156, CVE-2017-14140, CVE-2017-15115, CVE-2017-14489, CVE-2017-12153, CVE-2017-16525, CVE-2017-7542 and CVE-2017-8824.
- Partially addressed CVE-2017-5715 (Spectre Branch Target Injection) with Intel microcode updates version 20180108. CPU Models with updated microcode:
  - IVT C0
  - SKL-U/Y D0 and SKL-H/S R0
  - BDW-U/Y E/F and BDW-H E/G
  - HSW-ULT Cx/Dx and HSW Cx/Dx
  - Crystalwell Cx
  - HSX-EX E0 and HSX C0
  - BDX-DE V0/V1 and BDX-DE V2
  - KBL-U/Y H0, KBL Y0 / CFL D0 and KBL-H/S B0
  - CFL U0 and CFL B0
  - SKX H0
  - GLK B0
- Fixed kernel security issues CVE-2017-1000405 (aka Huge Dirty Cow).
- Fixed Intel meltdown problem CVE-2017-5754 with Kernel Page Table Isolation (KPTI) Patch.

### 7.33 Notes for Release 10.03.500

|                |            |              |
|----------------|------------|--------------|
| Software:      | Version    | 10.03.500    |
| Release Date:  | 2017-12-14 |              |
| Release Notes: | Version    | RN-1003500-1 |
| Last update:   | 2017-12-14 |              |

- [IGEL Universal Desktop / IGEL Zero 10.03.500](#)(see page 2354)
- [IGEL Universal Desktop OS3 / IGEL UD Pocket 10.03.500](#)(see page 2381)
- [IGEL Universal Desktop Converter \(UDC3\) 10.03.500](#)(see page 2407)



### 7.33.1 IGEL Universal Desktop / IGEL Zero 10.03.500

#### Supported Devices

##### Universal Desktop:

|          |                                                  |
|----------|--------------------------------------------------|
| UD2-LX:  | UD2-LX 40                                        |
| UD3-LX:  | UD3-LX 50<br>UD3-LX 42<br>UD3-LX 41<br>UD3-LX 40 |
| UD5-LX:  | UD5-LX 50<br>UD5-LX 40                           |
| UD6-LX:  | UD6-LX 51                                        |
| UD9-LX:  | UD9-LX Touch 41<br>UD9-LX 40                     |
| UD10-LX: | UD10-LX Touch 10<br>UD10-LX 10                   |

##### IGEL Zero:

|             |
|-------------|
| IZ2-RFX     |
| IZ2-HDX     |
| IZ2-HORIZON |
| IZ3-RFX     |
| IZ3-HDX     |



## IZ3-HORIZON

- [Versions for 10.03.500\(see page 2355\)](#)
- [Security Fixes 10.03.500\(see page 2358\)](#)
- [General Information 10.03.500\(see page 2364\)](#)
- [Known Issues 10.03.500\(see page 2365\)](#)
- [New Features 10.03.500\(see page 2366\)](#)
- [Resolved Issues 10.03.500\(see page 2378\)](#)

## Versions for 10.03.500

• **Clients**

| <b>Product</b>                     | <b>Version</b>                |
|------------------------------------|-------------------------------|
| Citrix HDX Realtime Media Engine   | 2.3.0-1075                    |
| Citrix Receiver                    | 13.3.2.366713                 |
| Citrix Receiver                    | 13.5.0.10185126               |
| Citrix Receiver                    | 13.7.0.10276927               |
| deviceTRUST Citrix Channel         | 17.2.100.0                    |
| deviceTRUST RDP Channel            | 17.2.100.0                    |
| Ericom PowerTerm                   | 12.0.1.0.20170219.2-dev-34574 |
| Evidian AuthMgr                    | 1.5.6362                      |
| FabulaTech USB for Remote Desktop  | 5.2.23                        |
| Firefox                            | 52.5.0                        |
| IBM iAccess Client Solutions       | 1.1.5.0                       |
| IGEL RDP Client                    | 2.2                           |
| Imprivata OneSign ProveID Embedded |                               |
| Leostream Java Connect             | 3.3.7.0                       |



|                                                             |                   |
|-------------------------------------------------------------|-------------------|
| NX Client                                                   | 5.3.12            |
| Open VPN                                                    | 2.3.10-1ubuntu2.1 |
| Oracle JRE                                                  | 1.8.0_152         |
| Parallels 2X Client                                         | 16.0.1.18456      |
| Remote Viewer for RedHat Enterprise Virtualization Desktops | 7.0               |
| Systancia AppliDis                                          | 4.0.0.17          |
| Thinlinc Client                                             | 4.8.0-5456        |
| ThinPrint Client                                            | 7.5.83            |
| Totem Media Player                                          | 2.30.2            |
| VMware Horizon Client                                       | 4.6.0-6617224     |

- **Dictation**

|                                                       |          |
|-------------------------------------------------------|----------|
| Diktamen driver for dictation                         |          |
| Driver for Grundig Business Systems dictation devices |          |
| Nuance Audio Extensions for dictation                 | B048     |
| Olympus driver for dictation                          | 20161103 |
| Philips Speech Driver                                 | 12.5.4   |

- **Signature**

|                         |       |
|-------------------------|-------|
| signotec Citrix Channel | 8.0.6 |
| signotec VCOM Daemon    | 2.0.0 |
| StepOver TCP Client     | 2.1.0 |

- **Smartcard**

|                                |         |
|--------------------------------|---------|
| PKCS#11 Library A.E.T SafeSign | 3.0.101 |
|--------------------------------|---------|



|                                               |                  |
|-----------------------------------------------|------------------|
| PKCS#11 Library Athena IDProtect              | 623.07           |
| PKCS#11 Library cryptovision sc/interface     | 6.6.3.502        |
| PKCS#11 Library Gemalto IDPrime               | 1.2.3            |
| PKCS#11 Library SecMaker NetID                | 6.6.0.30         |
| Reader Driver ACS CCID                        | 1.1.3            |
| Reader Driver Gemalto eToken                  | 9.0.43           |
| Reader Driver HID Global Omnikey CCID         | 4.2.4            |
| Reader Driver Identiv / SCM Microsystems CCID | 5.0.35           |
| Reader Driver Identiv eHealth200              | 1.0.5            |
| Reader Driver MUSCLE CCID                     | 1.4.27           |
| Reader Driver REINER SCT cyberJack            | 3.99.5final.SP09 |
| Resource Manager PC/SC Lite                   | 1.8.22           |
| Cherry USB2LAN Proxy                          | 3.0.0.4          |

- **System Components**

|                            |                                |
|----------------------------|--------------------------------|
| Bluetooth stack (bluez)    | 5.46-0ubuntu3                  |
| MESA OpenGL stack          | 17.2.2-0ubuntu1                |
| VAAPI ABI Version          | 0.40                           |
| VDPAU Library version      | 1.1.1-3ubuntu1                 |
| Graphics Driver INTEL      | 2.99.917+git20171109-igel      |
| Graphics Driver ATI/RADEON | 7.10.0-1                       |
| Graphics Driver ATI/AMDGPU | 1.4.0-1                        |
| Graphics Driver VIA        | 5.76.52.92-009-005f78-20150730 |



|                                 |                         |
|---------------------------------|-------------------------|
| Graphics Driver FBDEV           | 0.4.4-1build5           |
| Graphics Driver VESA            | 2.3.4-1build2           |
| Input Driver Evdev              | 2.10.5-1ubuntu1         |
| Input Driver Elographics        | 1.4.1-1build5           |
| Input Driver eGalax             | 2.5.5814                |
| Input Driver Synaptics          | 1.9.0-1ubuntu1          |
| Input Driver Vmmouse            | 13.1.0-1ubuntu2         |
| Input Driver Wacom              | 0.34.0-0ubuntu2         |
| Kernel                          | 4.10.17 #41.45-ud-r1938 |
| Xorg X11 Server                 | 1.19.5-0ubuntu2         |
| CUPS printing daemon            | 2.1.3-4ubuntu0.3        |
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1       |
| XFCE4 Windowmanager             | 4.12.3-1ubuntu2         |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.7       |
| NetworkManager                  | 1.2.0-0ubuntu0.16.04.3  |
| ModemManager                    | 1.4.12-1ubuntu1         |
| GStreamer                       | 0.10.0.10.36-2ubuntu0.1 |

- **Features with Limited IGEL Support**

|                          |  |
|--------------------------|--|
| Mobile Device Access USB |  |
|--------------------------|--|

## Security Fixes 10.03.500

- Fixed **wpa** security issues (KRACK vulnerability).

[More](#)



CVE-2017-13077

CVE-2017-13078

CVE-2017-13079

CVE-2017-13080

CVE-2017-13081

CVE-2017-13082

CVE-2017-13086

CVE-2017-13087

CVE-2017-13088

CVE-2016-4476

CVE-2016-4477

- Fixed **libgd2** security issues. CVE-2017-7890 and CVE-2017-6362.

- Fixed **graphite2** security issues.

**More**

CVE-2017-7778

CVE-2017-7777

CVE-2017-7776

CVE-2017-7775

CVE-2017-7774

CVE-2017-7773

CVE-2017-7772

CVE-2017-7771

- Fixed **ghostscript** security issues.

**More**

CVE-2017-9835

CVE-2017-9739

CVE-2017-9727

CVE-2017-9726

CVE-2017-9612

CVE-2017-9611

CVE-2017-11714

- Fixed **libmspack** security issues CVE-2017-6419 and CVE-2017-11423.

- Fixed **libsoup2.4** security issue CVE-2017-2885.

- Fixed **xorg-server** security issues.

**More**



CVE-2017-10971

CVE-2017-10972

CVE-2017-13721

CVE-2017-13723

CVE-2017-12176

CVE-2017-12177

CVE-2017-12178

CVE-2017-12179

CVE-2017-12180

CVE-2017-12181

CVE-2017-12182

CVE-2017-12183

CVE-2017-12184

CVE-2017-12185

CVE-2017-12186

CVE-2017-12187

- Fixed **bluez** security issue CVE-2017-1000250.
- Fixed **kernel** security issues.

**More**

CVE-2017-7541

CVE-2017-1000112

CVE-2017-1000111

CVE-2017-7487

CVE-2017-7533

CVE-2017-1000251

CVE-2017-14106

CVE-2017-11176

CVE-2017-10911

CVE-2017-14340

CVE-2017-10663

CVE-2017-1000252

CVE-2017-12188

CVE-2017-12146

- Fixed **gdk-pixbuf** security issues CVE-2017-6311, CVE-2017-2870 and CVE-2017-2862.
- Fixed **tcpdump** security issues.



**More**

CVE-2017-13725, CVE-2017-13690, CVE-2017-13689, CVE-2017-13688,  
CVE-2017-13687, CVE-2017-13055, CVE-2017-13054, CVE-2017-13053,  
CVE-2017-13052, CVE-2017-13051, CVE-2017-13050, CVE-2017-13049,  
CVE-2017-13048, CVE-2017-13047, CVE-2017-13046, CVE-2017-13045,  
CVE-2017-13044, CVE-2017-13043, CVE-2017-13042, CVE-2017-13041,  
CVE-2017-13040, CVE-2017-13039, CVE-2017-13038, CVE-2017-13037,  
CVE-2017-13036, CVE-2017-13035, CVE-2017-13034, CVE-2017-13033,  
CVE-2017-13032, CVE-2017-13031, CVE-2017-13030, CVE-2017-13029,  
CVE-2017-13028, CVE-2017-13027, CVE-2017-13026, CVE-2017-13025,  
CVE-2017-13024, CVE-2017-13023, CVE-2017-13022, CVE-2017-13021,  
CVE-2017-13020, CVE-2017-13019, CVE-2017-13018, CVE-2017-13017,  
CVE-2017-13016, CVE-2017-13015, CVE-2017-13014, CVE-2017-13013,  
CVE-2017-13012, CVE-2017-13011, CVE-2017-13010, CVE-2017-13009,  
CVE-2017-13008, CVE-2017-13007, CVE-2017-13006, CVE-2017-13005,  
CVE-2017-13004, CVE-2017-13003, CVE-2017-13002, CVE-2017-13001,  
CVE-2017-13000, CVE-2017-12999, CVE-2017-12998, CVE-2017-12997,  
CVE-2017-12996, CVE-2017-12995, CVE-2017-12994, CVE-2017-12993,  
CVE-2017-12992, CVE-2017-12991, CVE-2017-12990, CVE-2017-12989,  
CVE-2017-12988, CVE-2017-12987, CVE-2017-12986, CVE-2017-12985,  
CVE-2017-12902, CVE-2017-12901, CVE-2017-12900, CVE-2017-12899,  
CVE-2017-12898, CVE-2017-12897, CVE-2017-12896, CVE-2017-12895,  
CVE-2017-12894, CVE-2017-12893, CVE-2017-11543, CVE-2017-11542,  
CVE-2017-11541 and CVE-2017-11108.

- Fixed **libxml2** security issues.

**More**

CVE-2017-9050  
CVE-2017-9049  
CVE-2017-9048  
CVE-2017-9047  
CVE-2017-7376  
CVE-2017-7375  
CVE-2017-0663

- Fixed **samba** security issues.



**More**

CVE-2017-12163

CVE-2017-12151

CVE-2017-12150

CVE-2017-15275

CVE-2017-14746

- Fixed **libplist** security issue CVE-2017-7982.
- Fixed **nss** security issue CVE-2017-7805.
- Fixed **libidn** security issue CVE-2017-14062.
- Fixed **poppler** security issues.

**More**

CVE-2017-9776,

CVE-2017-14977

CVE-2017-14975

CVE-2017-14929

CVE-2017-14928

CVE-2017-14926

CVE-2017-14617

CVE-2017-14520

CVE-2017-14519

CVE-2017-14518

CVE-2017-15565

- Fixed **dnsmasq** security issues.

**More**

CVE-2017-14496

CVE-2017-14495

CVE-2017-14494

CVE-2017-14493

CVE-2017-14492

CVE-2017-14491

- Fixed **libxfont** security issues CVE-2017-13722, CVE-2017-13720 and CVE-2017-16611.
- Fixed **curl** security issues.

**More**

CVE-2016-9586

CVE-2017-2629



CVE-2017-7407

CVE-2017-7468

CVE-2017-1000100

CVE-2017-1000101

CVE-2017-1000254

CVE-2017-1000257

CVE-2017-8816

CVE-2017-8817

- Fixed **libxfont2** security issues CVE-2017-13722, CVE-2017-13720 and CVE-2017-16611.
- Fixed **nvidia** security issues CVE-2017-6266, CVE-2017-6267 and CVE-2017-6272.
- Fixed **icu** security issue CVE-2017-14952.
- Fixed **wget** security issues CVE-2017-6508, CVE-2017-13090, CVE-2017-13089 and CVE-2016-7098.
- Fixed **systemd** security issue CVE-2017-15908.
- Fixed **openssl** security issues CVE-2017-3736 and CVE-2017-3735.
- Fixed **perl** security issues CVE-2017-12883 and CVE-2017-12837.
- Fixed **webkit2gtk** security issues.

[More](#)

CVE-2017-13803

CVE-2017-13802

CVE-2017-13798

CVE-2017-13796

CVE-2017-13795

CVE-2017-13794

CVE-2017-13793

CVE-2017-13792

CVE-2017-13791

CVE-2017-13788

CVE-2017-13785

CVE-2017-13784

CVE-2017-13783

- Fixed **db5.3** security issue CVE-2017-10140.
- Fixed **ldns** security issues CVE-2017-1000232 and CVE-2017-1000231.
- Fixed **python2.7** security issue CVE-2017-1000158.
- Fixed **python3.5** security issue CVE-2017-1000158.
- Fixed **libxcursor** security issue CVE-2017-16612.
- Fixed a security issue in the base system regarding of not resetting certain environment variables.
- Updated Firefox to version 52.5 ESR:
  - Fixes for **mfsa2017-25**, also known as: CVE-2017-7828, CVE-2017-7830, CVE-2017-7826.



- Fixes for **mfsa2017-22**, also known as: CVE-2017-7793, CVE-2017-7818, CVE-2017-7819, CVE-2017-7824, CVE-2017-7805, CVE-2017-7814, CVE-2017-7823, CVE-2017-7810.

## General Information 10.03.500

The following clients and features are not supported anymore in version 10.03.500:

- Citrix Receiver 12.1 and 13.1
- Citrix Access Gateway Standard Plug-in
- Dell vWorkspace Connector for Linux
- Ericom PowerTerm Emulation 9 and 11
- Ericom Webconnect
- IGEL Legacy RDP Client (rdesktop)
- Virtual Bridges VERDE Client
- PPTP VPN Support
- IGEL Upgrade License Tool with IGEL Smartcard Token
- Remote Management by setup.ini file transfer (TFTP)
- XC Font Service
- Remote Access via RSH
- Legacy Philips Speech Driver
- Digital Persona Support
- Sane Scanner Support
- Softpro/Kofax Citrix Virtual Channel
- t-Systems TCOS Smartcard Support
- DUS Series touch screens
- Elo serial touch screens
- IGEL Smartcard without locking desktop
- Video Hardware Acceleration Support is discontinued on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, UD10-LX 10
- H.264 Hardware Acceleration Support is discontinued on UD3-LX 42, UD3-LX 41, UD3-LX 40 (M320C/M330C) and UD10-LX Touch 10, UD10-LX 10
- Storage Hotplug devices are not automatically removed anymore, instead they must be always ejected manually:
  - by panel tray icon
  - by an icon in the 'In-Session Control Bar' (configurable at **IGEL Setup > User Interface > Desktop**)
  - by a 'Safely Remove Hardware' session (configurable at **IGEL Setup > Accessories**)

The following clients and features are not available in the release 10.03.500:

- Voip Client Ekiga
- X session (Xorg Xephyr)
- XDMCP
- Cherry eGK Channel
- Open VPN Smartcard Support
- NCP Secure Client
- Asian Input Methods
- Composite Manager



## Known Issues 10.03.500

### Citrix Receiver 13

- On devices with AMD/Radeon graphics chipsets and activated DRI3 X driver option **the hardware accelerated Citrix H.264 decoder plugin can hang**. To solve this issue deactivation of DRI3 option is necessary (default setting).

[More](#)

|           |                                                         |
|-----------|---------------------------------------------------------|
| Parameter | Use DRI3                                                |
| Registry  | x.drivers.use_dri3                                      |
| Value     | enabled / <u>disabled</u>                               |
| Parameter | Force usage of DRI3                                     |
| Registry  | x.drivers.amdgpu.force_dri3<br>x.drivers.ati.force_dri3 |
| Value     | enabled / <u>disabled</u>                               |

- Citrix StoreFront login with **Gemalto smartcard middleware** does not detect smartcard correctly when the card is inserted after start of login. As a workaround, insert the smartcard before starting StoreFront login.
- No smooth playback** over **Nuance** channel if the dictation device isn't attached.

### VMware Horizon

- External drives** mounted already before connection do not appear in the remote desktop. **Workaround:** mapping the directory /media as a drive on desktop. Then the external devices will show up inside the media drive.
- Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local Storage Hotplug: On page **Devices > Storage Devices > Storage Hotplug**, put number of storage hotplug devices to 0.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Change on the following setup page is required: **Devices > Storage Devices > Storage Hotplug**.



Activate **Enable dynamic drive mapping** and set **Number of storage hotplug devices** to at least 1.

#### Firefox

- Because the **support for the gstreamer framework** was dropped by recent Firefox versions, support for H264 decoding in the browser is not possible anymore due to licensing restrictions.

#### OpenConnect VPN

- VPNs which need the OpenConnect** client cannot be used for firmware updates.

#### Evidian

- Active Directory users with a **password containing special characters** may have problems to authenticate with the configured session.  
Known special characters which result in errors are:
  - ˋ (grave accent, ASCII code 96)
  - ˊ (acute accent, ASCII code 239)

### New Features 10.03.500

#### Citrix Receiver 13

- Integrated **Citrix Receiver 13.8.0**.

##### More

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Use Citrix Cloud with receiver 13.8 or newer |
| Registry  | ica.cloudconnect                             |
| Value     | enabled / <u>disabled</u>                    |

- Support for **Azure Active Directory** (Azure AD) authentication
- Support for **Workspace** configuration from Citrix Cloud
- Integrated **Citrix Receiver 13.4.2**. Citrix Receiver version 13.5.0 was removed. Available Citrix Receiver versions: 13.3.2, 13.4.2, 13.7.0, 13.8.0 (default)
- Updated **Citrix HDX RTME** used for optimization of Skype for Business to 2.4.0.

#### RDP / IGEL RDP Client 2

- Added possibility to use **RDP local logon** for smartcard login. This can be activated in the setup.

##### More

|           |                                          |
|-----------|------------------------------------------|
| Parameter | Enable smartcard support for local logon |
| Registry  | rdp.login.smartcard-local-logon          |
| Value     | enabled / <u>disabled</u>                |



By enabling this parameter local logon can be used for smartcard authentication. If **Username** is left empty the connection to the RDP server will be made without sending credentials, so you can choose **Smartcard** as login method in the microsoft login window . However this will not work with **NLA**.

- Added support for CredSSP up to version 6.

#### VMware Horizon

- Updated **VMware Horizon Client** to version **4.7.0-7395152**.
- Added key to enable **seamless window mode** in each application session.

[More](#)

|           |                                                    |
|-----------|----------------------------------------------------|
| Parameter | Seamless Application Windows                       |
| Registry  | sessions.vdm_client.options.enable_seamless_window |
| Value     | enabled / <u>disabled</u>                          |

- Added possibility to use **Fabulatech USB Redirection** in a Horizon Client PCoIP session.

[More](#)

|            |                                                                                                |
|------------|------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Fabulatech USB Redirection</b> |
| Parameter  | Enable Fabulatech USB Redirection                                                              |
| Registry   | vmware.view.usb.enable-fabulatech-usb                                                          |
| Value      | enabled / <u>disabled</u>                                                                      |

#### Parallels Client

- Integrated **Parallels Client** version **16.2.0 (19039)**
- Added support for USB Redirection, configurable at new IGEL Setup page **Sessions > Parallels Client > Parallels Client Global > USB Redirection**.

[More](#)

|            |                                                                                         |
|------------|-----------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Parallels Client &gt; Parallels Client Global &gt; USB Redirection</b> |
| Parameter  | Enable USB Redirection                                                                  |
| Registry   | twox.usb_redirection.usb_enable                                                         |
| Value      | enabled / <u>disabled</u>                                                               |
| Parameter  | Product ID                                                                              |



|           |                                                                     |
|-----------|---------------------------------------------------------------------|
| Registry  | <code>twox.usb_redirection.devicepolicy.product_rule.product</code> |
| Parameter | Vendor ID                                                           |
| Registry  | <code>twox.usb_redirection.devicepolicy.product_rule.vendor</code>  |
| Parameter | Rule                                                                |
| Registry  | <code>twox.usb_redirection.devicepolicy.product_rule.rule</code>    |
| Value     | <u>Deny / Allow</u>                                                 |
| Parameter | Name                                                                |
| Registry  | <code>twox.usb_redirection.devicepolicy.product_rule.name</code>    |
| Value     | Policy Rule                                                         |
| Parameter | Automatically redirect all USB devices                              |
| Registry  | <code>twox.usb_redirection.devicepolicy.redirect_all</code>         |
| Value     | <u>enabled / disabled</u>                                           |

- Added support for **PTP/MTP** Redirection.

**More**

|            |                                                                                         |
|------------|-----------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Parallels Client &gt; Parallels Client Global &gt; USB Redirection</b> |
| Parameter  | Enable PTP/MTP Redirection                                                              |
| Registry   | <code>twox.mtp_redirection.mtp_enable</code>                                            |
| Value      | <u>enabled / disabled</u>                                                               |
| Parameter  | Product ID                                                                              |
| Registry   | <code>twox.mtp_redirection.devicepolicy.product_rule.product</code>                     |
| Parameter  | Vendor ID                                                                               |
| Registry   | <code>twox.mtp_redirection.devicepolicy.product_rule.vendor</code>                      |



|           |                                                                  |
|-----------|------------------------------------------------------------------|
| Parameter | Rule                                                             |
| Registry  | <code>twox.mtp_redirection.devicepolicy.product_rule.rule</code> |
| Value     | <u>Deny</u> / Allow                                              |
| Parameter | Name                                                             |
| Registry  | <code>twox.mtp_redirection.devicepolicy.product_rule.name</code> |
| Value     | Policy Rule                                                      |
| Parameter | Automatically redirect all PTP/MTP devices                       |
| Registry  | <code>twox.mtp_redirection.devicepolicy.redirect_all</code>      |
| Value     | <u>enabled</u> / <u>disabled</u>                                 |

- Added support for **Clipboard** Redirection.

**More**

|            |                                                                                                                         |
|------------|-------------------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Parallels Client &gt; Parallels Client Sessions &gt; Parallels Client Session &gt; Local Resources</b> |
| Parameter  | Connect clipboard                                                                                                       |
| Registry   | <code>sessions.twox.local_resources.connect_clipboard</code>                                                            |
| Value      | <u>enabled</u> / <u>disabled</u>                                                                                        |

## VoIP

- Added **VoIP client Ekiga 4.0.1**.

## Firefox

- Updated **Firefox** to version **52.7.2 ESR**.
- Updated **Adobe Flash Player** download URL to version 29.0.0.113.

## Network

- Added **TTLS/PAP** and **TTLS/MSCHAPv2** to possible 802.1x authentication methods.
- Improved support for **Sierra EM7305 LTE** device (e.g. in Toshiba Portégé and Fujitsu LIFEBOOK E Series).



The EM7305 comes in various variants, e.g. one with ProductId 9041 and another one with ProductId 9063. The latter comes at least with one or with two USB configuration options. A device with only one configuration option has been observed on a Toshiba Tecra Z-50-D-115 notebook. It only works in MBIM mode and with IGEL firmware, when the device has successfully connected before with the same settings (particularly APN), e.g. under Microsoft Windows 10.

- Added support for **Sierra EM7455 WWAN module**.
- Added support for running the **Huawei E3531i WWAN** device in modem mode (in addition to HiLink mode).
- Added possibility to adopt the **hostname from a DHCP lease** as **permanent** terminal name. The purpose is to use the name received as part of a DHCP lease in future interactions with the DHCP server.

**More**

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Adopt permanent Terminal Name from DHCP lease |
| Registry  | network.dns.hostname_adopt_from_dhcp          |
| Value     | enabled / <u>disabled</u>                     |

- **NetworkManager** updated to version **1.2.2**
- **ModemManager** updated to version **1.6.4**
- **usb\_modeswitch** updated to version **2.5.1**

#### Open VPN

- Added **Huawei HiLink Mobile Broadband USB** device as possible uplink to OpenVPN sessions.

#### OpenConnect VPN

- Added **OpenConnect** client version **7.08** to connect to **Cisco AnyConnect** and **Juniper VPN**. The feature must be enabled.

**More**

|            |                                                                                                  |
|------------|--------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>System &gt; Firmware Customization &gt; Features</b>                                          |
| Parameter  | VPN OpenConnect (Limited support - functionality "as is", see product documentation for details) |
| Registry   | services.unsupported02.enabled                                                                   |
| Value      | enabled / <u>disabled</u>                                                                        |

- The OpenConnect VPN configuration is available at IGEL Setup page **Network > VPN > OpenConnect VPN**.

**More**



|            |                                                                                |
|------------|--------------------------------------------------------------------------------|
| IGEL Setup | <b>Network &gt; VPN &gt; OpenConnect VPN &gt; VPN OpenConnect &gt; Session</b> |
| Parameter  | Gateway                                                                        |
| Registry   | sessions.openconnect.vpnopts.gateway                                           |
| Parameter  | Enable Name/Password Authentication                                            |
| Registry   | sessions.openconnect.vpnopts.enable-name-pwd                                   |
| Value      | enabled / <u>disabled</u>                                                      |
| Parameter  | User Name                                                                      |
| Registry   | sessions.openconnect.vpnopts.username                                          |
| Parameter  | Password                                                                       |
| Registry   | sessions.openconnect.vpnopts.crypt_password                                    |
| Parameter  | CA Certificate                                                                 |
| Registry   | sessions.openconnect.vpnopts.ca-cert                                           |
| Parameter  | User Certificate                                                               |
| Registry   | sessions.openconnect.vpnopts.user-cert                                         |
| Parameter  | Private Key                                                                    |
| Registry   | sessions.openconnect.vpnopts.priv-key                                          |
| Parameter  | Private Key password                                                           |
| Registry   | sessions.openconnect.vpnopts.priv-key-pwd.crypt_password                       |
| Parameter  | Connect to Juniper Networks VPN                                                |
| Registry   | sessions.openconnect%.vpnopts.is-juniper                                       |
| Value      | enabled / <u>disabled</u>                                                      |



Tray icon is placed in the panel to disconnect from a running OpenConnect VPN connection.

## Smartcard

- Added **CoolKey PKCS#11** library for access to **Common Access Card (CAC)** smartcards.  
[More](#)

|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Browser &gt; Browser Global &gt; Encryption</b>              |
| Parameter  | Coolkey Security Device                                                       |
| Registry   | browserglobal.security_device.coolkey                                         |
| Value      | enabled / <u>disabled</u>                                                     |
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Smartcard</b> |
| Parameter  | Horizon logon with smartcards supported by Coolkey library                    |
| Registry   | vmware.view.pkcs11.use_coolkey                                                |
| Value      | enabled / <u>disabled</u>                                                     |
| IGEL Setup | <b>Security &gt; Smartcard &gt; Middleware</b>                                |
| Parameter  | Coolkey                                                                       |
| Registry   | scard.pkcs11.use_coolkey                                                      |
| Value      | enabled / <u>disabled</u>                                                     |

- Updated **Gemalto SafeNet PKCS#11** library to version **10.0.37-0**. This package replaces **Gemalto/SafeNet eToken** and **Gemalto IDPrime** libraries.  
**Gemalto SafeNet** (formerly **Gemalto/SafeNet eToken**) now handles Gemalto cards and tokens including eToken and IDPrime.  
**Gemalto IDPrime** now handles IDPrime cards and tokens, preferred Common Criteria (CC) cards and tokens in Unlinked Mode.
- Added full integration of **OpenSC PKCS#11** library for access to smartcards.  
[More](#)

|            |                                                                  |
|------------|------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Browser &gt; Browser Global &gt; Encryption</b> |
| Parameter  | OpenSC Security Device                                           |



|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| Registry   | browserglobal.security_device.opensc                                          |
| Value      | enabled / <u>disabled</u>                                                     |
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Smartcard</b> |
| Parameter  | Horizon logon with smartcards supported by OpenSC library                     |
| Registry   | vmware.view.pkcs11.use_opensc                                                 |
| Value      | enabled / <u>disabled</u>                                                     |
| IGEL Setup | <b>Security &gt; Smartcard &gt; Middleware</b>                                |
| Parameter  | OpenSC                                                                        |
| Registry   | scard.pkcs11.use_opensc                                                       |
| Value      | enabled / <u>disabled</u>                                                     |

- Updated **MUSCLE CCID** smartcard reader driver to version **1.4.28**.
- Updated **ACS CCID** smartcard reader driver to version **1.1.5**.
- Updated **REINER SCT cyberJack** smartcard reader driver to version **3.99.5final.sp11**.
- Added parameter to disable **Identive CCID** smartcard reader driver. If this driver is disabled, some of the readers are handled by the MUSCLE CCID driver. This can help when problems with Identive reader driver occur.

**More**

|           |                                        |
|-----------|----------------------------------------|
| Parameter | Identive driver for smart card readers |
| Registry  | scard.pcscd.identiv_enable             |
| Value     | <u>enabled</u> / disabled              |

- Updated **cryptovision sc/interface PKCS#11** library to version **7.0.5.592**.
- New smartcard reader driver for **Fujitsu KB SCR eSIG** version **5.0.24**.

## HID

- Added **layout toggle** feature to on-screen keyboard.

**More**

|            |                                                            |
|------------|------------------------------------------------------------|
| IGEL Setup | <b>Accessories &gt; On-Screen Keyboard &gt; Appearance</b> |
|------------|------------------------------------------------------------|



|           |                                                                   |
|-----------|-------------------------------------------------------------------|
| Parameter | Enable switching to alternative layout                            |
| Registry  | <code>userinterface.softkeyboard.enable_alternative_layout</code> |
| Value     | <code>enabled</code> / <code>disabled</code>                      |

If this is enabled there is a key on the on-screen keyboard for toggling between the normal layout and a reduced layout, that saves space on the screen and has more or less the same features as the number block of an ordinary keyboard with some extensions.

#### Base System

- Added support for **UEFI Secure Boot**.

When booted with Secure Boot the downgrade to a firmware version older than 10.04.100 is locked.

- Updated **kernel to version 4.15.15**
- Boot time optimization** (up to 25% faster)
- Switch power off on USB ports on shutdown and reboot**. The feature can be enabled in IGEL Setup. At the moment only IGEL H830C is supported.

[More](#)

|            |                                              |
|------------|----------------------------------------------|
| IGEL Setup | <b>System &gt; Registry</b>                  |
| Parameter  | Power off on shutdown                        |
| Registry   | <code>devices.usb.poweroff_shutdown</code>   |
| Value      | <code>enabled</code> / <code>disabled</code> |

- Added Unit ID in Application Launcher **About > Hardware** section.
- Showing **number of CPU cores** in Application Launcher **About > Hardware** section now.

#### Storage Devices

- Added support for **Mobile Device Access** feature in **Appliance Mode**. The Mobile Device Access tool can be opened via a new icon in the **In-session control bar**. The Mobile Device Access tool can also be started automatically.

[More](#)

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Autostart                                    |
| Registry  | <code>sessions.mtp-devices0.autostart</code> |
| Value     | <code>enabled</code> / <code>disabled</code> |



Mobile Device Access must be enabled at **IGEL Setup > System > Firmware Customization > Features**. Appliance Mode must be enabled at **IGEL Setup > Sessions > Appliance Mode**.

- The **Mobile Device Access tool** is now configurable at **IGEL Setup > Accessories > Mobile Device Access**.
- The **Mobile Device Access tray icon** respects the current theme now.

#### X11 System

- Added support for **XDMCP Appliance Mode**. The XDMCP connection is configurable.  
[More](#)

|            |                                                               |
|------------|---------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b>                           |
| Parameter  | XDMCP for this Display                                        |
| Registry   | x.xdmcp0.enabled                                              |
| Value      | enabled / <u>disabled</u>                                     |
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b>                           |
| Parameter  | Connection Type                                               |
| Registry   | x.xdmcp0.server.connectiontype                                |
| Range      | <b>indirect via localhost</b> / indirect / direct / broadcast |
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b>                           |
| Parameter  | Name or IP of server                                          |
| Registry   | x.xdmcp0.server.servername                                    |
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b>                           |
| Parameter  | Enable hotkeys for XDMCP Display                              |
| Registry   | x.xdmcp0.hotkeys.enabled                                      |
| Value      | <u>enabled</u> / disabled                                     |

The default hotkey to open IGEL Setup is: CTRL + ALT + F2. The setup page **User Interface > Display > XDMCP** was removed.

- Added **XC Font Service** support.

**More**

|            |                                                               |
|------------|---------------------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
| Parameter  | Enable XC Font Service                                        |
| Registry   | x.xc_fontservice.enabled                                      |
| Value      | enabled / <u>disabled</u>                                     |
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
| Parameter  | XC Font Server                                                |
| Registry   | x.xc_fontservice.fontserver                                   |
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
| Parameter  | Port Number                                                   |
| Registry   | x.xc_fontservice.port                                         |
| Value      | <u>7100</u>                                                   |
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
| Parameter  | Prefer Local Fonts                                            |
| Registry   | x.xc_fontservice.prefer_localfonts                            |
| Value      | enabled / <u>disabled</u>                                     |

- Added **auto detection of monitor refresh rate**. This can be controlled with new parameters.

**More**

|            |                                                  |
|------------|--------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Display &gt; Advanced</b> |
| Parameter  | Detect refresh rate automatically                |
| Registry   | x.xserver0.auto_frequency                        |
| Value      | <u>enabled</u> / disabled                        |



|            |                                                  |
|------------|--------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Display &gt; Advanced</b> |
| Parameter  | Detect refresh rate automatically                |
| Registry   | x.xserver0.screen.auto_frequency                 |
| Value      | <u>enabled</u> / disabled                        |

- Added xorg debug script **/etc/igel/igel\_debug\_tools/xorg-debug.sh** to make collecting Xorg debug data easier (a /tmp/xorg-debug.log file is generated).

#### Window Manager

- Added possibility to
  - a) **change the preferred placement mode** and
  - b) **modify the threshold value** up to which window size this placement mode should be chosen (otherwise window placement defaults to so called smart mode which tries to minimize overlapping).

#### More

|           |                                                                        |
|-----------|------------------------------------------------------------------------|
| Parameter | Preferred Placement                                                    |
| Registry  | windowmanager.wm0.variables.placement_mode                             |
| Value     | At mouse position / <u>Centered</u>                                    |
| Parameter | Maximum window size for which the preferred placement should apply     |
| Registry  | windowmanager.wm0.variables.placement_ratio                            |
| Value     | 0% / 10% / <u>20%</u> / 30% / 40% / 50% / 60% / 70% / 80% / 90% / 100% |

#### Audio

- Volume** of audio output and input can now be configured up to 150% at **IGEL Setup page Accessories > Sound Preferences > Options**.
- Added a parameter for log level configuration of **Pulseaudio** service.

#### More

|           |                                        |
|-----------|----------------------------------------|
| Parameter | Log level                              |
| Registry  | multimedia.pulseaudio.daemon.log-level |



|       |                                                |
|-------|------------------------------------------------|
| Range | debug / info / <u>notice</u> / warning / error |
|-------|------------------------------------------------|

## Misc

- An EULA must be accepted now in IGEL setup assistant before finalizing it and using the IGEL OS.

## Java

- Updated **Oracle JRE to 1.8U162**.

## Remote Management

- Added **new log file transfer mechanism** for UMS feature **Save TC files for support** (UMS 5.08.110 or higher required). By default, it collects all log files visible in system log viewer, system configuration files group.ini, setup.ini and dhclient lease files. More files can be specified at **IGEL Setup > Accessories > System Log Viewer > Options**. The resulting zip file has now a folder structure.

## IGEL Cloud Gateway

- Added **UMS structure tag** handling for usage with **ICG agent**.

## Hardware

- Added support for **IGEL UD7-LX 10**.

## Resolved Issues 10.03.500

## Citrix

- Fixed sporadic crashes of the **Citrix USB Daemon**.

## RDP / IGEL RDP Client 2

- Fixed passing **Ctrl+Alt+C keyboard shortcut** to RDP session.
- Fixed **smartcard redirection**: after session reconnection readers and cards were not connected any more in some cases.
- Fixed the **rdpdebugger** to work again (was broken in the previous release).
- Fixed misleading **RDP error message 'Authentication failed'** on wakeup from suspend mode
- Fixed **TCP timeout value** to get more stable **RDP connections** under certain circumstances.

## VMware Horizon

- Fixed bug which prevented **microphone redirection** in Horizon Client RDP sessions.

**More**

|            |                                                                  |
|------------|------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; RDP &gt; RDP Global &gt; Mapping &gt; Audio</b> |
| Parameter  | Audio recording                                                  |
| Registry   | <code>rdp.winconnect.rdppeai.enable</code>                       |
| Value      | enabled / <u>disabled</u>                                        |



## RedHat Enterprise Virtualization Client

- Fixed **display corruption** with Windows connections.

## Firefox

- Fixed possibility to **download files in the browser** if needed. The parameter to enable/disable file download is available here.

[More](#)

| IGEL Setup | Sessions > Browser > Browser Sessions > Window |
|------------|------------------------------------------------|
| Parameter  | Hide local filesystem                          |
| Registry   | sessions.browser.app.filepicker_dialog_hidden  |
| Value      | enabled / <u>disabled</u>                      |

If enabled, the user is not allowed to download or use any save-as functionality from menu, context or keyboard shortcut.

- Fixed bug which **prevented the download using the file dialog** (in the case you open a link to a file of unkown type).
- Fixed **unmounting of the Firefox profile partition during shutdown** - now it is unmounted in a determinate manner after Custom Partition.

## Network

- Fixed bug: **Network tray icons** sometimes didn't reappear after network restart.
- Fixed bug: **tcpdump debug tool** terminated immediately during boot.
- Fixed issue with **naming of USB ethernet devices**.
- Fixed wrong **LinkMode (10baseT/Half)** with autonegotiation and some USB ethernet devices.

## AppliDis

- Changed default value of **PasswordMode** from **cmdline** to **prompt** as suggested by Systancia.

## Smartcard

- Fixed driver for **Elatec RFID readers**. Before this fix the readers sometimes were not available after boot.
- Fixed VMware Horizon logon with OpenSC smartcards.

## CUPS Printing

- Fixed bug where the **user for printjobs** was not set to the **domain user**.

## Base System

- Fixed **Kerberos password change** to work also with transport protocol **TCP**. To force protocol TCP, prepend Domain Controllers with prefix "tcp/", e.g. "tcp/dc.example.com".
- Fixed **occasional desktop hang** in the local login or the network login mask after successful authentication.
- Fixed **password expiry notification** showing negative expiry period.
- Fixed **update to connect to SFTP** servers with very restrictive key exchange settings.



- Fixed input of the **reset key in reset to defaults boot**, if the administrator password is not available anymore. If more than 255 characters were entered in the 1st try, it was not possible to enter the reset key for a 2nd or 3rd time.
- Fixed **Active Directory logon with smartcard**: If the smartcard contains logon certificates for multiple users, it is possible to switch between these certificates and log on with the chosen certificate now.
- Fixed missing names for some **partitions** in update notification when having a user interface **language other than English**.
- Fixed problems with **never ending bootcode** update with some EFI BIOS variants.
- Fixed **ssh server port** configuration.
- Fixed **signotec signature pad** channel for Citrix.
- Increased stability of **signotec VCOM Daemon**.
- Remove residual information belonging to a **removed content from a custom partition**.
- Fixed **crash of xfce4-power-manager** after adding or removing input devices.

#### Custom Partition

- Fixed **automatic update of custom partition** - if download source isn't accessible then the content of the custom partition got lost.

#### Appliance Mode

- Fixed post session command **Logoff** in Appliance Mode.

#### X11 System

- Fixed **Elo-USB Touchscreen functionality** after reboot.
- Fixed **DisplayLink USB Support on UD3 LX50**.
- Fixed issue with **two monitors connected via DVI-D to HDMI adapter on a UD3 M330 (VIA)**. Added registry key to disable the new HDMI autodetection.

#### More

|           |                                             |
|-----------|---------------------------------------------|
| Parameter | Autodetect if DVI to HDMI adapter is in use |
| Registry  | x.drivers.via.autodetect_hdmi_output        |
| Value     | <u>enabled</u> / disabled                   |

- Fixed **wrong automatic resolution detection** if monitor does not have a preferred mode.
- Fixed **sporadic display corruptions** after monitors leaving the power saving mode.
- Improved handling of more than 2 screens.

#### Shadowing/VNC

- Fixed **sporadic VNC server crash**.

#### Audio

- Fixed **volume control of internal speaker in HP T610**.
- Fixed **automatic switch to output** over analog headphones.
- Not existing **S/PDIF inputs and outputs in Plantronics and Jabra USB headsets** are now ignored by audio subsystem (Pulseaudio).



- Added workaround in the kernel USB audio driver for **volume control on Sennheiser USB headsets.**

#### Remote Management

- Fixed **calculation of Unit ID for UMS management.** In some cases, it could happen that the MAC address of wrong network interface was chosen.
- Fixed **IGEL Setup Assistant** to get stopped when settings were received from UMS.

### 7.33.2 IGEL Universal Desktop OS3 / IGEL UD Pocket 10.03.500

#### Supported Hardware:

[Third-Party Devices Supported by IGEL OS 10<sup>463</sup>](#)

- [Versions 10.03.500\(see page 2381\)](#)
- [Security Fixes 10.03.500\(see page 2385\)](#)
- [General Information 10.03.500\(see page 2390\)](#)
- [Known Issues 10.03.500\(see page 2391\)](#)
- [New Features 10.03.500\(see page 2392\)](#)
- [Resolved Issues 10.03.500\(see page 2404\)](#)

#### Versions 10.03.500

##### • Clients

| Product                          | Version                       |
|----------------------------------|-------------------------------|
| Citrix HDX Realtime Media Engine | 2.3.0-1075                    |
| Citrix Receiver                  | 13.3.2.366713                 |
| Citrix Receiver                  | 13.5.0.10185126               |
| Citrix Receiver                  | 13.7.0.10276927               |
| deviceTRUST Citrix Channel       | 17.2.100.0                    |
| deviceTRUST RDP Channel          | 17.2.100.0                    |
| Ericom PowerTerm                 | 12.0.1.0.20170219.2-dev-34574 |
| Evidian AuthMgr                  | 1.5.6362                      |

<sup>463</sup> <https://kb.igel.com/display/hardware/Third+Party+Devices+Supported+by+IGEL+OS+10>



|                                                             |                   |
|-------------------------------------------------------------|-------------------|
| FabulaTech USB for Remote Desktop                           | 5.2.23            |
| Firefox                                                     | 52.5.0            |
| IBM iAccess Client Solutions                                | 1.1.5.0           |
| IGEL RDP Client                                             | 2.2               |
| Imprivata OneSign ProveID Embedded                          |                   |
| Leostream Java Connect                                      | 3.3.7.0           |
| NX Client                                                   | 5.3.12            |
| Open VPN                                                    | 2.3.10-1ubuntu2.1 |
| Oracle JRE                                                  | 1.8.0_152         |
| Parallels 2X Client                                         | 16.0.1.18456      |
| Remote Viewer for RedHat Enterprise Virtualization Desktops | 7.0               |
| Systancia AppliDis                                          | 4.0.0.17          |
| Thinlinc Client                                             | 4.8.0-5456        |
| ThinPrint Client                                            | 7.5.83            |
| Totem Media Player                                          | 2.30.2            |
| VMware Horizon Client                                       | 4.6.0-6617224     |

- **Dictation**

|                                                       |          |
|-------------------------------------------------------|----------|
| Diktamen driver for dictation                         |          |
| Driver for Grundig Business Systems dictation devices |          |
| Nuance Audio Extensions for dictation                 | B048     |
| Olympus driver for dictation                          | 20161103 |



|                       |        |
|-----------------------|--------|
| Philips Speech Driver | 12.5.4 |
|-----------------------|--------|

- **Signature**

|                         |       |
|-------------------------|-------|
| signotec Citrix Channel | 8.0.6 |
| signotec VCOM Daemon    | 2.0.0 |
| StepOver TCP Client     | 2.1.0 |

- **Smartcard**

|                                               |                  |
|-----------------------------------------------|------------------|
| PKCS#11 Library A.E.T SafeSign                | 3.0.101          |
| PKCS#11 Library Athena IDProtect              | 623.07           |
| PKCS#11 Library cryptovision sc/interface     | 6.6.3.502        |
| PKCS#11 Library Gemalto IDPrime               | 1.2.3            |
| PKCS#11 Library SecMaker NetID                | 6.6.0.30         |
| Reader Driver ACS CCID                        | 1.1.3            |
| Reader Driver Gemalto eToken                  | 9.0.43           |
| Reader Driver HID Global Omnikey CCID         | 4.2.4            |
| Reader Driver Identiv / SCM Microsystems CCID | 5.0.35           |
| Reader Driver Identiv eHealth200              | 1.0.5            |
| Reader Driver MUSCLE CCID                     | 1.4.27           |
| Reader Driver REINER SCT cyberJack            | 3.99.5final.SP09 |
| Resource Manager PC/SC Lite                   | 1.8.22           |
| Cherry USB2LAN Proxy                          | 3.0.0.4          |

- **System Components**

|                         |                 |
|-------------------------|-----------------|
| Bluetooth stack (bluez) | 5.46-0ubuntu3   |
| MESA OpenGL stack       | 17.2.2-0ubuntu1 |



|                                         |                           |
|-----------------------------------------|---------------------------|
| VAAPI ABI Version                       | 0.40                      |
| VDPAU Library version                   | 1.1.1-3ubuntu1            |
| Graphics Driver INTEL                   | 2.99.917+git20171109-igel |
| Graphics Driver ATI/RADEON              | 7.10.0-1                  |
| Graphics Driver ATI/AMDGPU              | 1.4.0-1                   |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.15-2                  |
| Graphics Driver Nvidia                  | 384.90-0ubuntu0.16.04.2   |
| Graphics Driver Vboxvideo               | 5.1.30-dfsg-1             |
| Graphics Driver VMware                  | 13.2.1-1build1            |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1             |
| Graphics Driver FBDEV                   | 0.4.4-1build5             |
| Graphics Driver VESA                    | 2.3.4-1build2             |
| Input Driver Evdev                      | 2.10.5-1ubuntu1           |
| Input Driver Elographics                | 1.4.1-1build5             |
| Input Driver eGalax                     | 2.5.5814                  |
| Input Driver Synaptics                  | 1.9.0-1ubuntu1            |
| Input Driver Vmmouse                    | 13.1.0-1ubuntu2           |
| Input Driver Wacom                      | 0.34.0-0ubuntu2           |
| Kernel                                  | 4.10.17 #41.45-udos-r1938 |
| Xorg X11 Server                         | 1.19.5-0ubuntu2           |
| CUPS printing daemon                    | 2.1.3-4ubuntu0.3          |



|                                 |                         |
|---------------------------------|-------------------------|
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1       |
| XFCE4 Windowmanager             | 4.12.3-1ubuntu2         |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.7       |
| NetworkManager                  | 1.2.0-0ubuntu0.16.04.3  |
| ModemManager                    | 1.4.12-1ubuntu1         |
| GStreamer                       | 0.10.0.10.36-2ubuntu0.1 |

- **Features with Limited IGEL Support**

|                          |  |
|--------------------------|--|
| Mobile Device Access USB |  |
|--------------------------|--|

## Security Fixes 10.03.500

- Fixed **wpa** security issues (KRACK vulnerability).

[More](#)

CVE-2017-13077

CVE-2017-13078

CVE-2017-13079

CVE-2017-13080

CVE-2017-13081

CVE-2017-13082

CVE-2017-13086

CVE-2017-13087

CVE-2017-13088

CVE-2016-4476

CVE-2016-4477

- Fixed **libgd2** security issues. CVE-2017-7890 and CVE-2017-6362.

- Fixed **graphite2** security issues.

[More](#)

CVE-2017-7778

CVE-2017-7777

CVE-2017-7776

CVE-2017-7775



CVE-2017-7774

CVE-2017-7773

CVE-2017-7772

CVE-2017-7771

- Fixed **ghostscript** security issues.

**More**

CVE-2017-9835

CVE-2017-9739

CVE-2017-9727

CVE-2017-9726

CVE-2017-9612

CVE-2017-9611

CVE-2017-11714

- Fixed **libmspack** security issues CVE-2017-6419 and CVE-2017-11423.

- Fixed **libsoup2.4** security issue CVE-2017-2885.

- Fixed **xorg-server** security issues.

**More**

CVE-2017-10971

CVE-2017-10972

CVE-2017-13721

CVE-2017-13723

CVE-2017-12176

CVE-2017-12177

CVE-2017-12178

CVE-2017-12179

CVE-2017-12180

CVE-2017-12181

CVE-2017-12182

CVE-2017-12183

CVE-2017-12184

CVE-2017-12185

CVE-2017-12186

CVE-2017-12187

- Fixed **bluez** security issue CVE-2017-1000250.

- Fixed **kernel** security issues.



**More**

CVE-2017-7541  
CVE-2017-1000112  
CVE-2017-1000111  
CVE-2017-7487  
CVE-2017-7533  
CVE-2017-1000251  
CVE-2017-14106  
CVE-2017-11176  
CVE-2017-10911  
CVE-2017-14340  
CVE-2017-10663  
CVE-2017-1000252  
CVE-2017-12188  
CVE-2017-12146

- Fixed **gdk-pixbuf** security issues CVE-2017-6311, CVE-2017-2870 and CVE-2017-2862.
- Fixed **tcpdump** security issues.

**More**

CVE-2017-13725, CVE-2017-13690, CVE-2017-13689, CVE-2017-13688,  
CVE-2017-13687, CVE-2017-13055, CVE-2017-13054, CVE-2017-13053,  
CVE-2017-13052, CVE-2017-13051, CVE-2017-13050, CVE-2017-13049,  
CVE-2017-13048, CVE-2017-13047, CVE-2017-13046, CVE-2017-13045,  
CVE-2017-13044, CVE-2017-13043, CVE-2017-13042, CVE-2017-13041,  
CVE-2017-13040, CVE-2017-13039, CVE-2017-13038, CVE-2017-13037,  
CVE-2017-13036, CVE-2017-13035, CVE-2017-13034, CVE-2017-13033,  
CVE-2017-13032, CVE-2017-13031, CVE-2017-13030, CVE-2017-13029,  
CVE-2017-13028, CVE-2017-13027, CVE-2017-13026, CVE-2017-13025,  
CVE-2017-13024, CVE-2017-13023, CVE-2017-13022, CVE-2017-13021,  
CVE-2017-13020, CVE-2017-13019, CVE-2017-13018, CVE-2017-13017,  
CVE-2017-13016, CVE-2017-13015, CVE-2017-13014, CVE-2017-13013,  
CVE-2017-13012, CVE-2017-13011, CVE-2017-13010, CVE-2017-13009,  
CVE-2017-13008, CVE-2017-13007, CVE-2017-13006, CVE-2017-13005,  
CVE-2017-13004, CVE-2017-13003, CVE-2017-13002, CVE-2017-13001,  
CVE-2017-13000, CVE-2017-12999, CVE-2017-12998, CVE-2017-12997,



CVE-2017-12996, CVE-2017-12995, CVE-2017-12994, CVE-2017-12993,  
CVE-2017-12992, CVE-2017-12991, CVE-2017-12990, CVE-2017-12989,  
CVE-2017-12988, CVE-2017-12987, CVE-2017-12986, CVE-2017-12985,  
CVE-2017-12902, CVE-2017-12901, CVE-2017-12900, CVE-2017-12899,  
CVE-2017-12898, CVE-2017-12897, CVE-2017-12896, CVE-2017-12895,  
CVE-2017-12894, CVE-2017-12893, CVE-2017-11543, CVE-2017-11542,  
CVE-2017-11541 and CVE-2017-11108.

- Fixed **libxml2** security issues.

**More**

CVE-2017-9050  
CVE-2017-9049  
CVE-2017-9048  
CVE-2017-9047  
CVE-2017-7376  
CVE-2017-7375  
CVE-2017-0663

- Fixed **samba** security issues.

**More**

CVE-2017-12163  
CVE-2017-12151  
CVE-2017-12150  
CVE-2017-15275  
CVE-2017-14746

- Fixed **libplist** security issue CVE-2017-7982.
- Fixed **nss** security issue CVE-2017-7805.
- Fixed **libidn** security issue CVE-2017-14062.
- Fixed **poppler** security issues.

**More**

CVE-2017-9776,  
CVE-2017-14977  
CVE-2017-14975  
CVE-2017-14929  
CVE-2017-14928  
CVE-2017-14926



CVE-2017-14617

CVE-2017-14520

CVE-2017-14519

CVE-2017-14518

CVE-2017-15565

- Fixed **dnsmasq** security issues.

[More](#)

CVE-2017-14496

CVE-2017-14495

CVE-2017-14494

CVE-2017-14493

CVE-2017-14492

CVE-2017-14491

- Fixed **libxfont** security issues CVE-2017-13722, CVE-2017-13720 and CVE-2017-16611.

- Fixed **curl** security issues.

[More](#)

CVE-2016-9586

CVE-2017-2629

CVE-2017-7407

CVE-2017-7468

CVE-2017-1000100

CVE-2017-1000101

CVE-2017-1000254

CVE-2017-1000257

CVE-2017-8816

CVE-2017-8817

- Fixed **libxfont2** security issues CVE-2017-13722, CVE-2017-13720 and CVE-2017-16611.

- Fixed **nvidia** security issues CVE-2017-6266, CVE-2017-6267 and CVE-2017-6272.

- Fixed **icu** security issue CVE-2017-14952.

- Fixed **wget** security issues CVE-2017-6508, CVE-2017-13090, CVE-2017-13089 and CVE-2016-7098.

- Fixed **systemd** security issue CVE-2017-15908.

- Fixed **openssl** security issues CVE-2017-3736 and CVE-2017-3735.

- Fixed **perl** security issues CVE-2017-12883 and CVE-2017-12837.

- Fixed **webkit2gtk** security issues.

[More](#)

CVE-2017-13803

CVE-2017-13802



CVE-2017-13798

CVE-2017-13796

CVE-2017-13795

CVE-2017-13794

CVE-2017-13793

CVE-2017-13792

CVE-2017-13791

CVE-2017-13788

CVE-2017-13785

CVE-2017-13784

CVE-2017-13783

- Fixed **db5.3** security issue CVE-2017-10140.
- Fixed **ldns** security issues CVE-2017-1000232 and CVE-2017-1000231.
- Fixed **python2.7** security issue CVE-2017-1000158.
- Fixed **python3.5** security issue CVE-2017-1000158.
- Fixed **libxcursor** security issue CVE-2017-16612.
- Fixed a security issue in the base system regarding of not resetting certain environment variables.
- Updated Firefox to version 52.5 ESR:
  - Fixes for **mfsa2017-25**, also known as: CVE-2017-7828, CVE-2017-7830, CVE-2017-7826.
  - Fixes for **mfsa2017-22**, also known as: CVE-2017-7793, CVE-2017-7818, CVE-2017-7819, CVE-2017-7824, CVE-2017-7805, CVE-2017-7814, CVE-2017-7823, CVE-2017-7810.

## General Information 10.03.500

The following clients and features are not supported anymore in version 10.03.550:

- Citrix Receiver 12.1 and 13.1
- Citrix Access Gateway Standard Plug-in
- Dell vWorkspace Connector for Linux
- Ericom PowerTerm Emulation 9 and 11
- Ericom Webconnect
- IGEL Legacy RDP Client (rdesktop)
- Virtual Bridges VERDE Client
- PPTP VPN Support
- IGEL Upgrade License Tool with IGEL Smartcard Token
- Remote Management by setup.ini file transfer (TFTP)
- XC Font Service
- Remote Access via RSH
- Legacy Philips Speech Driver
- Digital Persona Support
- Sane Scanner Support
- Softpro/Kofax Citrix Virtual Channel



- t-Systems TCOS Smartcard Support
- DUS Series touch screens
- Elo serial touch screens
- IGEL Smartcard without locking desktop
- VIA Graphics Support
- Storage Hotplug devices are not automatically removed anymore, instead they must be always ejected manually:
  - by panel tray icon
  - by an icon in the 'In-Session Control Bar' (configurable at **IGEL Setup > User Interface > Desktop**)
  - by a 'Safely Remove Hardware' session (configurable at **IGEL Setup > Accessories**)

The following clients and features are not available in release 10.03.550:

- Voip Client Ekiga
- X session (Xorg Xephyr)
- XDMCP
- Cherry eGK Channel
- Open VPN Smartcard Support
- NCP Secure Client
- Asian Input Methods
- Composite Manager

## Known Issues 10.03.500

### Citrix Receiver 13

- On devices with AMD/Radeon graphics chipsets and activated DRI3 X driver option **the hardware accelerated Citrix H.264 decoder plugin can hang**. To solve this issue deactivation of DRI3 option is necessary (default setting).

[More](#)

|           |                                                         |
|-----------|---------------------------------------------------------|
| Parameter | Use DRI3                                                |
| Registry  | x.drivers.use_dri3                                      |
| Value     | enabled / <u>disabled</u>                               |
| Parameter | Force usage of DRI3                                     |
| Registry  | x.drivers.amdgpu.force_dri3<br>x.drivers.ati.force_dri3 |
| Value     | enabled / <u>disabled</u>                               |



- Citrix StoreFront login with **Gemalto smartcard middleware** does not detect smartcard correctly when the card is inserted after start of login. As a workaround, insert the smartcard before starting StoreFront login.
- **No smooth playback** over **Nuance** channel if the dictation device isn't attached.

#### VMware Horizon

- **External drives** mounted already before connection do not appear in the remote desktop.  
**Workaround:** mapping the directory /media as a drive on desktop.  
 Then the external devices will show up inside the media drive.
- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local Storage Hotplug: On page **Devices > Storage Devices > Storage Hotplug**, put number of storage hotplug devices to 0.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Change on the following setup page is required: **Devices > Storage Devices > Storage Hotplug**.
 Activate **Enable dynamic drive mapping** and set **Number of storage hotplug devices** to at least 1.

#### Firefox

- Because the **support for the gstreamer framework** was dropped by recent Firefox versions, support for H264 decoding in the browser is not possible anymore due to licensing restrictions.

#### OpenConnect VPN

- **VPNs which need the OpenConnect** client cannot be used for firmware updates.

#### Evidian

- Active Directory users with a **password containing special characters** may have problems to authenticate with the configured session.  
 Known special characters which result in errors are:
  - ˋ (grave accent, ASCII code 96)
  - ˊ (acute accent, ASCII code 239)

#### New Features 10.03.500

##### Citrix Receiver 13

- Integrated **Citrix Receiver 13.8.0**.  
[More](#)

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Use Citrix Cloud with receiver 13.8 or newer |
|-----------|----------------------------------------------|



|          |                           |
|----------|---------------------------|
| Registry | ica.cloudconnect          |
| Value    | enabled / <u>disabled</u> |

- Support for **Azure** Active Directory (Azure AD) authentication
- Support for **Workspace** configuration from Citrix Cloud
- Integrated **Citrix Receiver 13.4.2**. Citrix Receiver version 13.5.0 was removed. Available Citrix Receiver versions: 13.3.2, 13.4.2, 13.7.0, 13.8.0 (default)
- Updated **Citrix HDX RTME** used for optimization of Skype for Business to 2.4.0.

#### RDP / IGEL RDP Client 2

- Added possibility to use **RDP local logon** for smartcard login. This can be activated in the setup.  
**More**

|           |                                          |
|-----------|------------------------------------------|
| Parameter | Enable smartcard support for local logon |
| Registry  | rdp.login.smartcard-local-logon          |
| Value     | enabled / <u>disabled</u>                |

By enabling this parameter local logon can be used for smartcard authentication. If **Username** is left empty the connection to the RDP server will be made without sending credentials, so you can choose **Smartcard** as login method in the microsoft login window. However this will not work with **NLA**.

- Added support for CredSSP up to version 6.

#### VMware Horizon

- Updated **VMware Horizon Client** to version **4.7.0-7395152**.
- Added key to enable **seamless window mode** in each application session.  
**More**

|           |                                                    |
|-----------|----------------------------------------------------|
| Parameter | Seamless Application Windows                       |
| Registry  | sessions.vdm_client.options.enable_seamless_window |
| Value     | enabled / <u>disabled</u>                          |

- Added possibility to use **Fabulatech USB Redirection** in a Horizon Client PCoIP session.  
**More**

|            |                                                                                                |
|------------|------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Fabulatech USB Redirection</b> |
| Parameter  | Enable Fabulatech USB Redirection                                                              |



|          |                                                    |
|----------|----------------------------------------------------|
| Registry | <code>vmware.view.usb.enable-fabulatech-usb</code> |
| Value    | <u>enabled</u> / <u>disabled</u>                   |

## Parallels Client

- Integrated **Parallels Client** version **16.2.0 (19039)**
  - Added support for USB Redirection, configurable at new IGEL Setup page **Sessions > Parallels Client > Parallels Client Global > USB Redirection.**
- [More](#)

| IGEL Setup | <b>Sessions &gt; Parallels Client &gt; Parallels Client Global &gt; USB Redirection</b> |
|------------|-----------------------------------------------------------------------------------------|
| Parameter  | Enable USB Redirection                                                                  |
| Registry   | <code>twox.usb_redirection.usb_enable</code>                                            |
| Value      | <u>enabled</u> / <u>disabled</u>                                                        |
| Parameter  | Product ID                                                                              |
| Registry   | <code>twox.usb_redirection.devicepolicy.product_rule.product</code>                     |
| Parameter  | Vendor ID                                                                               |
| Registry   | <code>twox.usb_redirection.devicepolicy.product_rule.vendor</code>                      |
| Parameter  | Rule                                                                                    |
| Registry   | <code>twox.usb_redirection.devicepolicy.product_rule.rule</code>                        |
| Value      | <u>Deny</u> / <u>Allow</u>                                                              |
| Parameter  | Name                                                                                    |
| Registry   | <code>twox.usb_redirection.devicepolicy.product_rule.name</code>                        |
| Value      | Policy Rule                                                                             |
| Parameter  | Automatically redirect all USB devices                                                  |
| Registry   | <code>twox.usb_redirection.devicepolicy.redirect_all</code>                             |



|       |                           |
|-------|---------------------------|
| Value | <u>enabled / disabled</u> |
|-------|---------------------------|

- Added support for **PTP/MTP** Redirection.

**More**

| IGEL Setup | <b>Sessions &gt; Parallels Client &gt; Parallels Client Global &gt; USB Redirection</b> |
|------------|-----------------------------------------------------------------------------------------|
| Parameter  | Enable PTP/MTP Redirection                                                              |
| Registry   | twox.mtp_redirection.mtp_enable                                                         |
| Value      | <u>enabled / disabled</u>                                                               |
| Parameter  | Product ID                                                                              |
| Registry   | twox.mtp_redirection.devicepolicy.product_rule.product                                  |
| Parameter  | Vendor ID                                                                               |
| Registry   | twox.mtp_redirection.devicepolicy.product_rule.vendor                                   |
| Parameter  | Rule                                                                                    |
| Registry   | twox.mtp_redirection.devicepolicy.product_rule.rule                                     |
| Value      | <u>Deny / Allow</u>                                                                     |
| Parameter  | Name                                                                                    |
| Registry   | twox.mtp_redirection.devicepolicy.product_rule.name                                     |
| Value      | Policy Rule                                                                             |
| Parameter  | Automatically redirect all PTP/MTP devices                                              |
| Registry   | twox.mtp_redirection.devicepolicy.redirect_all                                          |
| Value      | <u>enabled / disabled</u>                                                               |

- Added support for **Clipboard** Redirection.

**More**



|            |                                                                                                                         |
|------------|-------------------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Parallels Client &gt; Parallels Client Sessions &gt; Parallels Client Session &gt; Local Resources</b> |
| Parameter  | Connect clipboard                                                                                                       |
| Registry   | sessions.twox.local_resources.connect_clipboard                                                                         |
| Value      | <u>enabled</u> / disabled                                                                                               |

## VoIP

- Added **VoIP client Ekiga 4.0.1**.

## Firefox

- Updated **Firefox** to version **52.7.2 ESR**.
- Updated **Adobe Flash Player** download URL to version 29.0.0.113.

## Network

- Added **TTLS/PAP** and **TTLS/MSCHAPv2** to possible 802.1x authentication methods.
- Improved support for **Sierra EM7305 LTE** device (e.g. in Toshiba Portégé and Fujitsu LIFEBOOK E Series).

The EM7305 comes in various variants, e.g. one with ProductId 9041 and another one with ProductId 9063. The latter comes at least with one or with two USB configuration options. A device with only one configuration option has been observed on a Toshiba Tecra Z-50-D-115 notebook. It only works in MBIM mode and with IGEL firmware, when the device has successfully connected before with the same settings (particularly APN), e.g. under Microsoft Windows 10.

- Added support for **Sierra EM7455 WWAN module**.
- Added support for running the **Huawei E3531i WWAN** device in modem mode (in addition to HiLink mode).
- Added possibility to adopt the **hostname from a DHCP lease** as **permanent** terminal name. The purpose is to use the name received as part of a DHCP lease in future interactions with the DHCP server.

**More**

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Adopt permanent Terminal Name from DHCP lease |
| Registry  | network.dns.hostname_adopt_from_dhcp          |
| Value     | <u>enabled</u> / <u>disabled</u>              |

- NetworkManager** updated to version **1.2.2**
- ModemManager** updated to version **1.6.4**
- usb\_modeswitch** updated to version **2.5.1**



## Open VPN

- Added **Huawei HiLink Mobile Broadband USB** device as possible uplink to OpenVPN sessions.

## OpenConnect VPN

- Added **OpenConnect** client version **7.08** to connect to **Cisco AnyConnect** and **Juniper VPN**. The feature must be enabled.

[More](#)

|            |                                                                                                  |
|------------|--------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>System &gt; Firmware Customization &gt; Features</b>                                          |
| Parameter  | VPN OpenConnect (Limited support - functionality "as is", see product documentation for details) |
| Registry   | services.unsupported02.enabled                                                                   |
| Value      | enabled / <u>disabled</u>                                                                        |

- The OpenConnect VPN configuration is available at IGEL Setup page **Network > VPN > OpenConnect VPN**.

[More](#)

|            |                                                                                |
|------------|--------------------------------------------------------------------------------|
| IGEL Setup | <b>Network &gt; VPN &gt; OpenConnect VPN &gt; VPN OpenConnect &gt; Session</b> |
| Parameter  | Gateway                                                                        |
| Registry   | sessions.openconnect.vpnopts.gateway                                           |
| Parameter  | Enable Name/Password Authentication                                            |
| Registry   | sessions.openconnect.vpnopts.enable-name-pwd                                   |
| Value      | enabled / <u>disabled</u>                                                      |
| Parameter  | User Name                                                                      |
| Registry   | sessions.openconnect.vpnopts.username                                          |
| Parameter  | Password                                                                       |
| Registry   | sessions.openconnect.vpnopts.crypt_password                                    |
| Parameter  | CA Certificate                                                                 |



|           |                                                                       |
|-----------|-----------------------------------------------------------------------|
| Registry  | <code>sessions.openconnect.vpnopts.ca-cert</code>                     |
| Parameter | User Certificate                                                      |
| Registry  | <code>sessions.openconnect.vpnopts.user-cert</code>                   |
| Parameter | Private Key                                                           |
| Registry  | <code>sessions.openconnect.vpnopts.priv-key</code>                    |
| Parameter | Private Key password                                                  |
| Registry  | <code>sessions.openconnect.vpnopts.priv-key-pwd.crypt_password</code> |
| Parameter | Connect to Juniper Networks VPN                                       |
| Registry  | <code>sessions.openconnect%.vpnopts.is-juniper</code>                 |
| Value     | enabled / <u>disabled</u>                                             |

Tray icon is placed in the panel to disconnect from a running OpenConnect VPN connection.

#### Smartcard

- Added **CoolKey PKCS#11** library for access to **Common Access Card (CAC)** smartcards.  
[More](#)

|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Browser &gt; Browser Global &gt; Encryption</b>              |
| Parameter  | Coolkey Security Device                                                       |
| Registry   | <code>browserglobal.security_device.coolkey</code>                            |
| Value      | enabled / <u>disabled</u>                                                     |
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Smartcard</b> |
| Parameter  | Horizon logon with smartcards supported by Coolkey library                    |
| Registry   | <code>vmware.view.pkcs11.use_coolkey</code>                                   |



|            |                                                |
|------------|------------------------------------------------|
| Value      | <u>enabled / disabled</u>                      |
| IGEL Setup | <b>Security &gt; Smartcard &gt; Middleware</b> |
| Parameter  | Coolkey                                        |
| Registry   | scard.pkcs11.use_coolkey                       |
| Value      | <u>enabled / disabled</u>                      |

- Updated **Gemalto SafeNet PKCS#11** library to version **10.0.37-0**. This package replaces **Gemalto/ SafeNet eToken** and **Gemalto IDPrime** libraries.  
**Gemalto SafeNet** (formerly **Gemalto/SafeNet eToken**) now handles Gemalto cards and tokens including eToken and IDPrime.  
**Gemalto IDPrime** now handles IDPrime cards and tokens, preferred Common Criteria (CC) cards and tokens in Unlinked Mode.
- Added full integration of **OpenSC PKCS#11** library for access to smartcards.  
[More](#)

|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Browser &gt; Browser Global &gt; Encryption</b>              |
| Parameter  | OpenSC Security Device                                                        |
| Registry   | browserglobal.security_device.opensc                                          |
| Value      | <u>enabled / disabled</u>                                                     |
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Smartcard</b> |
| Parameter  | Horizon logon with smartcards supported by OpenSC library                     |
| Registry   | vmware.view.pkcs11.use_opensc                                                 |
| Value      | <u>enabled / disabled</u>                                                     |
| IGEL Setup | <b>Security &gt; Smartcard &gt; Middleware</b>                                |
| Parameter  | OpenSC                                                                        |
| Registry   | scard.pkcs11.use_opensc                                                       |
| Value      | <u>enabled / disabled</u>                                                     |

- Updated **MUSCLE CCID** smartcard reader driver to version **1.4.28**.



- Updated **ACS CCID** smartcard reader driver to version **1.1.5**.
- Updated **REINER SCT cyberJack** smartcard reader driver to version **3.99.5final.sp11**.
- Added parameter to disable **Identive CCID** smartcard reader driver. If this driver is disabled, some of the readers are handled by the MUSCLE CCID driver. This can help when problems with Identive reader driver occur.

**More**

|           |                                        |
|-----------|----------------------------------------|
| Parameter | Identive driver for smart card readers |
| Registry  | scard.pcscd.identiv_enable             |
| Value     | <u>enabled</u> / <u>disabled</u>       |

- Updated **cryptovision sc/interface PKCS#11** library to version **7.0.5.592**.
- New smartcard reader driver for **Fujitsu KB SCR eSIG** version **5.0.24**.

## HID

- Added **layout toggle** feature to on-screen keyboard.

**More**

|            |                                                            |
|------------|------------------------------------------------------------|
| IGEL Setup | <b>Accessories &gt; On-Screen Keyboard &gt; Appearance</b> |
| Parameter  | Enable switching to alternative layout                     |
| Registry   | userinterface.softkeyboard.enable_alternative_layout       |
| Value      | <u>enabled</u> / <u>disabled</u>                           |

If this is enabled there is a key on the on-screen keyboard for toggling between the normal layout and a reduced layout, that saves space on the screen and has more or less the same features as the number block of an ordinary keyboard with some extensions.

## Base System

- Added support for **UEFI Secure Boot**.

When booted with Secure Boot the downgrade to a firmware version older than 10.04.100 is locked.

- Updated **kernel to version 4.15.15**
- **Boot time optimization** (up to 25% faster)
- **Switch power off on USB ports on shutdown and reboot**. The feature can be enabled in IGEL Setup. At the moment only IGEL H830C is supported.

**More**

|            |                             |
|------------|-----------------------------|
| IGEL Setup | <b>System &gt; Registry</b> |
|------------|-----------------------------|



|           |                               |
|-----------|-------------------------------|
| Parameter | Power off on shutdown         |
| Registry  | devices.usb.poweroff_shutdown |
| Value     | enabled / <u>disabled</u>     |

- Added Unit ID in Application Launcher **About > Hardware** section.
- Showing **number of CPU cores** in Application Launcher **About > Hardware** section now.

#### Storage Devices

- Added support for **Mobile Device Access** feature in **Appliance Mode**. The Mobile Device Access tool can be opened via a new icon in the **In-session control bar**. The Mobile Device Access tool can also be started automatically.

**More**

|           |                                 |
|-----------|---------------------------------|
| Parameter | Autostart                       |
| Registry  | sessions.mtp-devices0.autostart |
| Value     | enabled / <u>disabled</u>       |

Mobile Device Access must be enabled at **IGEL Setup > System > Firmware Customization > Features**. Appliance Mode must be enabled at **IGEL Setup > Sessions > Appliance Mode**.

- The **Mobile Device Access tool** is now configurable at **IGEL Setup > Accessories > Mobile Device Access**.
- The **Mobile Device Access tray icon** respects the current theme now.

#### X11 System

- Added support for **XDMCP Appliance Mode**. The XDMCP connection is configurable.

**More**

|            |                                     |
|------------|-------------------------------------|
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b> |
| Parameter  | XDMCP for this Display              |
| Registry   | x.xdmcp0.enabled                    |
| Value      | enabled / <u>disabled</u>           |
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b> |
| Parameter  | Connection Type                     |



|            |                                                               |
|------------|---------------------------------------------------------------|
| Registry   | x.xdmcp0.server.connectiontype                                |
| Range      | <b>indirect via localhost</b> / indirect / direct / broadcast |
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b>                           |
| Parameter  | Name or IP of server                                          |
| Registry   | x.xdmcp0.server.servername                                    |
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b>                           |
| Parameter  | Enable hotkeys for XDMCP Display                              |
| Registry   | x.xdmcp0.hotkeys.enabled                                      |
| Value      | <u>enabled</u> / disabled                                     |

The default hotkey to open IGEL Setup is: CTRL + ALT + F2. The setup page **User Interface > Display > XDMCP** was removed.

- Added **XC Font Service** support.

**More**

|            |                                                               |
|------------|---------------------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
| Parameter  | Enable XC Font Service                                        |
| Registry   | x.xc_fontservice.enabled                                      |
| Value      | enabled / <u>disabled</u>                                     |
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
| Parameter  | XC Font Server                                                |
| Registry   | x.xc_fontservice.fontserver                                   |
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
| Parameter  | Port Number                                                   |
| Registry   | x.xc_fontservice.port                                         |



|            |                                                               |
|------------|---------------------------------------------------------------|
| Value      | <u>7100</u>                                                   |
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
| Parameter  | Prefer Local Fonts                                            |
| Registry   | x.xc_fontservice.prefer_localfonts                            |
| Value      | <u>enabled / disabled</u>                                     |

- Added **auto detection of monitor refresh rate**. This can be controlled with new parameters.  
**More**

|            |                                                  |
|------------|--------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Display &gt; Advanced</b> |
| Parameter  | Detect refresh rate automatically                |
| Registry   | x.xserver0.auto_frequency                        |
| Value      | <u>enabled / disabled</u>                        |

|            |                                                  |
|------------|--------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Display &gt; Advanced</b> |
| Parameter  | Detect refresh rate automatically                |
| Registry   | x.xserver0.screen.auto_frequency                 |
| Value      | <u>enabled / disabled</u>                        |

- Added xorg debug script **/etc/igel/igel\_debug\_tools/xorg-debug.sh** to make collecting Xorg debug data easier (a /tmp/xorg-debug.log file is generated).

## Window Manager

- Added possibility to
  - a) **change the preferred placement mode** and
  - b) **modify the threshold value** up to which window size this placement mode should be chosen (otherwise window placement defaults to so called smart mode which tries to minimize overlapping).

**More**

|           |                     |
|-----------|---------------------|
| Parameter | Preferred Placement |
|-----------|---------------------|



|           |                                                                        |
|-----------|------------------------------------------------------------------------|
| Registry  | windowmanager.wm0.variables.placement_mode                             |
| Value     | At mouse position / <u>Centered</u>                                    |
| Parameter | Maximum window size for which the preferred placement should apply     |
| Registry  | windowmanager.wm0.variables.placement_ratio                            |
| Value     | 0% / 10% / <u>20%</u> / 30% / 40% / 50% / 60% / 70% / 80% / 90% / 100% |

## Audio

- **Volume** of audio output and input can now be configured up to 150% at **IGEL Setup page Accessories > Sound Preferences > Options**.
- Added a parameter for log level configuration of **Pulseaudio** service.  
[More](#)

|           |                                                |
|-----------|------------------------------------------------|
| Parameter | Log level                                      |
| Registry  | multimedia.pulseaudio.daemon.log-level         |
| Range     | debug / info / <u>notice</u> / warning / error |

## Misc

- An EULA must be accepted now in IGEL setup assistant before finalizing it and using the IGEL OS.

## Java

- Updated **Oracle JRE to 1.8U162**.

## Remote Management

- Added **new log file transfer mechanism** for UMS feature **Save TC files for support** (UMS 5.08.110 or higher required). By default, it collects all log files visible in system log viewer, system configuration files group.ini, setup.ini and dhclient lease files. More files can be specified at **IGEL Setup > Accessories > System Log Viewer > Options**. The resulting zip file has now a folder structure.

## IGEL Cloud Gateway

- Added **UMS structure tag** handling for usage with **ICG agent**.

## Hardware

- Added support for **IGEL UD7-LX 10**.

## Resolved Issues 10.03.500

### Citrix



- Fixed sporadic crashes of the **Citrix USB Daemon**.

#### RDP / IGEL RDP Client 2

- Fixed passing **Ctrl+Alt+C keyboard shortcut** to RDP session.
- Fixed **smartcard redirection**: after session reconnection readers and cards were not connected any more in some cases.
- Fixed the **rdpdebugger** to work again (was broken in the previous release).
- Fixed misleading **RDP error message 'Authentication failed'** on wakeup from suspend mode
- Fixed **TCP timeout value** to get more stable **RDP connections** under certain circumstances.

#### VMware Horizon

- Fixed bug which prevented **microphone redirection** in Horizon Client RDP sessions.  
**More**

| IGEL Setup | <b>Sessions &gt; RDP &gt; RDP Global &gt; Mapping &gt; Audio</b> |
|------------|------------------------------------------------------------------|
| Parameter  | Audio recording                                                  |
| Registry   | rdp.winconnect.rdpai.enable                                      |
| Value      | enabled / <u>disabled</u>                                        |

#### RedHat Enterprise Virtualization Client

- Fixed **display corruption** with Windows connections.

#### Firefox

- Fixed possibility to **download files in the browser** if needed. The parameter to enable/disable file download is available here.

**More**

| IGEL Setup | <b>Sessions &gt; Browser &gt; Browser Sessions &gt; Window</b> |
|------------|----------------------------------------------------------------|
| Parameter  | Hide local filesystem                                          |
| Registry   | sessions.browser.app.filepicker_dialog_hidden                  |
| Value      | enabled / <u>disabled</u>                                      |

If enabled, the user is not allowed to download or use any save-as functionality from menu, context or keyboard shortcut.

- Fixed bug which **prevented the download using the file dialog** (in the case you open a link to a file of unknown type).
- Fixed **unmounting of the Firefox profile partition during shutdown** - now it is unmounted in a determinate manner after Custom Partition.

#### Network



- Fixed bug: **Network tray icons** sometimes didn't reappear after network restart.
- Fixed bug: **tcpdump debug tool** terminated immediately during boot.
- Fixed issue with **naming of USB ethernet devices**.
- Fixed wrong **LinkMode (10baseT/Half)** with autonegotiation and some USB ethernet devices.

#### AppliDis

- Changed default value of **PasswordMode** from **cmdline** to **prompt** as suggested by Systancia.

#### Smartcard

- Fixed driver for **Elatec RFID readers**. Before this fix the readers sometimes were not available after boot.
- Fixed VMware Horizon logon with OpenSC smartcards.

#### CUPS Printing

- Fixed bug where the **user for printjobs** was not set to the **domain user**.

#### Base System

- Fixed **Kerberos password change** to work also with transport protocol **TCP**. To force protocol TCP, prepend Domain Controllers with prefix "tcp/", e.g. "tcp/dc.example.com".
- Fixed **occasional desktop hang** in the local login or the network login mask after successful authentication.
- Fixed **password expiry notification** showing negative expiry period.
- Fixed **update to connect to SFTP** servers with very restrictive key exchange settings.
- Fixed input of the **reset key in reset to defaults boot**, if the administrator password is not available anymore. If more than 255 characters were entered in the 1st try, it was not possible to enter the reset key for a 2nd or 3rd time.
- Fixed **Active Directory logon with smartcard**: If the smartcard contains logon certificates for multiple users, it is possible to switch between these certificates and log on with the chosen certificate now.
- Fixed missing names for some **partitions** in update notification when having a user interface **language other than English**.
- Fixed problems with **never ending bootcode** update with some EFI BIOS variants.
- Fixed **ssh server port** configuration.
- Fixed **signotec signature pad** channel for Citrix.
- Increased stability of **signotec VCOM Daemon**.
- Remove residual information belonging to a **removed content from a custom partition**.
- Fixed **crash of xfce4-power-manager** after adding or removing input devices.

#### Custom Partition

- Fixed **automatic update of custom partition** - if download source isn't accessible then the content of the custom partition got lost.

#### Appliance Mode

- Fixed post session command **Logoff** in Appliance Mode.

#### X11 System

- Fixed **Elo-USB Touchscreen functionality** after reboot.



- Fixed **DisplayLink USB Support on UD3 LX50**.
- Fixed issue with **two monitors connected via DVI-D to HDMI adapter on a UD3 M330 (VIA)**.  
Added registry key to disable the new HDMI autodetection.

[More](#)

|           |                                             |
|-----------|---------------------------------------------|
| Parameter | Autodetect if DVI to HDMI adapter is in use |
| Registry  | x.drivers.via.autodetect_hdmi_output        |
| Value     | <u>enabled</u> / disabled                   |

- Fixed **wrong automatic resolution detection** if monitor does not have a preferred mode.
- Fixed **sporadic display corruptions** after monitors leaving the power saving mode.
- Improved handling of more than 2 screens.

#### Shadowing/VNC

- Fixed **sporadic VNC server crash**.

#### Audio

- Fixed **volume control of internal speaker in HP T610**.
- Fixed **automatic switch to output** over analog headphones.
- Not existing **S/PDIF inputs and outputs in Plantronics and Jabra USB headsets** are now ignored by audio subsystem (Pulseaudio).
- Added workaround in the kernel USB audio driver for **volume control on Sennheiser USB headsets**.

#### Remote Management

- Fixed **calculation of Unit ID for UMS management**. In some cases, it could happen that the MAC address of wrong network interface was chosen.
- Fixed **IGEL Setup Assistant** to get stopped when settings were received from UMS.

### 7.33.3 IGEL Universal Desktop Converter (UDC3) 10.03.500

#### Supported Hardware:

[Third-Party Devices Supported by IGEL OS 10<sup>464</sup>](#)

- 
- [Versions 10.03.500\(see page 2407\)](#)
  - [New Features 10.03.500\(see page 2409\)](#)
  - [Resolved Issues 10.03.500\(see page 2421\)](#)

#### Versions 10.03.500

- **Clients**

---

<sup>464</sup> <https://kb.igel.com/display/hardware/Third+Party+Devices+Supported+by+IGEL+OS+10>



|            |                  |
|------------|------------------|
| Oracle JRE | <b>1.8.0_152</b> |
|------------|------------------|

- System Components**

|                                         |                           |
|-----------------------------------------|---------------------------|
| Bluetooth stack (bluez)                 | 5.46-0ubuntu3             |
| MESA OpenGL stack                       | 17.2.2-0ubuntu1           |
| VAAPI ABI Version                       | 0.40                      |
| Graphics Driver INTEL                   | 2.99.917+git20171109-igel |
| Graphics Driver ATI/Radeon              | 7.10.0-1                  |
| Graphics Driver ATI/AMDGPU              | 1.4.0-1                   |
| Graphics Driver Nouveau (Nvidia Legacy) | 1.0.15-2                  |
| Graphics Driver Vboxvideo               | 5.1.30-dfsg-1             |
| Graphics Driver VMware                  | 13.2.1-1build1            |
| Graphics Driver QXL (Spice)             | 0.1.5-2build1             |
| Graphics Driver FBDEV                   | 0.4.4-1build5             |
| Graphics Driver VESA                    | 2.3.4-1build2             |
| Input Driver Evdev                      | 2.10.5-1ubuntu1           |
| Input Driver Elographics                | 1.4.1-1build5             |
| Input Driver Synaptics                  | 1.9.0-1ubuntu1            |
| Input Driver Vmmouse                    | 13.1.0-1ubuntu2           |
| Input Driver Wacom                      | 0.34.0-0ubuntu2           |
| Kernel                                  | 4.10.17 #41.45-udos-r1938 |
| Xorg X11 Server                         | 1.19.5-0ubuntu2           |



|                                 |                   |
|---------------------------------|-------------------|
| Lightdm graphical login manager | 1.18.3-0ubuntu1.1 |
| XFCE4 Windowmanager             | 4.12.3-1ubuntu2   |
| ISC DHCP Client                 | 4.3.3-5ubuntu12.7 |

## New Features 10.03.500

### Citrix Receiver 13

- Integrated **Citrix Receiver 13.8.0**.

[More](#)

|           |                                              |
|-----------|----------------------------------------------|
| Parameter | Use Citrix Cloud with receiver 13.8 or newer |
| Registry  | ica.cloudconnect                             |
| Value     | enabled / <u>disabled</u>                    |

- Support for **Azure** Active Directory (Azure AD) authentication
- Support for **Workspace** configuration from Citrix Cloud
- Integrated **Citrix Receiver 13.4.2**. Citrix Receiver version 13.5.0 was removed. Available Citrix Receiver versions: 13.3.2, 13.4.2, 13.7.0, 13.8.0 (default)
- Updated **Citrix HDX RTME** used for optimization of Skype for Business to 2.4.0.

### RDP / IGEL RDP Client 2

- Added possibility to use **RDP local logon** for smartcard login. This can be activated in the setup.

[More](#)

|           |                                          |
|-----------|------------------------------------------|
| Parameter | Enable smartcard support for local logon |
| Registry  | rdp.login.smartcard-local-logon          |
| Value     | enabled / <u>disabled</u>                |

By enabling this parameter local logon can be used for smartcard authentication. If **Username** is left empty the connection to the RDP server will be made without sending credentials, so you can choose **Smartcard** as login method in the microsoft login window. However this will not work with **NLA**.

- Added support for CredSSP up to version 6.

### VMware Horizon

- Updated **VMware Horizon Client** to version **4.7.0-7395152**.
- Added key to enable **seamless window mode** in each application session.

[More](#)



|           |                                                    |
|-----------|----------------------------------------------------|
| Parameter | Seamless Application Windows                       |
| Registry  | sessions.vdm_client.options.enable_seamless_window |
| Value     | enabled / <u>disabled</u>                          |

- Added possibility to use **Fabulatech USB Redirection** in a Horizon Client PCoIP session.

[More](#)

|            |                                                                                                |
|------------|------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Fabulatech USB Redirection</b> |
| Parameter  | Enable Fabulatech USB Redirection                                                              |
| Registry   | vmware.view.usb.enable-fabulatech-usb                                                          |
| Value      | enabled / <u>disabled</u>                                                                      |

#### Parallels Client

- Integrated **Parallels Client** version **16.2.0 (19039)**
- Added support for USB Redirection, configurable at new IGEL Setup page **Sessions > Parallels Client > Parallels Client Global > USB Redirection**.

[More](#)

|            |                                                                                         |
|------------|-----------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Parallels Client &gt; Parallels Client Global &gt; USB Redirection</b> |
| Parameter  | Enable USB Redirection                                                                  |
| Registry   | twox.usb_redirection.usb_enable                                                         |
| Value      | enabled / <u>disabled</u>                                                               |
| Parameter  | Product ID                                                                              |
| Registry   | twox.usb_redirection.devicepolicy.product_rule.product                                  |
| Parameter  | Vendor ID                                                                               |
| Registry   | twox.usb_redirection.devicepolicy.product_rule.vendor                                   |
| Parameter  | Rule                                                                                    |
| Registry   | twox.usb_redirection.devicepolicy.product_rule.rule                                     |



|           |                                                     |
|-----------|-----------------------------------------------------|
| Value     | <u>Deny / Allow</u>                                 |
| Parameter | Name                                                |
| Registry  | twox.usb_redirection.devicepolicy.product_rule.name |
| Value     | Policy Rule                                         |
| Parameter | Automatically redirect all USB devices              |
| Registry  | twox.usb_redirection.devicepolicy.redirect_all      |
| Value     | <u>enabled / disabled</u>                           |

- Added support for **PTP/MTP Redirection**.

[More](#)

|            |                                                                                         |
|------------|-----------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Parallels Client &gt; Parallels Client Global &gt; USB Redirection</b> |
| Parameter  | Enable PTP/MTP Redirection                                                              |
| Registry   | twox.mtp_redirection.mtp_enable                                                         |
| Value      | <u>enabled / disabled</u>                                                               |
| Parameter  | Product ID                                                                              |
| Registry   | twox.mtp_redirection.devicepolicy.product_rule.product                                  |
| Parameter  | Vendor ID                                                                               |
| Registry   | twox.mtp_redirection.devicepolicy.product_rule.vendor                                   |
| Parameter  | Rule                                                                                    |
| Registry   | twox.mtp_redirection.devicepolicy.product_rule.rule                                     |
| Value      | <u>Deny / Allow</u>                                                                     |
| Parameter  | Name                                                                                    |
| Registry   | twox.mtp_redirection.devicepolicy.product_rule.name                                     |



| Value     | Policy Rule                                    |
|-----------|------------------------------------------------|
| Parameter | Automatically redirect all PTP/MTP devices     |
| Registry  | twox.mtp_redirection.devicepolicy.redirect_all |
| Value     | <u>enabled</u> / <u>disabled</u>               |

- Added support for **Clipboard** Redirection.

|            |                                                                                                                         |
|------------|-------------------------------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Parallels Client &gt; Parallels Client Sessions &gt; Parallels Client Session &gt; Local Resources</b> |
| Parameter  | Connect clipboard                                                                                                       |
| Registry   | sessions.twox.local_resources.connect_clipboard                                                                         |
| Value      | <u>enabled</u> / <u>disabled</u>                                                                                        |

## VoIP

- Added **VoIP client Ekiga 4.0.1**.

## Firefox

- Updated **Firefox** to version **52.7.2 ESR**.
- Updated **Adobe Flash Player** download URL to version 29.0.0.113.

## Network

- Added **TTLS/PAP** and **TTLS/MSCHAPv2** to possible 802.1x authentication methods.
- Improved support for **Sierra EM7305 LTE** device (e.g. in Toshiba Portégé and Fujitsu LIFEBOOK E Series).

The EM7305 comes in various variants, e.g. one with ProductId 9041 and another one with ProductId 9063. The latter comes at least with one or with two USB configuration options. A device with only one configuration option has been observed on a Toshiba Tecra Z-50-D-115 notebook. It only works in MBIM mode and with IGEL firmware, when the device has successfully connected before with the same settings (particularly APN), e.g. under Microsoft Windows 10.

- Added support for **Sierra EM7455 WWAN module**.
- Added support for running the **Huawei E3531i WWAN** device in modem mode (in addition to HiLink mode).
- Added possibility to adopt the **hostname from a DHCP lease** as **permanent** terminal name. The purpose is to use the name received as part of a DHCP lease in future interactions with the DHCP server.

**More**

|           |                                               |
|-----------|-----------------------------------------------|
| Parameter | Adopt permanent Terminal Name from DHCP lease |
| Registry  | network.dns.hostname_adopt_from_dhcp          |
| Value     | enabled / <u>disabled</u>                     |

- **NetworkManager** updated to version **1.2.2**
- **ModemManager** updated to version **1.6.4**
- **usb\_modeswitch** updated to version **2.5.1**

## Open VPN

- Added **Huawei HiLink Mobile Broadband USB** device as possible uplink to OpenVPN sessions.

## OpenConnect VPN

- Added **OpenConnect** client version **7.08** to connect to **Cisco AnyConnect** and **Juniper VPN**. The feature must be enabled.

**More**

|            |                                                                                                  |
|------------|--------------------------------------------------------------------------------------------------|
| IGEL Setup | <b>System &gt; Firmware Customization &gt; Features</b>                                          |
| Parameter  | VPN OpenConnect (Limited support - functionality "as is", see product documentation for details) |
| Registry   | services.unsupported02.enabled                                                                   |
| Value      | enabled / <u>disabled</u>                                                                        |

- The OpenConnect VPN configuration is available at IGEL Setup page **Network > VPN > OpenConnect VPN**.

**More**

|            |                                                                                |
|------------|--------------------------------------------------------------------------------|
| IGEL Setup | <b>Network &gt; VPN &gt; OpenConnect VPN &gt; VPN OpenConnect &gt; Session</b> |
| Parameter  | Gateway                                                                        |
| Registry   | sessions.openconnect.vpnopts.gateway                                           |
| Parameter  | Enable Name/Password Authentication                                            |
| Registry   | sessions.openconnect.vpnopts.enable-name-pwd                                   |
| Value      | enabled / <u>disabled</u>                                                      |



|           |                                                          |
|-----------|----------------------------------------------------------|
| Parameter | User Name                                                |
| Registry  | sessions.openconnect.vpnopts.username                    |
| Parameter | Password                                                 |
| Registry  | sessions.openconnect.vpnopts.crypt_password              |
| Parameter | CA Certificate                                           |
| Registry  | sessions.openconnect.vpnopts.ca-cert                     |
| Parameter | User Certificate                                         |
| Registry  | sessions.openconnect.vpnopts.user-cert                   |
| Parameter | Private Key                                              |
| Registry  | sessions.openconnect.vpnopts.priv-key                    |
| Parameter | Private Key password                                     |
| Registry  | sessions.openconnect.vpnopts.priv-key-pwd.crypt_password |
| Parameter | Connect to Juniper Networks VPN                          |
| Registry  | sessions.openconnect%.vpnopts.is-juniper                 |
| Value     | enabled / <u>disabled</u>                                |

Tray icon is placed in the panel to disconnect from a running OpenConnect VPN connection.

## Smartcard

- Added **CoolKey PKCS#11** library for access to **Common Access Card (CAC)** smartcards.  
[More](#)

|            |                                                                  |
|------------|------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Browser &gt; Browser Global &gt; Encryption</b> |
| Parameter  | Coolkey Security Device                                          |



|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| Registry   | browserglobal.security_device.coolkey                                         |
| Value      | enabled / <u>disabled</u>                                                     |
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Smartcard</b> |
| Parameter  | Horizon logon with smartcards supported by Coolkey library                    |
| Registry   | vmware.view.pkcs11.use_coolkey                                                |
| Value      | enabled / <u>disabled</u>                                                     |
| IGEL Setup | <b>Security &gt; Smartcard &gt; Middleware</b>                                |
| Parameter  | Coolkey                                                                       |
| Registry   | scard.pkcs11.use_coolkey                                                      |
| Value      | enabled / <u>disabled</u>                                                     |

- Updated **Gemalto SafeNet PKCS#11** library to version **10.0.37-0**. This package replaces **Gemalto/SafeNet eToken** and **Gemalto IDPrime** libraries.  
**Gemalto SafeNet** (formerly **Gemalto/SafeNet eToken**) now handles Gemalto cards and tokens including eToken and IDPrime.  
**Gemalto IDPrime** now handles IDPrime cards and tokens, preferred Common Criteria (CC) cards and tokens in Unlinked Mode.
- Added full integration of **OpenSC PKCS#11** library for access to smartcards.  
[More](#)

|            |                                                                               |
|------------|-------------------------------------------------------------------------------|
| IGEL Setup | <b>Sessions &gt; Browser &gt; Browser Global &gt; Encryption</b>              |
| Parameter  | OpenSC Security Device                                                        |
| Registry   | browserglobal.security_device.opensc                                          |
| Value      | enabled / <u>disabled</u>                                                     |
| IGEL Setup | <b>Sessions &gt; Horizon Client &gt; Horizon Client Global &gt; Smartcard</b> |
| Parameter  | Horizon logon with smartcards supported by OpenSC library                     |
| Registry   | vmware.view.pkcs11.useOpensc                                                  |



|            |                                                |
|------------|------------------------------------------------|
| Value      | <u>enabled / disabled</u>                      |
| IGEL Setup | <b>Security &gt; Smartcard &gt; Middleware</b> |
| Parameter  | OpenSC                                         |
| Registry   | scard.pkcs11.use_opensc                        |
| Value      | <u>enabled / disabled</u>                      |

- Updated **MUSCLE CCID** smartcard reader driver to version **1.4.28**.
- Updated **ACS CCID** smartcard reader driver to version **1.1.5**.
- Updated **REINER SCT cyberJack** smartcard reader driver to version **3.99.5final.sp11**.
- Added parameter to disable **Identive CCID** smartcard reader driver. If this driver is disabled, some of the readers are handled by the MUSCLE CCID driver. This can help when problems with Identive reader driver occur.

[More](#)

|           |                                        |
|-----------|----------------------------------------|
| Parameter | Identive driver for smart card readers |
| Registry  | scard.pcscd.identiv_enable             |
| Value     | <u>enabled / disabled</u>              |

- Updated **cryptovision sc/interface PKCS#11** library to version **7.0.5.592**.
- New smartcard reader driver for **Fujitsu KB SCR eSIG** version **5.0.24**.

## HID

- Added **layout toggle** feature to on-screen keyboard.

[More](#)

|            |                                                            |
|------------|------------------------------------------------------------|
| IGEL Setup | <b>Accessories &gt; On-Screen Keyboard &gt; Appearance</b> |
| Parameter  | Enable switching to alternative layout                     |
| Registry   | userinterface.softkeyboard.enable_alternative_layout       |
| Value      | <u>enabled / disabled</u>                                  |

If this is enabled there is a key on the on-screen keyboard for toggling between the normal layout and a reduced layout, that saves space on the screen and has more or less the same features as the number block of an ordinary keyboard with some extensions.

## Base System



- Added support for **UEFI Secure Boot**.

When booted with Secure Boot the downgrade to a firmware version older than 10.04.100 is locked.

- Updated **kernel to version 4.15.15**
- Boot time optimization** (up to 25% faster)
- Switch power off on USB ports on shutdown and reboot.** The feature can be enabled in IGEL Setup. At the moment only IGEL H830C is supported.

[More](#)

|            |                               |
|------------|-------------------------------|
| IGEL Setup | <b>System &gt; Registry</b>   |
| Parameter  | Power off on shutdown         |
| Registry   | devices.usb.poweroff_shutdown |
| Value      | enabled / <u>disabled</u>     |

- Added Unit ID in Application Launcher **About > Hardware** section.
- Showing **number of CPU cores** in Application Launcher **About > Hardware** section now.

## Storage Devices

- Added support for **Mobile Device Access** feature in **Appliance Mode**. The Mobile Device Access tool can be opened via a new icon in the **In-session control bar**. The Mobile Device Access tool can also be started automatically.

[More](#)

|           |                                 |
|-----------|---------------------------------|
| Parameter | Autostart                       |
| Registry  | sessions.mtp-devices0.autostart |
| Value     | enabled / <u>disabled</u>       |

Mobile Device Access must be enabled at **IGEL Setup > System > Firmware Customization > Features**. Appliance Mode must be enabled at **IGEL Setup > Sessions > Appliance Mode**.

- The **Mobile Device Access tool** is now configurable at **IGEL Setup > Accessories > Mobile Device Access**.
- The **Mobile Device Access tray icon** respects the current theme now.

## X11 System

- Added support for **XDMCP Appliance Mode**. The XDMCP connection is configurable.

[More](#)

|            |                                     |
|------------|-------------------------------------|
| IGEL Setup | <b>Sessions &gt; Appliance Mode</b> |
|------------|-------------------------------------|



|                                                                                                                                      |                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Parameter                                                                                                                            | XDMCP for this Display                                        |
| Registry                                                                                                                             | x.xdmcp0.enabled                                              |
| Value                                                                                                                                | enabled / <u>disabled</u>                                     |
| IGEL Setup                                                                                                                           | <b>Sessions &gt; Appliance Mode</b>                           |
| Parameter                                                                                                                            | Connection Type                                               |
| Registry                                                                                                                             | x.xdmcp0.server.connectiontype                                |
| Range                                                                                                                                | <b>indirect via localhost</b> / indirect / direct / broadcast |
| IGEL Setup                                                                                                                           | <b>Sessions &gt; Appliance Mode</b>                           |
| Parameter                                                                                                                            | Name or IP of server                                          |
| Registry                                                                                                                             | x.xdmcp0.server.servername                                    |
| IGEL Setup                                                                                                                           | <b>Sessions &gt; Appliance Mode</b>                           |
| Parameter                                                                                                                            | Enable hotkeys for XDMCP Display                              |
| Registry                                                                                                                             | x.xdmcp0.hotkeys.enabled                                      |
| Value                                                                                                                                | <u>enabled</u> / disabled                                     |
| The default hotkey to open IGEL Setup is: CTRL + ALT + F2. The setup page <b>User Interface &gt; Display &gt; XDMCP</b> was removed. |                                                               |

- Added **XC Font Service** support.  
[More](#)

|            |                                                               |
|------------|---------------------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
| Parameter  | Enable XC Font Service                                        |
| Registry   | x.xc_fontservice.enabled                                      |
| Value      | enabled / <u>disabled</u>                                     |
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |



|            |                                                               |
|------------|---------------------------------------------------------------|
| Parameter  | XC Font Server                                                |
| Registry   | x.xc_fontservice.fontserver                                   |
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
| Parameter  | Port Number                                                   |
| Registry   | x.xc_fontservice.port                                         |
| Value      | <u>7100</u>                                                   |
| IGEL Setup | <b>User Interface &gt; Font Services &gt; XC Font Service</b> |
| Parameter  | Prefer Local Fonts                                            |
| Registry   | x.xc_fontservice.prefer_localfonts                            |
| Value      | enabled / <u>disabled</u>                                     |

- Added **auto detection of monitor refresh rate**. This can be controlled with new parameters.  
[More](#)

|            |                                                  |
|------------|--------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Display &gt; Advanced</b> |
| Parameter  | Detect refresh rate automatically                |
| Registry   | x.xserver0.auto_frequency                        |
| Value      | <u>enabled</u> / disabled                        |

|            |                                                  |
|------------|--------------------------------------------------|
| IGEL Setup | <b>User Interface &gt; Display &gt; Advanced</b> |
| Parameter  | Detect refresh rate automatically                |
| Registry   | x.xserver0.screen.auto_frequency                 |
| Value      | <u>enabled</u> / disabled                        |

- Added xorg debug script **/etc/igel/igel\_debug\_tools/xorg-debug.sh** to make collecting Xorg debug data easier (a /tmp/xorg-debug.log file is generated).



## Window Manager

- Added possibility to
  - a) **change the preferred placement mode** and
  - b) **modify the threshold value** up to which window size this placement mode should be chosen (otherwise window placement defaults to so called smart mode which tries to minimize overlapping).

**More**

|           |                                                                        |
|-----------|------------------------------------------------------------------------|
| Parameter | Preferred Placement                                                    |
| Registry  | windowmanager.wm0.variables.placement_mode                             |
| Value     | At mouse position / <u>Centered</u>                                    |
| Parameter | Maximum window size for which the preferred placement should apply     |
| Registry  | windowmanager.wm0.variables.placement_ratio                            |
| Value     | 0% / 10% / <u>20%</u> / 30% / 40% / 50% / 60% / 70% / 80% / 90% / 100% |

## Audio

- Volume** of audio output and input can now be configured up to 150% at **IGEL Setup page Accessories > Sound Preferences > Options**.
- Added a parameter for log level configuration of **Pulseaudio** service.

**More**

|           |                                                |
|-----------|------------------------------------------------|
| Parameter | Log level                                      |
| Registry  | multimedia.pulseaudio.daemon.log-level         |
| Range     | debug / info / <u>notice</u> / warning / error |

## Misc

- An EULA must be accepted now in IGEL setup assistant before finalizing it and using the IGEL OS.

## Java

- Updated **Oracle JRE to 1.8U162**.

## Remote Management

- Added **new log file transfer mechanism** for UMS feature **Save TC files for support** (UMS 5.08.110 or higher required). By default, it collects all log files visible in system log viewer, system configuration files group.ini, setup.ini and dhclient lease files. More files can be specified at **IGEL**



**Setup > Accessories > System Log Viewer > Options.** The resulting zip file has now a folder structure.

#### IGEL Cloud Gateway

- Added **UMS structure tag** handling for usage with **ICG agent**.

#### Hardware

- Added support for **IGEL UD7-LX 10**.

### Resolved Issues 10.03.500

#### Citrix

- Fixed sporadic crashes of the **Citrix USB Daemon**.

#### RDP / IGEL RDP Client 2

- Fixed passing **Ctrl+Alt+C keyboard shortcut** to RDP session.
- Fixed **smartcard redirection**: after session reconnection readers and cards were not connected any more in some cases.
- Fixed the **rdpdebugger** to work again (was broken in the previous release).
- Fixed misleading **RDP error message 'Authentication failed'** on wakeup from suspend mode
- Fixed **TCP timeout value** to get more stable **RDP connections** under certain circumstances.

#### VMware Horizon

- Fixed bug which prevented **microphone redirection** in Horizon Client RDP sessions.
- More**

| IGEL Setup | Sessions > RDP > RDP Global > Mapping > Audio |
|------------|-----------------------------------------------|
| Parameter  | Audio recording                               |
| Registry   | rdp.winconnect.rdppeai.enable                 |
| Value      | enabled / <u>disabled</u>                     |

#### RedHat Enterprise Virtualization Client

- Fixed **display corruption** with Windows connections.

#### Firefox

- Fixed possibility to **download files in the browser** if needed. The parameter to enable/disable file download is available here.

| IGEL Setup | Sessions > Browser > Browser Sessions > Window |
|------------|------------------------------------------------|
| Parameter  | Hide local filesystem                          |



|          |                                               |
|----------|-----------------------------------------------|
| Registry | sessions.browser.app.filepicker_dialog_hidden |
| Value    | enabled / <u>disabled</u>                     |

If enabled, the user is not allowed to download or use any save-as functionality from menu, context or keyboard shortcut.

- Fixed bug which **prevented the download using the file dialog** (in the case you open a link to a file of unknown type).
- Fixed **unmounting of the Firefox profile partition during shutdown** - now it is unmounted in a determinate manner after Custom Partition.

#### Network

- Fixed bug: **Network tray icons** sometimes didn't reappear after network restart.
- Fixed bug: **tcpdump debug tool** terminated immediately during boot.
- Fixed issue with **naming of USB ethernet devices**.
- Fixed wrong **LinkMode (10baseT/Half)** with autonegotiation and some USB ethernet devices.

#### AppliDis

- Changed default value of **PasswordMode** from **cmdline** to **prompt** as suggested by Systancia.

#### Smartcard

- Fixed driver for **Elatec RFID readers**. Before this fix the readers sometimes were not available after boot.
- Fixed VMware Horizon logon with OpenSC smartcards.

#### CUPS Printing

- Fixed bug where the **user for printjobs** was not set to the **domain user**.

#### Base System

- Fixed **Kerberos password change** to work also with transport protocol **TCP**. To force protocol TCP, prepend Domain Controllers with prefix "tcp/", e.g. "tcp/dc.example.com".
- Fixed **occasional desktop hang** in the local login or the network login mask after successful authentication.
- Fixed **password expiry notification** showing negative expiry period.
- Fixed **update to connect to SFTP** servers with very restrictive key exchange settings.
- Fixed input of the **reset key in reset to defaults boot**, if the administrator password is not available anymore. If more than 255 characters were entered in the 1st try, it was not possible to enter the reset key for a 2nd or 3rd time.
- Fixed **Active Directory logon with smartcard**: If the smartcard contains logon certificates for multiple users, it is possible to switch between these certificates and log on with the chosen certificate now.
- Fixed missing names for some **partitions** in update notification when having a user interface **language other than English**.
- Fixed problems with **never ending bootcode** update with some EFI BIOS variants.
- Fixed **ssh server port** configuration.
- Fixed **signotec signature pad** channel for Citrix.



- Increased stability of **signotec VCOM Daemon**.
- Remove residual information belonging to a **removed content from a custom partition**.
- Fixed **crash of xfce4-power-manager** after adding or removing input devices.

#### Custom Partition

- Fixed **automatic update of custom partition** - if download source isn't accessible then the content of the custom partition got lost.

#### Appliance Mode

- Fixed post session command **Logoff** in Appliance Mode.

#### X11 System

- Fixed **Elo-USB Touchscreen functionality** after reboot.
- Fixed **DisplayLink USB Support on UD3 LX50**.
- Fixed issue with **two monitors connected via DVI-D to HDMI adapter on a UD3 M330 (VIA)**.  
Added registry key to disable the new HDMI autodetection.

##### [More](#)

|           |                                             |
|-----------|---------------------------------------------|
| Parameter | Autodetect if DVI to HDMI adapter is in use |
| Registry  | x.drivers.via.autodetect_hdmi_output        |
| Value     | <u>enabled</u> / disabled                   |

- Fixed **wrong automatic resolution detection** if monitor does not have a preferred mode.
- Fixed **sporadic display corruptions** after monitors leaving the power saving mode.
- Improved handling of more than 2 screens.

#### Shadowing/VNC

- Fixed **sporadic VNC server crash**.

#### Audio

- Fixed **volume control of internal speaker in HP T610**.
- Fixed **automatic switch to output** over analog headphones.
- Not existing **S/PDIF inputs and outputs in Plantronics and Jabra USB headsets** are now ignored by audio subsystem (Pulseaudio).
- Added workaround in the kernel USB audio driver for **volume control on Sennheiser USB headsets**.

#### Remote Management

- Fixed **calculation of Unit ID for UMS management**. In some cases, it could happen that the MAC address of wrong network interface was chosen.
- Fixed **IGEL Setup Assistant** to get stopped when settings were received from UMS.