

Endpoint Management (UMS)

Exported on 11/19/2021



Table of Contents

1	UMS Articles.....	30
1.1	Getting Started: Setting Up the UMS.....	30
1.1.1	Problem	30
1.1.2	Goal.....	30
1.1.3	Solution	30
1.1.4	Installation on Windows	31
	Standard Installation	31
	Silent Installation of the UMS Console.....	32
1.1.5	Installation on Linux	33
1.1.6	System Configuration	35
1.1.7	Creating Device Structures.....	41
1.1.8	Administrator Accounts	42
1.1.9	Registering Devices	45
1.1.10	Creating Profiles.....	45
1.2	Devices Supported by IGEL Universal Management Suite (UMS).....	47
1.2.1	Question	47
1.2.2	Answer	47
1.3	UMS Communication Ports	48
1.3.1	Sorted by UMS Feature	48
1.3.2	Sorted by Port Number.....	54
1.3.3	Internal Communication	59
	UMS with Internal Database	59
	UMS with External Database	60
	Indexing for UMS Web App Search	61
1.3.4	IGEL Management Interface (IMI)	61
1.3.5	UMS and Devices: Settings and Control.....	62
	Devices and UMS Server Contacting Each Other via ICG	62
	Devices Contacting UMS	64
	UMS Contacting Devices	65
1.3.6	UMS and Devices: Shadowing	66
	UMS Console.....	66
	UMS Web App	67
1.3.7	UMS and Devices: Secure Shadowing.....	68



Internal VNC Viewer - Direct Connection	68
UMS Web App - Direct Connection	69
Internal VNC Viewer - Over ICG	70
UMS Web App - Over ICG	71
External VNC Viewer - Direct Connection	72
External VNC Viewer - Over ICG	73
1.3.8 UMS and Devices: Secure Terminal.....	74
Direct Connection	74
Over ICG	75
1.3.9 UMS and Devices: File Transfer	76
1.3.10 Universal Firmware Update.....	77
UMS Contacting the Download Server to Check for New Updates.....	77
UMS Downloading the Firmware.....	79
1.3.11 Automatic License Deployment (ALD)	81
UMS Contacting the Licensing Server	82
UMS Sending New Settings to the Devices	84
Devices Contacting the UMS to Download License Files	85
1.4 UMS Installation	86
1.4.1 Using Special Characters during the UMS Installation on Linux	86
Question	86
Answer	87
1.4.2 UMS Installation on 64-Bit Systems	87
Question	87
Answer	87
1.4.3 No Permissions after the UMS Update.....	88
Symptom	88
Environment.....	89
Problem	89
Solution	89
1.5 Customization	91
1.5.1 User Authorization Rules	91
Problem	91
Reason	91
Solution	92
1.5.2 Managing User Permissions via UMS	93



1.5.3	Automating the Roll-out-Process.....	94
	Problem	94
	Goal.....	95
	Solution	95
	TechChannel	96
1.5.4	Using Structure Tags.....	97
	Problem	97
	Goal.....	97
	Solution	97
1.5.5	Deploying an IGEL made Custom Partition via UMS	98
	Goal.....	98
	Solution	98
1.6	UMS Environment	99
1.6.1	Migrating a UMS Server.....	99
	Purpose.....	99
	Scenarios	99
	With the Same Embedded Database	100
	With the Same External Database	103
	With a Different Database	106
	Transferring or Registering the UMS Licensing ID	106
	Updating Host Assignment for Job Execution.....	111
1.6.2	Migrating a UMS Database From Embedded DB to Microsoft SQL Server	112
	Setting Up the SQL Database	112
	Copying Database Contents	114
1.6.3	Restore and Recover Corrupted UMS Embedded DB.....	118
	Environment.....	118
	Restoring a Database Backup Made with the UMS Administrator	118
	Restoring a File-Based Backup.....	118
1.6.4	Disaster Recovery: UMS with an External Database.....	119
	Execution Order in Case of the Disaster Recovery	119
1.6.5	ICG Reinstallation after the Migration of the UMS Server	121
	Situation	121
	Question	121
	Answer	121
1.6.6	UMS Does Not Connect to ICG: "TrustAnchor ...is not a CA certificate"	121



Symptom	121
Environment.....	122
Problem.....	122
Solution	122
1.6.7 Using Your Own Certificates for Communication over the Web Port (Default: 8443).....	123
Overview	123
Deploying a Self-Signed Corporate Certificate Chain	123
Deploying a Certificate Chain with a Public Root CA.....	134
1.6.8 Wake on LAN.....	144
Deploying a Wake on LAN Proxy for Distributed Environments	144
Distributing Wake on LAN Packets	150
Use a WoL Proxy for Waking up Devices	151
1.6.9 Using an HTTP Proxy for Firmware Updates in UMS.....	152
Symptom	152
Problem.....	152
Solution	152
1.6.10 UMS Cannot Contact Download Server Any More.....	154
Symptom	154
Environment.....	154
Problem.....	154
Solution	154
1.6.11 Error During Firmware Upload in UMS: No Space on WebDAV	154
Issue	154
Cause	155
Solution	155
1.6.12 How to Check the Current State of the IGEL UMS Server through Your Existing Monitoring Solution	156
IGEL Environment	156
How to Request the Current Status of the UMS Server	156
Monitoring the UMS Server: Possible Statuses.....	157
Related Topics.....	157
1.7 High Availability	157
1.7.1 New Installation of an HA Network	158
1.7.2 Load Balancer Is Not Stopping during the Update of the HA Installation	158
Symptom	158
Environment.....	158



Problem	158
Solution	159
1.7.3 How to Detect Which Files Are Synchronized Automatically.....	159
Prerequisites	159
General Overview.....	159
Synchronization of Universal Firmware Updates.....	160
1.7.4 Load Distribution with a Number of Load Balancers	162
1.7.5 License Error Because HA Servers Are out of Sync.....	163
Symptom	163
Environment.....	163
Problem	163
Solution	164
1.7.6 Manual Synchronization of the UMS Licensing ID	164
Overview.....	164
Environment.....	164
Instructions	164
1.7.7 Error Message When Switching Back from an Externally Signed CA to the Internal CA	169
Symptom	169
Environment.....	170
Solution	170
1.8 Device	170
1.8.1 Device Scan or Online Check fails	170
Symptom	170
Problem	170
Solution	171
1.8.2 Registration of a Device fails	171
Symptom	171
Problem	171
Solution	171
1.8.3 Device Registration fails with Error Message: Unexpected end of input stream	172
Symptom	172
Problem	172
Solution	172
1.8.4 Device Registration Behind SonicWall Firewall Fails	173
Symptom	173



Possible Causes.....	173
Solution	173
1.8.5 Renaming IGEL OS Devices.....	173
Renaming upon Registration.....	174
Renaming Already Registered Devices.....	175
1.8.6 Changing the Hostname of an Endpoint Device via UMS	176
Option 1:.....	176
Option 2:.....	176
1.8.7 Monitoring Device Health and Searching for Lost Devices	177
Overview	177
Environment.....	177
Online Check (UMS Polls the Devices)	177
Last Contact between Device and UMS (Devices Send Data to the UMS)	178
1.9 Start of the UMS Console / Web App	187
1.9.1 UMS Web App: The Browser Displays a Security Warning (Certificate Error).....	187
Symptom	187
Environment.....	188
Problem	188
Solution	188
1.9.2 Starting UMS Console Crashes NX Session	204
Symptom	204
Solution	205
1.9.3 UMS Console doesn't start on Linux System without X11	205
Symptom	205
Problem	205
Solution	205
1.9.4 UMS Web App: "404 - System Error" Message	205
Symptom	205
Environment.....	206
Problem	206
Solution	206
1.10 Logon failures.....	206
1.10.1 UMS Console Logon fails	206
Symptom	206
Problem	206



Solution	207
1.10.2 UMS Console Login with AD User Account fails	207
Symptom	207
Problem	207
Solution	207
1.10.3 Login to the UMS Fails after the Update	207
Symptom	207
Problem	208
Solution	208
1.11 Active Directory / LDAP	208
1.11.1 Integrating Active Directory	208
Problem	208
Reason	208
Solution	208
Configuring an AD Connection	209
Importing Users from AD to UMS	210
Assigning Permissions	213
Configuring an LDAP Connection	217
1.11.2 Problems When Configuring an Active Directory with LDAP over SSL	218
Symptom	218
Problem	218
Solution	219
1.11.3 Import of Administrator Accounts from Active Directory Fails	219
Symptom	219
Problem	219
Solution	219
1.12 Profiles	219
1.12.1 Find Out a Profile's Priority	219
1.12.2 Precedence of Profiles and Universal Firmware Updates	220
General Order of Priority	220
Universal Firmware Update vs. Profile	220
Profile vs. Local Settings	221
Universal Firmware Update vs. Universal Firmware Update	221
Compatibility	221
1.12.3 Assigning Profiles to Devices filtered by Views or Search	221



1.13 Java Web Start	222
1.13.1 UMS Console via Java Web Start.....	222
Requirements.....	222
Starting the UMS Console via Java Web Start	222
1.13.2 Error when connecting to UMS via Java Web Start: "received fatal alert: handshake_failure"	223
Symptom	223
Problem	224
Solution	224
1.13.3 VNC Connection Error with Java Web Start Console and external VNC Viewer	224
Symptom	224
Problem	225
Solution	225
1.14 Misc	225
1.14.1 Where Can I Find the UMS Log Files?	225
UMS Server	225
UMS Load Balancer	226
UMS Watchdog	226
UMS Console.....	227
UMS Administrator	227
1.14.2 Clearing up the UMS.....	227
Problem	227
Goal.....	227
Solution	227
Downloading the new Firmware	228
Moving Clients to the New Firmware	228
Moving Profiles to New Firmware	228
Deleting old Firmware, Clients and Profiles that are no longer required	228
1.14.3 Removing a Certificate.....	229
1.14.4 Notifications - Always Be Informed	229
About Notifications	229
The Notification Window	229
Enabling the Notification Function	230
Exporting Notification and Sending It by Email	230
Configuring the Notifications Pop-Up.....	230
Disk Usage	231



Global Notifications	232
Admin Tasks	232
1.14.5 Updating Timezone Information (Daylight Saving Time, DST).....	233
Symptom	233
Problem.....	233
Solution	233
1.14.6 E-Mail Settings for Gmail Accounts	235
Purpose.....	235
Solution	235
Additional Information	236
1.14.7 Searching With Regular Expressions in UMS	236
1.14.8 Copy Sessions in Setup or UMS	237
1.14.9 Drag & Drop Acceleration for Large Structure Trees	237
1.14.10 Which UMS Directories Should Be Scanned for Viruses, Which Can Be Excluded?	238
Question	238
Environment.....	238
Answer	238
1.14.11 Licensing with Smartcard fails	239
Symptom	239
Problem.....	239
Solution	239
1.14.12 Finding UD Devices for PowerTerm Activation using a View	239
Symptom	239
Problem.....	239
Solution	239
2 Installation and Sizing Guidelines for IGEL UMS	242
2.1 General Preconditions	242
2.1.1 Recommended Additional Information.....	242
2.2 Installation Types & Diagrams.....	243
2.2.1 Small Environment: UMS S	244
Small Size UMS Installation (<5k Devices) or Demo/POV Environment with an Embedded Database	244
Architecture: Small Environment.....	245
Architecture: Small Environment + ICG in Cloud.....	245
2.2.2 Medium Environment: UMS M	246
Medium Size UMS Installations (up to ~15k Devices); No High Availability	246



Architecture: Medium Environment + ICG	247
2.2.3 Small and Medium Environments: UMS M/S (HA)	247
Small and Medium Size UMS Installations (up to ~15k devices); High Availability	247
Architecture: Small and Medium Environment (HA) + ICG	248
2.2.4 Large Environment: UMS L (HA)	249
Large UMS Installations with up to 50k Devices; High Availability + ICG	249
Architecture: Large Environment (HA) + ICG	249
2.2.5 Extra Large Environment: UMS XL (HA)	250
Extra Large UMS Installations with up to 300k Devices; High Availability + ICG	250
Architecture: Extra Large Environment (HA) + ICG	251
2.3 Performance Optimizations	251
2.3.1 Data Sizing	251
2.3.2 Latencies	251
2.3.3 Performance Optimizations	252
2.3.4 Limitations: UMS HA	252
3 UMS Reference Manual	253
3.1 What Is New in IGEL UMS 6.09.100?	253
3.1.1 Text Expert Mode of Views: Auto-completion for Operators	253
3.1.2 Monitoring Endpoint for Requesting the Status of the UMS Server	254
3.1.3 UMS Administrator Command-Line Interface	254
3.1.4 ICG Certificates as Part of the Support Information	254
3.1.5 UMS Web App: Login Brute-Force Protection	254
3.2 Overview	254
3.2.1 Typical Areas of Use	254
3.2.2 Attributes of the IGEL UMS	255
3.2.3 IGEL UMS Components	256
UMS Server	256
UMS Administrator	257
UMS Console / UMS Web App	257
3.3 UMS Installation and Update	258
3.3.1 Installation Requirements for the IGEL UMS	258
Standard UMS (Includes UMS Server and UMS Administrator)	259
Only UMS Console	259
Database Systems (DBMS)	260
High Availability	260



3.3.2	Installing a UMS Server	260
	IGEL UMS Installation under Linux.....	261
	IGEL UMS Installation under Windows.....	283
3.3.3	Updating UMS	285
	Updating under Linux	286
	Updating under Windows.....	288
3.3.4	Connecting External Database Systems.....	289
	Oracle.....	290
	Oracle RAC	290
	Microsoft SQL Server.....	291
	Microsoft SQL Server Cluster.....	291
	Connecting the UMS to an SQL Server via Active Directory	292
	PostgreSQL.....	304
	Apache Derby	305
3.4	Connecting the UMS Console to the Server.....	306
3.5	Registering Devices on the UMS Server	306
3.5.1	Searching for Devices.....	307
3.5.2	Registering Devices	307
3.5.3	Importing Devices	308
	Import with Short Format.....	309
	Import with Long Format.....	309
	Import with IGEL Serial Number	311
3.5.4	Registering Devices Automatically.....	312
3.5.5	Setting up Devices Manually.....	313
3.6	UMS Console User Interface	313
3.6.1	The Console Window	314
3.6.2	Menu Bar.....	315
	System	315
	Edit.....	316
	Devices.....	316
	Misc	317
	Help.....	323
3.6.3	Structure Tree	324
3.6.4	Symbol Bar	325
3.6.5	Content Panel.....	326



Illustrative List of Details Shown in the Content Panel for Some Objects from the UMS Structure Tree.....	326
3.6.6 UMS Administration	327
3.6.7 Messages	327
3.6.8 Status Bar	328
3.6.9 Assigned Objects	328
3.6.10 Context Menu	329
3.6.11 Search for Objects in the UMS	329
Quick Search	329
Search Function	329
Views	330
3.6.12 Deleting Objects in UMS / Recycle Bin	330
3.7 Profiles.....	331
3.7.1 When Is It a Good Idea to Use Profiles?.....	331
3.7.2 Managing Profiles.....	333
3.7.3 Choosing the Right Profile	333
Standard Profiles	333
Master Profiles.....	333
User-Specific Profiles	333
3.7.4 Configuration Levels.....	334
Normal Parameters and Fixed Instances.....	334
Free Instances	334
3.7.5 Effectiveness of Settings.....	334
3.7.6 Using Profiles.....	335
Managing Profiles.....	335
Creating Profiles.....	335
Copy Profile	340
Copy Profile Directory	341
Exporting and Importing Profiles	341
How to Allocate IGEL UMS Profiles.....	344
Checking Profiles	346
Removing Assigned Profiles from a Device.....	347
Deleting Profiles	348
Comparing Profiles	348
3.7.7 Prioritization of Profiles.....	350
Order of Effectiveness	350



Order of Effectiveness of Profiles	351
Order of Effectiveness of Profiles in Shared Workplace	353
Order of Effectiveness of Master Profiles	354
Order of Effectiveness of All Profiles	358
Summary	358
3.8 Master Profiles.....	359
3.8.1 Most Important Features of Master Profiles	360
3.8.2 Enabling Master Profiles	360
3.9 Template Profiles.....	361
3.9.1 Example	362
3.9.2 Previous Solution	362
3.9.3 Problem	362
3.9.4 Solution	362
3.9.5 Activating Template Profiles	363
3.9.6 Creating Template Keys and Values.....	364
Creating Keys and Values in the Profile	367
3.9.7 Using Template Keys in Profiles	370
3.9.8 Assigning Template Profiles and Values to the Devices.....	371
3.9.9 Value Groups	373
3.9.10 Export Template Keys and Value Groups.....	374
3.9.11 Import Template Keys and Value Groups	375
3.10 Mobile-Device Profiles	375
3.11 Firmware Customizations.....	375
3.11.1 Mode of Action	376
3.11.2 Create Firmware Customization	376
Start Button.....	377
Start Menu	377
Taskbar Background.....	378
Screensaver	378
Screensaver (Custom Partition)	379
Bootsplash.....	380
Background Image.....	381
3.11.3 Export Firmware Customizations.....	381
3.11.4 Import Firmware Customizations	381
3.12 Devices.....	382



3.12.1 Icons for an IGEL OS Device	382
3.12.2 Icons for a UD Pocket	383
3.12.3 Device	384
System Information	384
Template Definition Check Results	385
Monitor Information	385
Features	385
Windows Updates and Hotfixes	385
Partial Updates	386
File Transfer Status	386
User Login History	386
3.12.4 Managing Devices	387
Creating a Directory	387
Copying a Device Directory	388
Importing a Directory	388
Deleting a Directory	389
Moving Devices	389
Assigning Updates	390
Default Directories	391
3.12.5 Configuring Devices	391
Copying a Session	392
3.12.6 Exporting and Importing Data	392
Export Firmwares	392
Import Firmwares	393
Export Device Settings	393
Import Devices as Profiles	394
3.12.7 Send Message	394
Own Icon	395
Message Editor	395
3.12.8 View Asset Information	395
Read out Asset Data via API	396
3.12.9 Secure Terminal (Secure Shell)	397
For IGEL OS 10.01.100 or newer	397
For IGEL Linux v5	397
Configuring the Secure Terminal	397
Using the Secure Terminal	398



3.12.10 Shadowing (VNC)	399
Launching a VNC Session.....	399
IGEL VNC Viewer	400
External VNC Viewer.....	401
Secure Shadowing (VNC with SSL/TLS)	401
3.13 Shared Workplace Users.....	402
3.14 Views.....	402
3.14.1 How to Create a New View in the IGEL UMS.....	403
How to Create a View: Standard Procedure	404
How to Create a View: Expert Mode	406
Possible Search Criteria.....	414
Example: Creating a View	416
Text Mode of Views: Matrix of Possible Criteria and Operators	417
3.14.2 Copying a View	421
3.14.3 Copying a View Directory.....	422
3.14.4 Saving the View Results List	422
3.14.5 Sending a View as Mail.....	423
3.14.6 Assigning Objects to a View	424
3.15 Jobs	425
3.15.1 Setting Up a New Job.....	426
3.15.2 Commands for Jobs.....	426
3.15.3 Details	427
Options	427
Job Info.....	427
3.15.4 Schedule.....	428
3.15.5 Assignment.....	428
3.15.6 Execution Results.....	429
3.16 Files.....	430
3.16.1 Registering a File on the UMS Server	430
3.16.2 Transferring a File to a Device	430
Transferring a File Without Assignment.....	431
3.16.3 Removing a File from a Device	431
3.16.4 Transferring a File to the UMS Server.....	432
Example	432
3.17 Universal Firmware Update.....	433



3.17.1	Check for New Firmware Updates.....	433
	Universal Firmware Updates.....	434
3.17.2	Snapshot -> Universal Firmware Update	434
3.17.3	Firmware Archive (Zip File) -> Universal Firmware Update	435
3.18	Search History	435
3.18.1	Context Menu of a Search Query	435
3.19	Recycle Bin	436
3.20	UMS Administration	437
3.20.1	UMS Network.....	437
	Server - View Your IGEL UMS Server Information	437
	Load Balancer - View Your IGEL UMS Load Balancer Information.....	439
	IGEL Cloud Gateway.....	441
3.20.2	Global Configuration.....	442
	Licenses	443
	Mobile Devices.....	451
	Certificate Management	453
	Device Network Settings.....	457
	Server Network Settings.....	459
	Cloud Gateway Options	460
	Device Attributes.....	463
	Administrative Tasks.....	464
	Proxy Server	484
	Default Directory Rules	485
	Universal Firmware Update	493
	Wake-on-LAN	495
	Active Directory / LDAP	497
	Remote Access	498
	Logging	500
	Mail Settings	501
	Messages to Devices.....	502
	Misc Settings.....	503
	UMS Features	504
3.21	Importing Active Directory Users	505
3.21.1	Searching in the Active Directory	506
3.21.2	Import Results List	507



3.22 Create Administrator Accounts	508
3.22.1 Administrators and Groups	508
3.22.2 Access Rights	509
Basic Access Rights	511
General Administrator Rights	512
Object-Related Access Rights	515
Access Rights in the Administration Area	520
3.23 User Logs	521
3.23.1 Administration	521
3.23.2 Displaying Logs	521
3.23.3 Logging Dialog Window: Setting a Filter	522
Setting a Filter for Events	522
Filter for Messages	523
Setting a Filter for Categories	524
Notes	524
3.24 Save Support Information / Send Log Files to Support	525
3.24.1 Support Wizard in the IGEL UMS	525
How to Send Log Files via Support Wizard in the IGEL UMS	525
Related Topics	527
3.25 Save Device Files for Support	527
3.25.1 Saving the Log Files of a Device	527
3.25.2 Log Files Collected with IGEL OS 10.04 or Higher	528
3.25.3 Log Files Collected with Other IGEL OS Versions	528
3.25.4 Log Files Collected with Windows IoT 4.03 or Higher	528
3.26 The IGEL UMS Administrator	529
3.26.1 Settings for IGEL UMS Administrator	530
IGEL Universal Management Suite (UMS) Administrator Settings:	531
Ports	531
Database Setup Configuration	532
Cipher (Server-Side)	532
SSL Certificates	534
3.26.2 UMS Licensing ID Backup	534
UMS Licensing ID Backup	534
Creating a Backup	535
3.26.3 UMS Licensing ID Backup on the Command Line	535



Program Launch Options.....	535
3.26.4 Backups	536
Creating a Backup	536
Restoring a Backup	540
Deleting a Backup	541
Backup on the Command Line	542
Planned Backup	543
3.26.5 Data Source	543
How to Set Up a Data Source in the IGEL UMS Administrator	543
Activating a Data Source.....	546
Copying a Data Source.....	546
Optimizing the Active Embedded DB	546
Changing the UMS Superuser	547
3.26.6 IGEL UMS Administrator Command-Line Interface.....	547
Basic Usage	547
Global Options	549
Exit Codes	550
Command Reference	550
Error Numbers.....	563
4 UMS Release Notes	565
4.1 Notes for Release 6.09.100.....	565
4.1.1 Supported Environment 6.09.100	565
4.1.2 New Features 6.09.100	567
UMS Web App	567
4.1.3 Resolved Issues 6.09.100	568
UMS Web App	569
4.2 Notes for Release 6.08.120.....	569
4.2.1 Supported Environment 6.08.120	569
4.2.2 Resolved Issues 6.08.120	571
4.3 Notes for Release 6.08.110.....	571
4.3.1 Supported Environment 6.08.110	571
4.3.2 New Features 6.08.110	573
4.3.3 Resolved Issues 6.08.110	573
4.4 Notes for Release 6.08.100.....	573
4.4.1 Supported Environment 6.08.100	573



4.4.2	Known Issues 6.08.100	575
4.4.3	New Features 6.08.100	575
	UMS Web App	575
4.4.4	Resolved Issues 6.08.100	576
	UMS Web App	577
4.5	Notes for Release 6.07.100.....	578
4.5.1	Supported Environment 6.07.100	578
4.5.2	Removed Support 6.07.100	580
4.5.3	Added Support 6.07.100	580
4.5.4	Known Issues 6.07.100	580
4.5.5	New Features 6.07.100	580
4.5.6	Resolved Issues 6.07.100	581
4.6	Notes for Release 6.06.110.....	583
4.6.1	Supported Environment 6.06.110	583
4.6.2	Resolved Issues 6.06.110	584
4.7	Notes for Release 6.06.100.....	585
4.7.1	Supported Environment 6.06.100	586
4.7.2	New Features 6.06.100	587
4.7.3	Resolved Issues 6.06.100	589
4.7.4	Known Issues 6.06.100	591
4.8	Notes for Release 6.05.110.....	591
4.8.1	Supported Environment 6.05.110	591
4.8.2	Resolved Issues 6.05.110	593
4.9	Notes for Release 6.05.100.....	594
4.9.1	Supported Environment 6.05.100	594
4.9.2	Removed Support 6.05.100	595
4.9.3	Added Support 6.05.100	596
4.9.4	Known Issues 6.05.100	596
4.9.5	New Features 6.05.100	596
4.9.6	Resolved Issues 6.05.100	597
4.10	Notes for Release 6.04.120.....	600
4.10.1	Supported Environment 6.04.120	600
4.10.2	Removed Support 6.04.120	602
4.10.3	New Features 6.04.120	602
4.10.4	Resolved Issues 6.04.120	602



4.11	Notes for Release 6.04.110.....	602
4.11.1	Supported Environment 6.04.110	603
4.11.2	Resolved Issues 6.04.110	604
4.12	Notes for Release 6.04.100.....	605
4.12.1	Supported Environment 6.04.100	605
4.12.2	New Features 6.04.100.....	606
4.12.3	Resolved Issues 6.04.100	608
4.13	Notes for Release 6.03.130.....	611
4.13.1	Supported Environment 6.03.130	611
4.13.2	New Features 6.03.130.....	612
4.13.3	Resolved Issues 6.03.130	613
4.14	Notes for Release 6.03.110.....	613
4.14.1	Supported Environment 6.03.110	613
4.14.2	Resolved Issues 6.03.110	615
4.15	Notes for Release 6.03.100.....	615
4.15.1	Supported Environment 6.03.100	615
4.15.2	Known Issues 6.03.100	617
4.15.3	New Features 6.03.100.....	617
4.15.4	Resolved Issues 6.03.100	618
4.16	Notes for Release 6.02.110.....	620
4.16.1	Supported Environment 6.02.110	621
4.16.2	New Features 6.02.110.....	622
4.16.3	Resolved Issues 6.02.110	622
4.17	Notes for Release 6.02.100.....	623
4.17.1	Supported Environment 6.02.100	623
4.17.2	New Features 6.02.100.....	624
4.17.3	Security Fixes 6.02.100.....	625
4.17.4	Resolved Issues 6.02.100	625
4.18	Notes for Release 6.01.100.....	629
4.18.1	Supported Environment 6.01.100	630
4.18.2	New Features 6.01.100.....	631
4.18.3	Resolved Issues 6.01.100	631
4.19	Notes for Release 5.09.100.....	633
4.19.1	Supported Environment 5.09.100	634



4.19.2	Warnings 5.09.100	635
4.19.3	New Features 5.09.100	636
4.19.4	Resolved Issues 5.09.100	637
4.20	Notes for Release 5.08.120.....	641
4.20.1	Supported Environment 5.08.120	642
4.20.2	Resolved Issues 5.08.120	643
4.21	Notes for Release 5.08.110.....	643
4.21.1	Supported Environment 5.08.110	644
4.21.2	New Features 5.08.110	645
4.21.3	Resolved Issues 5.08.110	645
4.22	Notes for Release 5.08.100.....	646
4.22.1	Supported Environment 5.08.100	647
4.22.2	New Features 5.08.100	648
4.22.3	Resolved Issues 5.08.100	649
4.23	Notes for Release 5.07.110.....	650
4.23.1	Resolved Issues 5.07.110	651
4.24	Notes for Release 5.07.100.....	651
4.24.1	New Features 5.07.100	652
4.24.2	Resolved Issues 5.07.100	654
5	UMS Extensions.....	657
5.1	High Availability (HA)	657
5.1.1	Licensing with the IGEL OS 11 Licensing Model	658
5.1.2	Configuration Options	658
	UMS Server & UMS Load Balancer Are Installed on the Same Host Machine.....	658
	UMS Server & UMS Load Balancer are Installed on Separate Host Machines.....	659
5.1.3	HA Installation.....	660
	HA: Installation Requirements	660
	Installing the First Server in an HA Network	662
	Adding Further Servers to the HA Network.....	667
5.1.4	Updating the Installation of an HA Network.....	671
	Use Case	671
	General Overview	671
	Updating HA Installation: With Downtime of the Servers	673
	Updating HA Installation: Without Downtime of the Servers	676
5.1.5	Switching from a Standard UMS Installation to an HA Installation.....	680



Use Case	680
Prerequisites	680
Instructions	680
Preparing the Migration.....	681
Setting Up the New Database and Transferring Data (If the Embedded DB is in Use)	683
Installing the First HA Server and Transferring the Data from the Existing UMS Server	684
Installing Further HA Components.....	687
5.1.6 Licensing the High Availability Extension	687
With the IGEL OS 11 Licensing Model.....	687
Before IGEL OS 11.....	688
5.1.7 UMS HA Health Check	688
Messaging.....	689
WebDav.....	690
Port 30001.....	690
Port 30002.....	690
Certificates	690
More Checks	691
Detailed Report	691
5.1.8 HA Services and Processes	691
5.2 Shared Workplace (SWP)	693
5.2.1 Licensing with IGEL OS 11.....	693
5.2.2 Licensing with IGEL OS 10.....	693
5.2.3 Typical Uses for Shared Workplace.....	693
5.2.4 SWP Configuration in the UMS Console.....	694
Linking an Active Directory.....	694
Assigning a User Profile	695
Enabling IGEL Shared Workplace on the Thin Client	696
User login.....	696
Logout and Change of User	697
5.2.5 Parameters Configurable in the User Profile	697
UD Linux Device-specific Parameters	697
UD W7 Device-specific Settings	698
5.2.6 Display Configuration for Shared Workplace (SWP)	698
Best Practice.....	699
Debugging	699



5.3	Asset Inventory Tracker (AIT)	699
5.4	IGEL Management Interface (IMI)	699
5.5	Universal Customization Builder (UCB)	699
5.5.1	UCB Reference Manual	700
	Overview	700
	Partial Update for IGEL Devices with Windows Embedded Standard	700
5.6	Mobile Device Management Essentials (MDM)	704
5.6.1	Basic Overview	704
	Apple Push Notification Service (APNs)	704
	Connecting Devices	705
	Managing Devices	705
5.6.2	MDM Manual	706
	Prerequisites	706
	Supported Mobile Devices	706
	Communication Chart	707
	Supported Features	707
5.6.3	MDM How-Tos	715
	MDM Setup Guide	715
	Connecting Mobile Devices to the UMS	716
	Creating Mobile Device Profiles	718
	Sending Profiles to Mobile Devices	718
5.6.4	MDM Troubleshooting	718
	Profile Installation Fails When Connecting Mobile Device to the ICG	718
6	UMS Web App	720
6.1	Video	720
6.2	Basic Overview	721
6.2.1	Devices	721
6.2.2	Search	723
6.2.3	Configuration	725
6.2.4	Network	726
6.2.5	Logging	727
6.3	Important Information	727
6.3.1	Login	728
6.3.2	Permissions	728



6.3.3	Synchronization between the UMS Console and the UMS Web App	728
6.3.4	Logging	728
6.3.5	Shadowing (VNC)	728
6.3.6	Certificate	728
6.3.7	Bulk Actions.....	729
6.3.8	Supported Resolution.....	729
6.3.9	Installation	729
6.3.10	RAM and Disk Space Requirements	729
6.4	Installation	729
6.4.1	Windows	729
6.4.2	Linux	731
6.5	Supported Environment.....	731
6.5.1	Supported Browsers	731
6.5.2	Supported Resolution.....	731
6.6	How to Log In to the IGEL UMS Web App	732
6.6.1	How to Access the IGEL UMS Web App.....	732
6.6.2	Login Data for the IGEL UMS Web App	732
6.7	UMS Web App Manual	732
6.7.1	Menu Bar.....	733
6.7.2	Search.....	734
	Exporting Search Results.....	736
6.7.3	Devices.....	737
	Status Displays	740
	Device Commands	741
	Creating a Directory	742
	Copying a Device Directory.....	743
	Moving a Device Directory	743
	Renaming a Directory	744
	Deleting a Directory	744
	Moving Devices.....	745
	Assigning Objects	746
6.7.4	Configuration	748
6.7.5	Network	752
	Status Displays	753
6.7.6	Logging	754



7	Fact Sheets	756
7.1	UMS Web App	756



Installation and Configuration

[UMS Installation and Update](#)(see page 258), [Database](#)(see page 258), [Requirements](#)(see page 258), [Connecting to the UMS](#)(see page 306), [User Management](#)(see page 505), [UMS Administration](#)(see page 437), [Getting Started: Setting Up the UMS](#)(see page 30), [Installation and Sizing Guidelines for IGEL UMS](#)(see page 242)

Licenses

[Automatic License Deployment](#)¹, [UMS Licenses](#)(see page 445), [Device Licenses](#)(see page 446)

Endpoint Devices Deployment

[Registering Devices](#)(see page 306), [Configuring](#)(see page 391) and [Managing Devices](#)(see page 387)

User Assistance

[Support Information](#)(see page 323), [VNC](#)(see page 400), [Shadowing](#)(see page 399), [Terminal](#)(see page 397), [Messages](#)(see page 327), [Logging](#)(see page 500)

Endpoint Configuration

[Using Profiles](#)(see page 335), [Master Profiles](#)(see page 359), [Template Profiles](#)(see page 361), [Effectiveness of Settings](#)(see page 334)

Firmware Management

[Firmware Update](#)(see page 433), [Export Firmwares](#)(see page 392), [Import Firmwares](#)(see page 393), [Check for new Universal Firmware Updates](#)(see page 433)

¹ <https://kb.igel.com/pages/viewpage.action?pageId=10325058>



Custom Design

[Themes](#)(see page 319), [Background Images](#)(see page 381), [Firmware Customizations](#)(see page 375)

Views and Searches

[Quick Search](#)(see page 329), [Views](#)(see page 402), [Search with regular expressions](#)(see page 236)



1 UMS Articles

- [Getting Started: Setting Up the UMS](#)(see page 30)
- [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)(see page 47)
- [UMS Communication Ports](#)(see page 48)
- [UMS Installation](#)(see page 86)
- [Customization](#)(see page 91)
- [UMS Environment](#)(see page 99)
- [High Availability](#)(see page 157)
- [Device](#)(see page 170)
- [Start of the UMS Console / Web App](#)(see page 187)
- [Logon failures](#)(see page 206)
- [Active Directory / LDAP](#)(see page 208)
- [Profiles](#)(see page 219)
- [Java Web Start](#)(see page 222)
- [Misc](#)(see page 225)

1.1 Getting Started: Setting Up the UMS

1.1.1 Problem

You want to set up the UMS for the first time and you are not sure how to proceed.

1.1.2 Goal

The aim is not only to install the UMS, but also to achieve a solid setup of the most important features.

1.1.3 Solution

We will show you an easy method for best practice setup with the following steps:

- [Installation on Windows](#)(see page 31)
- [Installation on Linux](#)(see page 33)
- [System Configuration](#)(see page 35)
- [Creating Device Structures](#)(see page 41)
- [Administrator Accounts](#)(see page 42)
- [Registering Devices](#)(see page 45)
- [Creating Profiles](#)(see page 45)



- i** You can also use the [IGEL Software Suite: Step-by-Step Getting Started Guide provided by the IGEL Community](#)². Its goal is to provide you with the tools, knowledge, and understanding of how to download the IGEL software and perform basic installation and configuration without being forced to read many manuals and numerous web support articles. This document will walk you, step-by-step, through what is required for you to get up and running in a proof-of-concept or lab scenario. When finished, you will have a fully working IGEL endpoint management platform consisting of the IGEL Universal Management Suite (UMS), IGEL Cloud Gateway (ICG), and IGEL OS devices installed, connected and centrally managed. You can download the guide here: <http://files.igelcommunity.com/IGEL-Getting-Started-Guide.zip>.

1.1.4 Installation on Windows

- i** For the supported operating systems, see the "Supported Environment" section of the [release notes](#)(see page 565).

Standard Installation

To install the IGEL Universal Management Suite under Windows, proceed as follows:

1. Download the current version of the IGEL Universal Management Suite from the [IGEL Download Server](#)³.
2. Launch the installer.

i You will need administrator rights in order to install the UMS.
3. Read and confirm the **License Agreement**.
4. Read the **Information** regarding the installation process and click **Next**.
5. Only if this is an update installation: If you already have a UMS installation, select the file name for the **backup** of your embedded database. If you do not choose a file name and click on **Next**, no backup will be created. See also [Updating under Windows](#)(see page 288).
6. Only if this is a new installation: Select the folder for the installation under **Select Destination Location**. (Default: C:\Program Files\IGEL\RemoteManager)
7. Choose the components to be installed under **Select Components**.
 - **Standard UMS**
 - **with UMS Console**
 - **with Embedded Database**
 - **Only UMS Console**
 - **UMS High Availability Network**
 - **UMS Server**
 - **UMS Load Balancer**
 - **UMS Web App (early feature set)**

² <https://www.igelcommunity.com/igel-getting-started-guide>

³ <https://www.igel.com/software-downloads/workspace-edition/>



- i** The embedded database is suitable for most purposes. If not disabled, the embedded database will automatically be installed if you select **Standard UMS**.

The use of an external database system is recommended in the following cases:

- You manage a large network of devices.
- A dedicated database system is already in use in your company.
- You integrate the High Availability solution.

8. Read the **Memory (RAM) requirements** and click **Next** if your system fulfills them.
9. Select the **UMS data directory**. (Default: C:\Program Files\IGEL\RemoteManager)
10. Under **User Credentials for DB-connect**, enter the user name and password for the database connection – unless you are planning to connect the UMS to an MS SQL Server via Active Directory. For more information on connecting via AD, see [Connecting the UMS to an SQL Server via Active Directory](#)(see page 292).

The credentials for the database connection are created.

- i** Initially, the credentials entered here are also the credentials of the UMS superuser. After the installation, the credentials for the database user and those for the UMS superuser can be changed independently from each other. For more information about the UMS superuser, see [Changing the UMS Superuser](#)(see page 547).

11. If the internal Windows firewall is active on your host: Review the settings under **Windows firewall settings** and change them where necessary. Each port that is activated here will be set as rule in the Windows firewall. For more information about the usage of ports, see [UMS Communication Ports](#)(see page 48).
12. Choose a folder name under **Select Start Menu Folder**.
13. Read the summary and start the installation process.
The installer will install the UMS, create entries in the Windows software directory, and in the start menu, and will place a shortcut for the UMS Console on the desktop.
14. Close the program after completing the installation by clicking on **Finish**.
If you have chosen the standard installation, the UMS Server will run with the embedded database.
15. Start the UMS Console.
16. Connect the UMS Console to the UMS Server using the access data for the database that you entered during the installation.
You will find information regarding the use of the UMS with external databases under [Connecting External Database Systems](#)(see page 289).

Silent Installation of the UMS Console

You can carry out the installation silently by first creating an .inf file and then launching the installation using a command line.

- i** Silent installation is only possible for the UMS Console. It is not possible for the UMS Server, the UMS Administrator, or the UMS Web App.

For further information, see [Unattended/Silent Installation of UMS Console](#)(see page 284).



1.1.5 Installation on Linux

- i** For the supported operating systems, see the "Supported Environment" section of the [release notes](#)(see [page 565](#)).

The procedure for installing the IGEL Universal Management Suite under Linux is as follows:

1. Download the current version of the IGEL Universal Management Suite from the [IGEL Download Server](#)⁴.
2. Open a terminal emulator such as xterm and switch to the directory in which the installation file `setup-igel-ums-linux-[Version].bin` is located.
3. Check whether the installation file is executable. If not, it can be made executable with the following command:
`chmod u+x setup*.bin`

i You will need root/sudo rights to carry out the installation.

4. Execute the installation file as root or with sudo:
`sudo ./setup-igel-ums-linux-[Version].bin`
This unzips the files into the `/tmp` directory, starts the included Java Virtual Machine, and removes the temporary files once the installation has been completed.
 5. Start the installation procedure by pressing **Enter**.
- !** You can cancel the installation at any time by pressing the [Esc] key twice.
6. Read and confirm the license agreement.
 7. Choose whether the installer will install the required dependencies:
 - **Now:** Installs the necessary dependencies automatically.
 - **Manual:** Skips the installation. You will have to install the required dependencies manually if this has not already been done.
 - **Cancel installer:** Aborts the installation procedure.
 8. Under **Destination directory**, select the directory in which the UMS is to be installed. (Default: `/opt/IGEL/RemoteManager`)
 9. If you are updating an existing UMS installation: Under **Database backup**, select a file for the backup of the embedded database, licenses, and certificates. If you have already created a backup, you can select **No (continue)** in order to skip this step. See also [Updating under Linux](#)(see [page 286](#)).
 10. Under **Installation type**, select the scope of installation:
 - **Complete:** [UMS Server](#)(see [page 256](#)) and [UMS Console / UMS Web App](#)(see [page 257](#))
 - **Client only:** UMS Console only
 - **HA Net:** [High Availability](#)(see [page 657](#)) configuration

⁴ <https://www.igel.com/software-downloads/workspace-edition/>



! Custom file transfer directories are no longer supported. After completing the installation, move the existing files to the `ums_filetransfer/` directory and edit **Files** and **Firmware update** in the UMS Console to bring them online again. You may also need to amend download addresses in the device configurations and profiles.

11. Choose whether the [UMS Web App](#)(see page 720) should be installed.
12. Confirm the **system requirements** dialog if your system fulfills them.
13. Under **Data directory**, select the directory in which Universal Firmware Updates and files are to be saved. (Default: `/opt/IGEL/RemoteManager`)
14. Under **Database selection**, select the desired database system.
 - Internal: The embedded database
 - Other: An external database server

i The embedded database is suitable for most purposes. It is included in the standard installation. If you manage a large network of devices and a dedicated database system is already in use in your company, it is advisable to use this external database system. The same applies if you integrate the High Availability solution.
15. Under **User name**, enter a **user name** and **password** for the database connection.
The credentials for the database connection are created.

i Initially, the credentials entered here are also the credentials of the UMS superuser. After the installation, the credentials for the database user and those for the UMS superuser can be changed independently from each other. For more information about the UMS superuser, see [Changing the UMS Superuser](#)(see page 547).
16. Specify whether you would like to create **shortcuts** for the UMS Console and UMS Administrator on the menu.
17. Check the summary of the installation settings and start the procedure by selecting **Start installation**.
If you have selected the standard installation, the UMS Server along with the embedded database will be installed and started.
18. Once the installation procedure is complete, open the UMS Console via the menu or with the command `/opt/IGEL/RemoteManager/RemoteManager.sh`

i It is generally NOT recommended to execute the command `RemoteManager.sh` with sudo. On Red Hat Enterprise Linux 8, `RemoteManager.sh` can be executed only without sudo.
19. Connect the UMS Console to the UMS Server by entering the login data for the database that you specified during the installation.

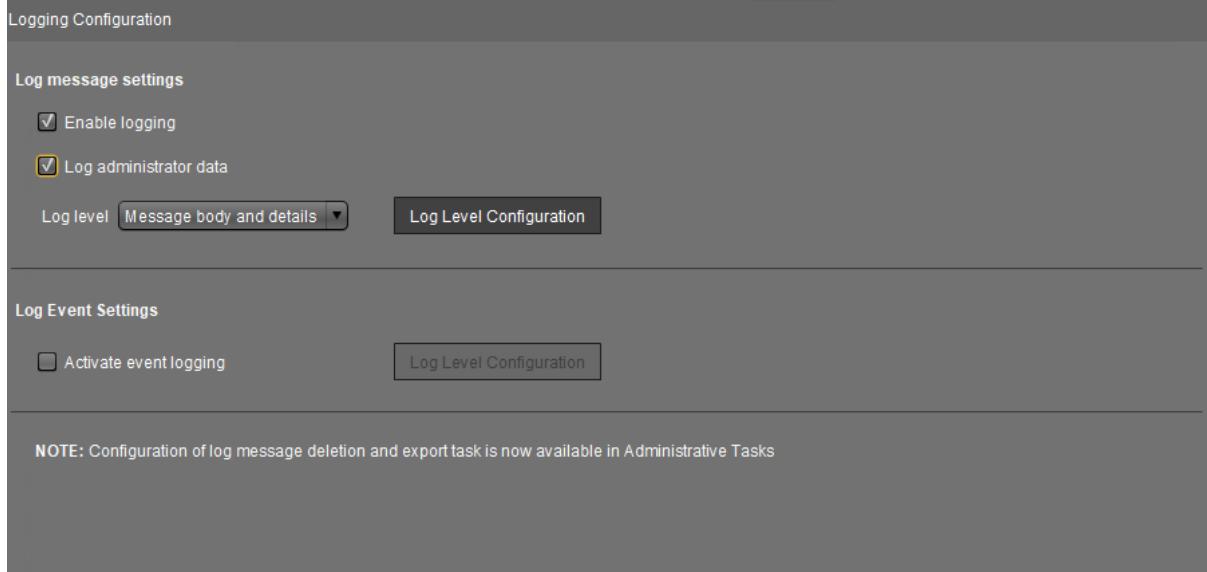
- [Preparing Amazon Linux 2 for UMS Installation](#)(see page 263)
- [Installing UMS on Red Hat Enterprise Linux \(RHEL\) 8](#)(see page 263)
- [Installing UMS on Red Hat Enterprise Linux \(RHEL\) 7.3](#)(see page 264)
- [Installing UMS on Oracle Linux Server](#)(see page 265)
- [Installing a UMS Network on Microsoft Azure](#)(see page 267)

1.1.6 System Configuration

This document describes various recommended settings for UMS.

To define the settings, proceed as follows:

1. Start the **UMS Console**.
2. Go to **UMS Administration > Global Configuration > Logging** and copy the following settings:



The screenshot shows the "Logging Configuration" section of the UMS Global Configuration. It includes two main sections: "Log message settings" and "Log Event Settings". In "Log message settings", there are two checked checkboxes: "Enable logging" and "Log administrator data". Below these are two buttons: "Log level" (set to "Message body and details") and "Log Level Configuration". In "Log Event Settings", there is one unchecked checkbox: "Activate event logging". To the right of this checkbox is a "Log Level Configuration" button. At the bottom of the screen, a note states: "NOTE: Configuration of log message deletion and export task is now available in Administrative Tasks".

3. Confirm the setting with **Yes**.
4. Go to **Administrative Tasks**.
5. Click **add (+)** to create a new administrative task.
The **Create Administrative Task** dialog opens.



6. Copy the following settings:

A screenshot of the UMS Administration interface. On the left, there is a navigation tree with various settings like UMS Network, Global Configuration, Licenses, Mobile Devices, Device Attributes, and Administrative Tasks. The 'Administrative Tasks' node is selected. In the main pane, there is a table titled 'Administrative Tasks' with one row: 'Name: DB backup, Job: Create backup'. A modal window titled 'Create Administrative Task' is open over this table. The 'General' tab is selected in the modal. Inside, the 'Name' field is set to 'Logging' and the 'Action' dropdown is set to 'Delete logging data'. There are checkboxes for 'Send result as mail' and 'Send to default recipient (not defined)', both of which are unchecked. Below these checkboxes is a 'Rich Message Templates' input field and a checked 'Active' checkbox. At the bottom of the modal are buttons for 'Back', 'Next', 'Finish', and 'Cancel'.



7. Click **Next** and copy the following settings:

Create Administrative Task

Configuration

Target directory for export-files:

Target directory: C:\Program Files\IGEL\RemoteManager\rmguiserver\temp

Log message deletion settings

Keep no more than Messages

Delete messages older than Days

Log event deletion settings

Keep no more than Events

Delete events older than Days

< Back **> Next** **Finish** **Cancel**

8. Click **Next** and **Finish**.

- i** Having logging activated is important for reproducing errors. In this way, you are able to trace the log and event messages in the UMS under **System > Logging**.



9. Click **Device Network Settings** and copy the following settings:

Device Network Settings

Configuration of the System Information Update

Update system information on selection of a device

Advanced Device's Status Updates

Devices send updates

Automatic Registration

Enable automatic registration (without mac address import)

Device Requests

Maximum number of concurrent threads for device requests:

Queue limit:

No limit
(Additional requests should wait until a free thread is available.)

Queue size:
(Additional requests that exceed the queue size should be rejected.)

Adjust Names of devices

Adjust UMS-internal name if network name has been changed

Adjust network name if UMS-internal name has been changed

Naming Convention

Enable naming convention

Prefix:

Minimum digits: 2 3 4 5 6

Reset counter and renumber



10. Click **Server Network Settings** and copy the following settings:

11. Go back to **Administrative Tasks** in the **UMS Administration** tree.

12. Create another **Administrative Task** for the database backups:

13. Click **Next**.

14. Enter the required **target directory**:



Create Administrative Task

Configuration

Maximum amount of backups	0
Target directory:	C:\Program Files\IGEL\Remotemanager

i We recommend that you create a database backup in order to be able to recover the original UMS data in the event of data loss.

15. Click **Next**.
16. Set a rhythm to repeat the backup as shown below and click **Finish**:

Create Administrative Task

Schedule

Trigger

Start: 2019-06-27 13:18

Repeat Job

Task starts every 1 Minutes

Weekdays Mon Tue Wed Thu Fri Sat Sun

Monthly

Exclude Public Holidays

Date	Comment

Expiration 2019-06-27 13:18

Back **Next** **Finish** **Cancel**

17. Go to **Active Directory / LDAP** and add a new Active Directory/LDAP service with the following values:



The screenshot shows the UMS Administration interface on a server at 172.30.91.30. The left sidebar lists various configuration categories. The 'Active Directory / LDAP' category is selected and highlighted in blue. A modal dialog box titled 'Add Active Directory / LDAP Service' is open. In the dialog, the 'Type' dropdown is set to 'Active Directory Service'. The 'Domain Name' field contains 'IGEL.LOCAL'. The 'Domain Controller(s)' field contains 'dc02.igel.local; dc03.igel.local; dc0'. The 'Page Size' field is set to '1000'. The 'Port' field is set to '389'. The 'Use LDAPS connection' checkbox is unchecked. The 'User name' field contains 'igel'. The 'Password' field contains '*****'. Below the password field is a link 'Import SSL Certificate'. The 'UPN Suffix' field is empty. At the bottom of the dialog is a 'Test connection' button, and at the very bottom are 'Ok' and 'Cancel' buttons.

18. Click the **Test connection** button to check if your configuration is working.

1.1.7 Creating Device Structures

You may freely organize your device structure in the IGEL UMS tree.

Take advantage of this freedom and build well thought out, intelligent directory structures. How deeply you want to structure your tree is up to you. The system allows you to nest directories as deeply as you want.

It would be advisable to arrange the directories referring to your company's structure.

You could classify the devices according to branch offices, departments or tasks, for example:





Keep in mind that you also need a smart structure for automatic registration with indirect profiles. Devices will inherit the profiles assigned to the root directory they are subordinated to.

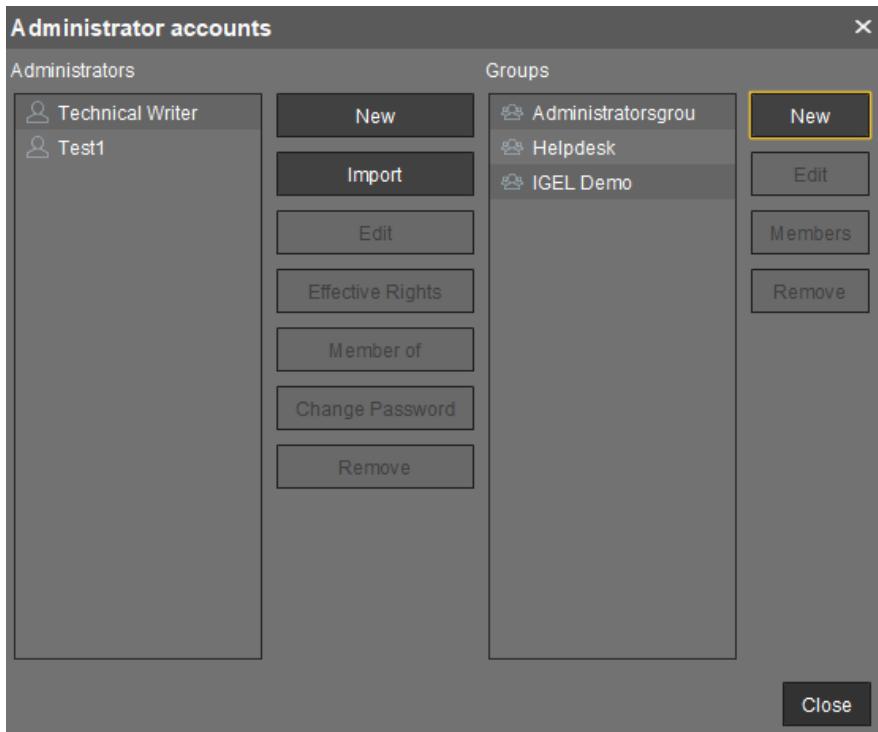
1.1.8 Administrator Accounts

Import administrative accounts from the Active Directory, groups as well as users.

- ▶ Click **System > Administrator Accounts** to set up groups of administrators in order to manage their permissions more conveniently.

Where required, add local administrators. Permission settings are performed in the same way for both groups and individual administrators.

- ⓘ If you do not wish to completely adopt the Active Directory structure, you may create new local administrators or groups.





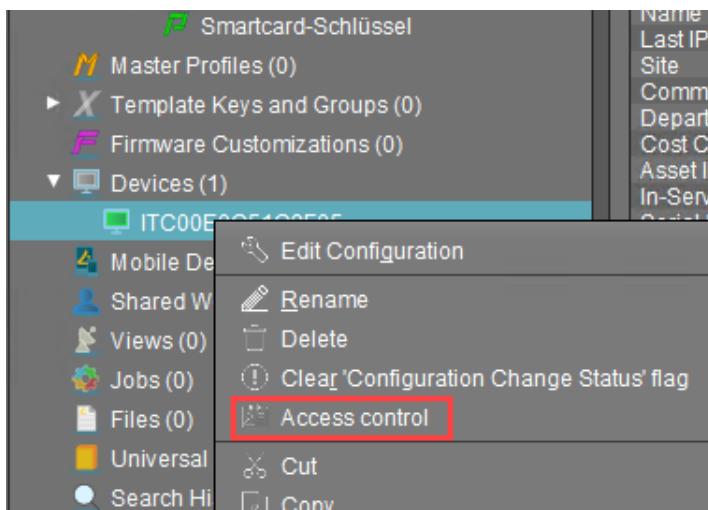
- Click **Edit** in the **Administrator Accounts** mask to set permissions for specific menu items:

Edit group permissions

Group Name	Administratorsgrou	
	Allow	Deny
Allow all	<input type="checkbox"/>	<input type="checkbox"/>
Deny all	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Deselect all	<input type="checkbox"/>	<input type="checkbox"/>
'System' Menu	Allow	Deny
Administrator accounts	<input type="checkbox"/>	<input type="checkbox"/>
Firmware management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
License management	<input type="checkbox"/>	<input type="checkbox"/>
Logging (events and messages)	<input type="checkbox"/>	<input type="checkbox"/>
WebDAV access (ums-filetransfer)	<input type="checkbox"/>	<input type="checkbox"/>
'Device' Menu		
Scan for devices	<input checked="" type="checkbox"/>	<input type="checkbox"/>
'Misc' Menu		
Cache management	<input type="checkbox"/>	<input type="checkbox"/>
Host Assignment (Jobs)	<input type="checkbox"/>	<input type="checkbox"/>
Public Holidays Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Sql Console	<input checked="" type="checkbox"/>	<input type="checkbox"/>
'Help' Menu		
Save support information	<input type="checkbox"/>	<input type="checkbox"/>
Ok	Cancel	

i Note for all other value sets: Each administrator can be granted specific permissions with regard to objects in the navigation tree.

- Right-click an object in the structure tree.



- ▶ Click **Access Control** in the context menu to set object permissions.

Access Control

Thin Client: /Devices/ITC00E0C51C9F05

Administrators

Permission	Allow	Deny	Effective Rights
Browse	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for group Administrators
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for group Administrators
Move	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Administrators
Edit Configuration	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Administrators
Write	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Administrators
Edit System Information	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Administrators
Access Control	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Administrators
Assign	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Administrators
Power Control	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Administrators
Firmware Control	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Administrators
Settings Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for group Administrators
Remote access	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for group Administrators



For more information on UMS administrator accounts and their access rights, refer to [Create Administrator Accounts](#)(see page 508).

1.1.9 Registering Devices

During the preparation and [System Configuration](#)(see page 35), we put in place the basis for automatic device registration; see also [Registering Devices Automatically](#)(see page 312). For more information on the registration of devices, refer to [Registering Devices on the UMS Server](#)(see page 306).

- All you need to do is to start the devices or, if they are already in operation, to restart them.

If automatic registration fails, e.g. in WAN with NAT, register the missing devices manually.

After the registration, refresh the console editor view (F5) to show the new devices. Check the device structure and, if necessary, move the devices into the desired directories.

A device can only be registered to one UMS Server. If it is registered once, no other UMS can capture it.

- ⓘ We highly recommend disabling automatic registration after the roll-out to avoid all types of devices automatically being registered without your control.

Now you have a well-configured IGEL UMS which will allow you to work with the system professionally.

1.1.10 Creating Profiles

Create **Profiles** according to the different task areas such as

- Network configuration
- Sessions
- Printer
- Monitor configuration



- ✓ The best practice is to define one profile for each task and not to mix them up. Otherwise, you will have problems maintaining your configuration settings later on.

In this case, we created a profile exclusively for the English keyboard layout:



The screenshot shows the UMS Configuration interface with the 'Input' section selected in the left sidebar. Under 'Keyboard', the 'Repeat delay' is set to 660 and 'Repeat rate' is set to 40. There is also a 'Test' button and a checkbox for 'Start with numlock on'.

After creating a profile and adjusting its settings, you can assign it to some Devices. You can assign an arbitrary number of profiles to each device.

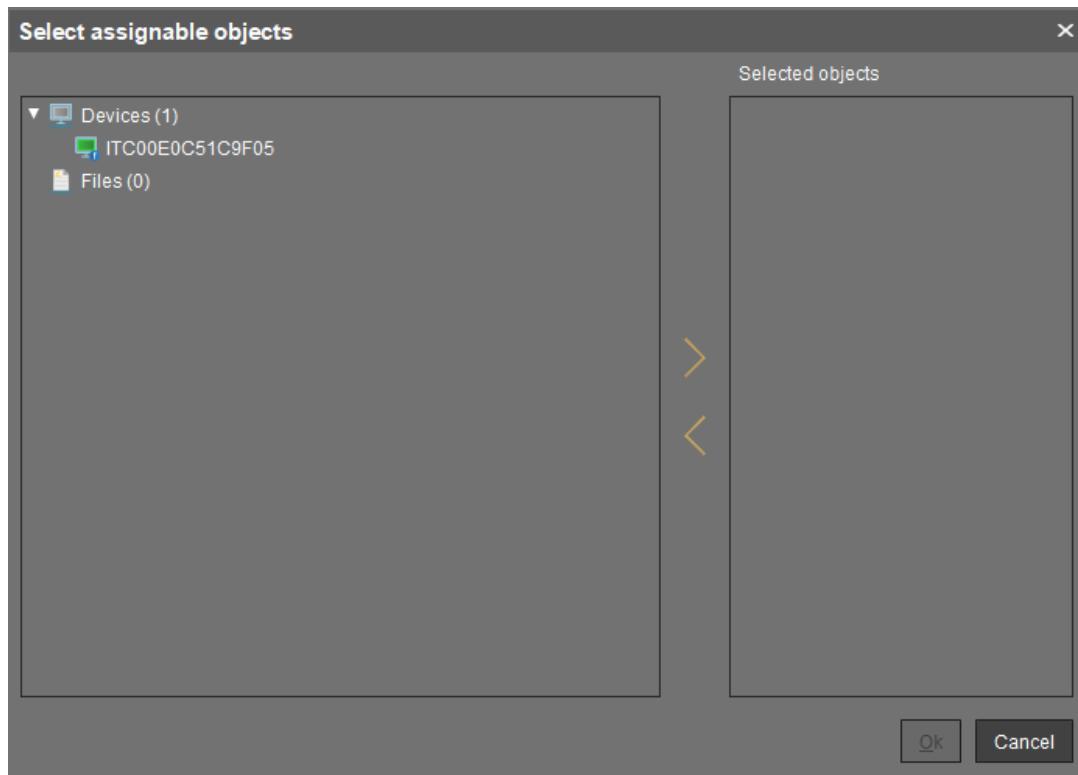
Basically, there are two modes of assignment: **direct** or **indirect**.

Indirect means that you assign the profile to a device directory rather than to a single device. All devices within the directory then inherit the settings of this profile.

- ▶ Select a **Profile** in the UMS tree and drag and drop the selection onto a device or device directory.
- or
- ▶ Select a device directory in the UMS tree and click the **Add (+)** button above the **Assigned Objects** panel.

The screenshot shows the 'Assigned objects' panel within the Profile Selection dialog. It lists a single item: 'Name'. The left side of the dialog shows profile details: Name (Smartcard-Schlüssel), Description, Based on (IGEL Universal Desktop LX 10.05.500.01), Profile ID (3320), Expert mode, and Overwrite Sessions.

- ▶ In the **Profile Selection** dialog that appears, select the profile to assign and press **Ok**:



i You can also do it the other way round: Select a profile in the UMS tree and assign a device directory to it.

For more information on profiles and their assignment to devices, refer to [Profiles\(see page 331\)](#).

1.2 Devices Supported by IGEL Universal Management Suite (UMS)

1.2.1 Question

Which devices are supported by IGEL Universal Management Suite (UMS)?

1.2.2 Answer

- ⚠** To ensure that you can use all new features of IGEL OS:
- ▶ Update your UMS to the current version.
 - ▶ For all relevant profiles, set **Based on** to the appropriate firmware version.

The latest UMS version supports

- all IGEL devices that have not yet reached their [end of maintenance](#)⁵;

⁵ <https://kb.igel.com/display/hardware/Legacy+IGEL+Devices>



- devices converted with IGEL OS Creator (OSC);
- devices converted with IGEL Universal Desktop Converter 3 (UDC3);
- devices converted with IGEL Universal Desktop Converter 2 (UDC2);
- Windows 7 devices with IGEL Unified Management Agent (UMA) installed.

Older UMS releases support

- IGEL devices that were released before the UMS release
- and that had not reached their [end of maintenance](#)⁶ at the time of the UMS release.

1.3 UMS Communication Ports

Which ports are used by the components of IGEL UMS and the other components of a UMS infrastructure?

The following table shows the ports used by the components that play a role in a UMS infrastructure.

1.3.1 Sorted by UMS Feature

Required by UMS Feature	Port (Protocol)	Who is Listening? (Protocols) Applications/ Service Binding to Port	Who is Talking? Applications /Services Initiating Communications	Description
Automatic License Deployment (ALD)	443 (TCP)	IGEL licensing server (at susi.igel.com ⁷)	UMS Server	The UMS Server requests licenses; see UMS Contacting the Licensing Server (see page 82).
Automatic License Deployment (ALD)	443 (TCP)	IGEL download server (HTTP server at fwus.igel.com ⁸)	UMS Server	The UMS Server requests the connection details required for connecting to the IGEL license server (at susi.igel.com ⁹). See UMS Contacting the Licensing Server (see page 82).
Core	8443 (TCP)	UMS Server (Windows: service IGELRMGUIS)	UMS Console /	See UMS with Internal Database (see page 59) or UMS with External Database (see page 60).

⁶ <https://kb.igel.com/display/hardware/Legacy+IGEL+Devices>

⁷ <http://susi.igel.com>

⁸ <http://fwus.igel.com>

⁹ <http://susi.igel.com>



Required by UMS Feature	Port (Protocol)	Who is Listening? Applications/Service Binding to Port	Who is Talking? Applications /Services Initiating Communications	Description
		server; Linux: daemon igelRMServer)	UMS Web App	
Core (directly, without ICG)	30002 (TCP)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	HA Load Balancer	If the UMS Server and the HA Load Balancer are running on the same host, the UMS Server will use port 30002 instead of 30001, and the HA Load Balancer will use port 30001.
Core (direct device communication, not used with communication via ICG)	30001 (TCP)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	Device	See Devices Contacting UMS (see page 64).
Core (file transfer)	8443 (TCP)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	Device	The device requests a file from the UMS; see UMS and Devices: File Transfer (see page 76).
Core (firmware customization)	8443 (TCP)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	Device	The UMS provides files for customizing the look and feel of the device's GUI; see UMS and Devices: File Transfer (see page 76).



Required by UMS Feature	Port (Protocol)	Who is Listening? Applications/Service Binding to Port	Who is Talking? Applications /Services Initiating Communications	Description
Core (if Active Directory is used), Shared Workplace	88 (TCP/UDP)	MS Active Directory Service	UMS Server	The UMS Server sends a Kerberos request to MS Active Directory.
Core (if Active Directory is used), Shared Workplace	389 (TCP)	MS Active Directory Service	UMS Server	The UMS Server sends an LDAP request to MS Active Directory.
Core (if Apache Derby is used)	1527 (TCP)	Apache Derby database (Derby Network Server)	UMS Server	See UMS with External Database (see page 60).
Core (if LDAPS server is used)	636 (TCP)	LDAPS server (other than MS Active Directory)	UMS Server	The UMS Server sends an LDAP request over SSL.
Core (if MS SQL Server is used)	1433 (TCP)	Microsoft SQL Server database	UMS Server	See UMS with External Database (see page 60).
Core (if Oracle is used)	1521 (TCP)	Oracle database	UMS Server	See UMS with External Database (see page 60).
Core (if PostgreSQL is used)	5432 (TCP)	PostgreSQL database	UMS Server	See UMS with External Database (see page 60).
Core (licenses)	8443 (TCP)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	Device	The UMS provides license files for the devices; see UMS and Devices: File Transfer (see page 76).



Required by UMS Feature	Port (Protocol)	Who is Listening? Applications/Service Binding to Port	Who is Talking? Applications /Services Initiating Communications	Description
Core (online check)	Auto ("high port") (UDP)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	Device	<p>The device responds to a message sent by the UMS to check if the device is online.</p> <p>The port number to be used is contained in the UDP packet sent by the UMS.</p>
Core (scanning for device)	30005 (TCP/UDP)	Device (UMS agent)	Device	<p>The device responds to a broadcast sent by the UMS during a scan.</p> <p>The port number to be used is contained in the UDP packet sent by the UMS.</p> <p>See UMS Server(see page 256).</p>
Core (scanning for device)	Auto ("high port") (UDP)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	Device	<p>The device responds to a broadcast sent by the UMS during a scan.</p> <p>The port number to be used is contained in the UDP packet sent by the UMS.</p>
Core (secure terminal)	30022 (TCP)	Device (UMS agent)	UMS Server	See UMS and Devices: Secure Terminal (see page 74).
Core (shadowing)	5900 (TCP)	Device (UMS agent)	UMS Console	The UMS Console initiates a VNC session for shadowing; see UMS and Devices: Shadowing (see page 66).
Core (shadowing) via UMS Web App	5900 (TCP)	Device (UMS agent)	UMS Server	The UMS Web App triggers the UMS Server to initiate a VNC session for shadowing. The VNC session is routed through the UMS Server;



Required by UMS Feature	Port (Protocol)	Who is Listening? Applications/Service Binding to Port	Who is Talking? Applications /Services Initiating Communications	Description
				see UMS and Devices: Shadowing (see page 66).
Core (unencrypted, no SSL)	9080 (TCP)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	Device	<p>The device requests a file from the UMS (regular file transfer or Universal Firmware Update). This port is only used if Allow SSL Connections only is deactivated in the UMS Administrator. If Allow SSL Connections only is activated, port 8443 is used for firmware updates and file transfer.</p>
Core (unencrypted, no SSL)	Auto ("high port")	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	UMS Console	<p>The GUI is started via Java Webstart console. This port is only used if Allow SSL Connections only is deactivated in the UMS Administrator. If Allow SSL Connections only is activated, port 8443 is used for firmware updates and file transfer.</p>
Core (Universal Firmware Update)	443 (TCP)	IGEL download server (HTTP server at fwus.igel.com ¹⁰)	UMS Server	See UMS Contacting the Download Server to Check for New Updates (see page 77).
Core (Universal Firmware Update)	8443 (TCP)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	Device	In the course of a Universal Firmware Update, the device requests a file from the UMS; see UMS and Devices: File Transfer (see page 76).

¹⁰ <http://fwus.igel.com>



Required by UMS Feature	Port (Protocol)	Who is Listening? Applications/Service Binding to Port	Who is Talking? Applications /Services Initiating Communications	Description
Core (Wake on LAN)	9 (UDP)	Device	UMS Server	The UMS Server sends magic packets to the devices.
Core (with ICG)	8443 (TCP)	ICG (IGEL Cloud Gateway)	UMS Server	See Devices and UMS Server Contacting Each Other via ICG (see page 62) or UMS Server (see page 256).
Core (with ICG)	8443 (TCP)	ICG (IGEL Cloud Gateway)	Device	See Devices and UMS Server Contacting Each Other via ICG (see page 62).
High Availability (HA)	6155 (UDP)	HA Load Balancer UMS Server	HA Load Balancer UMS Server	Both HA Load Balancer and UMS Server listen on port 6155 and use it for communication.
High Availability (HA)	8443 (TCP)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	File synchronization between UMS Servers
High Availability (HA)	61616 (TCP/UDP)	HA Load Balancer UMS Server	HA Load Balancer UMS Server	Both HA Load Balancer and UMS Server listen on port 61616 and use it for communication.
IMI	8443 (TCP)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	3rd party component using IMI (IGEL Management Interface)	See IGEL Management Interface (IMI) (see page 61).



1.3.2 Sorted by Port Number

Port (Protocol)	Who is Listening? Applications/ Service Binding to Port	Who is Talking? Applications /Services Initiating Communicat ions	Description	Required by UMS Feature
9 (UDP)	Device	UMS Server	The UMS Server sends magic packets to the devices.	Core (Wake on LAN)
88 (TCP/ UDP)	MS Active Directory Service	UMS Server	The UMS Server sends a Kerberos request to MS Active Directory.	Core (if Active Directory is used), Shared Workplace
389 (TCP)	MS Active Directory Service	UMS Server	The UMS Server sends an LDAP request to MS Active Directory.	Core (if Active Directory is used), Shared Workplace
443 (TCP)	IGEL licensing server (at susi.igel.com)	UMS Server	The UMS Server requests licenses; see UMS Contacting the Licensing Server (see page 82).	Automatic License Deployment (ALD)
443 (TCP)	IGEL download server (HTTP server at fwus.igel.com)	UMS Server	The UMS Server requests the connection details required for connecting to the IGEL license server (at susi.igel.com). See UMS Contacting the Licensing Server (see page 82).	Automatic License Deployment (ALD)
443 (TCP)	IGEL download server (HTTP server at fwus.igel.com)	UMS Server	See UMS Contacting the Download Server to Check for New Updates (see page 77).	Core (Universal Firmware Update)
636 (TCP)	LDAPS server (other than MS Active Directory)	UMS Server	The UMS Server sends an LDAP request over SSL.	Core (if LDAPS server is used)
1433 (TCP)	Microsoft SQL Server database	UMS Server	See UMS with External Database (see page 60).	Core (if MS SQL Server is used)
1521 (TCP)	Oracle database	UMS Server	See UMS with External Database (see page 60).	Core (if Oracle is used)



Port (Protocol)	Who is Listening? Applications/ Service Binding to Port	Who is Talking? Applications /Services Initiating Communicat ions	Description	Required by UMS Feature
1527 (TCP)	Apache Derby database (Derby Network Server)	UMS Server	See UMS with External Database (see page 60).	Core (if Apache Derby is used)
5432 (TCP)	PostgreSQL database	UMS Server	See UMS with External Database (see page 60).	Core (if PostgreSQL is used)
5900 (TCP)	Device (UMS agent)	UMS Console	The UMS Console initiates a VNC session for shadowing; see UMS and Devices: Shadowing (see page 66).	Core (shadowing)
5900 (TCP)	Device (UMS agent)	UMS Server	The UMS Web App triggers the UMS Server to initiate a VNC session for shadowing. The VNC session is routed through the UMS Server; see UMS and Devices: Shadowing (see page 66).	Core (shadowing) via UMS Web App
6155 (UDP)	HA Load Balancer UMS Server	HA Load Balancer UMS Server	Both HA Load Balancer and UMS Server listen on port 6155 and use it for communication.	High Availability (HA)
8443 (TCP)	UMS Server (Windows: service IGELRMGUIS erver; Linux: daemon igelRMServ er)	UMS Console / UMS Web App	See UMS with Internal Database (see page 59) or UMS with External Database (see page 60).	Core
8443 (TCP)	UMS Server (Windows: service IGELRMGUIS erver; Linux: daemon igelRMServ er)	Device	The device requests a file from the UMS; see UMS and Devices: File Transfer (see page 76).	Core (file transfer)



Port (Protocol)	Who is Listening? Applications/ Service Binding to Port	Who is Talking? Applications /Services Initiating Communicat ions	Description	Required by UMS Feature
8443 (TCP)	UMS Server (Windows: service IGELRMGUIS erver; Linux: daemon igelRMServ er)	Device	In the course of a Universal Firmware Update, the device requests a file from the UMS; see UMS and Devices: File Transfer (see page 76).	Core (Universal Firmware Update)
8443 (TCP)	UMS Server (Windows: service IGELRMGUIS erver; Linux: daemon igelRMServ er)	3rd party component using IMI (IGEL Management Interface)	See IGEL Management Interface (IMI) (see page 61).	IMI
8443 (TCP)	UMS Server (Windows: service IGELRMGUIS erver; Linux: daemon igelRMServ er)	Device	The UMS provides files for customizing the look and feel of the device's GUI; see UMS and Devices: File Transfer ¹¹ .	Core (firmware customization)
8443 (TCP)	UMS Server (Windows: service IGELRMGUIS erver; Linux: daemon igelRMServ er)	Device	The UMS provides license files for the devices; see UMS and Devices: File Transfer ¹² .	Core (licenses)
8443 (TCP)	ICG (IGEL Cloud Gateway)	UMS Server	See Devices and UMS Server Contacting Each Other via ICG (see page 62) or UMS Server (see page 256).	Core (with ICG)

¹¹ <https://kb.igel.com/display/ENLITEUMS/.UMS+and+Devices%3A+File+Transfer+v5.08>

¹² <https://kb.igel.com/display/ENLITEUMS/.UMS+and+Devices%3A+File+Transfer+v5.08>



Port (Protocol)	Who is Listening? Applications/ Service Binding to Port	Who is Talking? Applications /Services Initiating Communicat ions	Description	Required by UMS Feature
8443	ICG (IGEL Cloud (TCP) Gateway)	Device	See Devices and UMS Server Contacting Each Other via ICG (see page 62).	Core (with ICG)
8443	UMS Server (Windows: service IGELRMGUIS erver; Linux: daemon igelRMServ er)	UMS Server (Windows: service IGELRMGUIS erver; Linux: daemon MGUIServer; Linux: daemon igelR MServer)	File synchronization between UMS Servers	High Availability (HA)
9080	UMS Server (Windows: service IGELRMGUIS erver; Linux: daemon igelRMServ er)	Device	<p>The device requests a file from the UMS (regular file transfer or Universal Firmware Update).</p> <p>This port is only used if Allow SSL Connections only is deactivated in the UMS Administrator.</p> <p>If Allow SSL Connections only is activated, port 8443 is used for firmware updates and file transfer.</p>	Core (unencrypted, no SSL)
Auto ("high port")	UMS Server (Windows: service IGELRMGUIS erver; Linux: daemon igelRMServ er)	UMS Console	<p>The GUI is started via Java Webstart console.</p> <p>This port is only used if Allow SSL Connections only is deactivated in the UMS Administrator.</p> <p>If Allow SSL Connections only is activated, port 8443 is used for firmware updates and file transfer.</p>	Core (unencrypted, no SSL)
30001	UMS Server (TCP) (Windows: service IGELRMGUIS	Device	See Devices Contacting UMS (see page 64).	Core (direct device communication, not used with



Port (Protocol)	Who is Listening? Applications/ Service Binding to Port	Who is Talking? Applications /Services Initiating Communicat ions	Description	Required by UMS Feature
	server; Linux: daemon igelRMServ er)			communication via ICG)
30002 (TCP)	UMS Server (Windows: service IGELRMGUIS erver; Linux: daemon igelRMServ er)	HA Load Balancer	If the UMS Server and the HA Load Balancer are running on the same host, the UMS Server will use port 30002 instead of 30001, and the HA Load Balancer will use port 30001.	Core (directly, without ICG)
30005 (TCP/ UDP)	Device (UMS agent)	Device	<p>The device responds to a broadcast sent by the UMS during a scan.</p> <p>The port number to be used is contained in the UDP packet sent by the UMS.</p> <p>See UMS Server(see page 256).</p>	Core (scanning for device)
30022 (TCP)	Device (UMS agent)	UMS Server	See UMS and Devices: Secure Terminal (see page 74).	Core (secure terminal)
61616 (TCP/ UDP)	HA Load Balancer UMS Server	HA Load Balancer UMS Server	Both HA Load Balancer and UMS Server listen on port 61616 and use it for communication.	High Availability (HA)
Auto ("high port") (UDP)	UMS Server (Windows: service IGELRMGUIS erver; Linux: daemon igelRMServ er)	Device	<p>The device responds to a broadcast sent by the UMS during a scan.</p> <p>The port number to be used is contained in the UDP packet sent by the UMS.</p>	Core (scanning for device)



Port (Protocol)	Who is Listening? Applications/ Service Binding to Port	Who is Talking? Applications /Services Initiating Communicat ions	Description	Required by UMS Feature
Auto ("high port")	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	Device	<p>The device responds to a message sent by the UMS to check if the device is online.</p> <p>The port number to be used is contained in the UDP packet sent by the UMS.</p>	Core (online check)

- [Internal Communication](#)(see page 59)
- [IGEL Management Interface \(IMI\)](#)(see page 61)
- [UMS and Devices: Settings and Control](#)(see page 62)
- [UMS and Devices: Shadowing](#)(see page 66)
- [UMS and Devices: Secure Shadowing](#)(see page 68)
- [UMS and Devices: Secure Terminal](#)(see page 74)
- [UMS and Devices: File Transfer](#)(see page 76)
- [Universal Firmware Update](#)(see page 77)
- [Automatic License Deployment \(ALD\)](#)(see page 81)

1.3.3 Internal Communication

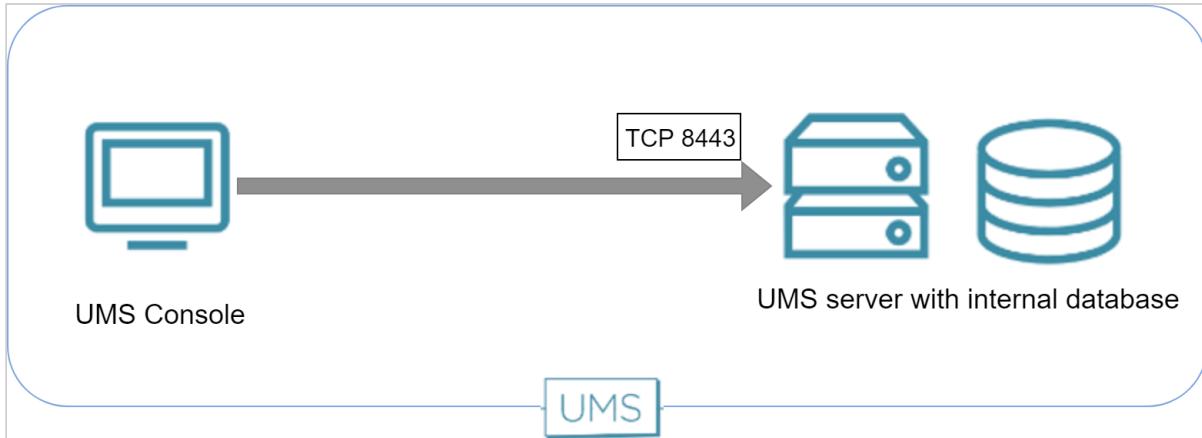
- [UMS with Internal Database](#)(see page 59)
- [UMS with External Database](#)(see page 60)
- [Indexing for UMS Web App Search](#)(see page 61)

UMS with Internal Database

Communication between the UMS Console and the UMS server happens via HTTPS. By default, the UMS server listens for requests on TCP port 8443. The port can be changed in the UMS Administrator under **Settings > GUI server port**.

The port used by the UMS for internal TCP requests to the embedded database can be changed in the UMS Administrator under **Settings > Database Port (Embedded DB)**. The default port is 1528.

The following figure illustrates the communication between the UMS components:



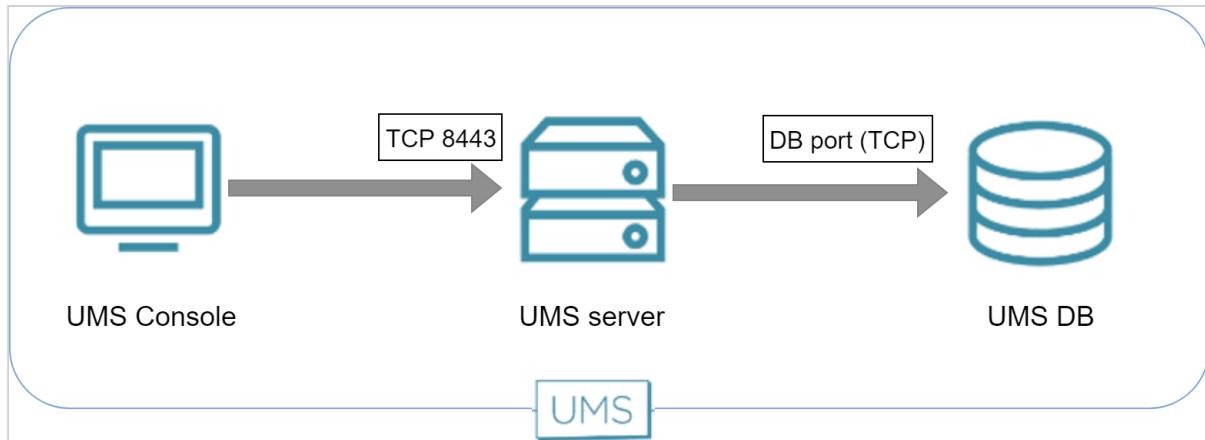
UMS with External Database

Communication between the UMS Console and the UMS server happens via HTTPS. By default, the UMS server listens to TCP requests on port 8443. The port can be changed in the UMS Administrator under **Settings > GUI server port**.

The ports used by the UMS for TCP requests to the database are defined as follows:

Database Type	Database Port (default)	Configuration
Apache Derby (Derby Network Server)	1527	(UMS Administrator) Datasource > Add... > [as DB-Type, select Derby] > Port
MS SQL Server	1433	(UMS Administrator) Datasource > Add... > [as DB-Type, select SQL Server] > Port
Oracle	1521	(UMS Administrator) Datasource > Add... > [as DB-Type, select Oracle] > Port
PostgreSQL	5432	(UMS Administrator) Datasource > Add... > [as DB-Type, select PostgreSQL] > Port

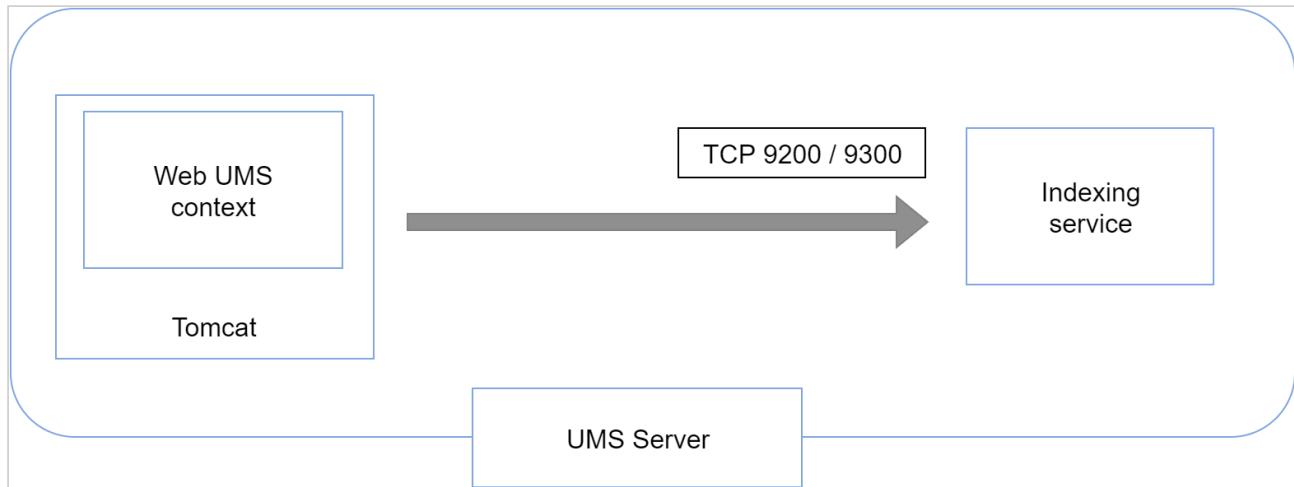
The following figure illustrates the communication between the UMS components:



Indexing for UMS Web App Search

The indexing service that is used by the search function of the UMS Web App is listening on ports 9200 and 9300. The Web UMS context reads and writes data via these ports. The ports are open internally, but cannot be reached from outside the UMS Server.

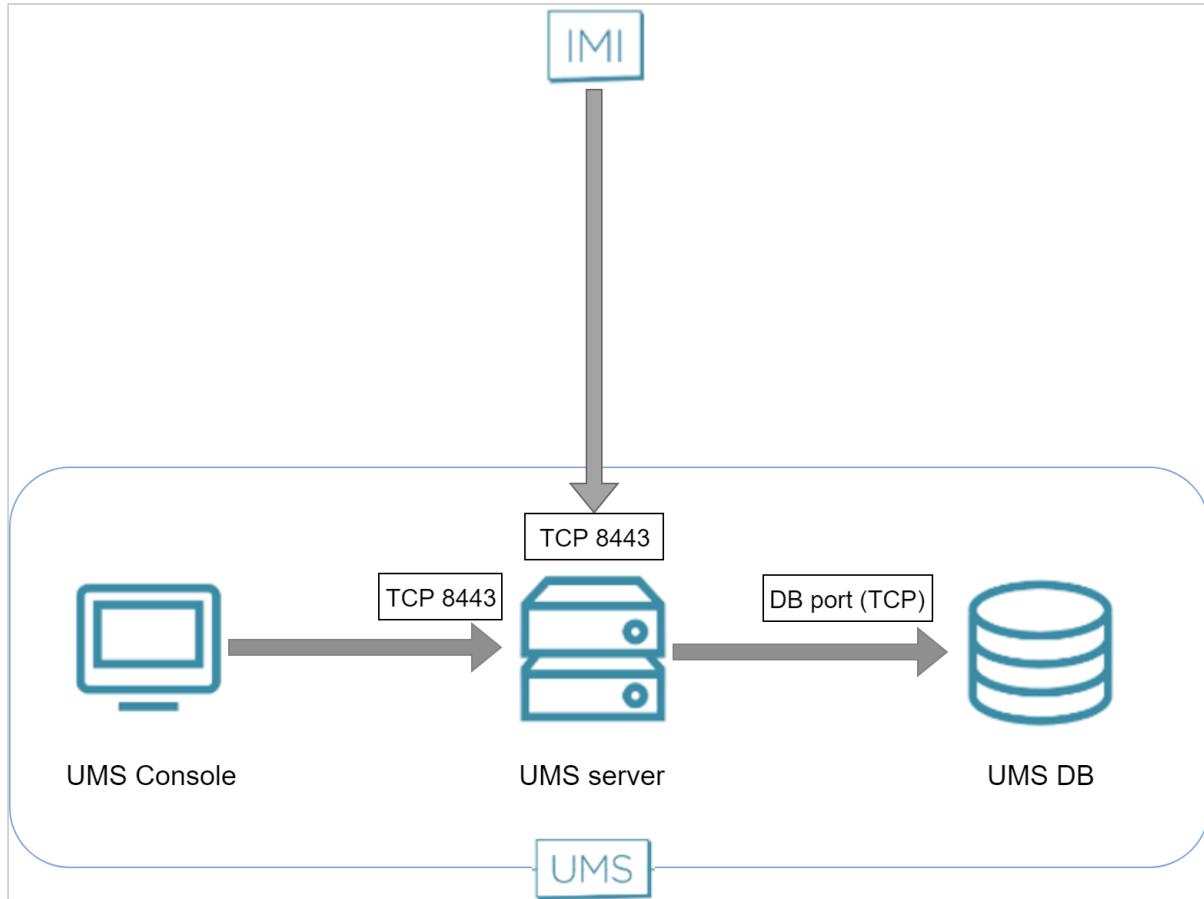
The following figure illustrates the communication within the UMS Server:



1.3.4 IGEL Management Interface (IMI)

The REST API provided by the IGEL Management Interface is served via HTTP on port 8443 (TCP).

The following figure illustrates the communication with the UMS server via IMI:



1.3.5 UMS and Devices: Settings and Control

- [Devices and UMS Server Contacting Each Other via ICG \(see page 62\)](#)
- [Devices Contacting UMS \(see page 64\)](#)
- [UMS Contacting Devices \(see page 65\)](#)

Devices and UMS Server Contacting Each Other via ICG

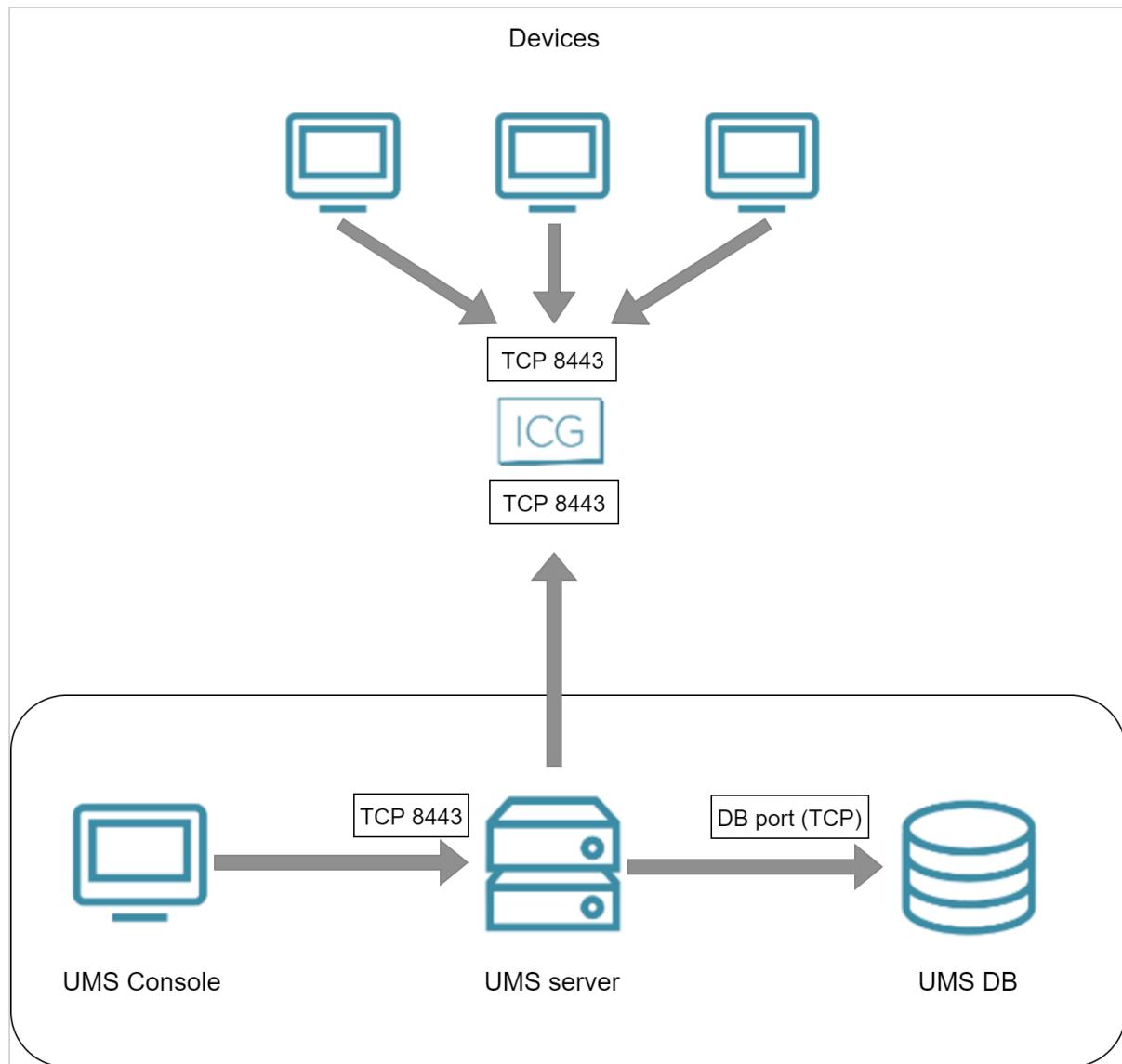
To communicate with the UMS, the devices initiate a TCP connection to the ICG.

To communicate with the devices, the UMS initiates a TCP connection to the ICG.

The default port on which the ICG is listening is port 8443. It can be changed during the installation of the ICG. With ICG 2.02 or higher, a privileged port can be used, e.g. port 443. When the installation is completed, the port is fixed.

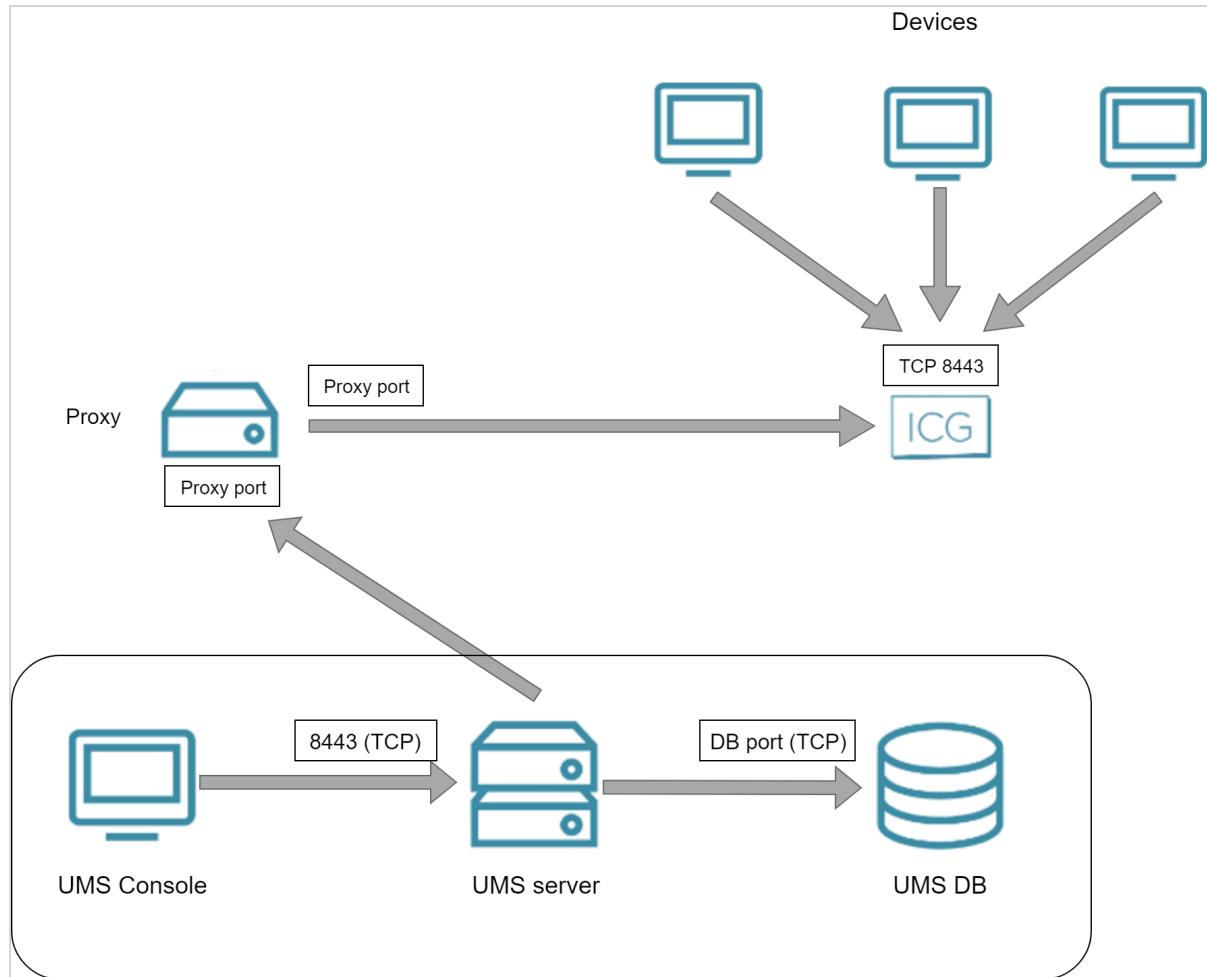
Direct Connection

The following figure illustrates the communication between the devices (thin clients) and the UMS via ICG:



Via Proxy

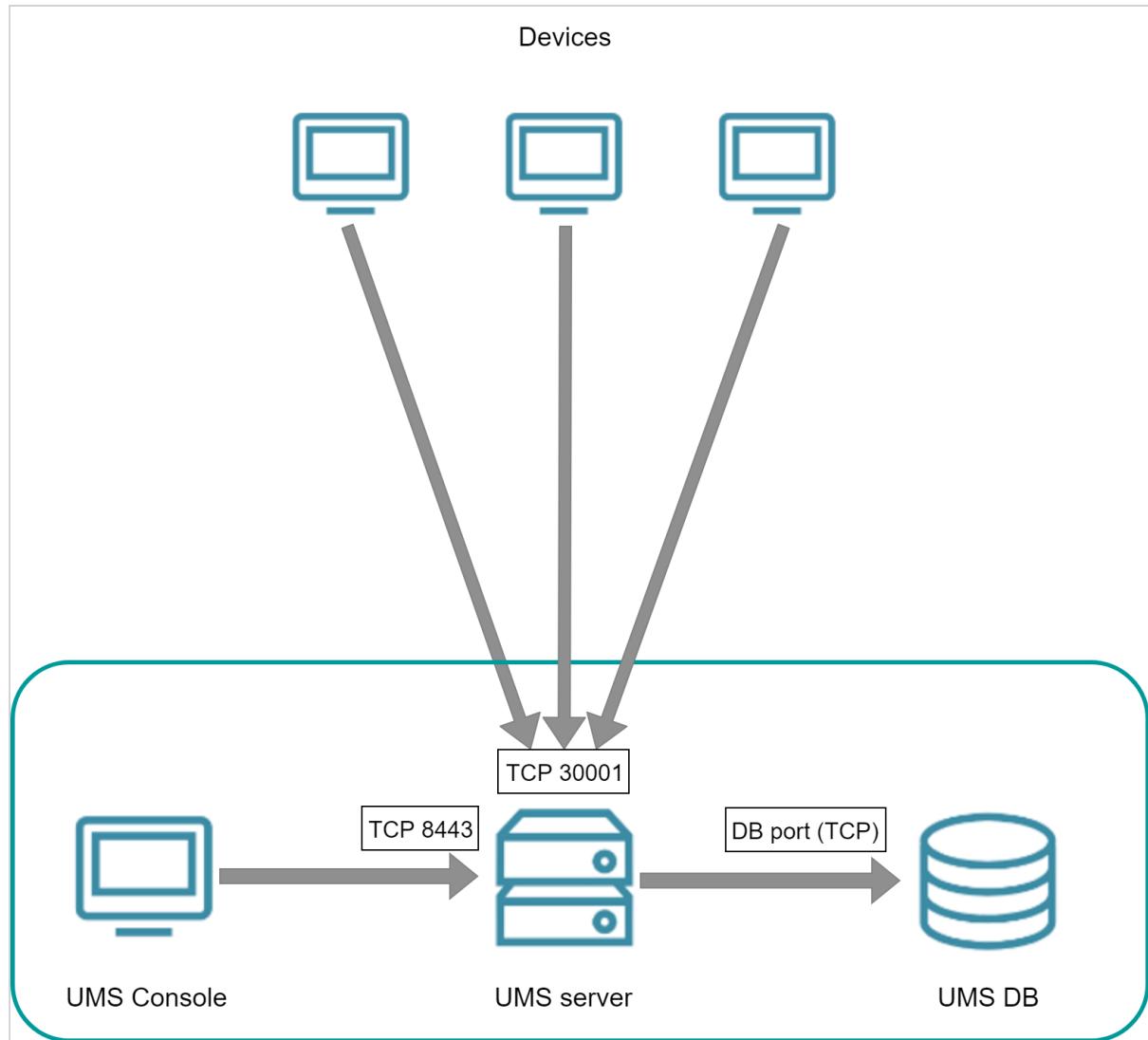
The following figure illustrates the communication between the devices (thin clients) and the UMS via ICG and a proxy:



Devices Contacting UMS

To communicate with the UMS, the devices initiate a TCP connection to the UMS server using port 30001.

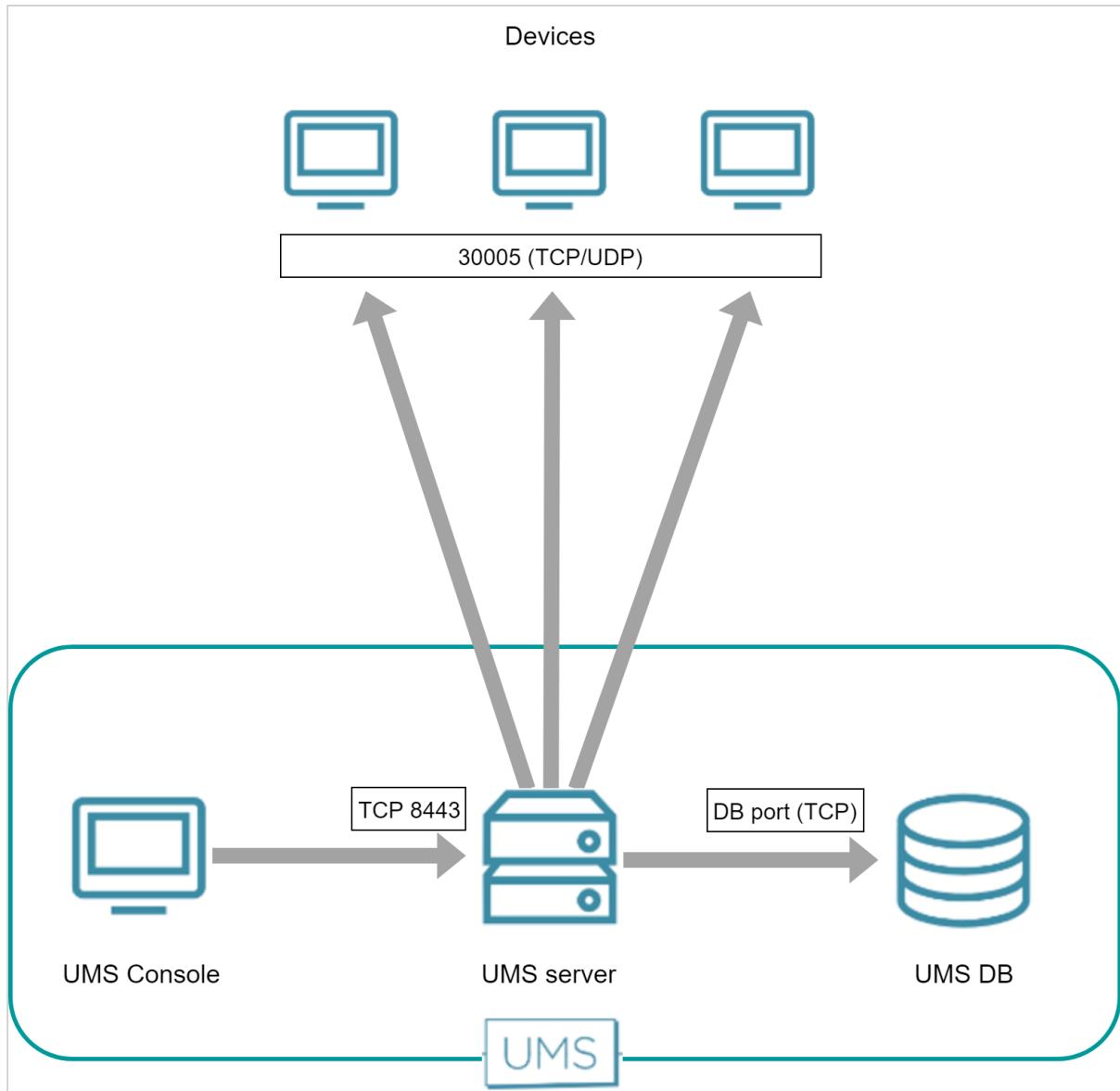
The following figure illustrates the communication between the devices (thin clients) and the UMS:



UMS Contacting Devices

To communicate with devices, the UMS initiates a TCP connection to the device's UMS agent using port 30005.

The following figure illustrates the communication between the UMS and the devices:

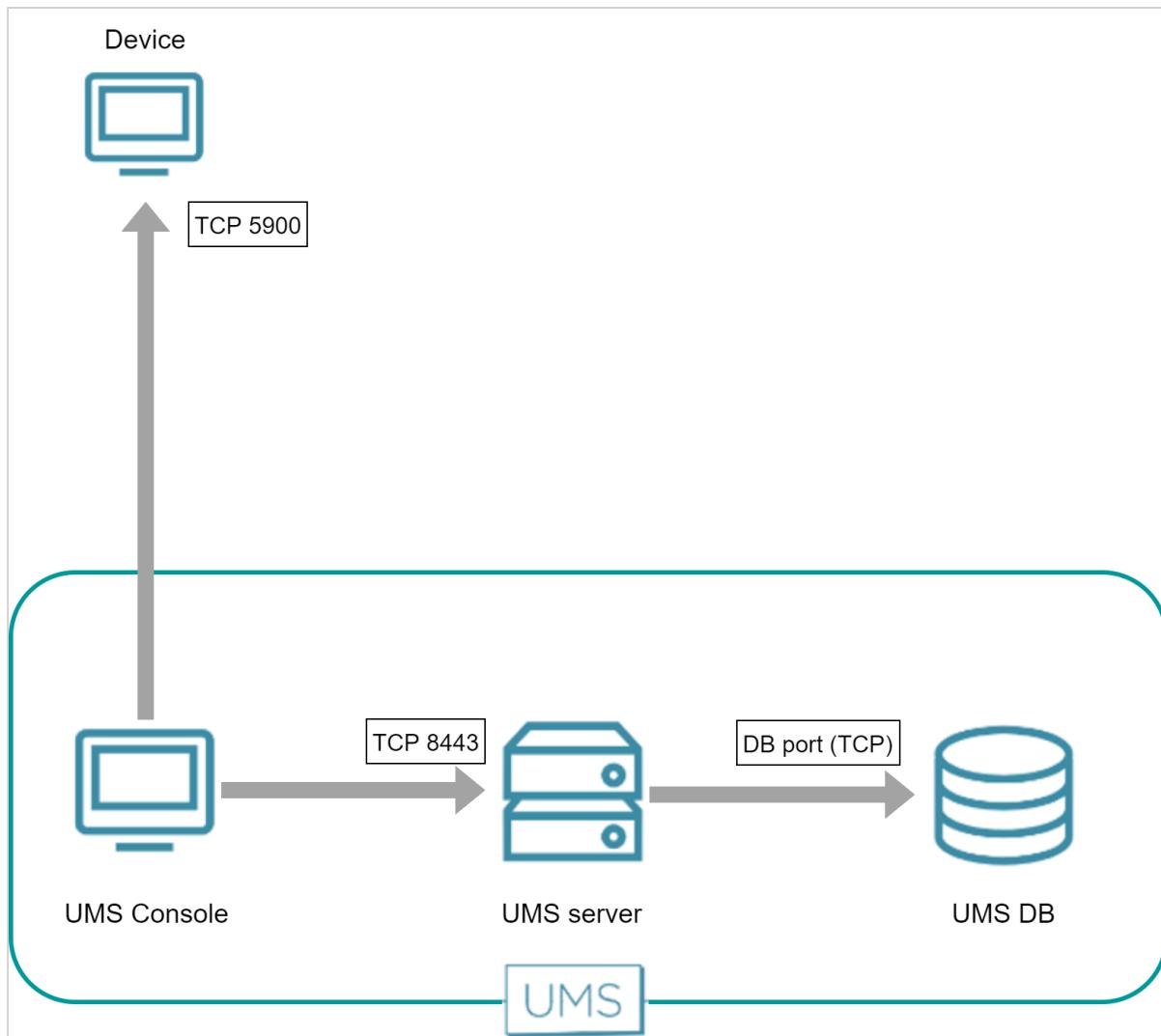


1.3.6 UMS and Devices: Shadowing

UMS Console

The UMS Console initiates a VNC session with the device. The standard port is 5900 (TCP); the port can be changed per session.

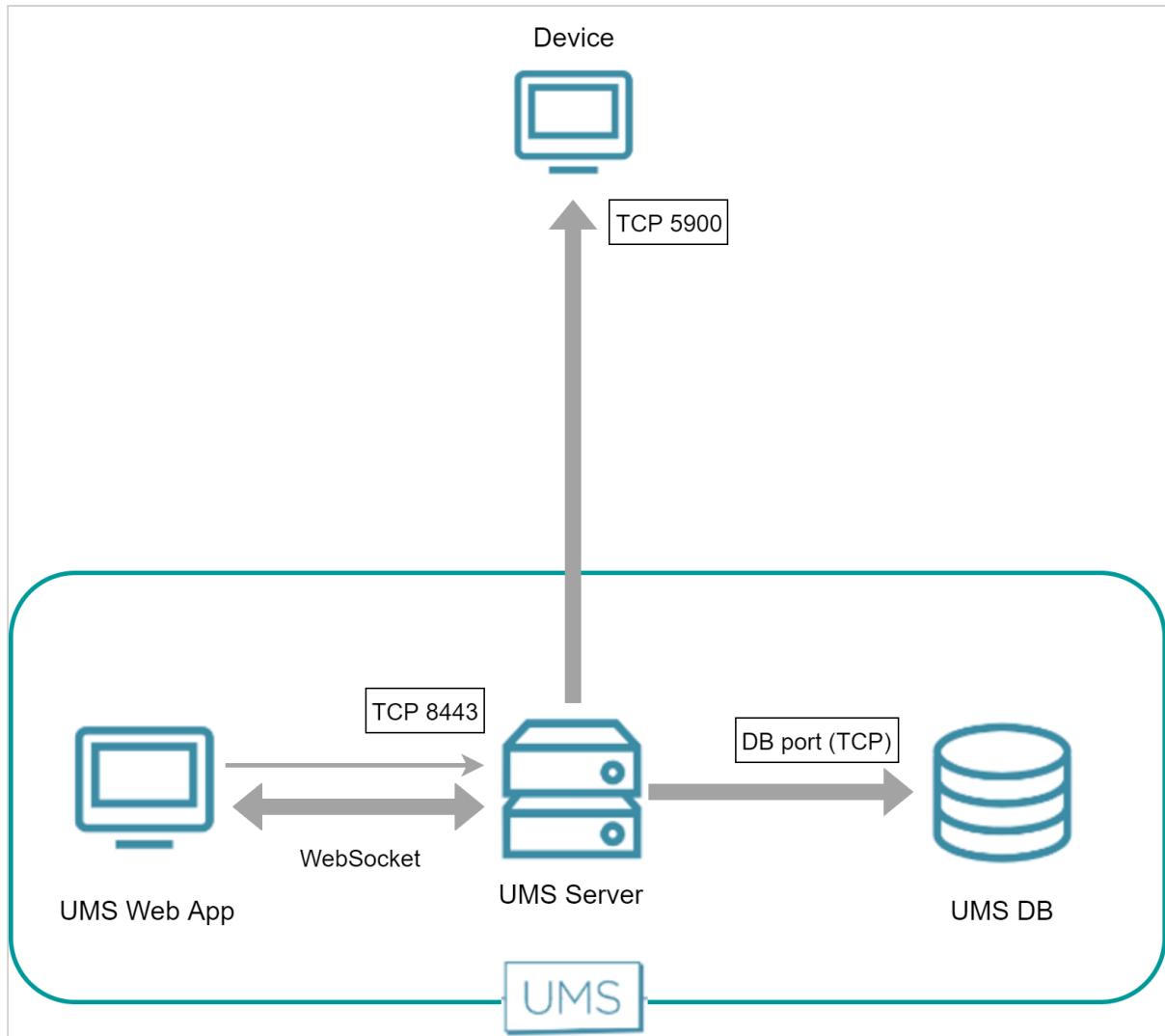
The following figure illustrates the communication between the UMS Console and a device:



UMS Web App

The UMS Web App requests the UMS Server to initiate a VNC session for shadowing. The VNC session is routed through the UMS Server; between the UMS Web App and the UMS Server, the data is transferred via WebSocket. The default port for the communication between the UMS Server and the devices is 5900 (TCP).

The following figure illustrates the communication between the UMS Web App, the UMS Server, and a device:

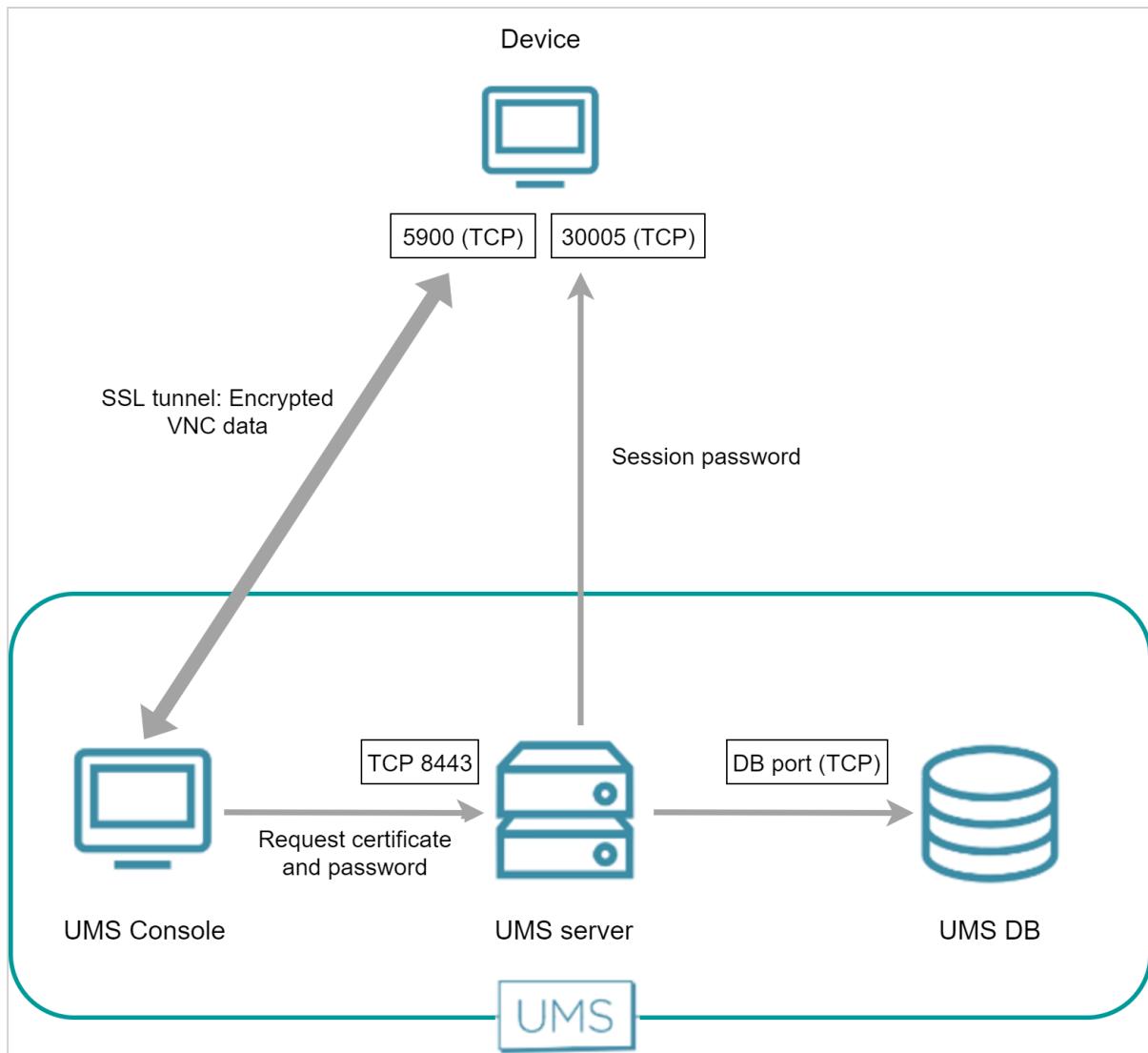


1.3.7 UMS and Devices: Secure Shadowing

The following figures illustrate the communication between the UMS Console, the VNC viewer, the UMS Server and the device.

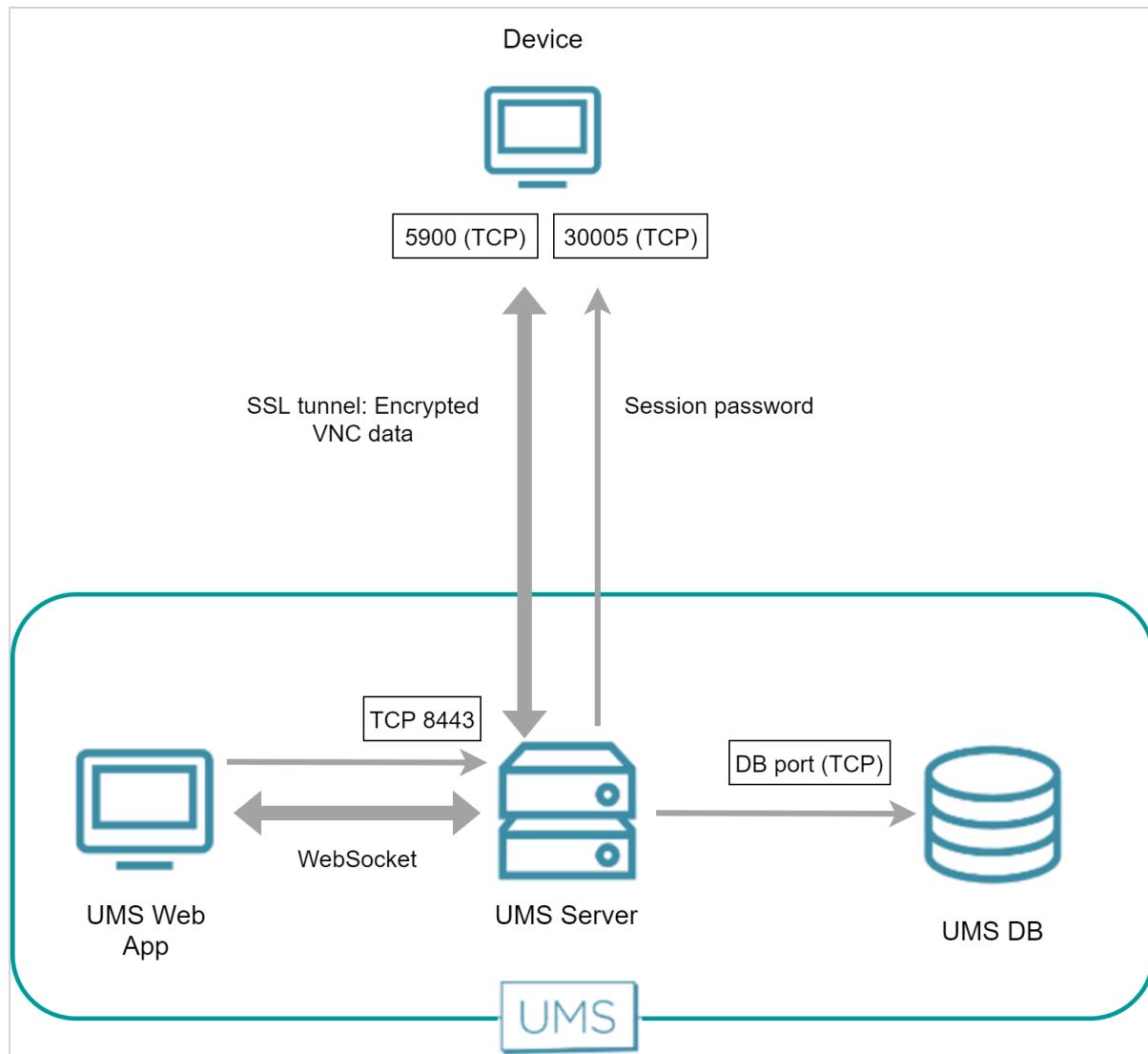
Internal VNC Viewer - Direct Connection

The UMS Console requests the device's certificate and the session password from the UMS Server. The UMS Console then establishes an SSL tunnel with the device using the session password. The device sends the certificate to the UMS Console; the UMS Console checks the certificate against the certificate it has received from the UMS Server. In return, the UMS Console sends the session password to the device. After that, the SSL tunnel between the UMS Console and device is established and can be used for exchanging VNC data.



UMS Web App - Direct Connection

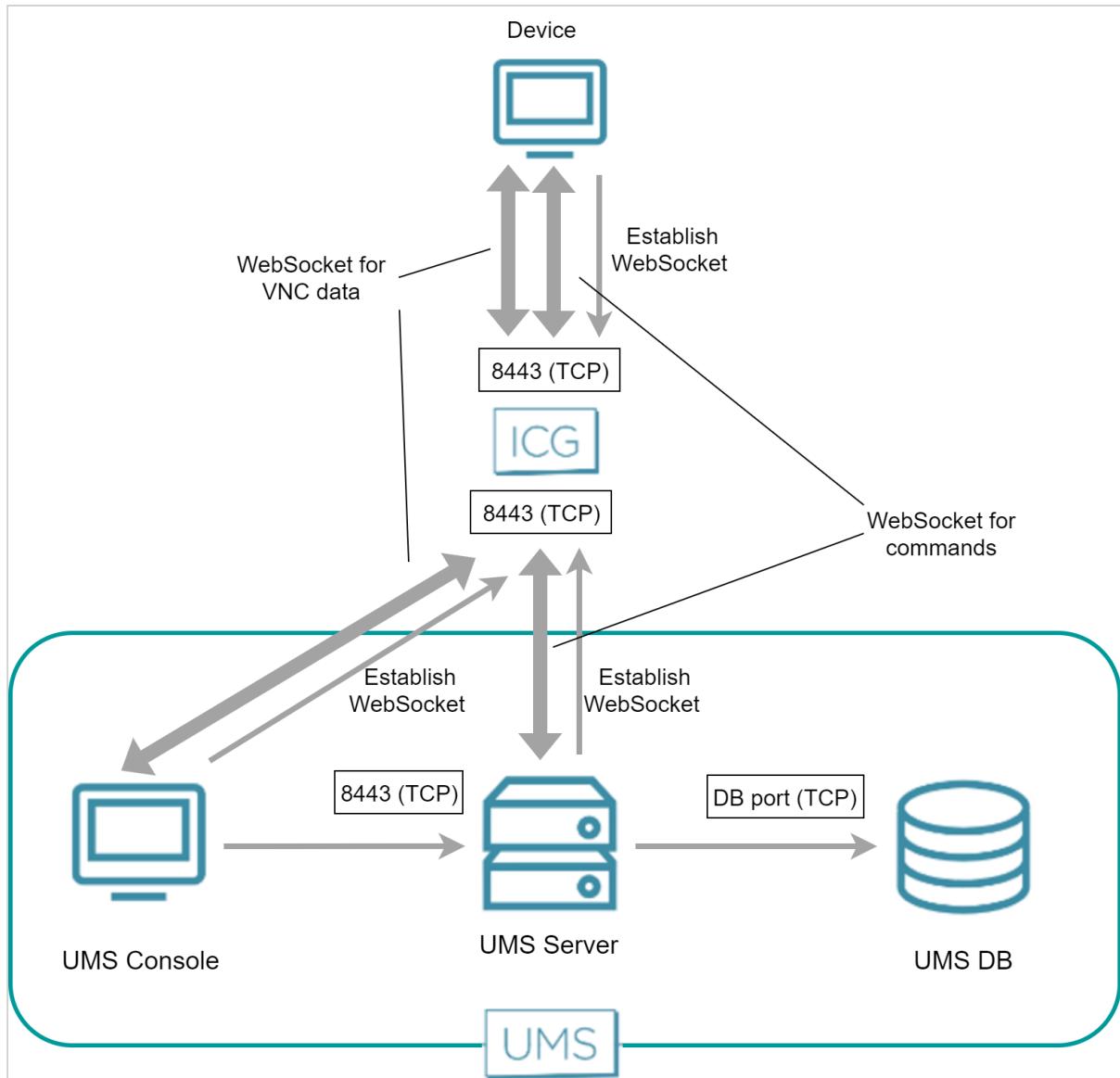
The UMS Web App requests the UMS Server to initiate a VNC session for shadowing. The UMS Server establishes an SSL tunnel with the device using a session password and the device's certificate. The UMS Web App and the UMS Server communicate via WebSocket, which also carries the VNC data.



Internal VNC Viewer - Over ICG

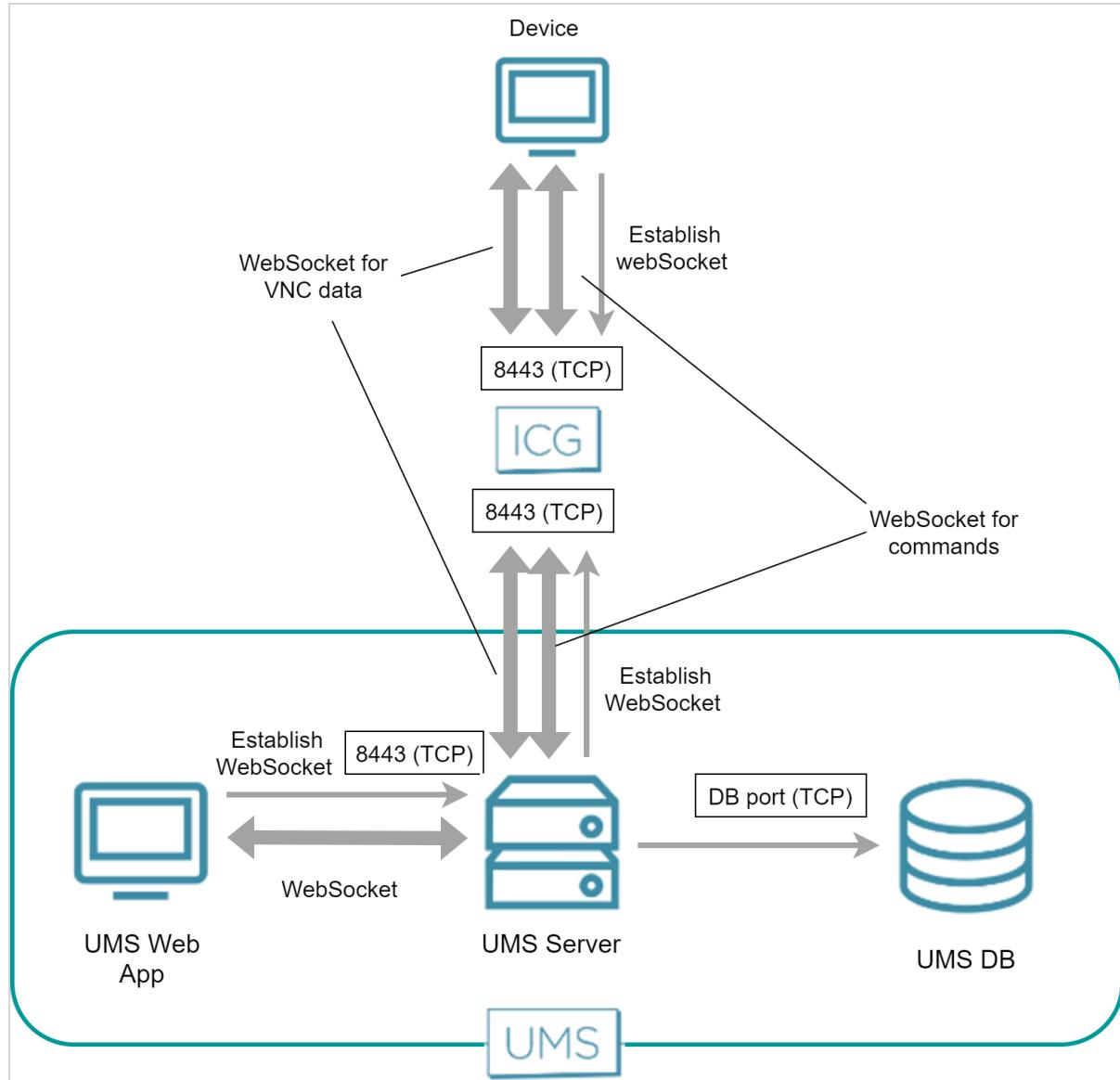
Both the UMS Server and the device have established a WebSocket connection to the ICG; this WebSocket is used for commands from the UMS and messages from the device.

The UMS Console and the device establish a dedicated WebSocket for secure shadowing with the ICG.



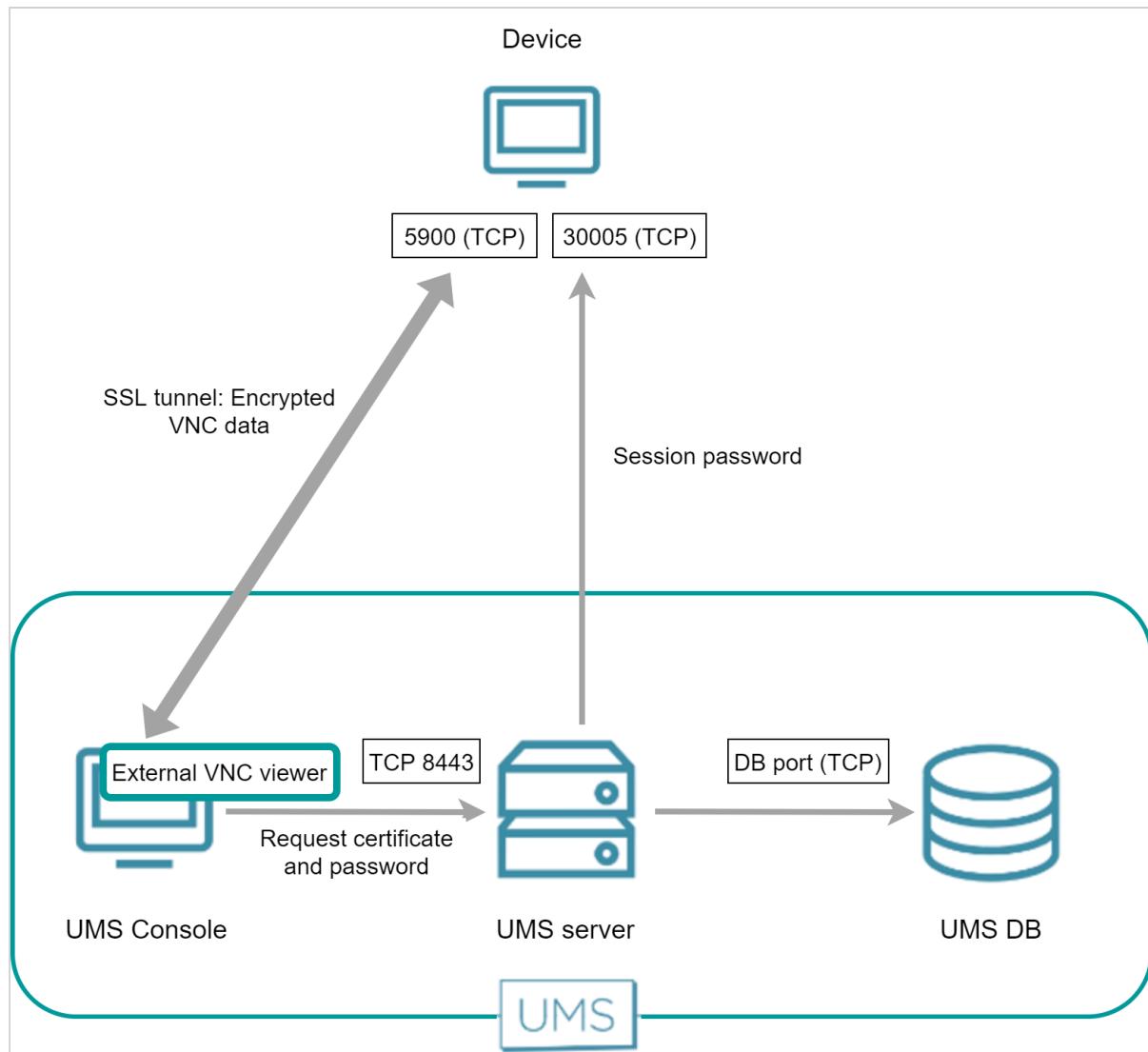
UMS Web App - Over ICG

The UMS Web App requests the UMS Server to initiate a VNC session for shadowing. The UMS Server creates an additional WebSocket connection for exchanging the VNC data. The UMS Web App and the UMS Server communicate via WebSocket, which also carries the VNC data.



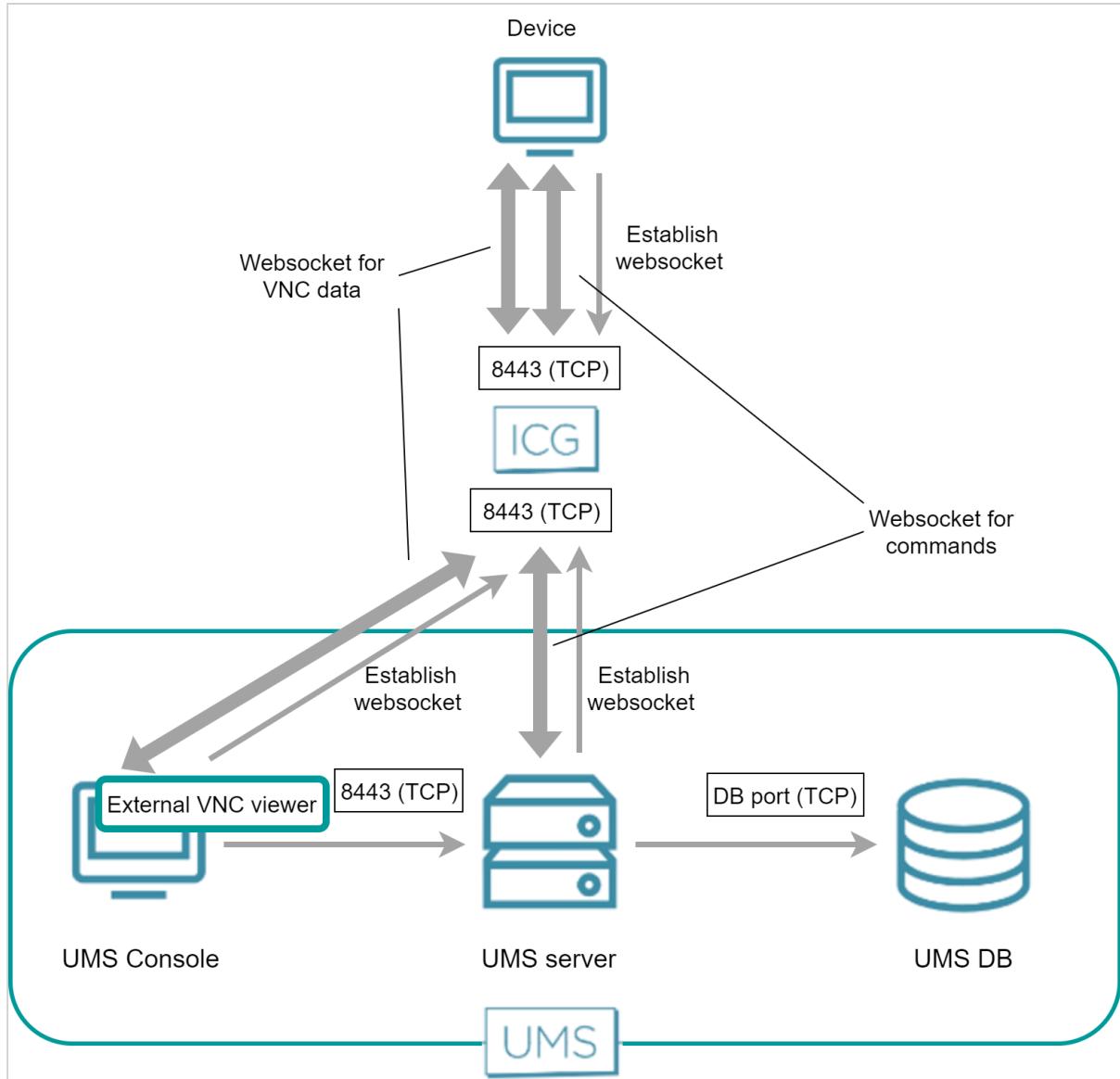
External VNC Viewer - Direct Connection

The external VNC viewer runs on the same machine as the UMS Console. The UMS Console starts the external viewer and then acts as a proxy between the device and the external VNC viewer.



External VNC Viewer - Over ICG

The external VNC viewer runs on the same machine as the UMS Console. The UMS Console starts the external viewer and then acts as a proxy between the ICG and the external VNC viewer.

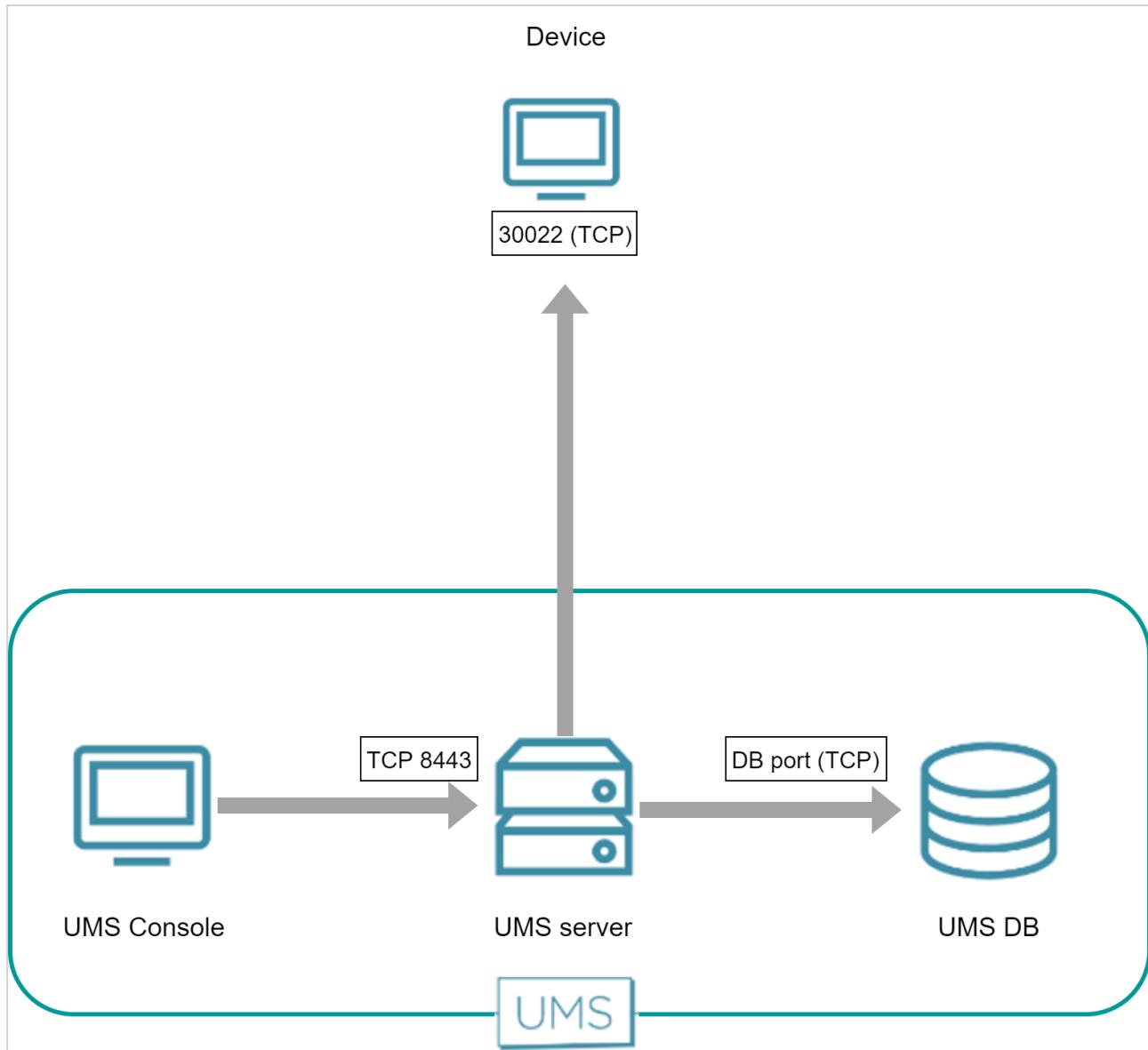


1.3.8 UMS and Devices: Secure Terminal

Direct Connection

The UMS Console establishes a connection to the UMS server. The UMS server then establishes a TLS tunnel to the device.

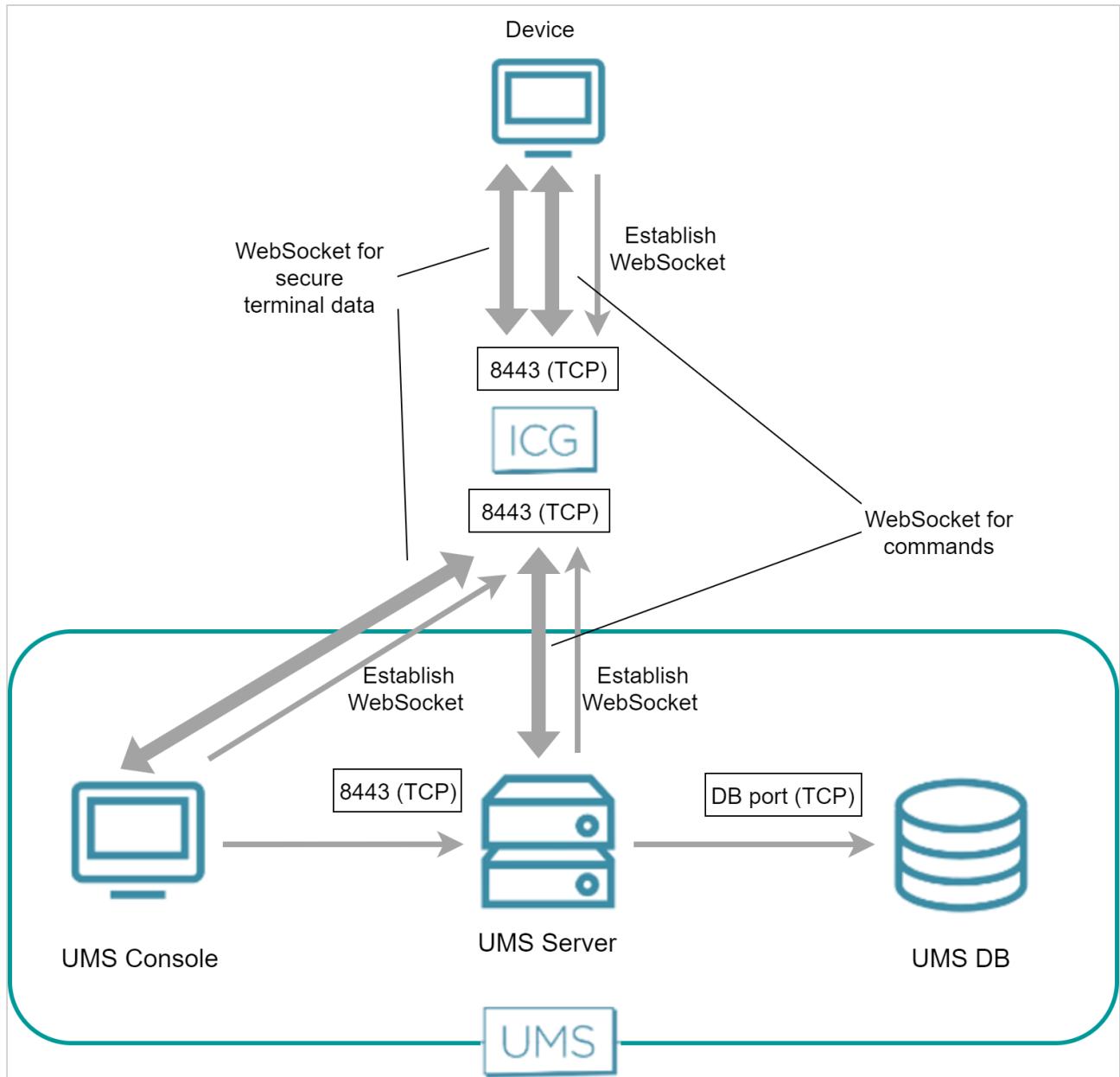
The following figure illustrates the communication between the UMS Console, the UMS server and a device:



Over ICG

Both the UMS Server and the device have established a WebSocket connection to the ICG; this WebSocket is used for commands from the UMS and messages from the device.

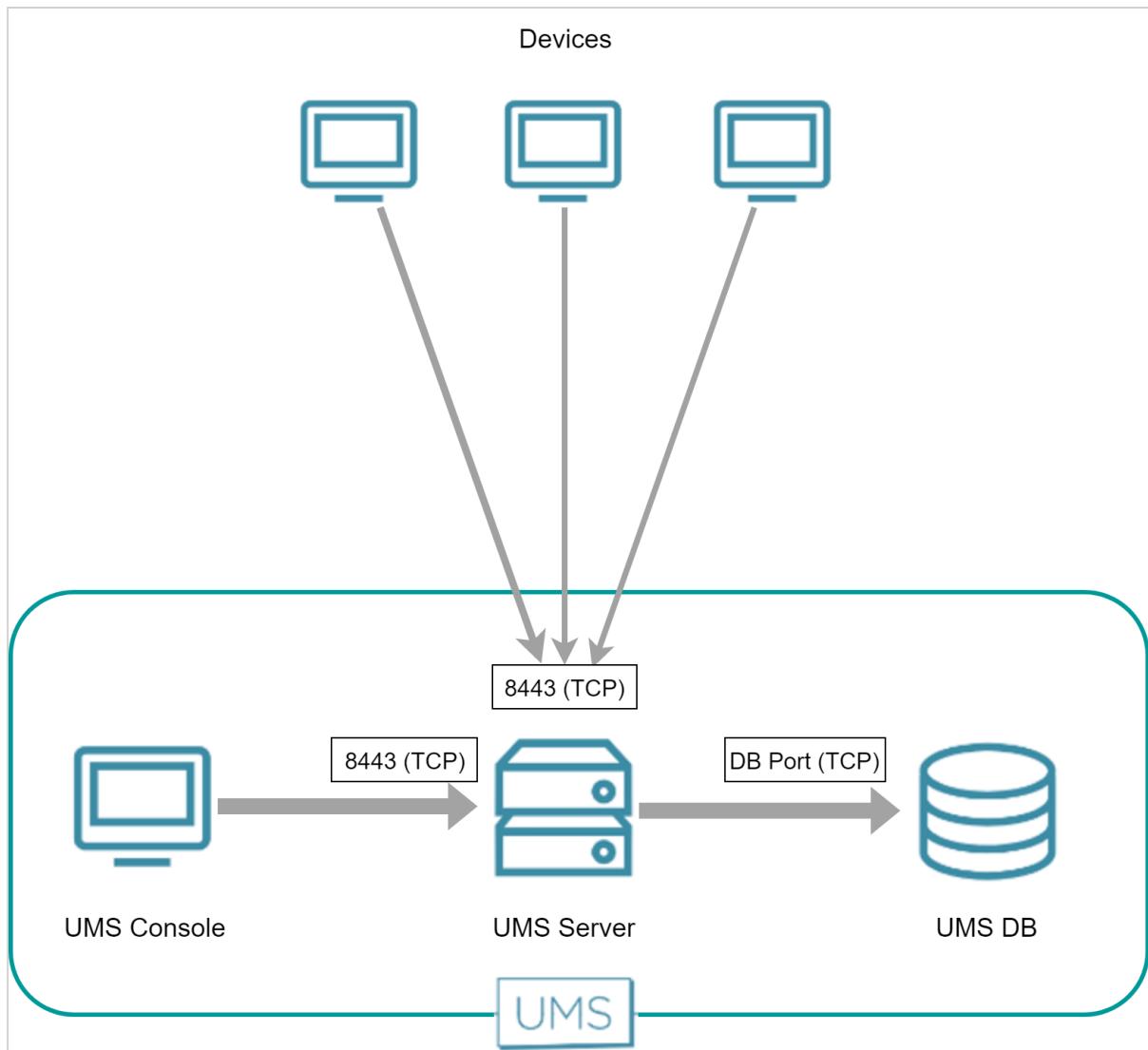
The UMS Console and the device establish a dedicated WebSocket for the secure terminal with the ICG.



1.3.9 UMS and Devices: File Transfer

To fetch files from the UMS, e.g. a background image or log files, the devices send an HTTPS request to the UMS server. The UMS server is listening on port 8443.

The following figure illustrates the communication between the devices and the UMS:



1.3.10 Universal Firmware Update

The Universal Firmware Update feature enables the UMS to check for new firmware updates and download the desired firmware to a WebDAV directory or FTP server. The connection to the IGEL download server can be direct or through a proxy.

For more information about this feature, see [Universal Firmware Update\(see page 493\)](#) in the UMS manual.

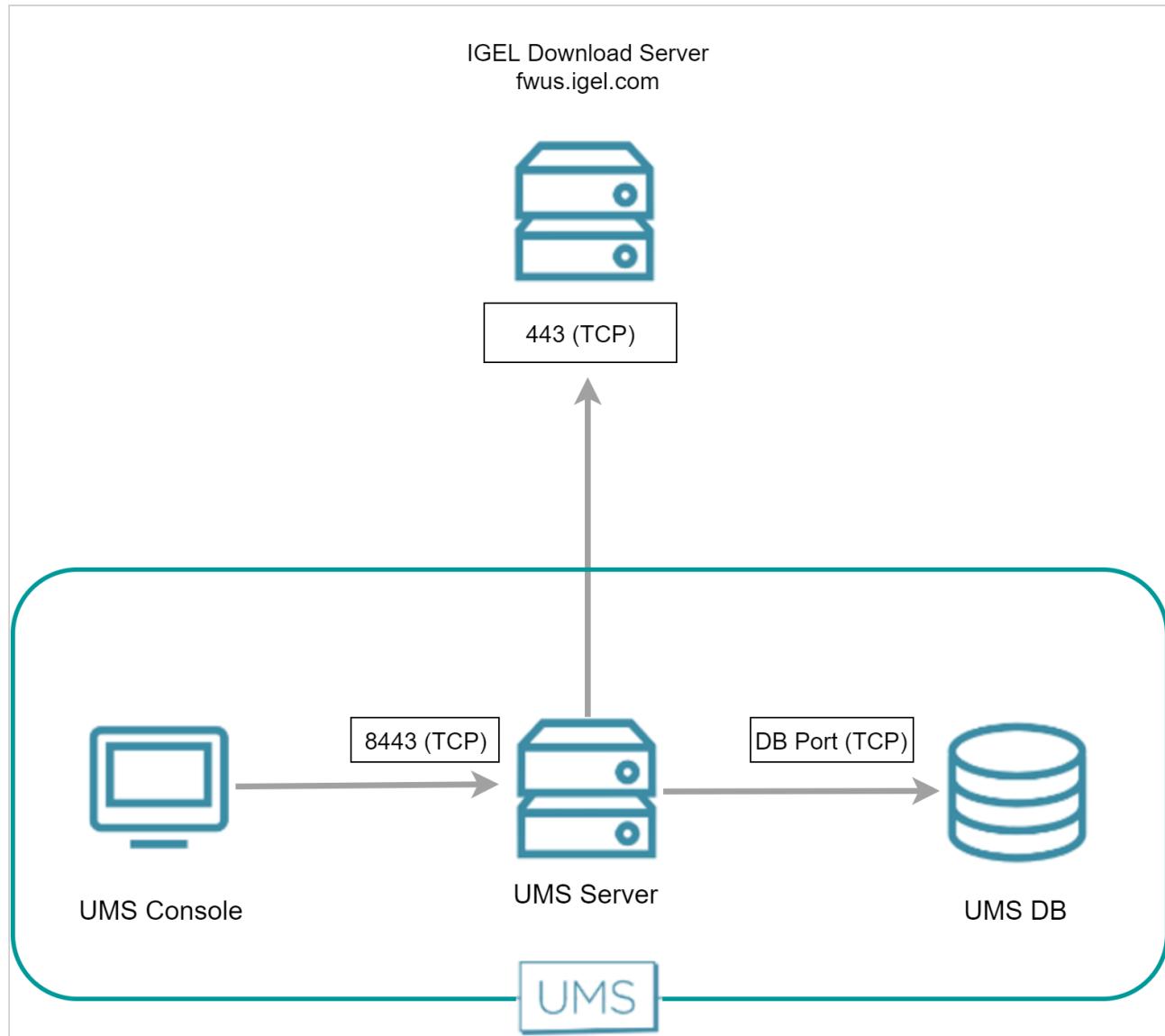
- [UMS Contacting the Download Server to Check for New Updates\(see page 77\)](#)
- [UMS Downloading the Firmware\(see page 79\)](#)

UMS Contacting the Download Server to Check for New Updates

The UMS initiates a TCP connection to port 443 at fwus.igel.com. The IGEL download server will send an answer containing a list of download links that enable the UMS to download the desired firmware.

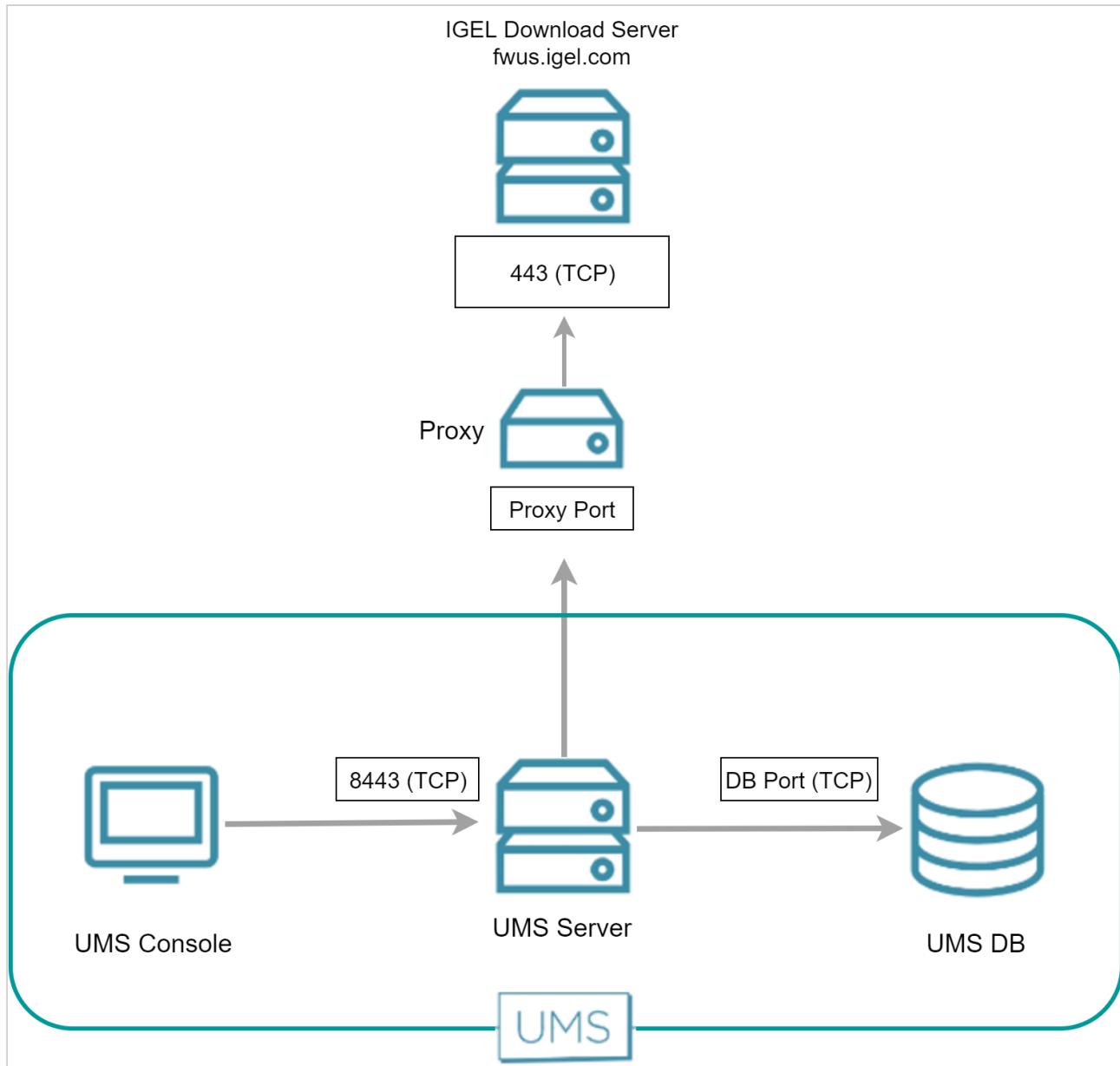
Direct Connection

The following figure illustrates the communication between the UMS server and the IGEL download servers:



Via Proxy

When a proxy is positioned between the UMS and the IGEL download servers, the port on which the proxy is listening must be specified under **UMS Administration > Global Configuration > Proxy Server**.

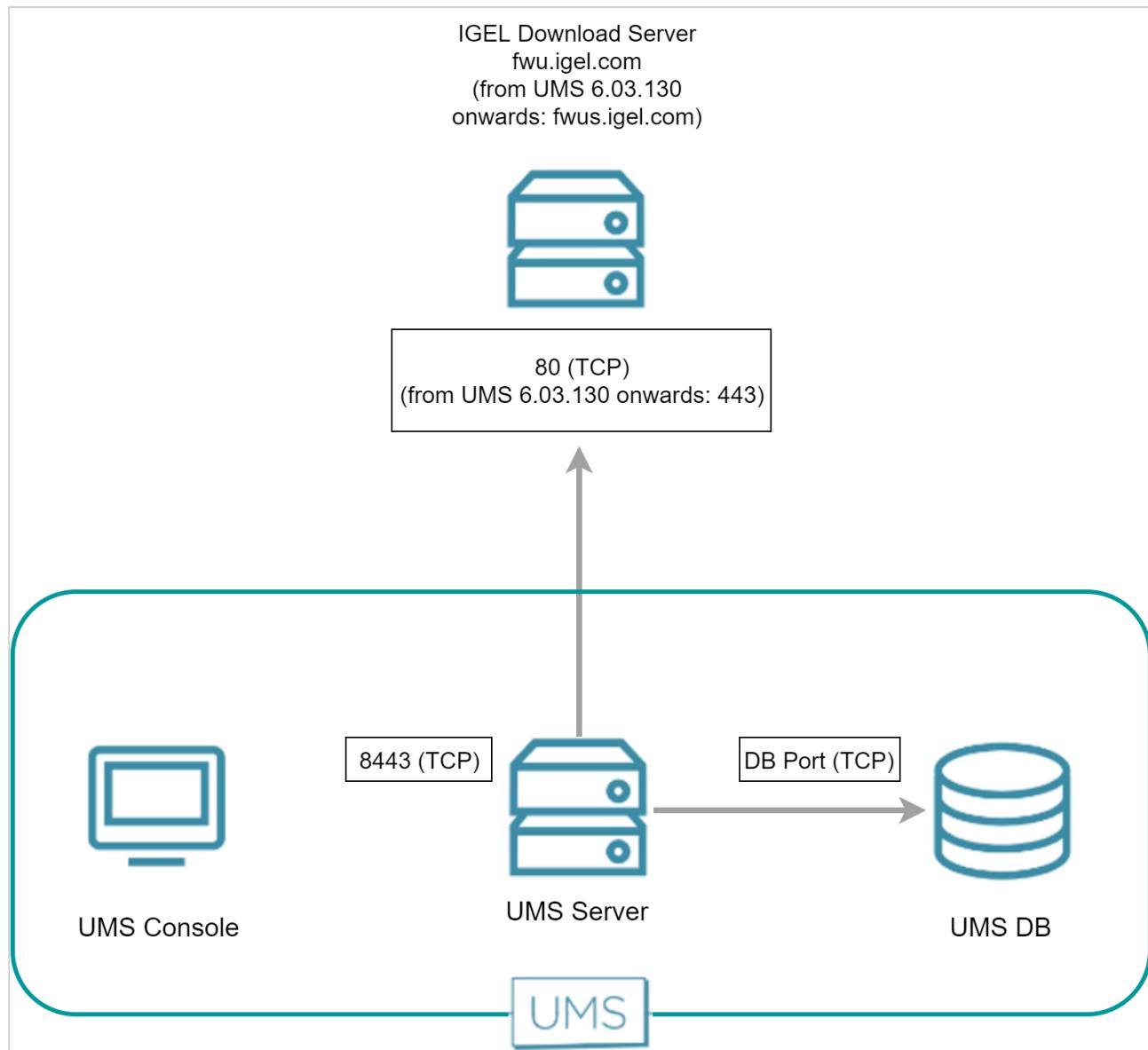


UMS Downloading the Firmware

The UMS downloads the desired firmware using the URLs it received from the download server. The UMS uses port 80 for fwu.igel.com (from UMS 6.03.130 onwards: port 443 at fwus.igel.com).

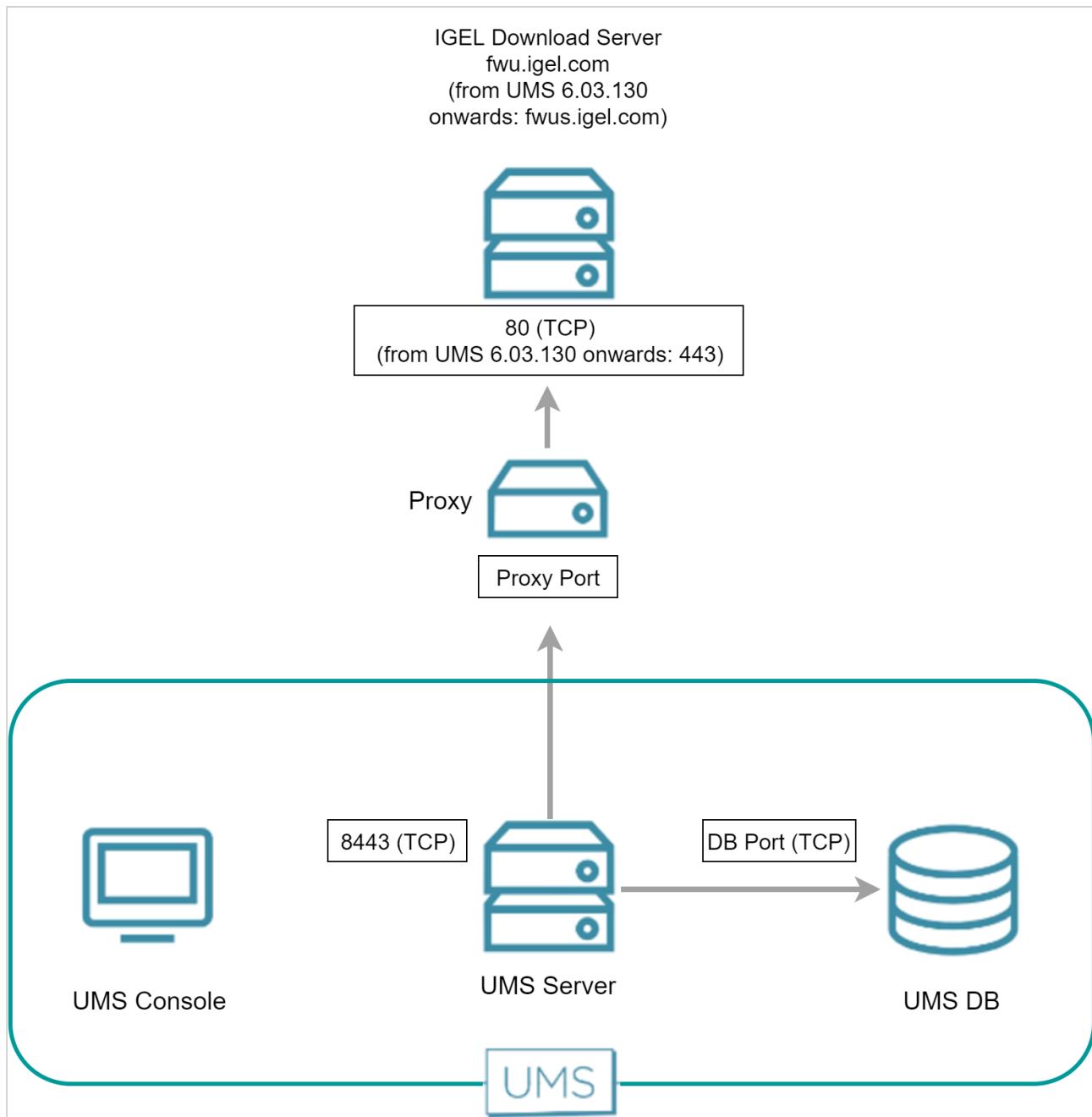
Direct Connection

The following figure illustrates the communication between the UMS Server and the IGEL download servers:



Via Proxy Server

When a proxy server is placed between the UMS Server and the IGEL download server, the port for the proxy server must be specified under **UMS Administration > Global Configuration > Proxy Server**.



1.3.11 Automatic License Deployment (ALD)

The Automatic License Deployment (ALD) feature is a method to deploy licenses to devices.

For more information about this feature, see [Setting up Automatic License Deployment \(ALD\)](#)¹³.

Automatic License deployment can be carried out via a direct connection or via a proxy.

¹³ <https://kb.igel.com/pages/viewpage.action?pageId=10325058>



The steps of the procedure are described in the following sections:

- [UMS Contacting the Licensing Server\(see page 82\)](#)
- [UMS Sending New Settings to the Devices\(see page 84\)](#)
- [Devices Contacting the UMS to Download License Files\(see page 85\)](#)

UMS Contacting the Licensing Server

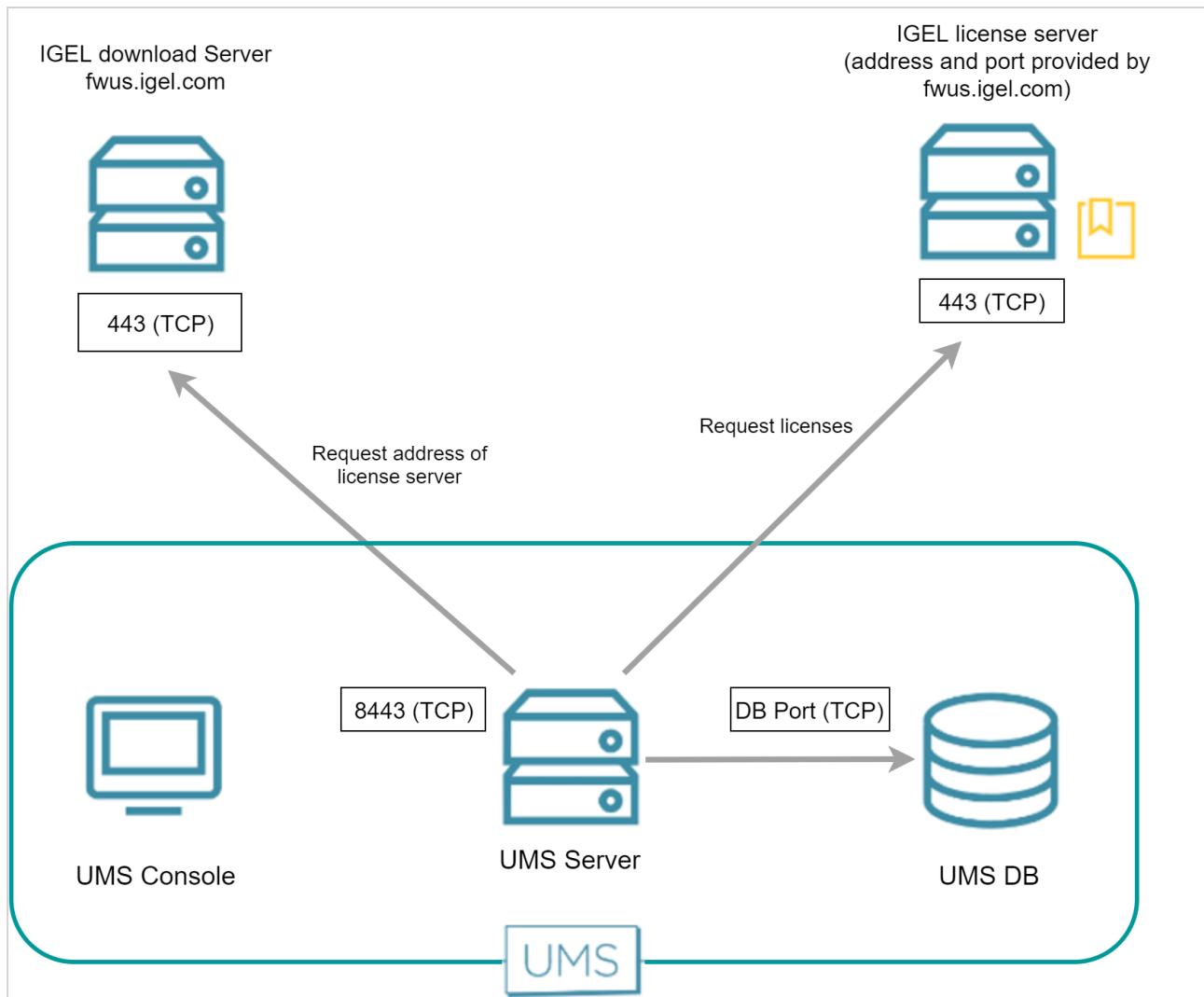
The UMS requests the connection details (URL and port) from the IGEL download server at fwu.igel.com and then contacts the IGEL licensing server. Currently, the connection details are as follows:

- URL: susi.igel.com
- Port: 443

i The connection details may be changed in the future.

Direct Connection

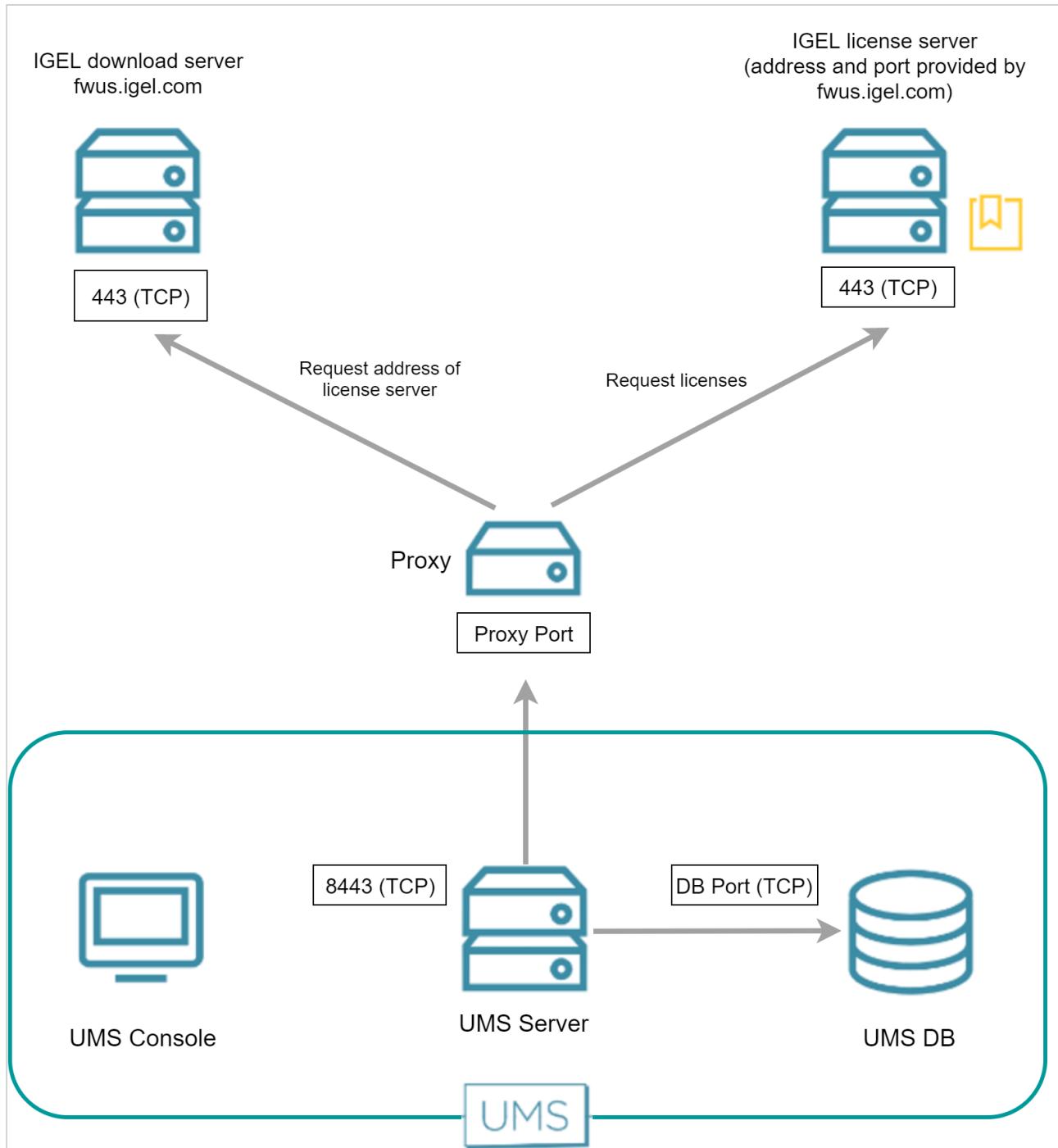
The following figure illustrates the communication between the UMS Server and the IGEL licensing server:



Via Proxy Server

When a proxy server is placed between the UMS and the IGEL licensing server, the port for the proxy server must be specified under **UMS Administration > Global Configuration > Proxy Server**.

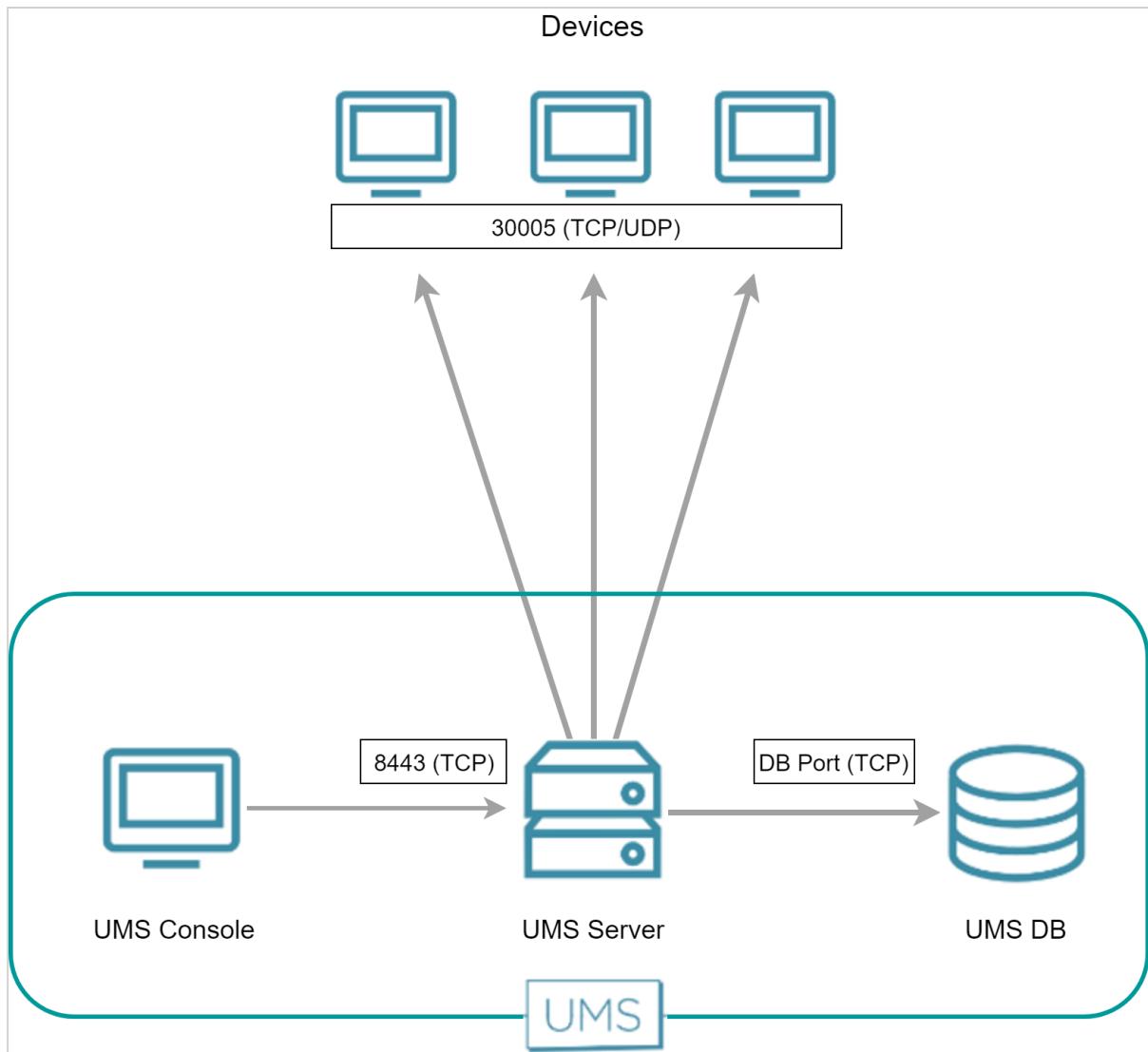
⚠️ If multiple proxies are configured, ensure to select the one that is defined for license deployment



UMS Sending New Settings to the Devices

After obtaining the licenses from the license server, the UMS sends new settings to each device in question, including a download link for the license files. The device is listening on port 30005.

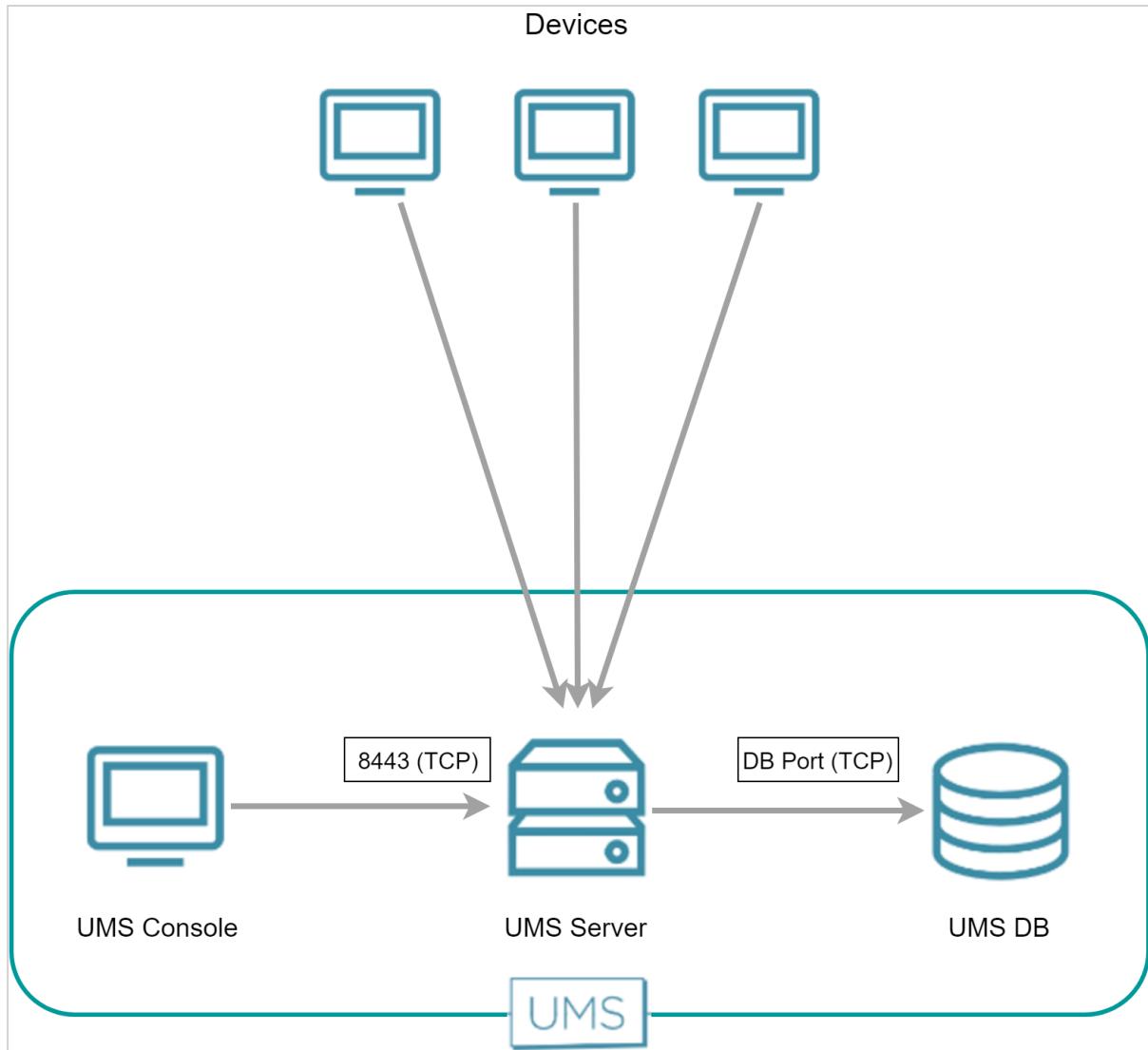
The following figure illustrates the communication between the UMS and the devices:



Devices Contacting the UMS to Download License Files

The devices have been informed by the UMS that license files are ready for download. Now, to fetch the license files from the UMS, the devices send an HTTPS request to the UMS server. The UMS server is listening on port 8443.

The following figure illustrates the communication between the devices and the UMS:



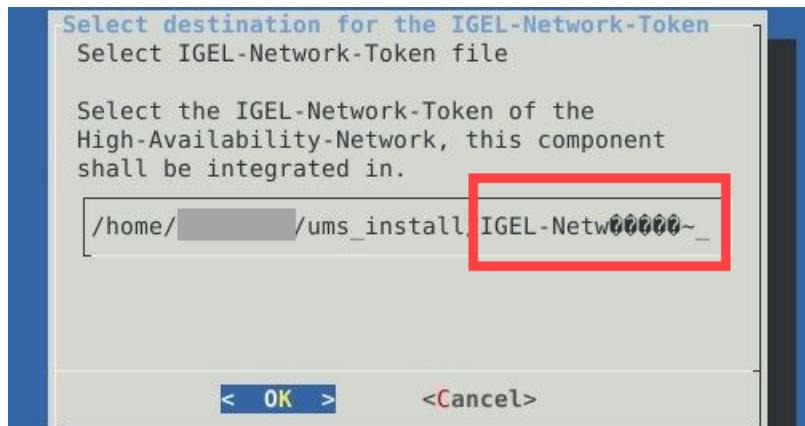
1.4 UMS Installation

- [Using Special Characters during the UMS Installation on Linux](#)(see page 86)
- [UMS Installation on 64-Bit Systems](#)(see page 87)
- [No Permissions after the UMS Update](#)(see page 88)

1.4.1 Using Special Characters during the UMS Installation on Linux

Question

Why do I see strange symbols in the UMS installer on Linux, e.g. when saving / loading the IGEL network token?



Answer

When you want to use language-specific characters, e.g. umlauts (ä,ö, etc.), for the UMS installation on Linux:

- the correct locale for the language must be set
- the system locale must also be correctly set

- ▶ Run the following command to list the available locales: `locale -a`
- ▶ If the necessary locale is not listed, you can generate and set it as the default locale for your system as follows (example for German):

```
sudo locale-gen de_DE.UTF-8
sudo update-locale LANG=de_DE.UTF-8
```

1.4.2 UMS Installation on 64-Bit Systems

i Since version 5.09.100, IGEL UMS is 64-bit based. This article serves now for information purposes only.

Question

What are the prerequisites for the installation of IGEL Universal Management Suite on 64-bit operating systems?

Answer

Since UMS 5.09

From UMS Version 5.09, the installation of 32-bit libraries is no longer required. The necessary dependencies are automatically installed if the corresponding option has been chosen during the UMS installation procedure. For information on UMS installation, see [Installing a UMS Server](#)(see page 260).



Since UMS 5.07.100

From UMS Version 5.07.100, the required 32-bit libraries can automatically be installed by the UMS installer if the corresponding option is chosen during the UMS installation procedure. For information on UMS installation, see [Installing a UMS Server](#)(see page 260).

Before UMS 5.07.100

- Windows: Use the 32-bit compatibility mode (which is activated by default) before installing IGEL UMS (e.g. on Windows Server 2008 R2).
See also [MSDN: "Running 32-bit Applications"](#)¹⁴
- Linux (amd64/x86_64): Install the 32-bit compatibility packages before installing IGEL UMS.
Examples with Ubuntu follow below, apart from that see:
 - [Installing UMS on Red Hat Enterprise Linux \(RHEL\) 7.3](#)(see page 264)
 - [Installing UMS on Oracle Linux Server](#)(see page 265)

Example with Ubuntu 14.04 LTS 64-bit:

```
# add i386 support
sudo dpkg --add-architecture i386
sudo apt-get update
# install libraries
sudo apt-get install lib32z1 \lib32ncurses5 \lib32bz2-1.0 \libxtst6:i386 \
libxinerama1:i386 \libxi6:i386 \libxext6:i386 \libxrender1:i386
```

Example with Ubuntu 16.04 LTS 64-bit:

```
# add i386 support
sudo dpkg --add-architecture i386
sudo apt-get update
# install libraries
sudo apt-get install lib32z1 \lib32ncurses5 \libbz2-1.0:i386 \libxtst6:i386 \
libxinerama1:i386 \libxi6:i386 \libxext6:i386 \libxrender1:i386
```

1.4.3 No Permissions after the UMS Update

Symptom

You have updated the UMS to version 6.05.100 or higher and have no permissions for an object/tree node in the UMS anymore. In the **Access Control** dialog, both checkboxes **Allow** and **Deny** are enabled but not editable:

¹⁴ <https://msdn.microsoft.com/en-us/library/aa384249%28VS.85%29.aspx>



Permission	Allow	Deny	Effective Rights
Browse	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	denied for user test (inherited from /ROOT/Profiles/)
Read	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	denied for user test (inherited from /ROOT/Profiles/)
Write	<input type="checkbox"/>	<input type="checkbox"/>	not set
Access Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign	<input type="checkbox"/>	<input type="checkbox"/>	not set

Environment

- UMS 6.05.100 or higher

Problem

Before UMS 6.05.100, permissions could be granted for a subnode even if they were denied for a node.

Permission	Allow	Deny	Effective Rights
Browse	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	allowed for user test
Read	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	allowed for user test
Write	<input type="checkbox"/>	<input type="checkbox"/>	not set
Access Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign	<input type="checkbox"/>	<input type="checkbox"/>	not set

With UMS version 6.05.100, the evaluation of UMS permissions has changed: If you set **Deny** on a node, you cannot set **Allow** permission on a subnode. The **Allow** checkbox is not editable.

Permission	Allow	Deny	Effective Rights
Browse	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for user test (inherited from /ROOT/Profiles/)
Read	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for user test (inherited from /ROOT/Profiles/)
Write	<input type="checkbox"/>	<input type="checkbox"/>	not set
Access Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign	<input type="checkbox"/>	<input type="checkbox"/>	not set

Solution

- Check the permissions in the **Access Control** dialog. If the **Allow** permissions should be given for a subnode, do not set any permissions for the node.

Permission	Allow	Deny	Effective Rights
Browse	<input type="checkbox"/>	<input type="checkbox"/>	not set
Read	<input type="checkbox"/>	<input type="checkbox"/>	not set
Write	<input type="checkbox"/>	<input type="checkbox"/>	not set
Access Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign	<input type="checkbox"/>	<input type="checkbox"/>	not set

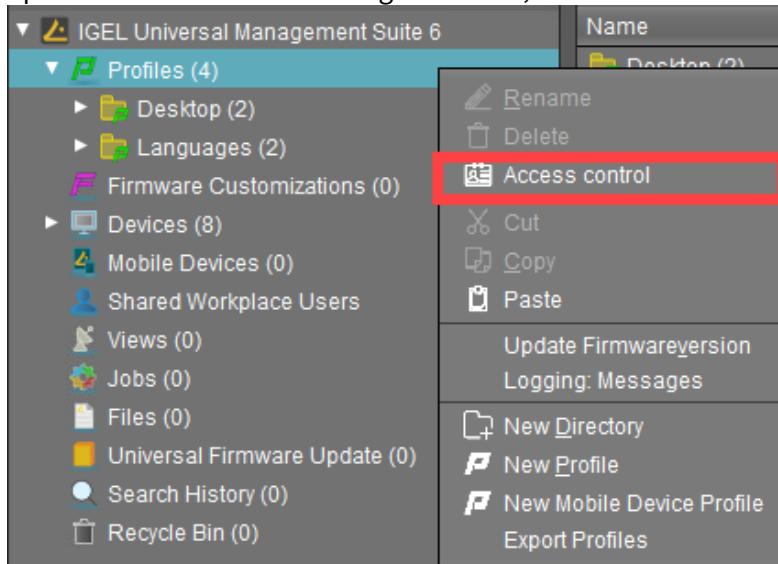


If the permissions are not set, the behavior is like by **Deny**. Therefore, the user will not have access rights on the node but can browse up to the subnode.

Example:

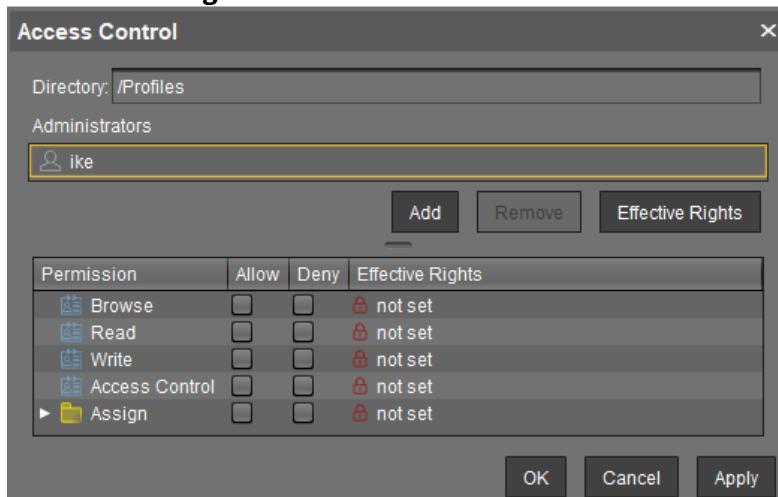
The user should have access rights only to the profile folder "Languages" and its contents:

1. Open the **Access Control** dialog for a node, **Profiles** in this case.



2. Disable checkboxes **Allow** and **Deny**.

The **Effective Rights** read now "not set".



3. Open the **Access Control** dialog for a subnode, for which permissions should be granted. In our case, it is the folder "Languages".



4. Set the required permissions and save the settings.

Permission	Allow	Deny	Effective Rights
Browse	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike
Write	<input type="checkbox"/>	<input type="checkbox"/>	not set
Access Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike

The user can only browse up to the subnode "Languages", for which the access rights have been given.

1.5 Customization

- [User Authorization Rules](#)(see page 91)
- [Managing User Permissions via UMS](#)(see page 93)
- [Automating the Roll-out-Process](#)(see page 94)
- [Using Structure Tags](#)(see page 97)
- [Deploying an IGEL made Custom Partition via UMS](#)(see page 98)

1.5.1 User Authorization Rules

Problem

In the IGEL UMS, you want to assign permissions or roles to administrators according to various responsibilities.

Reason

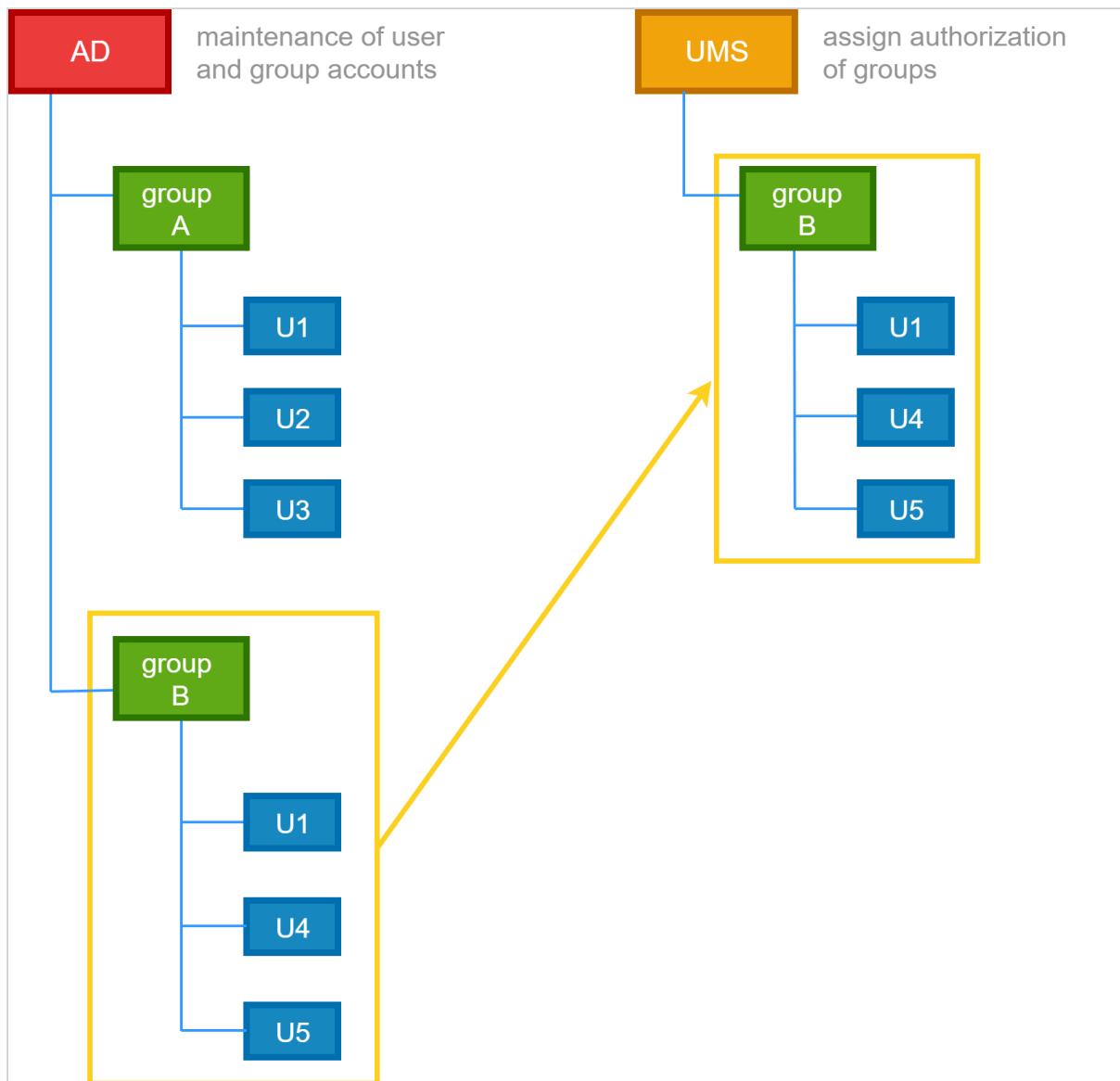
In the IGEL UMS, you can create user or administrator accounts, and you can assign rules to them, but it is not possible to assign roles.

You would like to group administrators according to their tasks in order to achieve a clearly structured management of user rights.

Within your company you already maintain employee accounts using an Active Directory or LDAP.

Solution

As best practice, we suggest connecting the UMS with the user accounts of the Active Directory. You maintain the user and group accounts in the Active Directory only. In the UMS, you assign rights to the imported groups.



Transferring Active Directory groups to the UMS and assigning permissions and roles to them:

- ▶ Click **UMS Administration > Global Configuration > Active Directory / LDAP** to integrate your Active Directory.



- ⓘ You may import Administrative Users / UMS administrators from an Active Directory as well as from an LDAP.

► In the UMS console click **System > Administrator accounts > Import**, to import groups from the tree of your Active Directory.

- ⓘ The successful import of a group cannot be undone. You have to manually delete the wrongly created UMS group in the "Administrator account" management. The name of the imported Active Directory group is taken from the account.

- Assigning roles to groups in the IGEL UMS on the basis of authorization rules:
- Click **System > Administrator accounts > Groups > Edit** to directly assign general group rights.
 - Assign object-related access rights via object permissions, choosing **Access Control** in the context menu of any object.

This way, you can assign certain roles to administrators of the UMS according to their group memberships.

Please note:

- Permissions are inherited from a parent directory to a child directory or to a subordinated object.
- It is possible to change indirect rights, i.e. rights which are given by group assignment. However, directly assigned rights take precedence over indirectly assigned rights.
- An administrator can be a member of different groups and receives the corresponding rights. If they are contradictory, the deprivation of a right takes precedence over the permission. If a prohibition for an action or an object of a group is issued, it will override any number of rights from other groups.
- Click **Effective Rights** to get more details about the rules collection, for example if a permission was given directly or if it was assigned by a group or by an inheritance within a tree structure.

1.5.2 Managing User Permissions via UMS

Purpose

It is necessary to globally manage the permissions of the thin client users, e.g. for editing system information.

Solution

Use the **Access Control** function in the UMS.



Additional Information

There are different places where to open the **Access Control** dialog:

- In the main menu under **Edit > Access Control**
- In the symbol bar under 
- In the context menu of a thin client or a thin client folder under **Access Control**

Defining end user permissions:

1. Click **Access Control** in the context menu of a thin client (folder).
The **Access Control** dialog opens.
2. Click **Add** to select a new user/group.
3. The corresponding **Effective Rights** will be listed in the lower part of the mask.
4. **Allow** or **Deny** the permissions of the selected group or user for the selected thin clients.
5. Confirm the settings with **OK**.
6. Click the **Refresh** button of the console to apply the changes in the UMS.

 If you have changed the rights of registered users they only take effect after a refresh.

For further details about authorization rules see our How-To [IGEL UMS: User Authorization Rules](#)(see page 91).

 Access rights to objects or actions within the *IGEL UMS* are attached to the administrator accounts and groups. The rights of the database user account cannot be restricted. They are created during installation or when setting up the data source. The account always has full access rights in the UMS.

1.5.3 Automating the Roll-out-Process

Problem

You want to install the IGEL UMS in such a way that new devices will be stored directly in the correct directory and will automatically be assigned the right profiles.

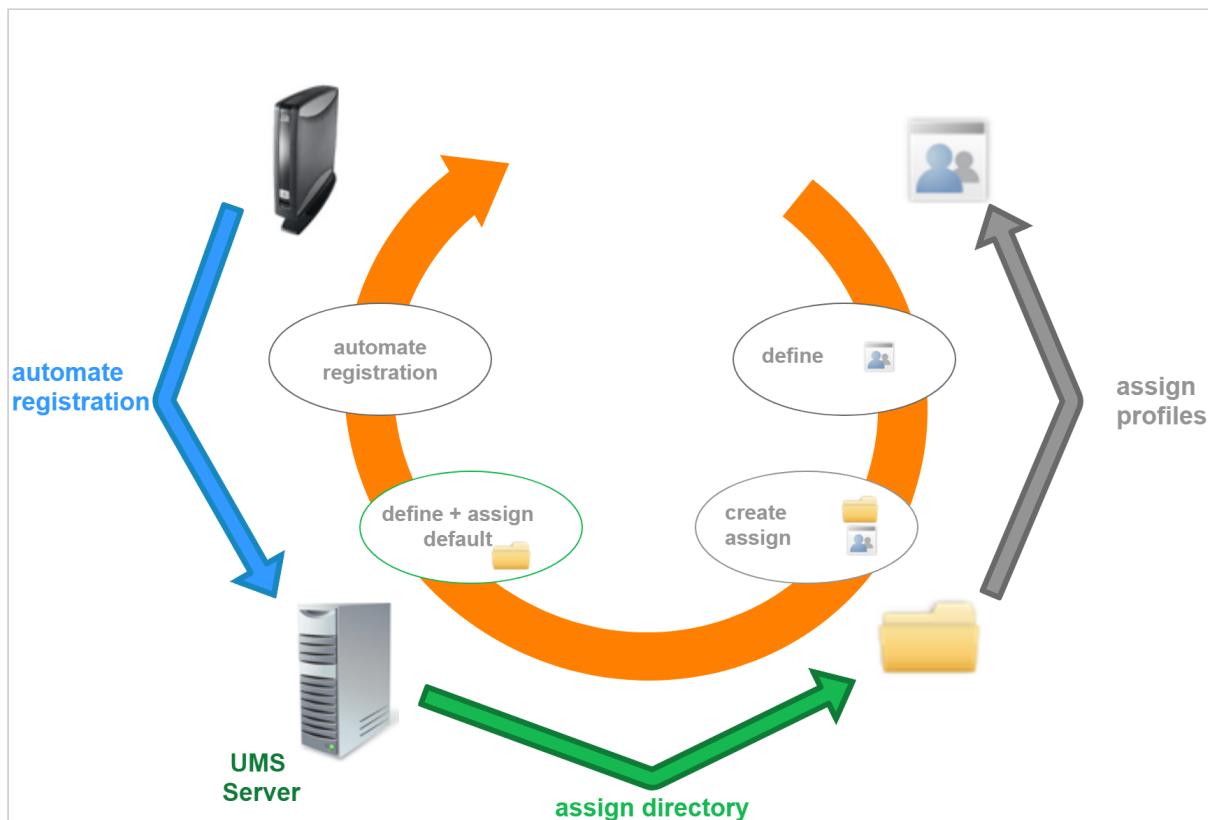
Goal

With Zero Touch Deployment in the roll-out, devices will be configured automatically according to the profiles, with almost zero management outlay.

Solution

The idea of Zero Touch Deployment means automatic registration with automatic assignment of profiles by default directory rules.

In the end the device will be registered automatically in the UMS, will be assigned automatically to the right directory and will be related automatically to the valid profiles. To prepare this automated process you have to go the other way around. First define the profiles, then assign them to the directories, then create a default rule for the directory and automate the registration.



Preparing automatic roll-out:

Configure your device globally, indirectly assigning profiles by a parent directory:

1. Create a new root directory.
2. Assign certain profiles to this root directory.



3. Move your devices or your directories containing devices to this root directory.
These devices will inherit the profiles assigned to the root directory.

Automating the roll-out:

1. Click **UMS Administration > Global Configuration > Default directory rules** to create a new default directory rule.
2. Choose the directory in which you want to store the thin clients according to the rule.
3. Register the new thin clients.
Thanks to the default directory rule these devices will be stored in the right directory and will automatically receive the correct profiles.

The IGEL UMS administrator allows configuration of the UMS server to automatically register all devices without certificate that boot within the server's network:

1. Activate **Enable automatic registration** under **UMS Administration > Global Configuration > Device Network Settings > Automatic Registration**, in order to register new devices.

i If this option is enabled, every thin client without a certificate within the network will be “sucked in” by this UMS Server installation. So if a client is reset to factory defaults and reboots, it will be registered to the server immediately! We recommend **Automatic Registration** only for the time you need to register new clients within the network and to disable it again after registration is finished.

2. To register IGEL devices automatically they have to get information on where to find the management server. There are two possibilities:

- **DNS entry igelrmserver** (The *Type must be: Record Type A*)

or

- **DHCP option (224)**

i DHCP option 224 has to be set as a string (not DWORD) to IP address of the UMS server.

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=FboMrzkx6uo>



1.5.4 Using Structure Tags

Problem

When rolling out devices automatically it can be difficult to assign each to the desired folder in the Universal Management Suite (UMS).

Goal

Newly registered thin clients will automatically have the information where they are to be placed in the structure tree of the UMS.

The UMS will have flexible rules to place a newly registered device into a folder of the structure tree.

Solution

One solution is using a structure tag, a text string bound to the device, that is transmitted to UMS. It can be assigned to devices either via a DHCP option or in their local setup.

1. Define a Structure Tag in your Default Directory Rules under **UMS Administration > Global Configuration > Default Directory Rules**.

Learn more in the UMS manual: [Default Directory Rules](#)(see page 485).

2. Assign a structure tag to a device manually or via DHCP:

Assigning a Structure Tag manually on the endpoint

- a. In **Setup**, go to **System > Remote Management**.
- b. Enter the structure tag value under **Structure tag**.
- c. Click **OK**.

Assigning a Structure Tag via DHCP Server

Use the appropriate DHCP option, depending on the IGEL OS version of your endpoint devices:

- IGEL OS 11.03.500 or lower: Use DHCP option 226 to distribute the tag value to the devices. Set the DHCP option 226 as a string - not as a DWORD.
- IGEL OS 11.04.100 or higher: As an alternative, you can use the DHCP option 43 (encapsulated vendor-specific options) to send the DHCP option 226 (name: "umsstructuretag") to the right endpoint devices. An endpoint device with IGEL OS 11.04.100 or higher sends option 60 (vendor class identifier) with `igel-dhcp-1` as the value.

i An IGEL specific DHCP option that is sent in DHCP option 43 overrides a corresponding DHCP option that is sent in the global namespace. The DHCP options 1, 224, and 226 can be embedded in option 43.
You can prevent a DHCP option 226 that has been sent in the global namespace from being interpreted. To achieve this, you must add option 1 (name "exclusive", type Byte, value 1) to DHCP option 43.



1.5.5 Deploying an IGEL made Custom Partition via UMS

Goal

You want to deploy a custom partition that you received from IGEL to a number of thin clients via the Universal Management Suite (UMS).

Solution

⚠ The procedure described here is only intended for installing custom partition packages that have been built by IGEL.

1. Save the *.zip archive you received locally and extract it.
2. Copy the contents of the directory target into the ums_filetransfer directory on the UMS Server, e.g. C:\Program Files (x86)\IGEL\RemoteManager\rmguiserver\webapps\ums_filetransfer
3. Check the accessibility of the data by opening its address in a web browser, e.g. http://[ums_server]:9080/ums_filetransfer/[name]/[name].inf
This access is password-protected, and you need to enter your UMS credentials.
4. Import the file profiles.zip (located in the igel\profiles directory of the package) into the UMS via **System > Import > Import Profiles**.
The imported profile should now appear in the UMS Console under **Profiles**.
5. Edit the profile and adapt the settings in **System > Firmware Customization > Custom Partition > Download** to match the **URL**, **Username** and **Password** for your UMS.

 A screenshot of a Windows-style dialog box titled "Add". The dialog has fields for "Automatic Update" (checked), "URL" (http://172.30.91.227:9080/ums_filetr), "User name" (USER), "Password" (*****), "Initializing Action" (/bin/sh /custom/init-putty.sh), and "Finalizing Action" (empty). At the bottom are "Ok" and "Cancel" buttons.

6. Assign the profile to one or more devices.
7. Reboot these devices.



1.6 UMS Environment

- Migrating a UMS Server(see page 99)
- Migrating a UMS Database From Embedded DB to Microsoft SQL Server(see page 112)
- Restore and Recover Corrupted UMS Embedded DB(see page 118)
- Disaster Recovery: UMS with an External Database(see page 119)
- ICG Reinstallation after the Migration of the UMS Server(see page 121)
- UMS Does Not Connect to ICG: "TrustAnchor ...is not a CA certificate"(see page 121)
- Using Your Own Certificates for Communication over the Web Port (Default: 8443)(see page 123)
- Wake on LAN(see page 144)
- Using an HTTP Proxy for Firmware Updates in UMS(see page 152)
- UMS Cannot Contact Download Server Any More(see page 154)
- Error During Firmware Upload in UMS: No Space on WebDAV(see page 154)
- How to Check the Current State of the IGEL UMS Server through Your Existing Monitoring Solution(see page 156)

1.6.1 Migrating a UMS Server

Purpose

You want to migrate your IGEL Universal Management Suite to a new server.

Scenarios

The following scenarios can occur when migrating the UMS to a new server:

- Migrating the UMS with the embedded data source: [With the Same Embedded Database\(see page 100\)](#).
- Migrating the UMS with the external data source: [With the Same External Database\(see page 103\)](#).
- Migrating the UMS and changing the data source: [With a Different Database\(see page 106\)](#).

The switch from a standard UMS installation to a [High Availability\(see page 657\)](#) installation, which involves the migration of the existing UMS Server to a new host and, if the embedded database is in use, the move to the external database, is described separately under [Switching from a Standard UMS Installation to an HA Installation\(see page 680\)](#).

⚠ Recommendation: The Same Software and Database State

It is NOT recommended to combine the migration and update procedures, e.g. to move from UMS 6.01 to 6.08. It is advised to update the UMS Server and migrate it afterward, or vice versa.

✓ Tip

The move provides an opportunity to remove any UMS database data which are no longer used. For example, you can

- delete endpoint devices that no longer exist
- delete profiles that are no longer used
- remove files and firmware updates that are no longer needed

It is highly recommended to create a backup before carrying out the cleanup (as a backup of the system running) and another one after the cleanup.

With the Same Embedded Database

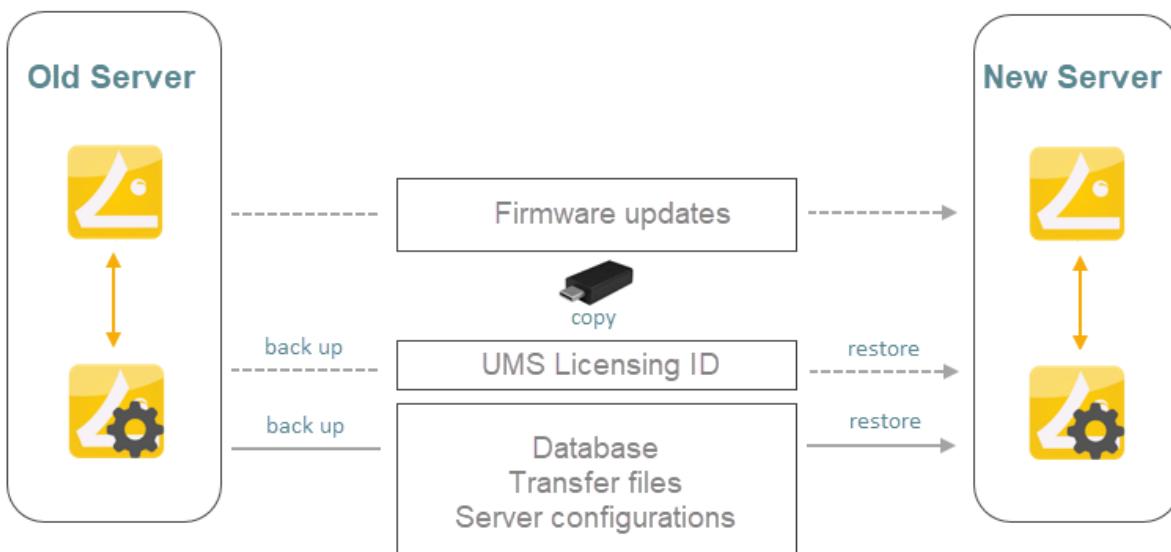
Use Case

You have a UMS installation with an embedded database and want to migrate to a new UMS Server with the same embedded database.

General Overview

The migration procedure generally involves the following steps:

1. Backing up the old server. Checklist for the backups:
 - Database**
 - Transfer files**
 - Server configurations** (host-specific server configurations that differ from the defaults are noted down separately)
 - Firmware updates**
 - UMS Licensing ID**
2. Stopping the IGEL RMGUIServer service on the old server
3. Transferring the created backups to the new server
4. Adjusting DHCP tag and DNS alias on the new server OR creating a profile with the IP of the new server for remote administration





Instructions

On the Old Server

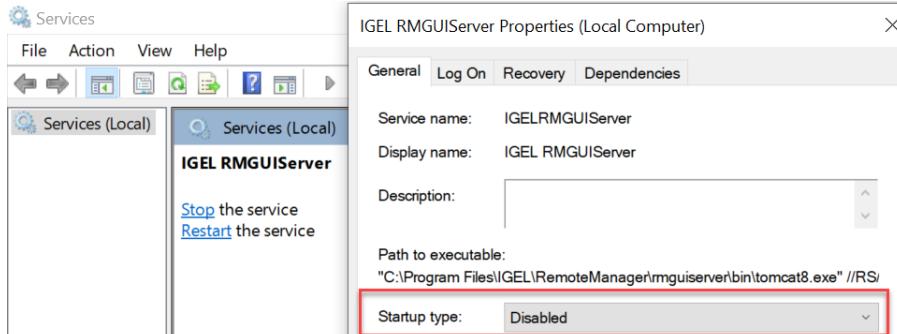
1. On the old server, create a backup under **UMS Administrator > Backups** and copy it to a storage medium. Include all options in the backup. For detailed instructions, see the "Embedded Database" section under [Creating a Backup](#)(see page 536).

i The backup of **Server configurations** includes most configurations of the [Settings for IGEL UMS Administrator](#)(see page 530) area in the UMS Administrator application. Exceptions: **Web server port**, **JWS server port**, and **ciphers** – they are host-specific, i.e. stored separately on each server and cannot be part of any backup. Therefore, you should note the values of these settings if they differ from the defaults and, in the case of recovery/migration procedure, they must be changed on each server manually.

2. Create a backup of the UMS Licensing ID in the **UMS Administrator > UMS Licensing ID Backup**. For detailed instructions, see [Transferring or Registering the UMS Licensing ID](#)(see page 106).
3. Copy all files from the following folder:

Files and firmware updates	<ul style="list-style-type: none"> • [IGEL installation directory]/rmguiserver/webapps/ ums_filetransfer
---	---

4. Stop the service **IGEL RMGUIServer** (for instructions, see [HA Services and Processes](#)(see page 691)) and set the startup type for it to "Disabled" in order to prevent accidental parallel operation with the new UMS Server.

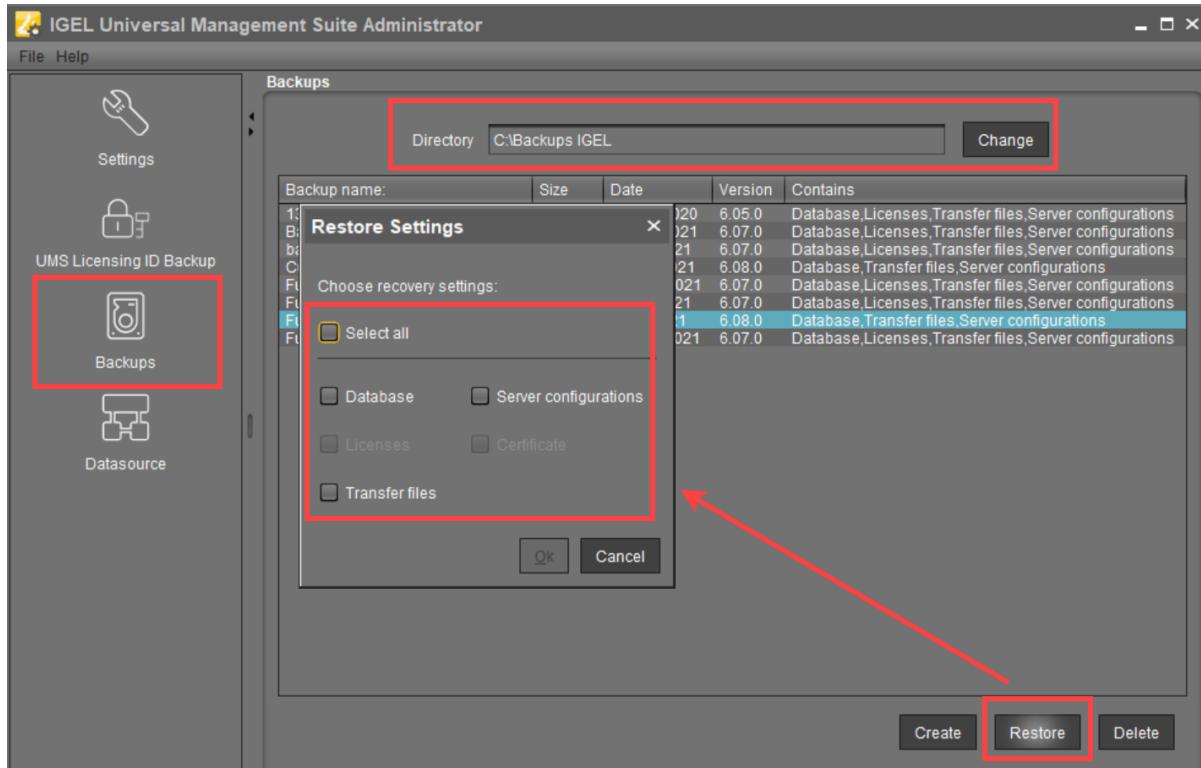


On the New Server

1. Install the UMS on the new server. If possible, use the same database user and password. For the installation instructions, see [Installing a UMS Server](#)(see page 260).
2. Under **UMS Administrator > Backups**, select the folder with your backup and restore the respective backup file with all options. Wait until the UMS Server fully starts, i.e. the UMS Console



can connect with it.



3. If necessary, transfer host-specific server configurations to the new server.
4. Transfer the UMS Licensing ID of the previous UMS installation to the new server: **UMS Administrator > UMS Licensing ID Backup > Restore**. Alternatively, you can register the new UMS Licensing ID, which was created during the installation of the new server. For detailed instructions, see [Transferring or Registering the UMS Licensing ID](#)(see page 106).
5. Copy files from [IGEL installation directory]/rmguiserver/webapps/ums_filetransfer to the new server – without the WEB-INF folder.
6. Restart the service IGEL RMGUIServer.
7. If ICG is used: All ICGs have to be reinstalled, see [ICG Reinstallation after the Migration of the UMS Server](#)(see page 121).
8. Adapt, if necessary, the DHCP tag and the DNS alias igelrmserver with the IP or FQDN of the new UMS Server. See [Registering Devices Automatically](#)(see page 312).

i The configuration of the DHCP tag and the DNS alias is not a setting that can be made within the IGEL software. You must configure these within your individual network environment on the corresponding DHCP and DNS servers.

i If you have used and adjusted the DNS alias and the DHCP option, the following step is NOT required since the device can resolve the name igelrmserver correctly.



In the local configuration, the device always remembers the IP of the UMS Server of its first registration. It is thus possible that the old IP address is displayed under **System > Remote Management**. Therefore, it makes sense to manually set an entry for remote administration after the migration:

- a. Create a profile in the UMS:
 - Go to **System > Remote Management** and click **Add**.
 - Under **UMS Server**, enter the IP of the new UMS Server.
- b. Apply this profile globally, to the entire structure.

- ✓ After the procedure is complete, open the UMS Console and go to **UMS Administration > UMS Network > Server** to check if there is an entry for the previous UMS Server among the listed components. If so, select the entry and click **Delete** in the context menu.

With the Same External Database

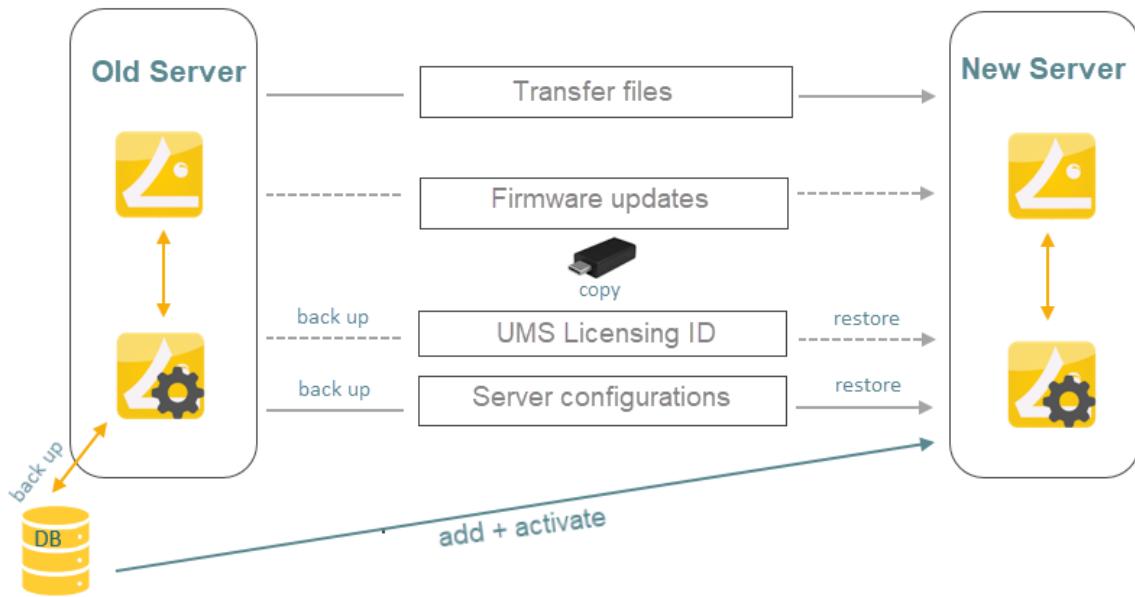
Use Case

You have a UMS installation with the external database and want to migrate to a new UMS Server with the same external database.

General Overview

The migration procedure generally involves the following steps:

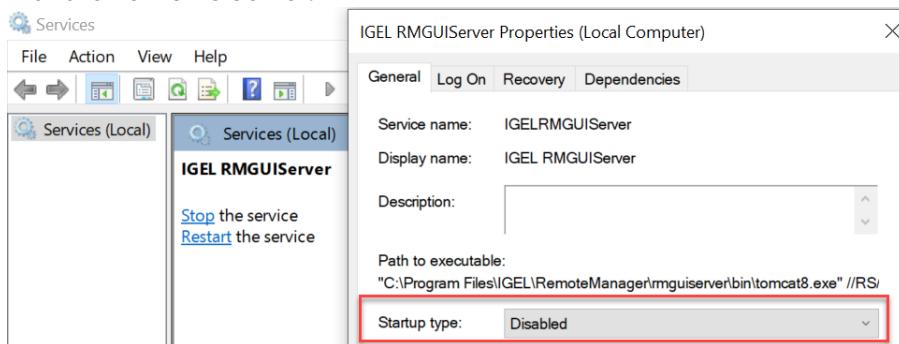
1. Backing up the old server. Checklist for the backups:
 - ✓ **Database**
 - ✓ **Transfer files**
 - ✓ **Firmware updates**
 - ✓ **Server configurations** (host-specific server configurations(see page 537) that differ from the defaults are noted down separately)
 - ✓ **UMS Licensing ID** (see [Transferring or Registering the UMS Licensing ID\(see page 106\)](#))
2. Stopping the IGEL RMGUIServer service on the old server
3. Adding the existing external database as the data source for the new server
4. Activating the data source
5. Transferring the backed-up data to the new server
6. Adjusting DHCP tag and DNS alias on the new server OR creating a profile with the IP of the new server for remote administration



Detailed Instructions

On the Old Server

1. Before the migration, make the backups as described in the "External Database" section under [Creating a Backup](#)(see page 536).
2. Stop the service **IGEL RMGUIServer** (for instructions, see [HA Services and Processes](#)(see page 691)) and set the startup type for it to "Disabled" in order to prevent accidental parallel operation with the new UMS Server.



On the New Server

1. Install the UMS on the new server. For the installation instructions, see [Installing a UMS Server](#)(see page 260).



2. Go to **UMS Administrator > Datasource > Add** and enter the connection properties of the existing database.

3. **Activate** the data source. Wait until the UMS Server fully starts, i.e. the UMS Console can connect with it.
4. In the **UMS Administrator > Backups**, restore the backup of server configurations. If necessary, transfer [host-specific server configurations](#)(see page 537) to the new server.
5. Transfer the UMS Licensing ID of the previous UMS installation to the new server: **UMS Administrator > UMS Licensing ID Backup > Restore**. Alternatively, you can register the new UMS Licensing ID, which was created during the installation of the new server. For detailed instructions, see [Transferring or Registering the UMS Licensing ID](#)(see page 106).
6. Copy files from [IGEL installation directory]/rmguiserver/webapps/ums_filetransfer to the new server – without the WEB-INF folder.
7. Restart the service IGEL_RMGUIServer.
8. If ICG is used: All ICGs have to be reinstalled, see [ICG Reinstallation after the Migration of the UMS Server](#)(see page 121).
9. Adapt, if necessary, the DHCP tag and the DNS alias igelrmserver with the IP or FQDN of the new UMS Server. See [Registering Devices Automatically](#)(see page 312).



- i** The configuration of the DHCP tag and the DNS alias is not a setting that can be made within the IGEL software. You must configure these within your individual network environment on the corresponding DHCP and DNS servers.

- i** If you have used and adjusted the DNS alias and the DHCP option, the following step is NOT required since the device can resolve the name igelrmserver correctly. In the local configuration, the device always remembers the IP of the UMS Server of its first registration. It is thus possible that the old IP address is displayed under **System > Remote Management**. Therefore, it makes sense to manually set an entry for remote administration after the migration:
- Create a profile in the UMS:
 - Go to **System > Remote Management** and click **Add**.
 - Under **UMS Server**, enter the IP of the new UMS Server.
 - Apply this profile globally, to the entire structure.

10. For HA installations only: Update the host assignment for job execution. For the instructions, see [Updating Host Assignment for Job Execution](#)(see page 111).

- ✓** After the procedure is complete, open the UMS Console and go to **UMS Administration > UMS Network > Server** to check if there is an entry for the previous UMS Server among the listed components. If so, select the entry and click **Delete** in the context menu.

With a Different Database

Transfer the UMS data to the new database before the migration process, see also [Data Source](#)(see page 543):

- Click **Data Source > Add...** in the UMS Administrator of the current server to set up a data source for the new database you wish to use.
- Click **Copy** to copy the old data source to the new one.
- Activate the new data source.
- Wait until the UMS Server fully starts, i.e. the UMS Console can connect with it.
- Now you can begin the migration procedure like described before:

If the new data source is	
• an embedded database:	UMS with embedded database (see page 100)
• an external database:	UMS with external database (see page 103)

Transferring or Registering the UMS Licensing ID

There are two different ways to handle the [UMS Licensing ID](#)(see page 444) if you migrate the UMS Server:

- [Transferring the UMS Licensing ID](#)(see page 107): With this method, you make a backup of the old UMS Licensing ID and take it with you. The UMS Licensing ID, which is automatically created during



the installation of the new UMS Server, is overwritten. Advantage: You do not have to reassign the license packages in the ILP.

- [Registering the New UMS Licensing ID in the ILP\(see page 110\)](#): With this method, you register the UMS Licensing ID of the new server in the IGEL License Portal. Advantage: You do not need to know the UMS Licensing ID of the old server.

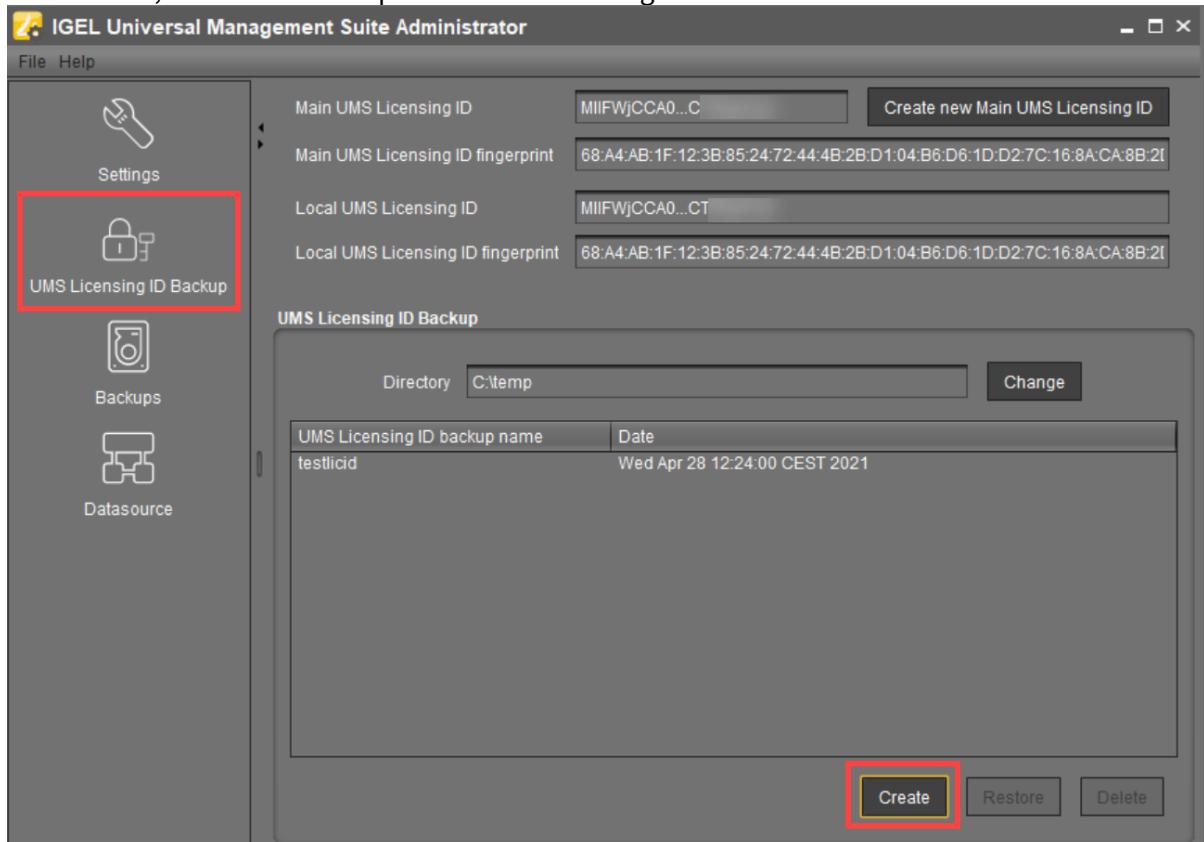
Transferring the UMS Licensing ID

Old Server: Create a Backup of the UMS Licensing ID

1. Open the UMS Administrator of your old server and go to **UMS Licensing ID Backup**.

i Default path to the UMS Administrator:
 Linux: /opt/IGEL/RemoteManager/RMAdmin.sh
 Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe

2. Click **Create**, to create a backup of the UMS Licensing ID.





- i** If you are using an HA environment, note the following:

It is always the UMS Licensing ID of the local server that is backed up. Therefore, make sure at first that the **local UMS Licensing ID** is the same as the **main UMS Licensing ID**. If not, restart the UMS Server to synchronize the local UMS Licensing ID with the main UMS Licensing ID and then proceed with creating the backup. See also [Manual Synchronization of the UMS Licensing ID¹⁵](#).

3. Enter a name for the UMS Licensing ID backup and a password.

UMS Licensing ID Backup

UMS Licensing ID backup name:

Set UMS Licensing ID password:
Password:
Confirm password:

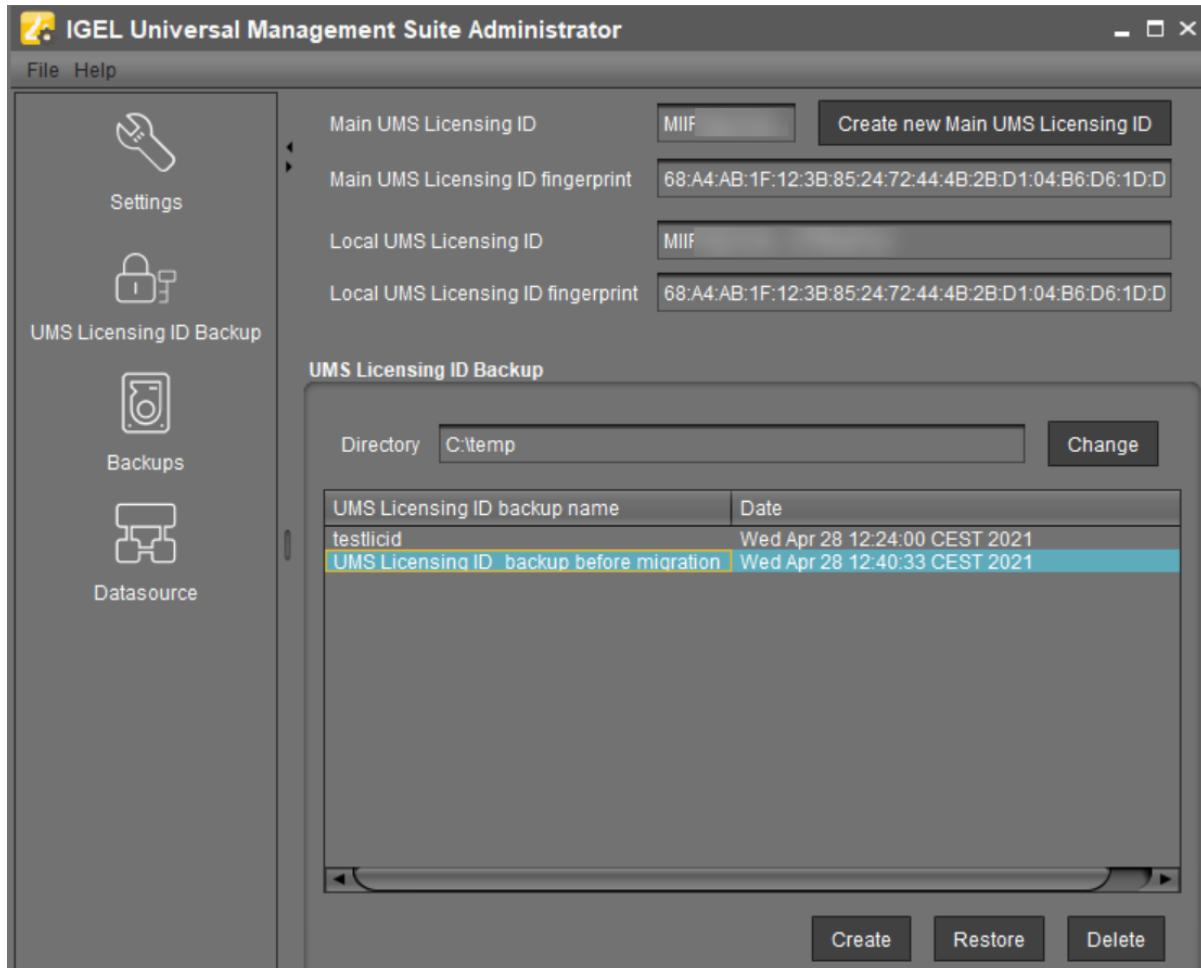
! Please note that this UMS Licensing ID backup can only be restored if you are able to supply the password entered here!

Ok **Cancel**

4. Click **OK**.

The new backup file is listed under **UMS Licensing ID Backup**.

¹⁵ <https://kb.igel.com/display/ENLITEUMS/.Manual+Synchronization+of+the+UMS+Licensing+ID+v6.01>



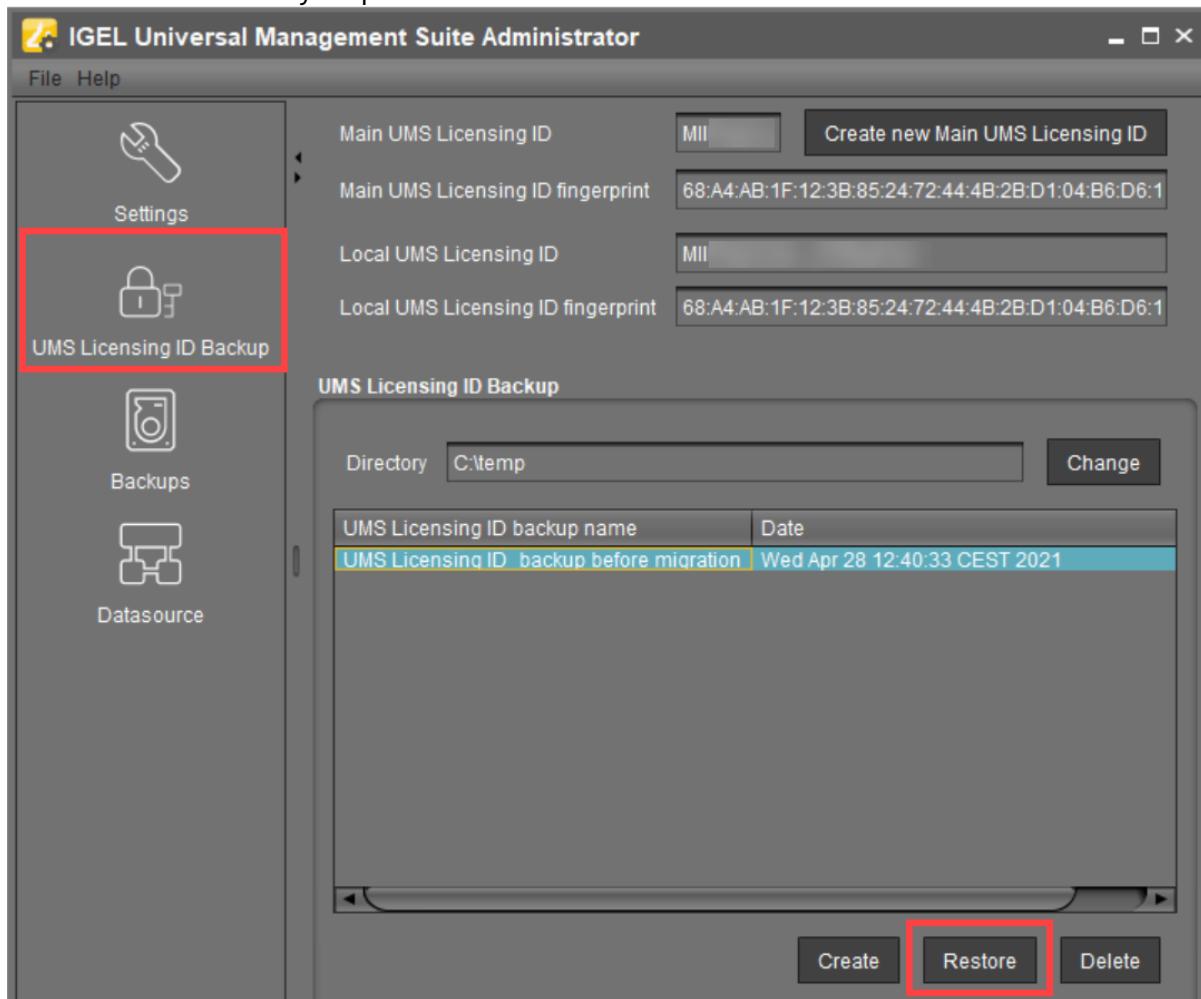
5. In your file explorer, go to the specified folder (in this case C:\temp).
6. Copy the UMS Licensing ID file (in this case UMS_Licensing_ID_backup_before_migration.ksbak) to a directory of your new UMS Server environment.

New Server: Restore the UMS Licensing ID to the New Server

1. Open the **UMS Administrator** of the new server and go to **UMS Licensing ID Backup**.
2. Click **Change** behind the **Directory** field to choose the directory where you stored the UMS Licensing ID.
The file with the UMS Licensing ID will be listed.



3. Click **Restore** and enter your password.



The UMS Licensing ID is now stored in the new UMS environment.

Registering the New UMS Licensing ID in the IGEL License Portal (ILP)

1. Log in to the IGEL License Portal (ILP) at <https://activation.igel.com>¹⁶. If you have not registered yet, you must register first.
Your dashboard is shown.
2. Select **UMS Licensing ID**.
The page **UMS Licensing ID** is shown.
3. Click **Register UMS Licensing ID**.
The dialog **Register UMS Licensing ID** opens.
4. Under **UMS Licensing ID Name**, enter a name for the UMS Licensing ID.

¹⁶ <https://activation.igel.com/>



5. Upload the certificate file you have exported in the UMS (see [Obtaining Your UMS Licensing ID¹⁷](#)) and click **OK**.
The UMS Licensing ID is registered. If this is the first UMS Licensing ID you registered, or if you just defined it as the default UMS Licensing ID, the dialog **Assign loose Product Packs** is shown.
6. If the dialog **Assign loose Product Packs** is shown, click **OK** to assign Product Packs and continue with [Assigning a Product Pack to the UMS Licensing ID¹⁸](#).

For a detailed instruction with screenshots, see [Registering Your UMS Licensing ID¹⁹](#).

Updating Host Assignment for Job Execution

Job execution in the UMS uses a device to UMS Server mapping to avoid multiple executions of one job with the same device. If a UMS Server is migrated, this mapping needs to be adjusted.

- i** The mapping is relevant for HA installations only. In standard (single instance) installations, the host assignments do not need to be adjusted. In HA installations, follow the steps below.

1. In the UMS Console, go to **UMS Administration > UMS Network > Server > [new server]**.
2. Find the process ID of the new server.

Attribute	Value
Process ID	9c7aa3b9-5a4b-4f6d-ac33-3e34d7d2449c
Cluster ID	UMS-CLUSTER-50102-1536569722693-2-0
Version	6.01.100.rc5
Host	DokuW10bl.IGEL.LOCAL
Port	30001
Operating Syst...	Windows 10
Timestamp	Feb 22, 2019 2:17 PM

3. In the menu bar of the UMS Console, select **Misc > Scheduled Jobs > Host Assignment**.
4. Select the new server and check the process ID.
5. Under **Available devices**, activate **Show all**.
6. In **List View** on the right side, select all devices.

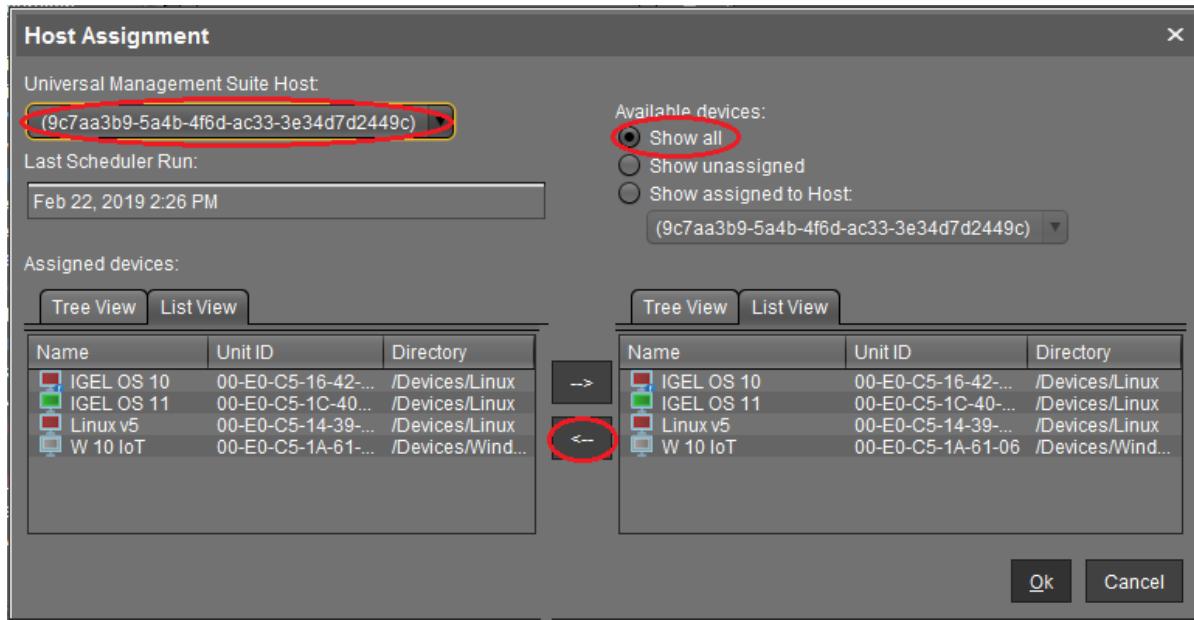
- i** To select all devices, set the focus in the list and press [Ctrl+a].

7. Click the left arrow to assign the devices to the new host.

¹⁷ <https://kb.igel.com/display/licensesmoreigelos11/Obtaining+Your+UMS+Licensing+ID>

¹⁸ <https://kb.igel.com/display/licensesmoreigelos11/Assigning+a+Product+Pack+to+the+UMS+Licensing+ID>

¹⁹ <https://kb.igel.com/display/licensesmoreigelos11/Registering+Your+UMS+Licensing+ID>



1.6.2 Migrating a UMS Database From Embedded DB to Microsoft SQL Server

This document describes how to migrate the database of a *Universal Management Suite (UMS)* installation from *Embedded DB* to a *Microsoft SQL Server*.

This is an exemplary representation. If you want to integrate the other way round or integrate other databases, the same steps are always performed. You can always use this description as a guide.

IGEL Demos Channel



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=_200UQppobw

- [Setting Up the SQL Database](#)(see page 112)
- [Copying Database Contents](#)(see page 114)

Setting Up the SQL Database

⚠ The UMS supports only those standard sortings of Microsoft SQL Server which are case insensitive ("CI"). Therefore, make sure that the parameter **Collation** in MS SQL Server is set appropriately.



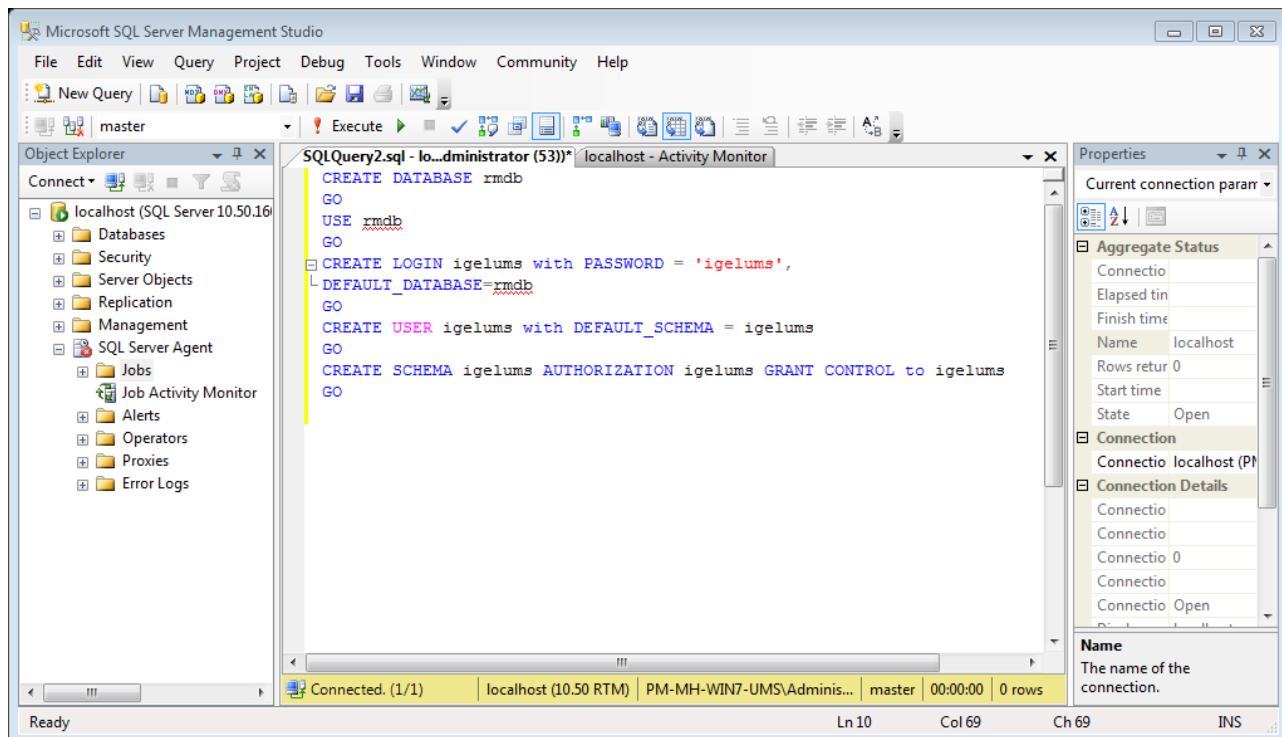
- Execute the following SQL script on the Microsoft SQL Server to create database, login, user, and schema. Replace the placeholders such as [databasename] with settings of your choice.

[sql-user] can be an SQL account or a Microsoft Active Directory (AD) account; for more information on the latter, see [Connecting the UMS to an SQL Server via Active Directory](#)(see page 292). The script uses the same string for login, user, and schema in order to simplify UMS setup.

- i** The **user name** for the external database may only be created with the following properties:
- it consists only of **lower case letters** or **upper case letters**.
 - the **low-cut character** ("_") is the only special character, which is allowed.

Do not mix upper and lower case letters. Don't use points, spaces, minus, or @ sign!

```
CREATE DATABASE [databasename]
GO
USE [databasename]
GO
CREATE LOGIN [sql-user] with PASSWORD = '[password]' ,
DEFAULT_DATABASE=[databasename]
GO
CREATE USER [sql-user] with DEFAULT_SCHEMA = [sql-user]
GO
CREATE SCHEMA [sql-user] AUTHORIZATION [sql-user] GRANT CONTROL to [sql-user]
GO
```



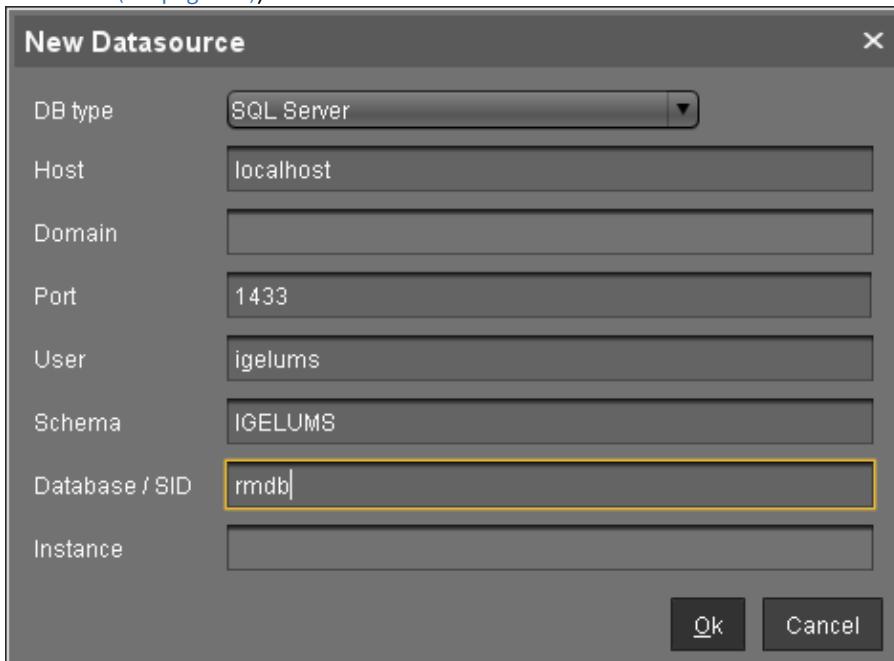


Copying Database Contents

1. Start IGEL Universal Management Suite Administrator.

i Default path to the UMS Administrator:
Linux: /opt/IGEL/RemoteManager/RMAdmin.sh
Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe

2. Go to **Datasource > Add...** to create a new SQL Server data source; use exactly the same database name and settings you have defined while setting up the SQL Database (see [Setting Up the SQL Database](#)(see page 112)).



The screenshot shows the 'New Datasource' dialog box. It has a dark gray header bar with the title 'New Datasource' and a close button. Below the header are eight input fields arranged in two columns. The left column contains labels: 'DB type', 'Host', 'Domain', 'Port', 'User', 'Schema', and 'Instance'. The right column contains corresponding input fields. The 'DB type' field is set to 'SQL Server'. The 'Host' field contains 'localhost'. The 'Port' field contains '1433'. The 'User' field contains 'igelums'. The 'Schema' field contains 'IGELUMS'. The 'Database / SID' field contains 'rmdb' and is highlighted with a yellow border. The 'Instance' field is empty. At the bottom right of the dialog are 'Ok' and 'Cancel' buttons.

3. Select the **Embedded DB** entry and click **Copy**.



Screenshot of the IGEL Universal Management Suite Administrator interface showing the Datasource configuration screen.

The interface includes a sidebar with icons for Settings, UMS Licensing ID B..., Backups, and Datasource. The main area shows the following configuration:

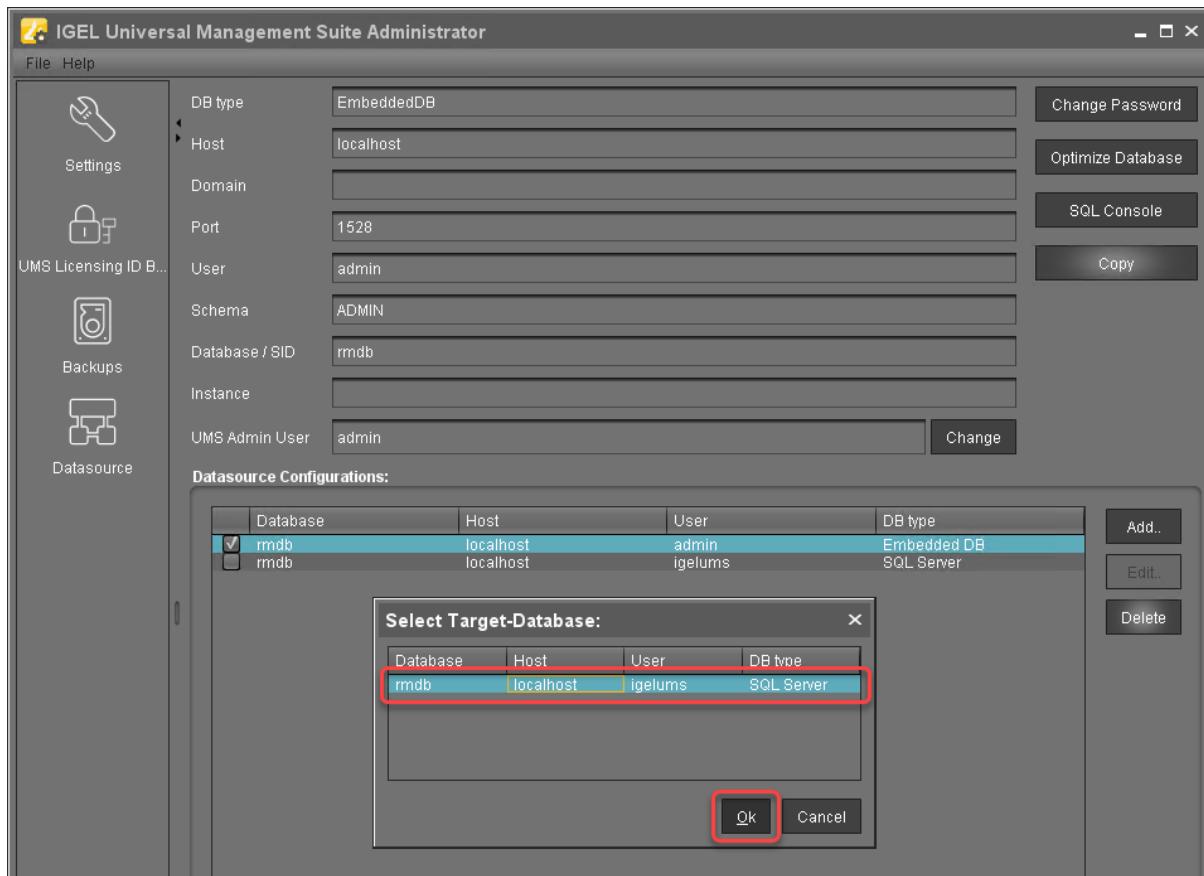
DB type	EmbeddedDB	Change Password
Host	localhost	Optimize Database
Domain		SQL Console
Port	1528	
User	admin	Copy (highlighted with a red box)
Schema	ADMIN	
Database / SID	rmdb	
Instance		
UMS Admin User	admin	Change

Datasource Configurations:

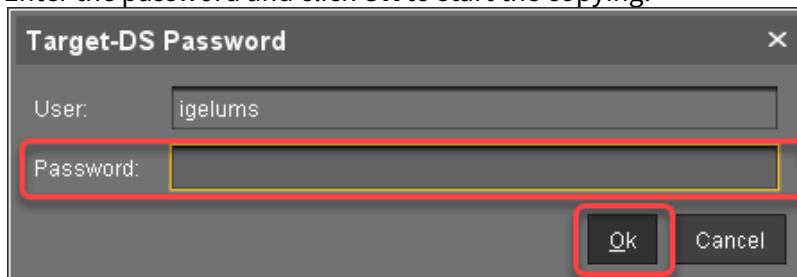
Database	Host	User	DB type
rmdb	localhost	admin	Embedded DB

Buttons at the bottom include Add.., Edit.., Delete, Test, Activate, and Deactivate.

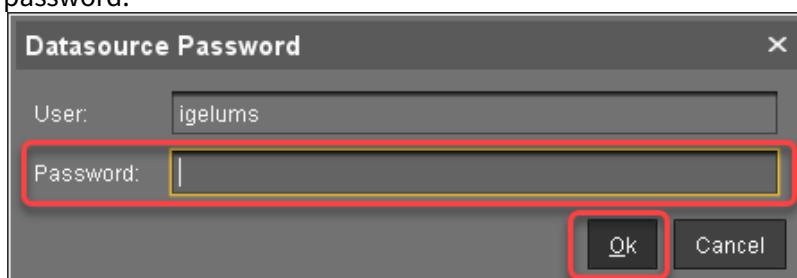
4. Select the newly created SQL Server entry as the target and click **OK**.



5. Enter the password and click **OK** to start the copying.



6. When the copying has completed, test the database connection by clicking **Test** and entering the password.





7. If the test was successful, select the **SQL Server** datasource and click **Activate**.

A screenshot of the IGEL Universal Management Suite Administrator window. On the left, there's a sidebar with icons for Settings, UMS Licensing ID B..., Backups, and Datasource. The main area shows configuration fields for a database connection: DB type (EmbeddedDB), Host (localhost), Port (1528), User (admin), Schema (ADMIN), Database / SID (rmdb), and Instance (empty). To the right are buttons for Change Password, Optimize Database, SQL Console, and Copy. Below these is a section titled "Datasource Configurations:" containing a table. The table has columns: Database, Host, User, and DB type. It lists two entries: "rmdb" (Host: localhost, User: admin, DB type: Embedded DB) and "igelums" (Host: localhost, User: igelums, DB type: SQL Server). The "igelums" row is highlighted with a red border. At the bottom right of the main window are buttons for Test, Activate (which is highlighted with a red box), and Deactivate.

8. Enter the password to confirm the activation.

A screenshot of a "Datasource Password" dialog box. It has a "User" field containing "igelums" and a "Password" field which is empty and highlighted with a red box. At the bottom are "Ok" and "Cancel" buttons, with "Ok" also highlighted with a red box.



- ⓘ Now the Microsoft SQL Server is set up as the datasource. From now on, back up the SQL Server in order to back up UMS data.
- ⓘ The same way you can go back to the embedded database, if you need.

1.6.3 Restore and Recover Corrupted UMS Embedded DB

Environment

- UMS 6 on Windows or Linux

If the embedded database of UMS* is corrupted, try the following measures to resolve the issue.

*The underlying technology of the embedded database is Apache Derby.

Restoring a Database Backup Made with the UMS Administrator

If a backup of the embedded database is available (see [Creating a Backup\(see page 536\)](#)), just restore the backup, see [Restoring a Backup\(see page 540\)](#).

Restoring a File-Based Backup

If an uncorrupted copy of the database files located under C:\Program Files...\IGEL\RemoteManager\db\rmdb (default installation path on Windows) and/or /opt/IGEL/RemoteManager/db/rmdb/ (default installation path on Linux) is available, you can restore the file copy. In the remainder of this how-to, the aforementioned possible paths will be referred to as RMDB_PATH.

To restore the backup, perform the following steps:

1. Open the UMS Administrator, and go to **Datasource** in the menu on the left.
 - ⓘ Default path to the UMS Administrator:
Linux: /opt/IGEL/RemoteManager/RMAdmin.sh
Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe
2. In the **Datasource** area, delete the corrupted Derby DB.
3. Create a new embedded DB with exactly the same user name and password as you used for the deleted DB.
4. Deactivate the newly created DB.
5. Stop the UMS Server service. For details on how you can stop it, see [HA Services and Processes\(see page 691\)](#).
6. Erase all files contained in the folder at RMDB_PATH.
7. Copy your previously backed-up files to RMDB_PATH.
8. Activate the DB with the UMS Administrator under **Datasource**.
9. Wait 1 - 2 minutes, then log in to the UMS Console.



1.6.4 Disaster Recovery: UMS with an External Database

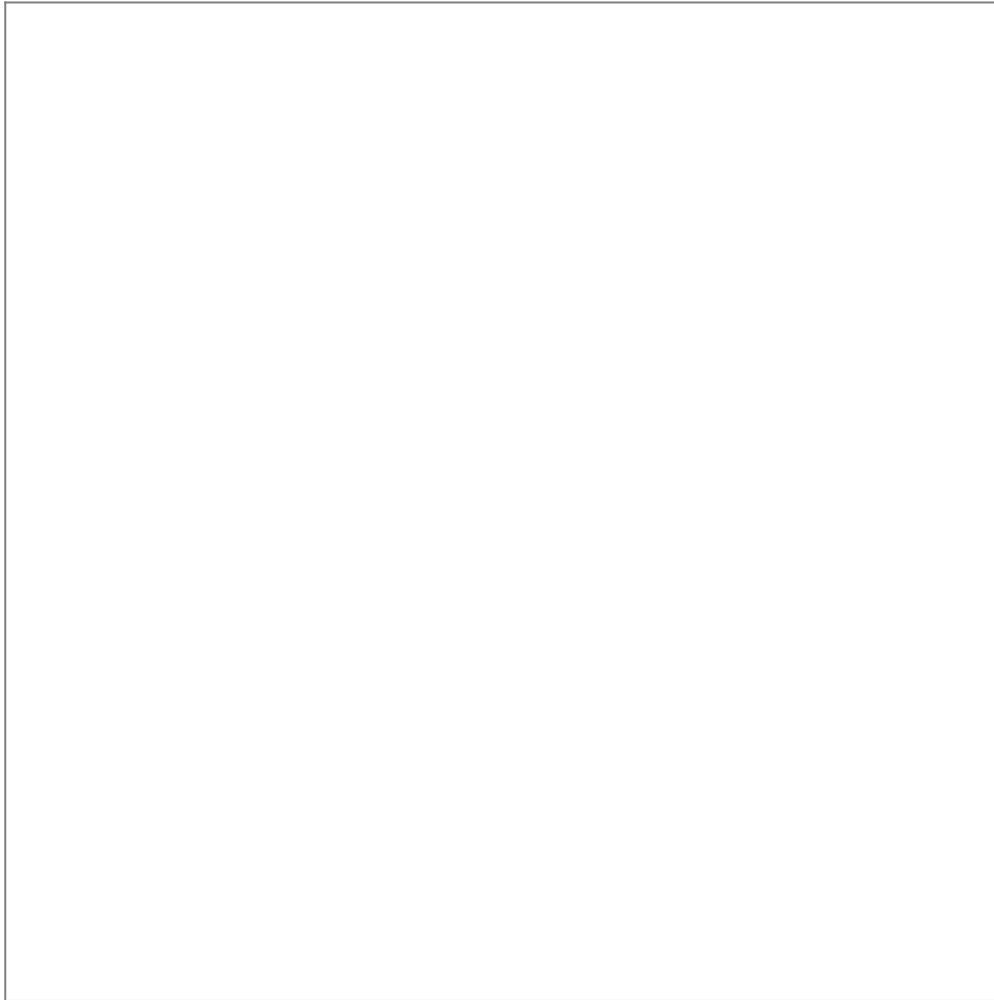
The following instructions require a proper backup of your environment, see the "External Database" section under [Creating a Backup](#)(see page 536).

Execution Order in Case of the Disaster Recovery

1. Install the UMS on the server, see [Installing a UMS Server](#)(see page 260). All the UMS components must be installed like before:
 - a. The same UMS version
 - b. The same network configuration of the host (the same IP addresses, ports)
 - c. For High Availability (HA) installations only: During the installation, use the backed-up IGEL network token. See the "Starting the Installation" section under [Adding Further Servers to the HA Network](#)(see page 667).
2. Stop the existing UMS Server(s). For the details on how you can do it, see [HA Services and Processes](#)(see page 691).
3. Copy all the saved files and firmware updates from `[IGEL installation directory] / rmguiserver/webapps/ums_filetransfer` to the new UMS Server(s) – without the WEB-INF folder.
If you deploy the HA environment, see also [How to Detect Which Files Are Synchronized Automatically](#)(see page 159).
4. Restore the database backup using the procedures recommended by the DBMS manufacturer.



5. Add the database connection to your external database on each UMS Server: **UMS Administrator > Datasource > Add.**



6. Click **Activate** to enable the data source.
The UMS Server will start automatically after that.
7. In the **UMS Administrator > Backups > Restore**, restore the backup of server configurations on each UMS Server. If necessary, transfer [host-specific server configurations](#)(see page 537) to the new server(s).
8. In the **UMS Administrator > UMS Licensing ID Backup > Restore**, restore the backup of the UMS Licensing ID.
Alternatively, you can register a new UMS Licensing ID, created during the server installation. See [Transferring or Registering the UMS Licensing ID](#)(see page 106).
9. For HA installations only: Check host assignments for job execution and, if required, adjust them.
See [Updating Host Assignment for Job Execution](#)(see page 111).

- ⓘ After the procedure is complete, open the UMS Console and go to **UMS Administration > UMS Network > Server** to check if there is an entry for the previous UMS Server among the listed components. If so, select the entry and click **Delete** in the context menu.



In the case of the HA installations, the same must be done for the load balancers: [UMS Administration > UMS Network > Load Balancer](#).

If you have a UMS installation with an embedded database, you may find it useful to read: [Restore and Recover Corrupted UMS Embedded DB](#)(see page 118).

1.6.5 ICG Reinstallation after the Migration of the UMS Server

Situation

The UMS has been migrated to a new server. The corresponding ICG must be reinstalled.

Question

What happens to the clients connected to the old ICG installation?

Answer

After the reinstallation, the previously bound devices can be managed via the new ICG and do not have to be re-registered



- The ICG must not move to a new server and must be reachable as before.
- The same root certificate must also be used for the installation.

1.6.6 UMS Does Not Connect to ICG: "TrustAnchor ...is not a CA certificate"

Symptom

The UMS fails to connect to the IGEL Cloud Gateway (ICG). The following message appears in the GUI or in the log file:

TrustAnchor ...is not a CA certificate

Caused by: sun.security.validator.ValidatorException: PKIX path validation failed:
sun.security.validator.ValidatorException: TrustAnchor with subject "CN=UMS-CLUSTER--xxx,
O=test, L=test, C=US" is not a CA certificate
at sun.security.validator.PKIXValidator.doValidate(PKIXValidator.java:380)
at sun.security.validator.PKIXValidator.engineValidate(PKIXValidator.java:273)
at sun.security.validator.Validator.validate(Validator.java:262)
at sun.security.ssl.X509TrustManagerImpl.validate(X509TrustManagerImpl.java:327)



```
at sun.security.ssl.X509TrustManagerImpl.checkTrusted(X509TrustManagerImpl.java:236)
at sun.security.ssl.X509TrustManagerImpl.checkServerTrusted(X509TrustManagerImpl.java:113)
at de.igel.apps.usg.connection.ssl.TrustedOnlyTrustManager.checkServerTrusted(TrustedOnlyTrustManager.java:74)
at sun.security.ssl.AbstractTrustManagerWrapper.checkServerTrusted(SSLContextImpl.java:1099)
at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1622)
... 54 more
```

Environment

- UMS 6.04 or higher
- ICG with older root certificates created with UMS 5.07 or UMS 5.08

Problem

Older ICG root certificates (created with UMS 5.07 or UMS 5.08) do not have the right CA modifier, which was never a problem with previous Java versions. But the Java version used in UMS 6.4.x onwards blocks these certificates.

To check whether you have an old ICG root certificate:

1. Open the UMS Console, go to **UMS Administration > Global Configuration > Cloud Gateway** and select your ICG root certificate.
2. Click to read the certificate content.
If **Certificate Authority** is set to "false", you have an old ICG root certificate.

Solution

If you do not want to exchange the ICG root certificate (involves installing the ICG anew and re-registering all endpoint devices), you can add a start parameter that tells the UMS Server to ignore the CA flag in the certificate.

This start parameter will be overwritten on each UMS update installation, so you must set it again after the update.

Follow the instructions below, according to your operating system.

For Windows

1. Open the Windows **Services** dialog and stop the service **IGELRMGUIServer**.
2. Navigate to the directory <UMS installation directory>\RemoteManager\rmguiserver\bin (example: C:\Program Files (x86)\IGEL\RemoteManager\rmguiserver\bin)
3. Double-click on **editTomcatService**.
4. Confirm the warning dialog.
5. Select the **Java** tab.



6. Under **Java Options**, add the following entry as a new line:
-Djdk.security.allowNonCaAnchor=true
7. Click **Ok** to save the changes.
8. In the Windows **Services** dialog, start the service **IGELRMGUIServer**.

For Linux

1. Stop the service igelRMserver
2. Navigate to the directory /opt/IGEL/RemoteManager/rmguiserver/bin
3. Open the file igelRMserver
4. Find the two entries -Xmx4096 and add a new line before each entry with the following content:
-Djdk.security.allowNonCaAnchor=true
5. Save the changes.
6. Start the service igelRMserver

1.6.7 Using Your Own Certificates for Communication over the Web Port (Default: 8443)

Overview

For all communication that is taking place over the Web Port (default: 8443, see also [UMS Communication Ports](#)(see page 48)), a specific self-signed certificate chain comes with the UMS on installation. Nevertheless, you can use a certificate chain of your own.

See also [Web](#)(see page 455) in the [UMS Reference Manual](#)(see page 253).

This article describes how to deploy a certificate chain with a corporate CA certificate or a public certificate:

- [Deploying a Self-Signed Corporate Certificate Chain](#)(see page 123) (recommended)

We recommend using a self-signed corporate certificate chain. This approach makes you independent from public CAs, which are in danger of being compromised by attackers. Of course, a self-signed certificate must be made known to the browsers first, otherwise, the browsers will display warning messages.

- [Deploying a Certificate Chain with a Public Root CA](#)(see page 134)

Deploying a Self-Signed Corporate Certificate Chain

Prerequisites

- You have a self-signed root CA certificate that serves as a trusted “root” certificate company-wide.
- Your self-signed root CA certificate has been applied to all relevant trust stores within your company.
- You have an intermediate CA certificate that is signed by your root CA certificate and a corresponding private key.



Importing the Root Certificate

1. In the UMS Console, go to **UMS Administration > Global Configuration > Certificate Management > Web**.

A screenshot of the IGEL Universal Management Suite 6 console. The left sidebar shows a tree view of administration categories. The 'Web' category under 'Device Communication' is highlighted with a red box. The main panel displays 'Web Certificates' information and a table of certificates. The table has columns: Display name, Expiring date, Key Specification, Signature, Used, Private Key known, and Status. Two rows are listed:

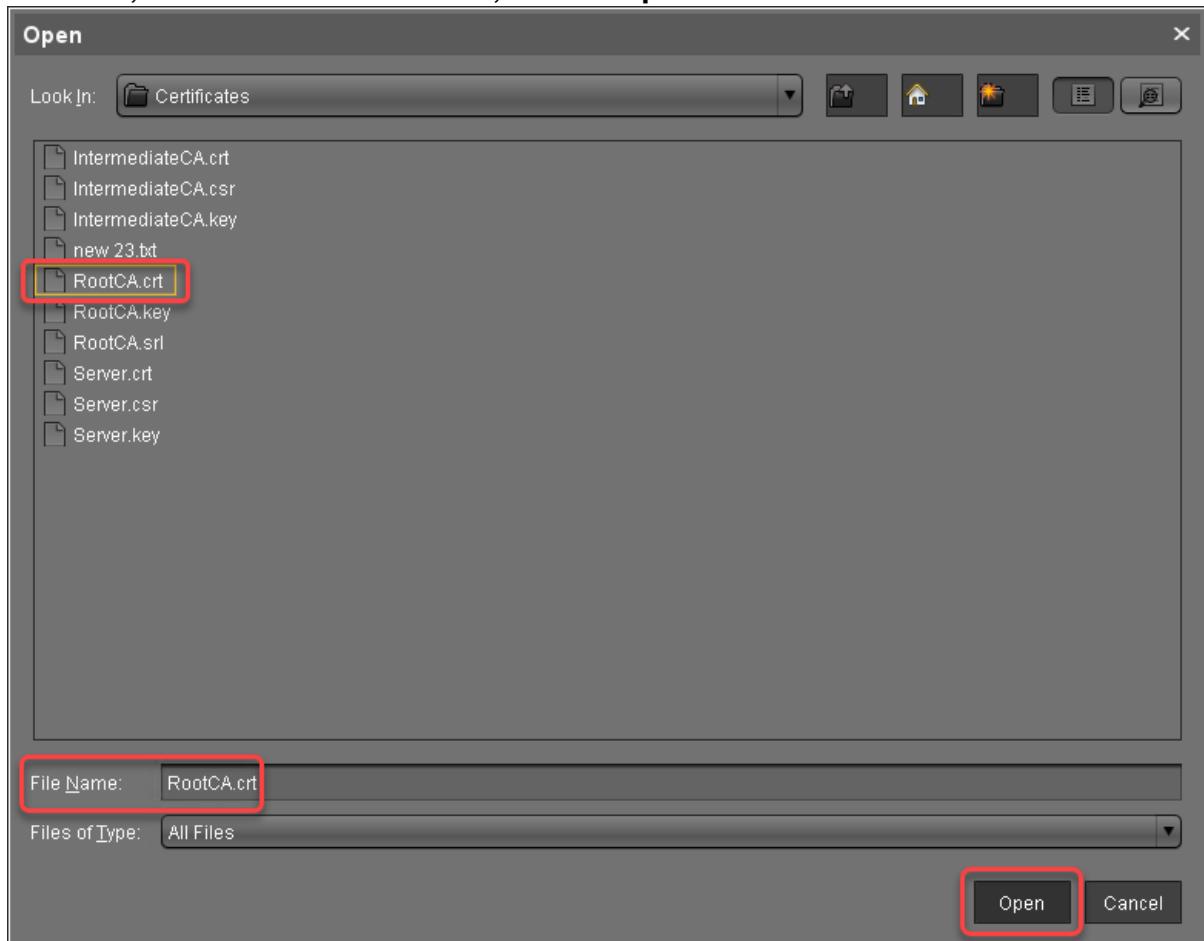
Display name	Expiring date	Key Specification	Signature	Used	Private Key known	Status
6209499...	Oct 30, 2040	RSA (4096 bits)	SHA512withRSA	✓	✓	✓
4204...	Oct 30, 2021	RSA (4096 bits)	SHA512withRSA	✓	✓	✓

A message at the bottom says: "Please select a certificate to see its assigned server(s)".

The 'Web' section is highlighted with a red box.



2. Click , select the root certificate file, and click **Open**.

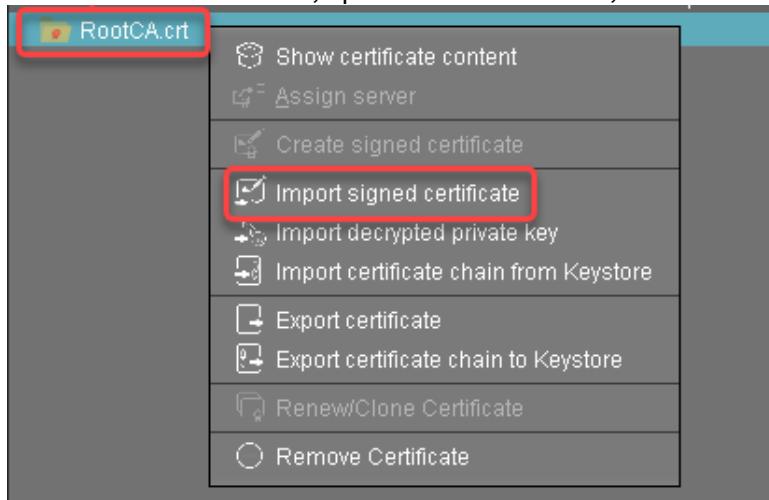


The root certificate is imported.



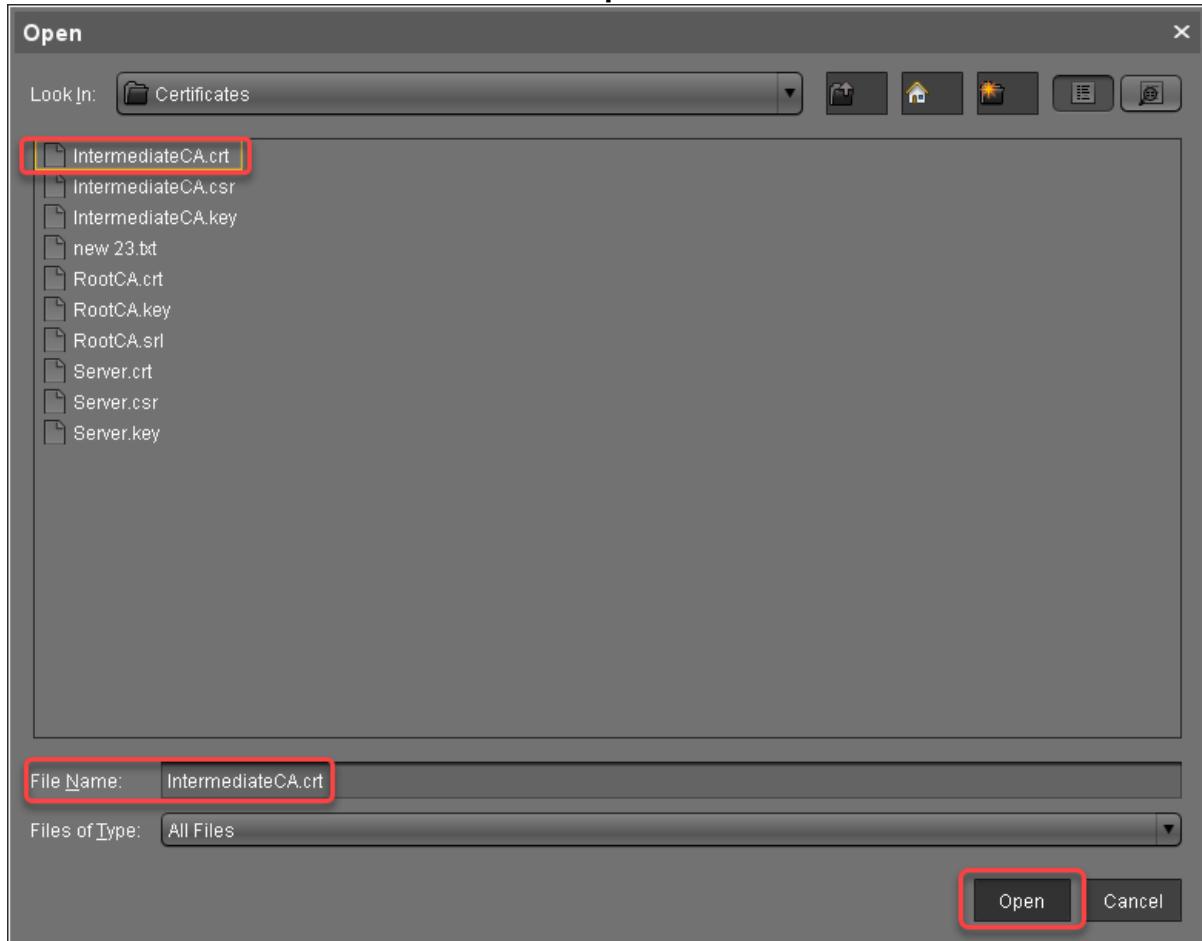
Importing the Intermediate Certificate

1. Select the root certificate, open the context menu, and select **Import signed certificate**.



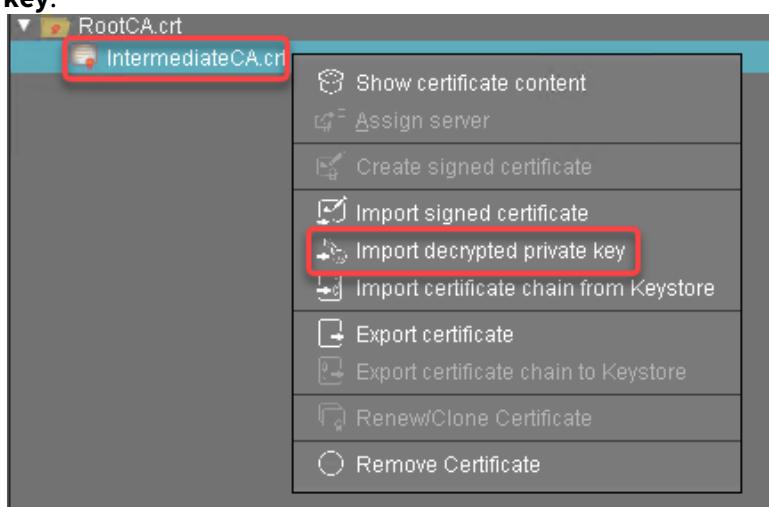


2. Select the intermediate certificate file and click **Open**.



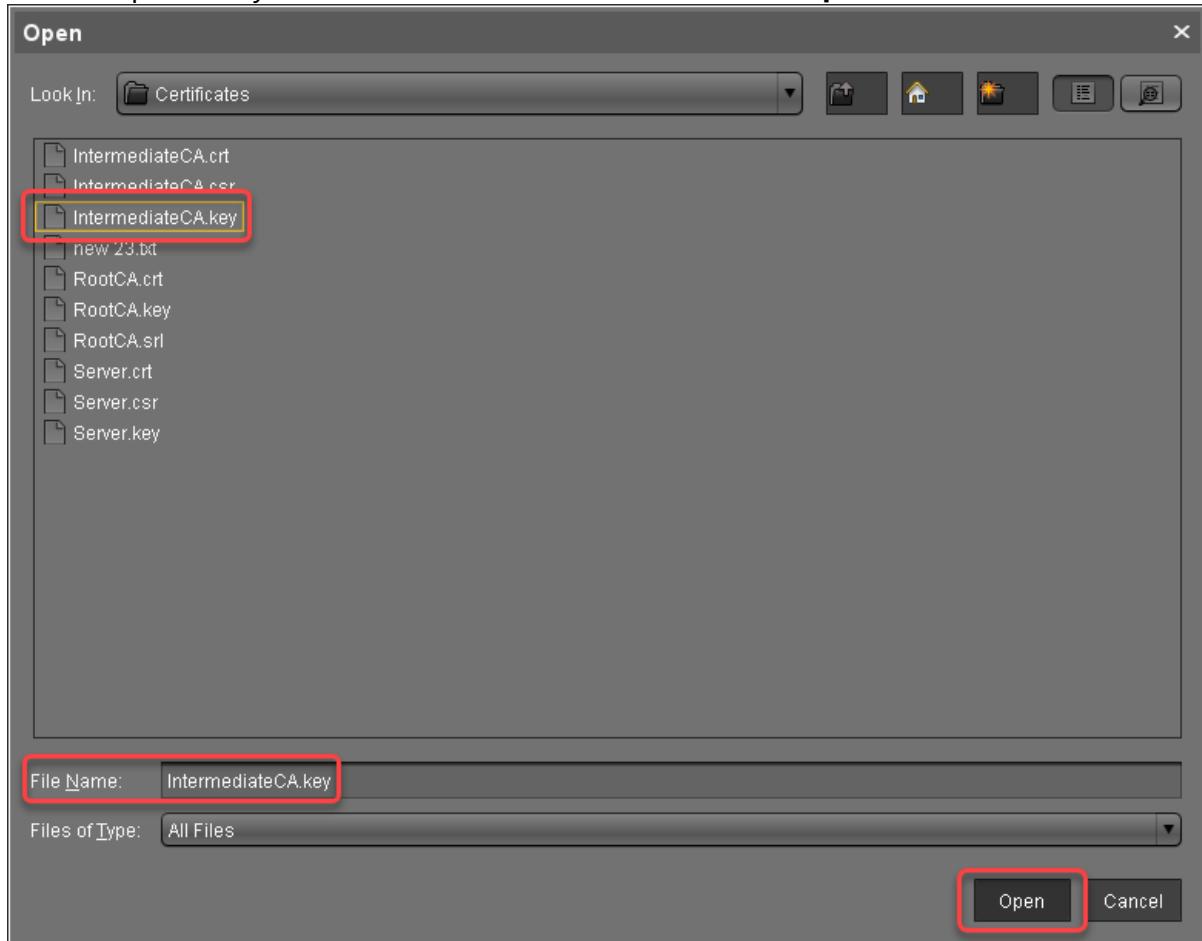
The intermediate certificate is imported.

3. Select the intermediate certificate, open the context menu, and select **Import decrypted private key**.





4. Select the private key file of the intermediate certificate and click **Open**.



The private key of the intermediate certificate is imported.

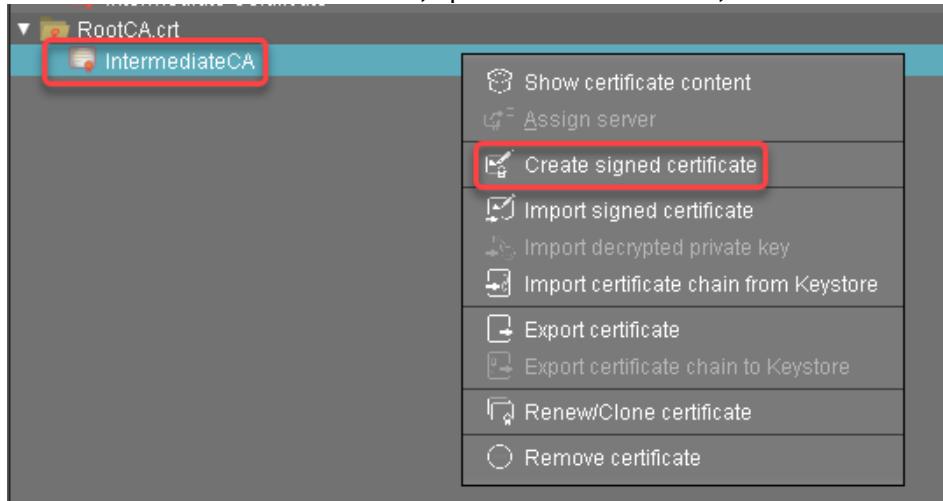
5. Continue with [Creating the End Certificates](#)(see page 128).

Creating the End Certificates

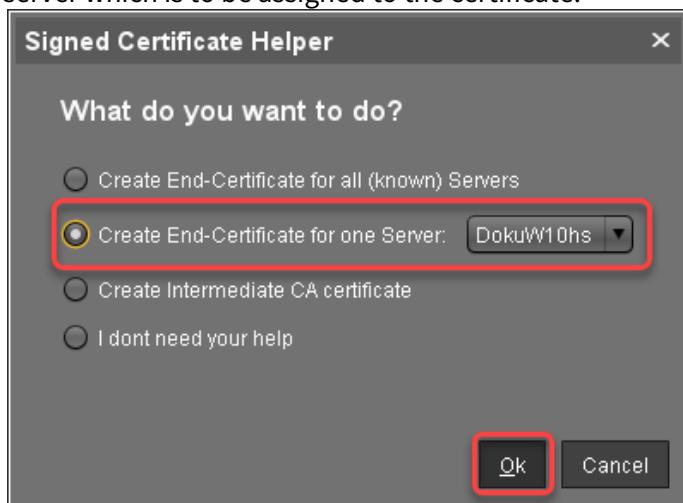
Repeat the following steps for each server in your UMS environment:



1. Select the intermediate certificate, open the context menu, and select **Create signed certificate**.



2. In the **Signed Certificate Helper**, select **Create end certificate for one server** and select the server which is to be assigned to the certificate.





3. In the dialog **Create Signed Certificate**, fill in the data as required.

Create signed certificate

Displayname	Server certificate
Your first and last name	Ike Igel
Your organization	My Company
Your locality (or random identifier)	Augsburg
Your two-letter country code	DE
Hostname and/or IP of certificate target server	Manage Hostnames
Key	RSA, 4096 bits Manage
Signature Algorithm	SHA256withRSA
Valid until	Oct 29, 2021
Certificate Type	<input type="radio"/> CA Certificate <input checked="" type="radio"/> End Entity
Ok Cancel	



4. Click **Manage hostnames**.

The screenshot shows the 'Create signed certificate' dialog box. It contains the following fields:

Displayname	Server certificate
Your first and last name	Ike Igel
Your organization	My Company
Your locality (or random identifier)	Augsburg
Your two-letter country code	DE
Hostname and/or IP of certificate target server	Manage Hostnames
Key	RSA, 4096 bits
Signature Algorithm	SHA256withRSA
Valid until	Oct 29, 2021
Certificate Type	<input type="radio"/> CA Certificate <input checked="" type="radio"/> End Entity

At the bottom right are 'Ok' and 'Cancel' buttons.

5. In the dialog **Set Hostnames for Certificate**, check if "localhost" and all IP addresses and FQDNs (Fully Qualified Domain Names) under which your server is reachable are displayed under **Assigned hostnames**. If not, add the missing IP addresses and FQDNs under **Add hostname manually**.



Set Hostnames for Certificate

Server Attributes

- ▼ DokuW10hs
 - DokuW10hs *[not FQDN-compliant]*
 - ✓ 169.254.144.38

Assigned Hostnames

- ✓ 169.254.144.38
- ✓ localhost

Add Hostname manually

Add

> <

Close

A modal dialog titled "Set Hostnames for Certificate". It contains two main sections: "Server Attributes" and "Assigned Hostnames". In "Server Attributes", there is a single item: "DokuW10hs" with a note "(not FQDN-compliant)". Below it, "169.254.144.38" is listed with a green checkmark. In the "Assigned Hostnames" section, "169.254.144.38" and "localhost" are listed with green checkmarks. A red box highlights the "Assigned Hostnames" list. Another red box highlights the "Add Hostname manually" input field and its "Add" button. A third red box highlights the "Close" button in the bottom right corner.



6. Close the dialog **Create Signed Certificate** with **Ok**.

The dialog box contains the following fields:

- Displayname: Server certificate
- Your first and last name: Ike Igel
- Your organization: My Company (highlighted)
- Your locality (or random identifier): Augsburg
- Your two-letter country code: DE
- Hostname and/or IP of certificate target server: Manage Hostnames
- Key: RSA, 4096 bits
- Signature Algorithm: SHA256withRSA
- Valid until: Oct 29, 2021
- Certificate Type: End Entity (radio button selected)
- Buttons: Ok (highlighted), Cancel

The signed server certificate is created.

7. Continue with [Assigning the Certificate to All Servers](#)(see page 133).

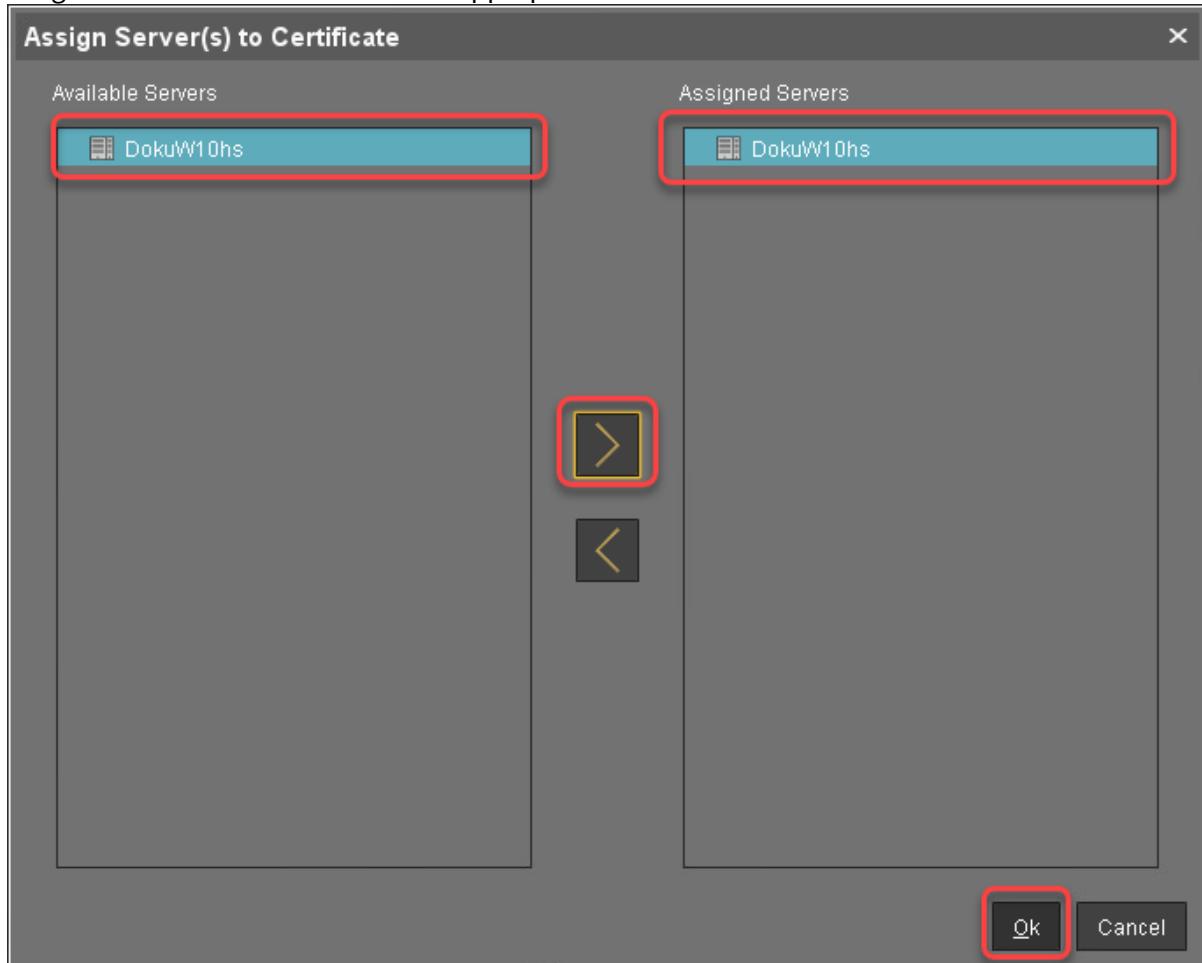
Assigning All Servers to the Certificate

Repeat the following steps for each server in your UMS environment:

1. Select the server certificate, open the context menu, and select **Assign server**.

The screenshot shows a tree view of certificates. Under 'RootCA.crt', there is a 'Server certificate' entry. A context menu is open over this entry, with the 'Assign server' option highlighted by a red box. Other options in the menu include 'Show certificate content', 'Create signed certificate', 'Import signed certificate', 'Import decrypted private key', 'Import certificate chain from Keystore', 'Export certificate', 'Export certificate chain to Keystore', 'Renew/Clone certificate', and 'Remove certificate'.

2. Assign the server to the certificate as appropriate.



3. If you are using the UMS Web App: To avoid warning messages from browsers, you must make the new certificates known to the browsers. For instructions, see [UMS Web App: The Browser Displays a Security Warning \(Certificate Error\)](#)(see page 187).

Deploying a Certificate Chain with a Public Root CA

Prerequisites

- You have a public certificate that is able to serve as a CA.
- All UMS Servers follow the same naming scheme, e.g. “something.ums.mycompany.de” if the company name is “mycompany.de”.



Importing the Root Certificate

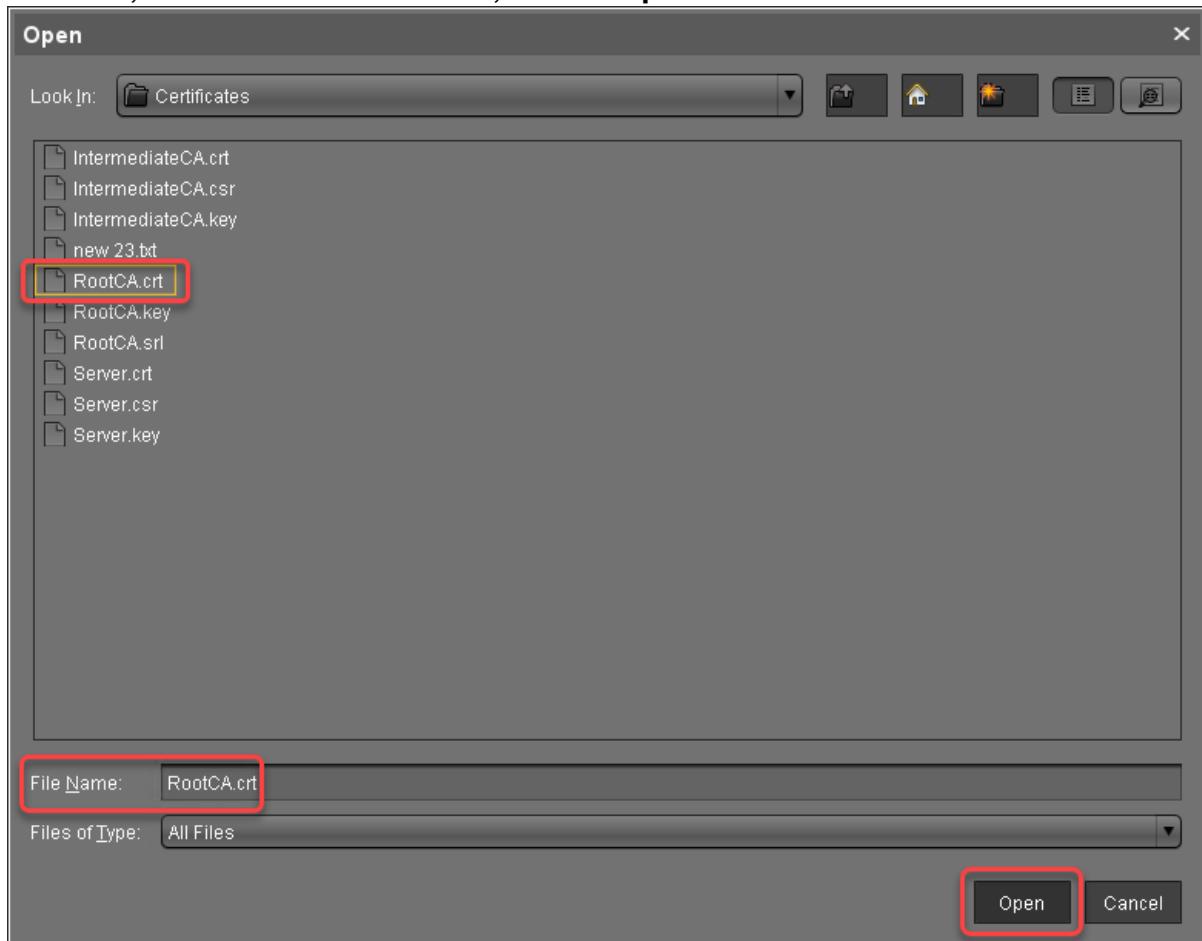
1. In the UMS Console, go to **UMS Administration > Global Configuration > Certificate Management > Web**.

The screenshot shows the UMS Administration interface with the 'Web' section selected in the navigation tree. The main panel displays 'Web Certificates' status: 'Server status: OK' and 'Certificate status: OK'. An 'Automatic renewal: ON' option is also visible. Below this, a table lists certificates under 'Certificates', showing columns for Display name, Expiring date, Key Specification, Signature, Used, Private Key known, and Status. Two certificates are listed: one for '6209499...' expiring on Oct 30, 2040, and another for '4204...' expiring on Oct 30, 2021. Both entries show green checkmarks in the 'Used' and 'Private Key known' columns. A note at the bottom says 'Please select a certificate to see its assigned server(s)'.

Display name	Expiring date	Key Specification	Signature	Used	Private Key known	Status
6209499...	Oct 30, 2040	RSA (4096 bits)	SHA512withRSA	✓	✓	✓
4204...	Oct 30, 2021	RSA (4096 bits)	SHA512withRSA	✓	✓	✓



2. Click , select the root certificate file, and click **Open**.

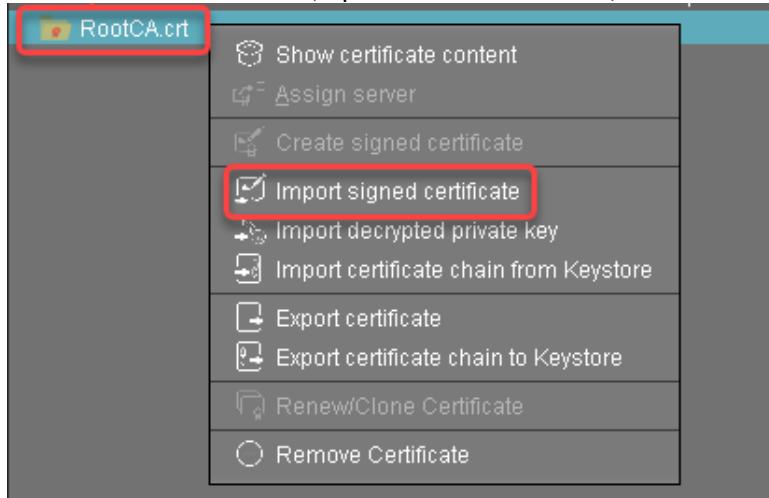


The root certificate is imported.

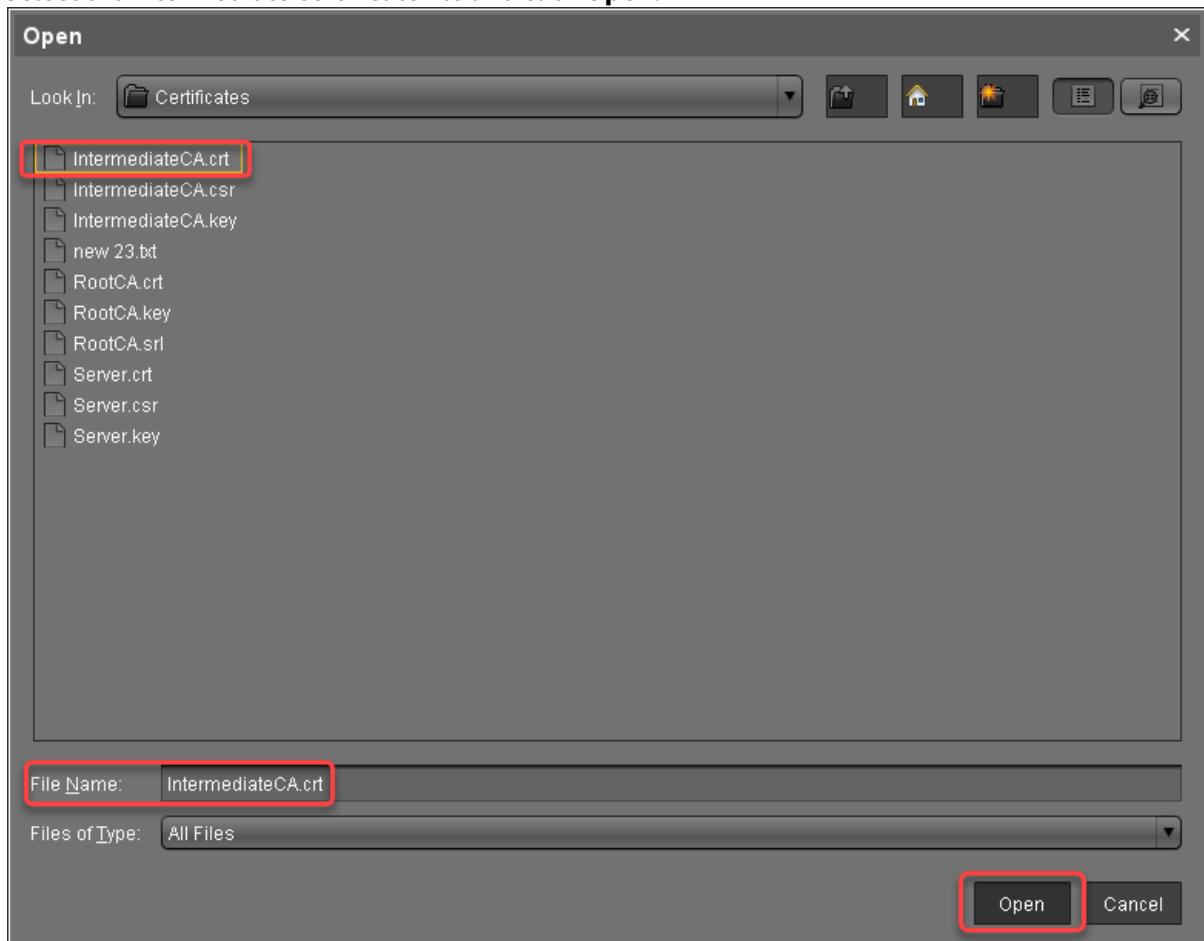


Importing the Intermediate Certificate

1. Select the root certificate, open the context menu, and select **Import signed certificate**.



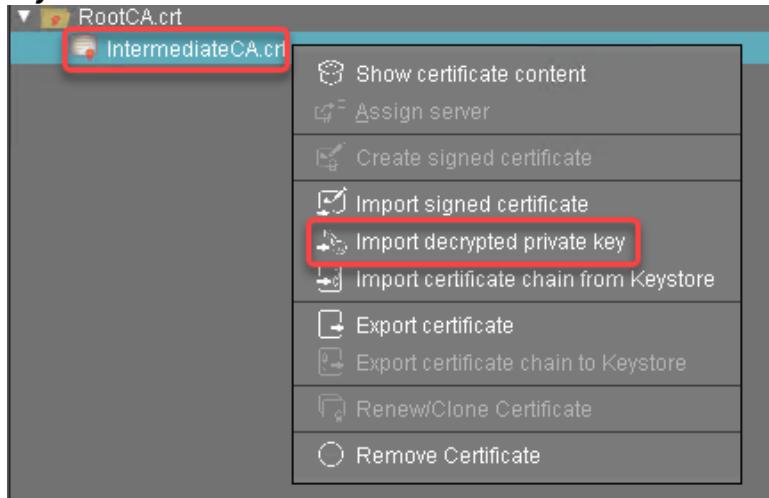
2. Select the intermediate certificate file and click **Open**.



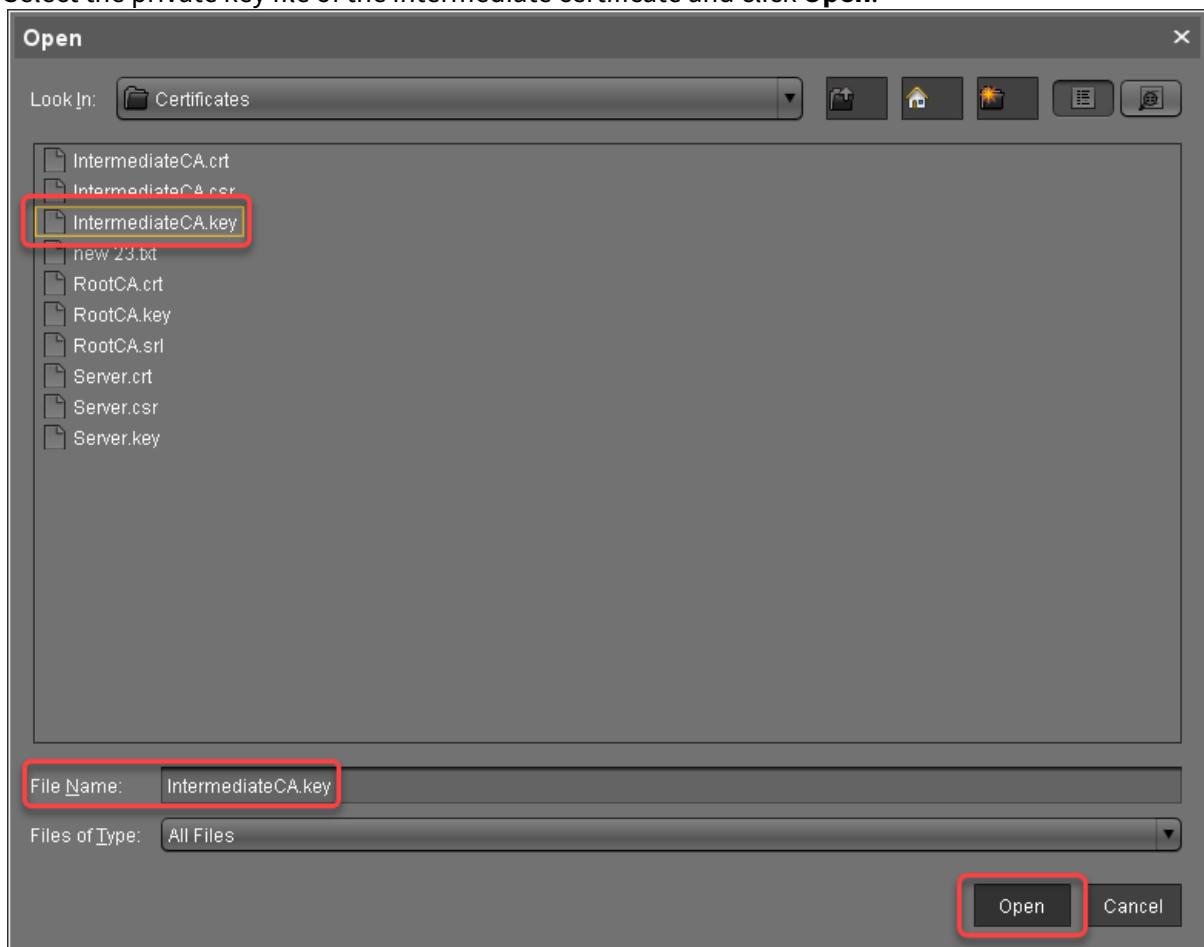
The intermediate certificate is imported.



3. Select the intermediate certificate, open the context menu, and select **Import decrypted private key**.



4. Select the private key file of the intermediate certificate and click **Open**.



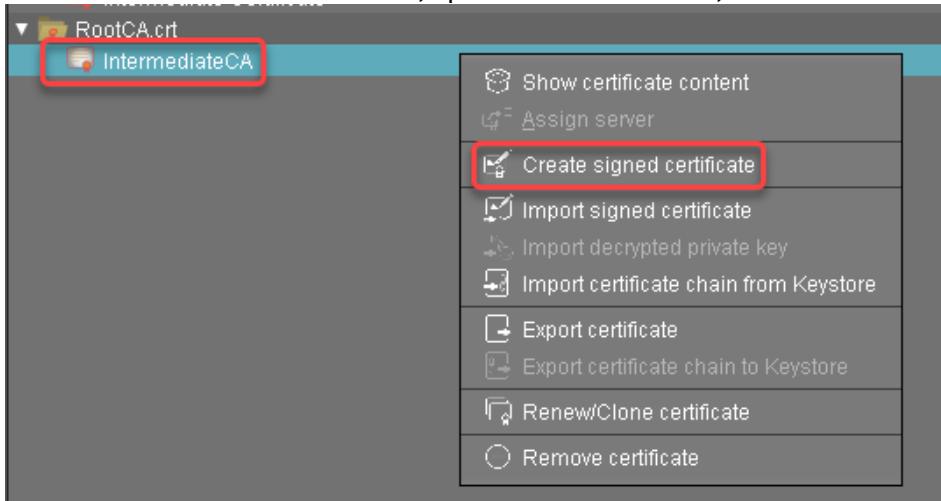
The private key of the intermediate certificate is imported.



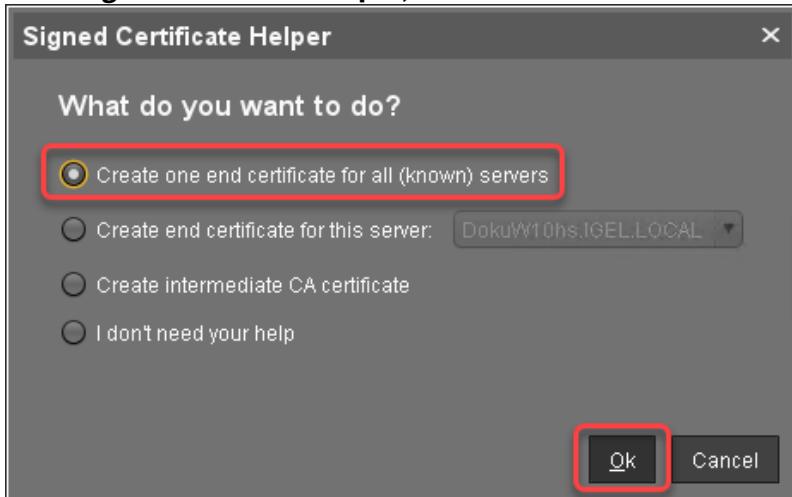
Creating End Certificates

Repeat the following steps for each server in your UMS environment:

1. Select the intermediate certificate, open the context menu, and select **Create signed certificate**.



2. In the **Signed Certificate Helper**, select **Create one end certificate for all (known) servers**.





3. In the dialog **Create Signed Certificate**, fill in the data as required.

Create signed certificate

Displayname	Server certificate
Your first and last name	Ike Igel
Your organization	My Company
Your locality (or random identifier)	Augsburg
Your two-letter country code	DE
Hostname and/or IP of certificate target server	Manage Hostnames
Key	RSA, 4096 bits Manage
Signature Algorithm	SHA256withRSA
Valid until	Oct 29, 2021
Certificate Type	<input type="radio"/> CA Certificate <input checked="" type="radio"/> End Entity
Ok Cancel	



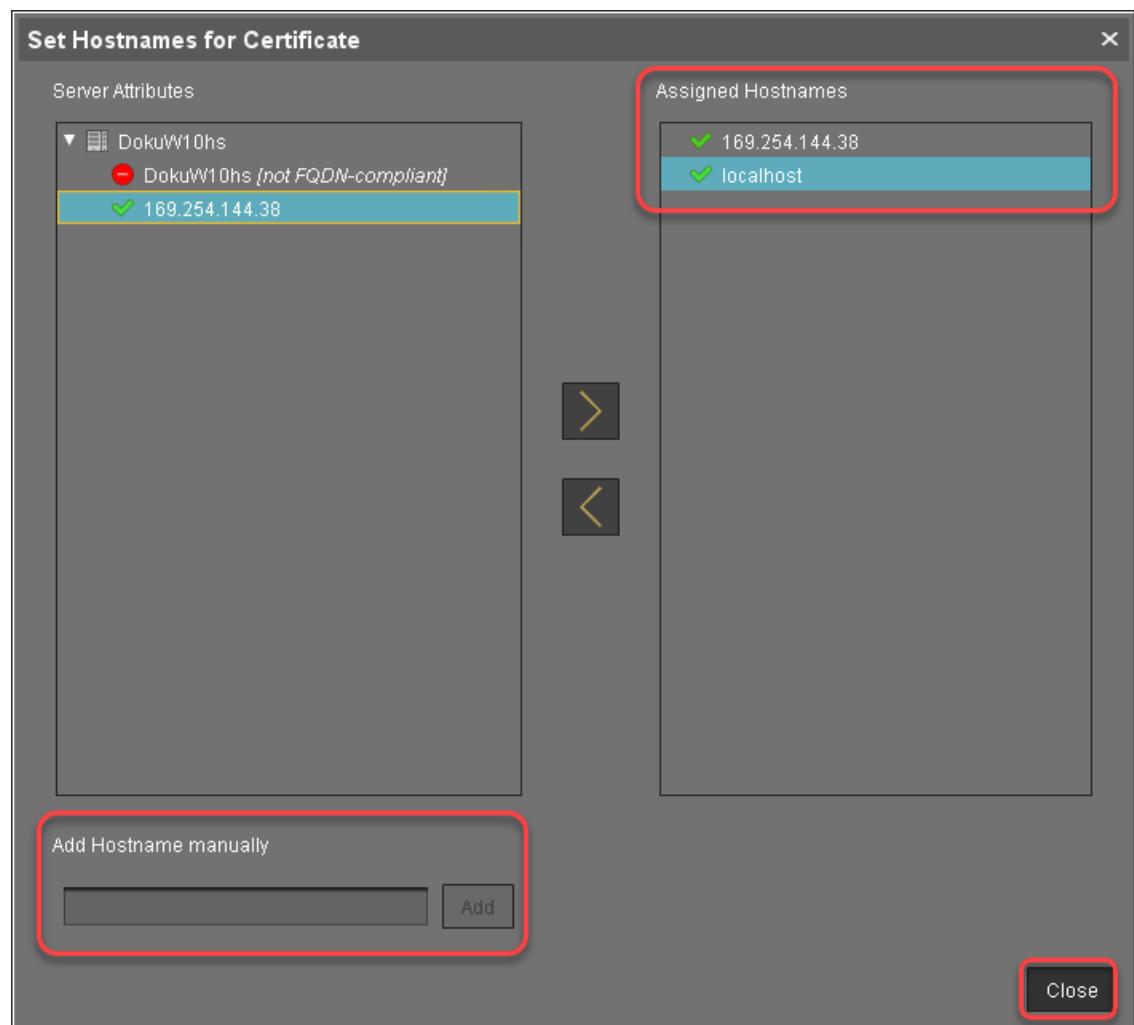
4. Click **Manage hostnames**.

Create signed certificate

Displayname	Server certificate
Your first and last name	Ike Igel
Your organization	My Company
Your locality (or random identifier)	Augsburg
Your two-letter country code	DE
Hostname and/or IP of certificate target server	Manage Hostnames
Key	RSA, 4096 bits
Signature Algorithm	SHA256withRSA
Valid until	Oct 29, 2021
Certificate Type	<input type="radio"/> CA Certificate <input checked="" type="radio"/> End Entity
Ok Cancel	

5. In the dialog **Set Hostnames for Certificate**, adjust the settings as follows:

- Check if "localhost" and all IP addresses and FQDNs (Fully Qualified Domain Names) under which your server is reachable are displayed under **Assigned hostnames**. If not, add the missing IP addresses and FQDNs under **Add hostname manually**.
- Remove all IP addresses and FQDNs you do not want to be part of the certificate.





6. Close the dialog **Create Signed Certificate** with **Ok**.

The dialog box contains the following fields:

- Displayname: Server certificate
- Your first and last name: Ike Igel
- Your organization: My Company (highlighted)
- Your locality (or random identifier): Augsburg
- Your two-letter country code: DE
- Hostname and/or IP of certificate target server: Manage Hostnames
- Key: RSA, 4096 bits
- Signature Algorithm: SHA256withRSA
- Valid until: Oct 29, 2021
- Certificate Type: End Entity (radio button selected)
- Buttons: Ok (circled in red), Cancel

The signed server certificate is created.

7. Continue with [Assigning all Servers to the Certificate](#)(see page 143).

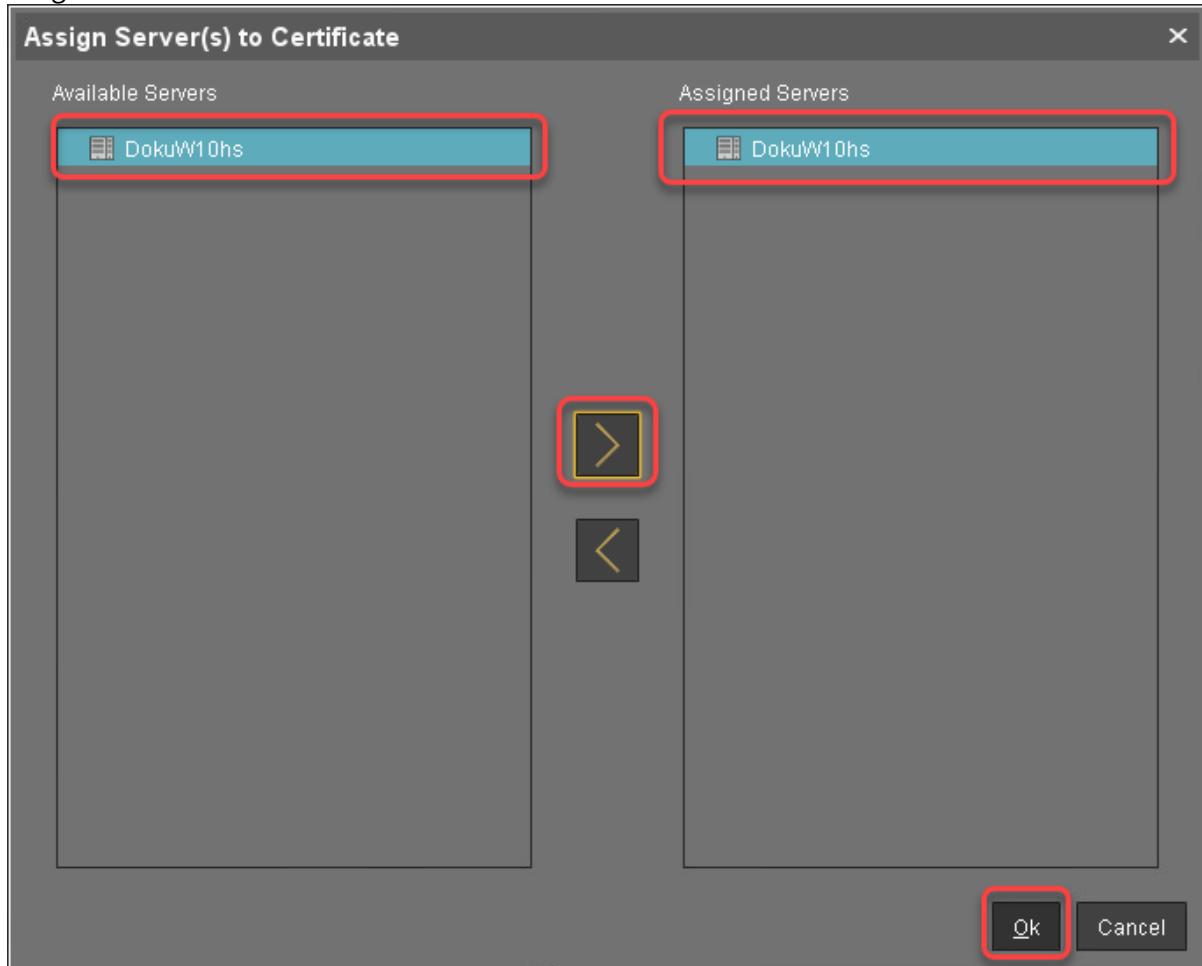
Assigning all Servers to the Certificate

1. Select the server certificate, open the context menu, and select **Assign server**.

The context menu options include:

- Show certificate content
- Assign server** (highlighted)
- Create signed certificate
- Import signed certificate
- Import decrypted private key
- Import certificate chain from Keystore
- Export certificate
- Export certificate chain to Keystore
- Renew/Clone certificate
- Remove certificate

2. Assign all servers to the certificate.



1.6.8 Wake on LAN

- [Deploying a Wake on LAN Proxy for Distributed Environments](#)(see page 144)
- [Distributing Wake on LAN Packets](#)(see page 150)
- [Use a WoL Proxy for Waking up Devices](#)(see page 151)

Deploying a Wake on LAN Proxy for Distributed Environments

Problem

The UMS is residing outside the network which contains your devices, so it cannot wake up your devices by Wake on LAN.

Goal

You want the UMS to wake up your devices from outside their network.



Solution

If you are using UMS version 5.02.100 or higher and devices running Linux version 5.09.100 or higher, you can make a device act as a proxy which sends the Wake on LAN packets on behalf of the UMS.

Defining Devices as Wake on LAN Proxy

You can define one or more devices as a Wake on LAN proxy.

To define a device as a Wake on LAN proxy:

1. Logon to the UMS console.
2. Go to **UMS Administration**.
3. Select **Wake on LAN**.

The screenshot shows the UMS Administration interface with the 'Wake on LAN' section selected. The main panel displays configuration options for sending magic packets to specific devices or subnets. It includes checkboxes for Broadcast address, Last known IP address of the device, Automatic Wake On LAN Proxy Detection, and All defined subnets. Below these are tables for defining subnets (with a single entry of CIDR 0) and network masks (empty). At the bottom, there is a table for Dedicated Wake On LAN Proxies (also empty).

Subnet	CIDR	Comment
	0	

Network Mask	Comment

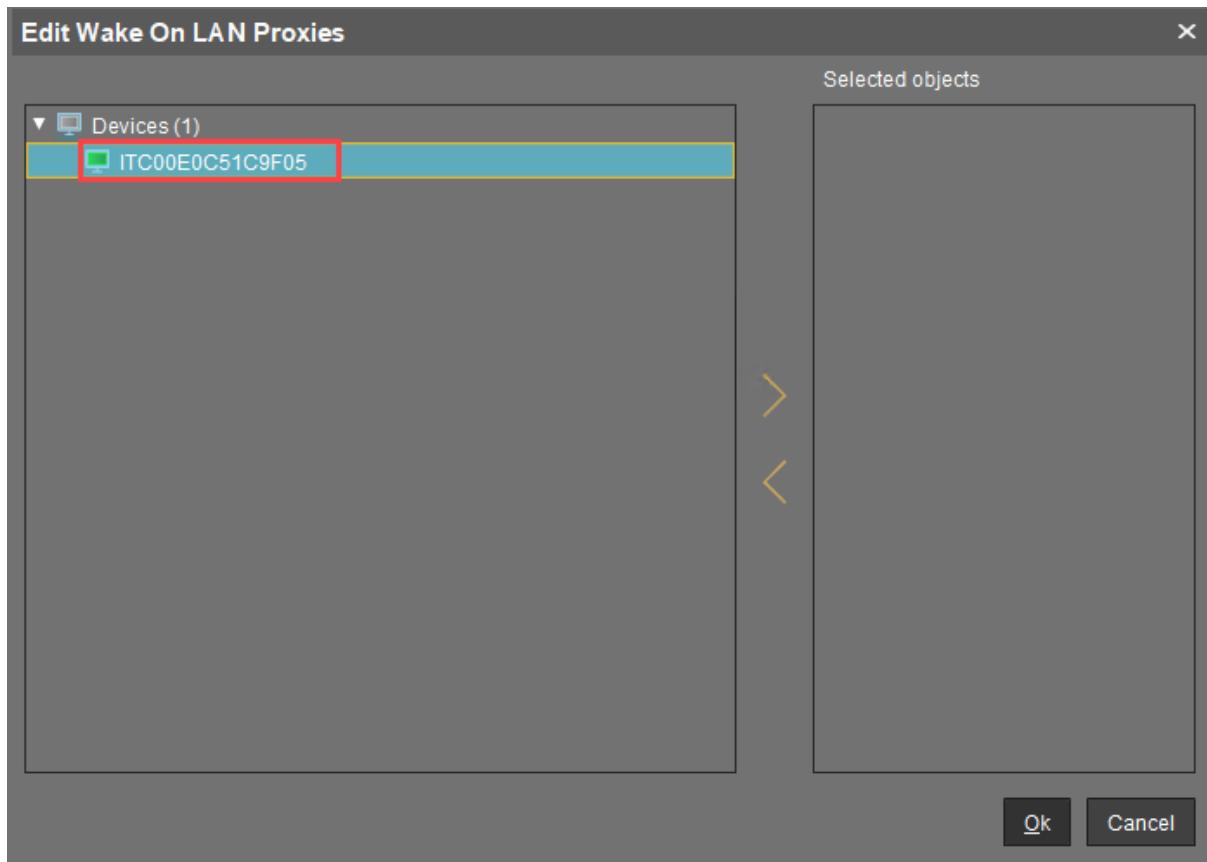
Name	MAC	Last Known IP Address

4. Activate **Dedicated Wake on LAN Proxies**.

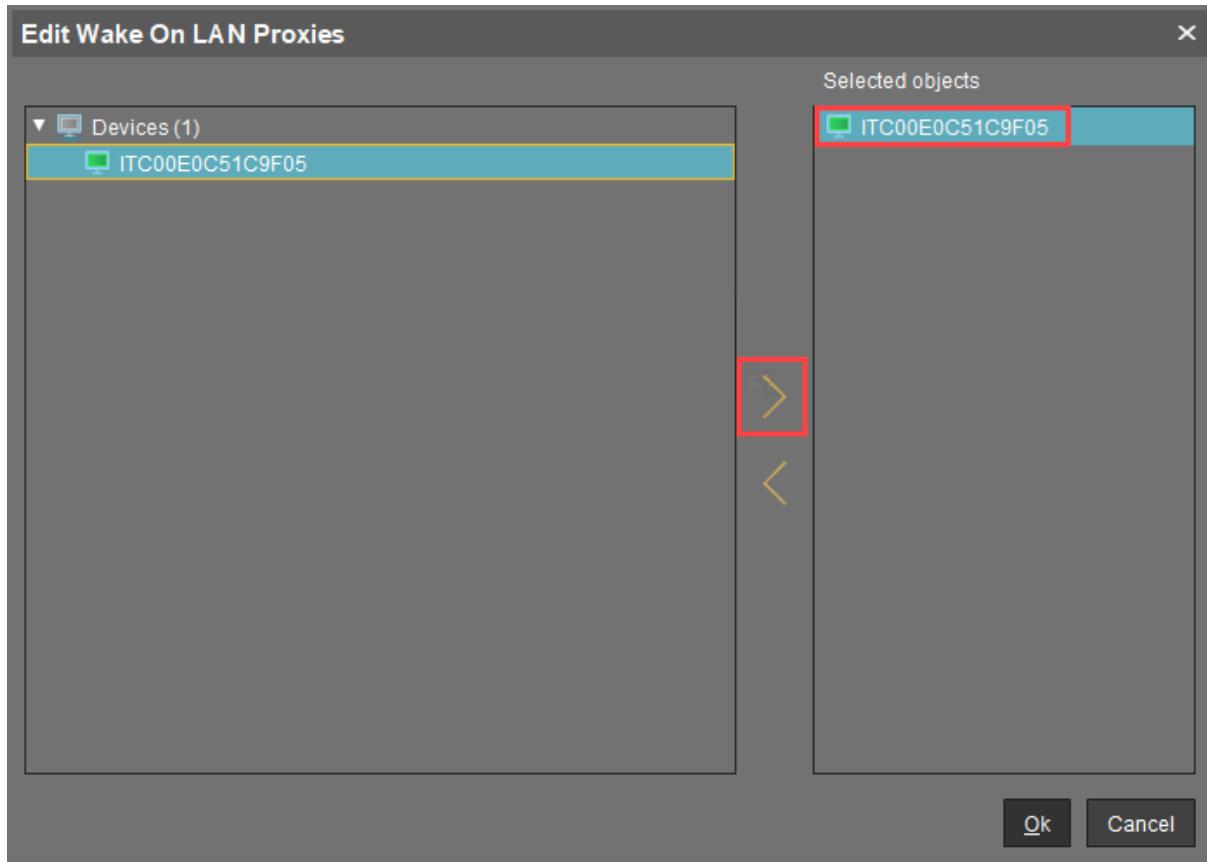
A screenshot of the IGEL Universal Management Suite 6 software interface. The window title is "IGEL Universal Management Suite 6" and the sub-title is "Server - 172.30.91.30". The left sidebar shows a tree view of "UMS Administration" with various sub-options like UMS Network, Global Configuration, Licenses, Mobile Devices, Certificate Management, Device Network Settings, Server Network Settings, Cloud Gateway Options, Device Attributes, Administrative Tasks, Proxy Server, Default Directory Rules, Universal Firmware Update, and Wake on LAN. The "Wake on LAN" option is selected and highlighted with a blue bar. The main panel is titled "Wake On LAN Configuration" and contains sections for "Send the 'magic packet' to ...", "Subnet" (with CIDR 0), "Network Mask", and a table for "Dedicated Wake On LAN Proxies" which is currently empty. A note says "Connected to 172.30.91.30 as admin".

Connected to 172.30.91.30 as admin

5. Click .
- The dialog **Edit Wake ON LAN Proxies** opens.
6. Select the device you want to use as a Wake on LAN proxy.



7. Click .
The selected device is listed under **Selected objects**.



8. Click **Ok**.

The selected device is configured as a Wake on LAN proxy. In the device's registry, the **parameter system.remotemanager.wol_proxy.enabled** is set to true.

i A device that is configured as a Wake on LAN proxy cannot be set to standby or shut down. This lock is in effect as soon as the device has received its settings from the UMS.

Removing a Wake on LAN proxy

You can remove the Wake on LAN proxy function from a device.

To define one or more devices as Wake on LAN Proxy:

1. Log in to the UMS Console.
2. Go to **UMS Administration**.



3. Select **Wake on LAN**.

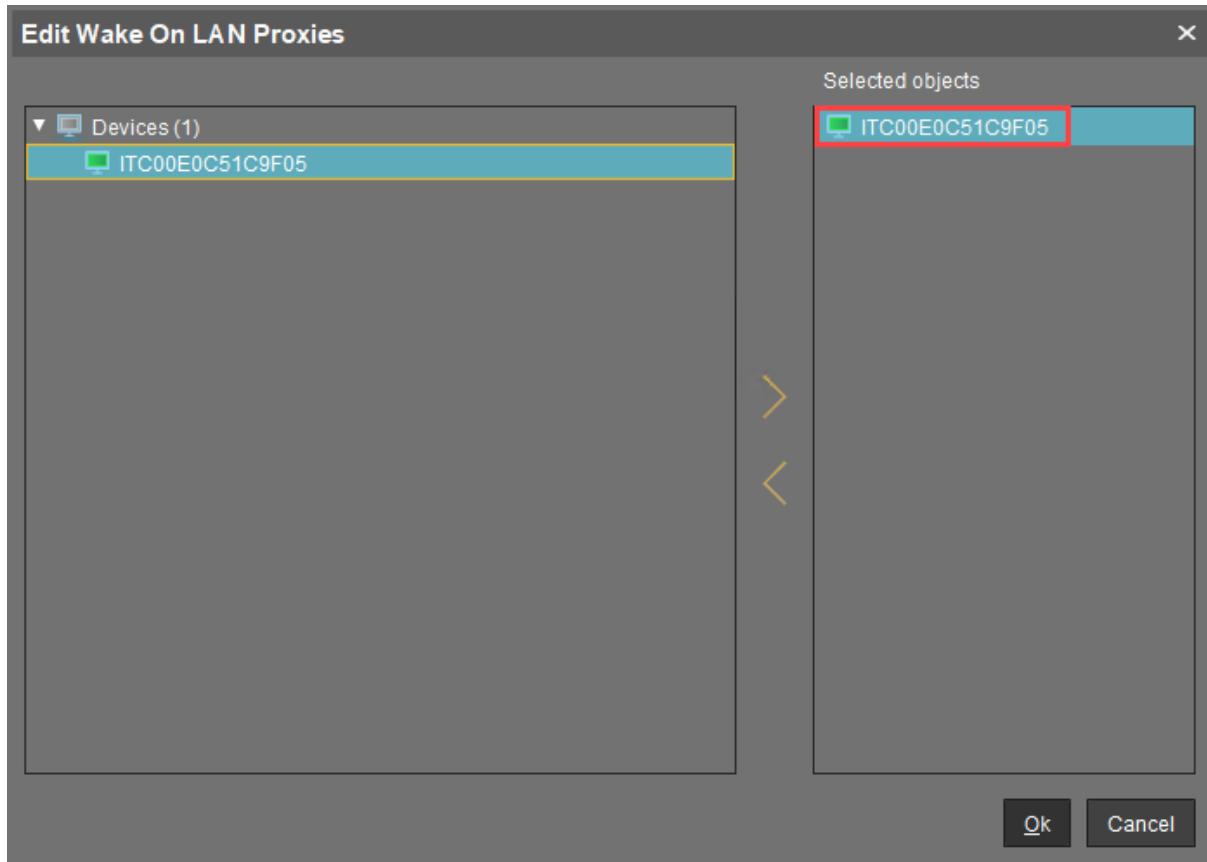
A screenshot of the IGEL Universal Management Suite 6 software interface. The window title is "IGEL Universal Management Suite 6". The menu bar includes "System", "Edit", "Devices", "Misc", and "Help". Below the menu is a toolbar with various icons. The left sidebar is titled "Server - UMS Administration" and contains a tree view with nodes like "UMS Network", "Server", "Global Configuration", "Licenses", "Mobile Devices", "Certificate Management", "Device Network Settings", "Cloud Gateway Options", "Device Attributes", "Administrative Tasks", "Proxy Server", "Default Directory Rules", "Universal Firmware Update", and "Wake on LAN". The "Wake on LAN" node is highlighted with a blue selection bar. The main content area is titled "Wake On LAN Configuration" and contains sections for "Send the 'magic packet'" to ... (with checkboxes for "Broadcast address", "Last known IP address of the device", "Automatic Wake On LAN Proxy Detection", and "All defined subnets"), "Network address of last known IP address" (with a table for "Subnet" and "CIDR"), "Network Mask" (with a table for "Network Mask" and "Comment"), and "Dedicated Wake On LAN Proxies" (with a table for "Name", "MAC", and "Last Known IP Address").

The "Wake on LAN" node in the sidebar is highlighted with a blue selection bar.

4. Click .

The dialog **Edit Wake ON LAN Proxies** opens.

5. Select the device you do not want to use as Wake on LAN proxy.



6. Click .
7. Click **Ok**.

The selected device is no longer configured as a Wake on LAN proxy. As soon as the device has received its settings from the UMS, it can be set to standby and shut down as normal. In the device's registry, the parameter **system > remotemanager > wol_proxy > enabled** is set to "false".

Distributing Wake on LAN Packets

IGEL UMS sends the magic packets as UDP datagrams to port 9. In order to work for different subnets, this has to be supported by the routers involved.

Wake on LAN settings can be configured in **UMS Console** under **UMS Administration > Global Configuration > Wake on LAN**.

UMS supports sending Wake on LAN magic packets to

- the broadcast address
- the last known IP address of the device
- all defined subnets
- the network address of the last known device IP address (define one or more network masks to be applied)



- a dedicated Wake on LAN proxy to wake up thin clients in another network; see [Use a WoL Proxy for Waking up Devices](#)(see page 151)

Use a WoL Proxy for Waking up Devices

You have the possibility to wake up devices even if they live in a different network that does not allow broadcast packets from the WAN. The trick is to set up one or more devices as Wake-on-LAN proxy. A device acting as a Wake-on-LAN proxy will never fall asleep itself, as its job is to listen to a special wake-up call from the UMS. This wake-up call tells the Wake-on-LAN proxy to send magic packets to all devices or a selection of devices in its network. To support this functionality, the Wake-on-LAN proxy device must have IGEL Linux version 5.09.100 or higher.

You can define a dedicated Wake-on-LAN proxy, or, alternatively, set the UMS to determine a Wake-on-LAN proxy automatically. However, the latter option cannot guarantee that a Wake-on-LAN proxy can be defined, as this depends on an appropriate device being online in the relevant subnet.

For detailed information, see the [Wake-on-LAN](#)(see page 495) chapter in the manual.

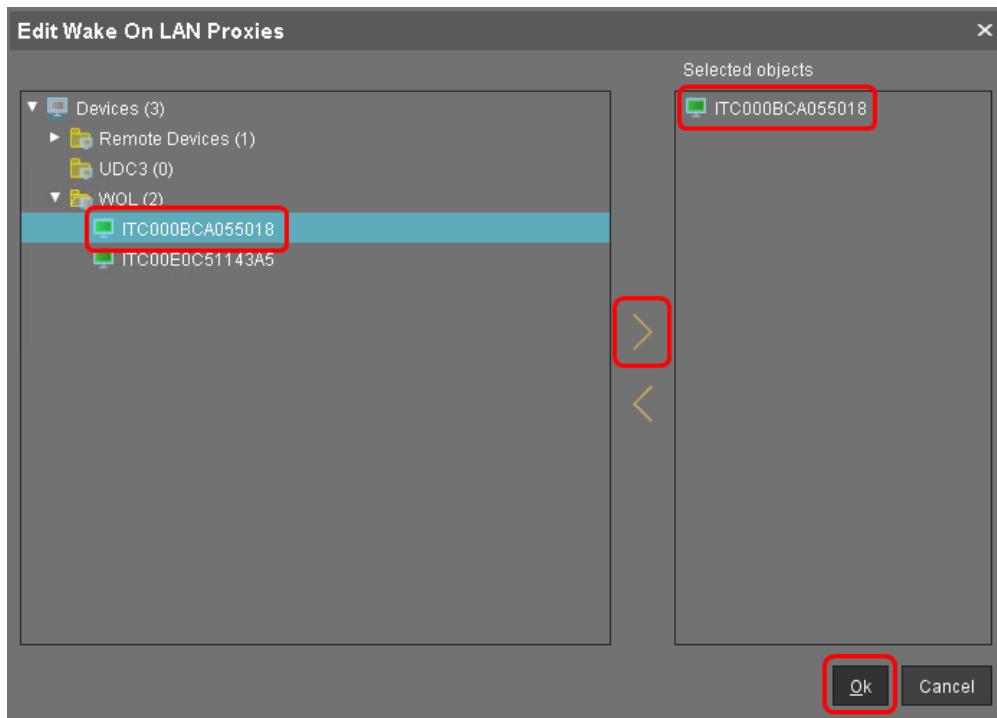
To define a dedicated Wake-on-LAN proxy:

1. Go to **UMS Administration > Global Configuration > Wake On LAN**.
2. Under **Send the "magic packet to ..."**, choose the address(es) to which the Wake-on-LAN proxies should send their wake-up calls.
3. Activate **Dedicated Wake On LAN Proxies**.

A screenshot of a software interface titled "Global Configuration" with a sub-section "Wake On LAN". At the top left, there is a checked checkbox labeled "Dedicated Wake On LAN Proxies". Below this, there is a table with three columns: "Name", "MAC", and "Last Known IP Address". In the top right corner of the table header, there is a small edit icon. The table is currently empty, showing no data rows.

Name	MAC	Last Known IP Address

4. In the area below **Dedicated Wake On LAN Proxies**, click on .
5. Highlight the desired device in the left-hand column.
6. Click on  to select the device.
7. Click on **OK**.



The device will now function as a Wake-on-LAN proxy.

- i A device that is configured as a Wake-on-LAN proxy can no longer be put on standby or shut down. This restriction applies as soon as the device receives the settings from the UMS.

- i As an alternative or parallel one can also use the **Automatic WoL Proxy Detection**. However, you cannot be sure that this proxy is always running, while the **Dedicated WoL Proxy** is always running.

1.6.9 Using an HTTP Proxy for Firmware Updates in UMS

Symptom

You want UMS to download firmware updates from the Internet.

Problem

Internet access is only available via an HTTP proxy in your environment.

Solution

Configure an HTTP proxy for firmware downloads in UMS:



1. In UMS Console, go to **UMS Administration > Global Configuration > Universal Firmware Update**
2. Click **Edit Proxy Configuration**

Universal Firmware Update

Universal update settings
The IGEL Universal Firmware files are downloaded from: 'dcjava'.

Proxy Server

Connection test

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

Host	<ftpServername>
Port	21
User name	<ftpUser>
Password	*****
Directory	<ftpServerpath>
Connection test	

The **Edit Proxy Configuration** dialog opens.

3. Check **Use proxy for HTTP connection to firmware update server**.

4. Enter the **Proxy-Host** name or IP address.
5. Enter the proxy host **Port**.
6. Enter the proxy **User**.
7. Enter the proxy **Password**.
8. Click **Save**.

The dialog closes.

9. To test the connection via the proxy, click **Test Server Connection**.

A green bar signifies success, if the bar is red, review your proxy configuration and test again.

Universal Firmware Update

Universal update settings
The IGEL Universal Firmware files are downloaded from 'http://myigel.biz'

Connection Test Result **Connection successfully tested !**



1.6.10 UMS Cannot Contact Download Server Any More

Symptom

After the UMS has been updated to version 6.03.130 or higher, it can not reach the download server anymore.

Environment

- UMS 6.03.130 or higher

Problem

From UMS 6.03.130 onwards, the UMS contacts <https://fwus.igel.com> (port 443) instead of <http://fwu.igel.com> (port 80). This may be blocked by a firewall.

Solution

- ▶ Allow <https://fwus.igel.com> (port 443) in your firewall.

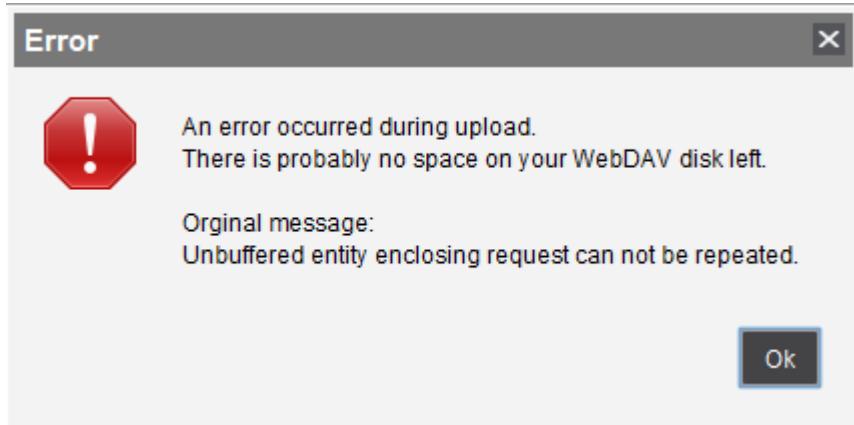
1.6.11 Error During Firmware Upload in UMS: No Space on WebDAV

⚠ 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

When importing a firmware into the UMS, the following error message appears:



An error occurred during upload.
There is probably no space on your WebDAV disk left.

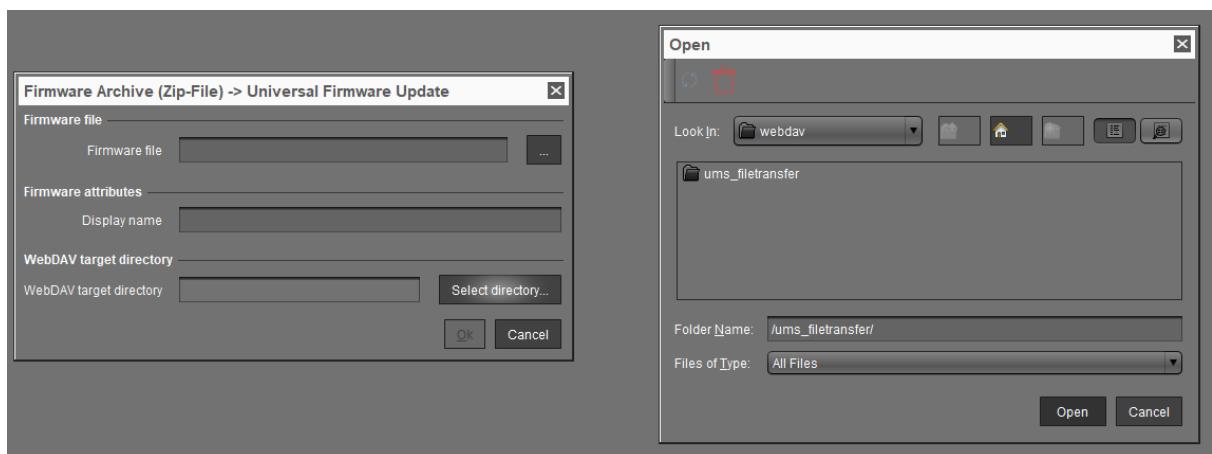
Original message:
Unbuffered entity enclosing request can not be repeated.

Cause

This error is caused when a file is being imported into a WebDAV folder which has no available space remaining.

Solution

1. Check that the host system of the UMS Server has available storage.
2. Ensure that the **ums_filetransfer** folder is selected during the firmware import process:





1.6.12 How to Check the Current State of the IGEL UMS Server through Your Existing Monitoring Solution

IGEL Universal Management Suite (UMS) includes a monitoring endpoint solution, which you can integrate into your existing monitoring infrastructure (e.g. Nagios, SolarWinds, Paessler, Logic Monitor, Sensu, etc.). With the monitoring endpoint, you can check the process/service states for the IGEL UMS Server and, thus, react accordingly if any problems are detected.

IGEL Environment

- IGEL UMS 6.09.100 or higher

How to Request the Current Status of the UMS Server

► Use the following requests to check the status of the UMS Server. If you use a browser for this purpose and the UMS deploys a self-signed certificate, the browser may display a security/certificate warning. Accept the risk and continue, or make the certificate known to the browser.

`https://[server]:[web_server_port]/ums/check-status`

OR

`http://[server]:[jws_server_port]/ums/check-status`

The following responses are possible:

1. If the (check status) service is up and running, HTTP status code 200 is returned. The response body contains a JSON document with information on the UMS Server status:
`{"status": "init|ok|warn|err"}`

For the details, see [Monitoring the UMS Server: Possible Statuses](#)(see page 157) below.

Example:

A screenshot of a web browser window. The address bar shows the URL `https://:8443/ums/check-status`. A red warning icon and the text "Not secure" are displayed next to the address. The main content area of the browser shows the JSON response: `{"status": "ok"}`.

2. If the check status service is not reachable, HTTP status code 404 is returned.
3. Other common HTTP status codes indicating standard HTTP errors might occur.



- i** Note that the status of the server updates every minute. For performance reasons, the status is NOT recalculated on each monitoring request, i.e., if a monitoring request is received, but a one-minute interval is not over, the previously saved server status will be shown.

Monitoring the UMS Server: Possible Statuses

The response statuses returned during the monitoring of the UMS Server indicate the following situations:

ok	The server is up and running.
warn	<ul style="list-style-type: none"> • The server is in HA(see page 657) update mode; see Updating the Installation of an HA Network(see page 671). • The server is not connected to one or more configured IGEL Cloud Gateways; see Connecting the UMS to the ICG²⁰. • Certificates used for communication with endpoint devices(see page 453), i.e., certificates of the tc.keystore file, are not in sync with the database. This might happen, for example, if you make changes to certificates and the automatic synchronization stops functioning due to some network issues or if the IGEL network token differs between the components, e.g., when a wrong network token was chosen during the server installation.
err	<ul style="list-style-type: none"> • There is no database connection – no database is configured, or the database connection has failed. For where to configure the database, see How to Set Up a Data Source in the IGEL UMS Administrator(see page 543). • The device communication port is not ready. For where to configure the device communication port, see Settings for IGEL UMS Administrator(see page 530); for details on UMS ports, see UMS Communication Ports(see page 48).
init	<p>Server initialization has not been completed yet.</p> <p>Note: If the initialization process is not finished within 120 seconds, the status automatically changes to err.</p>

Related Topics

[How to Monitor the IGEL Cloud Gateway²¹](#)

[Monitoring Device Health and Searching for Lost Devices\(see page 177\)](#)

[UMS HA Health Check\(see page 688\)](#)

1.7 High Availability

- [New Installation of an HA Network\(see page 158\)](#)

²⁰ <https://kb.igel.com/display/igelicg204/Connecting+the+UMS+to+the+ICG>

²¹ <https://kb.igel.com/display/igelicg204/How+to+Monitor+the+IGEL+Cloud+Gateway>



- Load Balancer Is Not Stopping during the Update of the HA Installation(see page 158)
- How to Detect Which Files Are Synchronized Automatically(see page 159)
- Load Distribution with a Number of Load Balancers(see page 162)
- License Error Because HA Servers Are out of Sync(see page 163)
- Manual Synchronization of the UMS Licensing ID(see page 164)
- Error Message When Switching Back from an Externally Signed CA to the Internal CA(see page 169)

1.7.1 New Installation of an HA Network

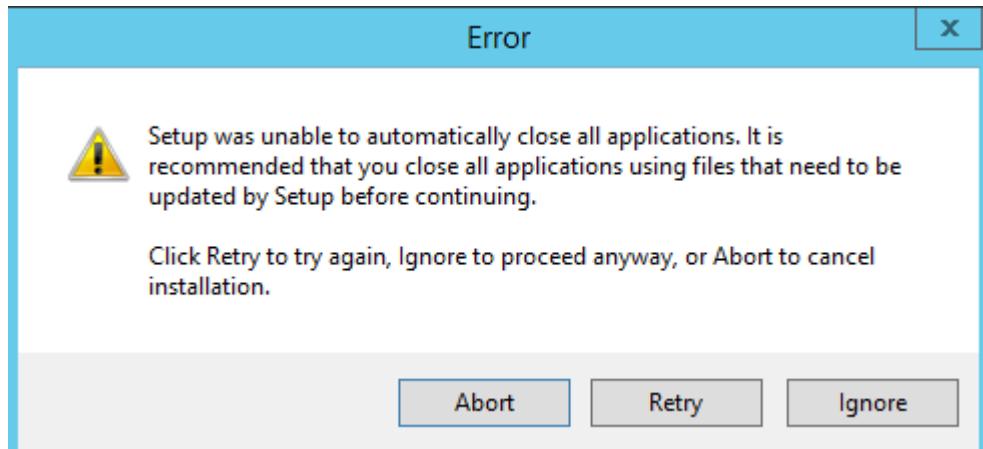
For installation requirements and details on how to install the High Availability Extension, see [HA Installation\(see page 660\)](#).

This page is due for deletion. Please check the above link and use it in the future.

1.7.2 Load Balancer Is Not Stopping during the Update of the HA Installation

Symptom

When updating the High Availability (HA) installation, an error message appears saying that not all applications could be closed before the update. A retry does not solve the problem.



Environment

- UMS HA installation

Problem

The load balancer does not stop and stays in the "Stopping" mode:



Services					
Name	Description	Status	Startup Type	Log On As	
IGEL UMS Load Balancer	IGEL Universal Management Suite - High-Availability-Network Load Balancer	Stopping	Disabled	Local System	
IGEL IKE and IPsec Keying...	THE IGELKEY SERVICE HOSTS THE INTERNET KEY EXCHANGE (IKE) AND AUTHENTICATED INTERNET PROTOCOL SECURITY (IPSEC)...	Running	Automatic (Trigger Start)	Local System	
Interactive Services Detection	Enables user notification of user input for interactive services, which enables access to...	Manual	Local System		
Internet Connection Sharin...	Provides network address translation, addressing, name resolution and/or intrusion pr...	Disabled	Local System		

Solution

- Stop the load balancer manually and proceed with the update. For information regarding stopping the HA services, see [HA Services and Processes](#)(see page 691).

1.7.3 How to Detect Which Files Are Synchronized Automatically

Prerequisites

- A High Availability (HA) environment with UMS 6.06.100 or higher

General Overview

Following files are synchronized between the HA servers automatically:

- Files registered in the UMS Console

i Files that are not created as file objects in UMS, but only stored in the file system in `ums_filetransfer`, are NOT synchronized. For details on how/where you can create a file object, see [Registering a File on the UMS Server](#)(see page 430) and [Create Firmware Customization](#)(see page 376).
- The files of [Universal Firmware Updates](#)(see page 433) if the synchronization is enabled under **UMS Administration > Global Configuration > Universal Firmware Update** and a WebDAV directory is set as the target path for the download. For details, see the section "["Syncrhonization of Universal Firmware Updates](#)(see page 160)" below.

The objects are synchronized immediately – unless a UMS Server is temporarily unreachable. In that case, the synchronization takes place every 5 minutes or at server startup.

The synchronization applies to the file system and does not refresh the view in any UMS Console other than the one in which the object has been created. Thus, you may need to press [F5] or the refresh button to view the object in the UMS Console on the other server.

- ⚠** To avoid problems with your HA installation, make sure that the time on the servers of the HA network does not differ by more than one minute. After each manual time reset, the HA services on the relevant server must be restarted.



Synchronization of Universal Firmware Updates

To enable the automatic synchronization of the firmware updates between the HA servers, proceed as follows:

1. In the UMS Console, go to **UMS Administration > Global Configuration > Universal Firmware Update**.
2. Activate **Synchronize downloaded Universal Firmware Updates within UMS WebDAV directories**.

The screenshot shows the UMS Administration interface with the 'Universal Firmware Update' section selected. The 'Universal update settings' panel contains a checkbox labeled 'Synchronize downloaded Universal Firmware Updates within UMS WebDAV directories', which is checked and highlighted with a red border. Below this, there are fields for 'Proxy server' and 'Connection test'. Under 'The FTP server settings where the files are downloaded to (optional)', there are fields for 'Protocol' (set to FTP), 'Host' (<ftpServername>), 'Port' (21), and 'User name' (<ftpUser>).

3. When adding a firmware update under **Universal Firmware Update > [context menu] > Check for new firmware updates**, set a WebDAV directory as a target path for the download.

The screenshot shows the 'Universal Firmware Updates' dialog. On the left, the navigation tree shows 'Universal Firmware Update (1)'. The main table lists several firmware updates, including IGEL UD LX, IGEL Zero, and IGEL OS 11 (IGEL M340C). The 'Target directory' column for the IGEL OS 11 entry is set to 'https://DokuW10rd.IGEL.LOCAL:8443/ums_filetransfer'. A red box highlights the 'Select the WebDAV target directory' button next to the 'Target directory' column header. At the bottom of the dialog, there is a checkbox for 'Show only latest firmware versions (hides already downloaded versions)' and two buttons: 'Download' and 'Cancel'.



When the download is complete, you can see under **Synchronization Status** the servers for which the firmware update has already been synchronized.

The screenshot shows the UMS Administration interface. On the left, there's a sidebar with various management options like Universal Management, Profiles, Firmware Customizations, Devices, Mobile Devices, Views, Jobs, Files, and Universal Firmware Updates. Under Universal Firmware Updates, several firmware versions are listed: IGEL OS 11-11.03.580, IGEL OS 11-11.04.130, and IGEL OS 11-11.04.200. The first one is selected. The main panel displays 'Firmware Update Settings' with fields for Host, Protocol (set to HTTPS (UMS WebDAV)), Port, Target URL, Snapshot file, User, and Password. Below that is the 'Download Status' section, which shows a progress bar at 'OK' and 'Finished'. The final section, 'Synchronization Status', lists two servers: miraculix4 and miraculix6, both of which show 'Firmware Update is present' with green checkmarks. This entire 'Synchronization Status' section is highlighted with a red box.

⚠ Universal Firmware Updates are synchronized between the HA servers only if **HTTPS (UMS WebDAV)** or **HTTP (UMS WebDAV)** is selected under **Protocol**. These protocols are used for transferring the firmware update files from the UMS WebDAV directory to the devices.

This is a close-up of the 'Firmware Update Settings' section. It shows the 'Host' field with the placeholder '<PUBLIC_ADDRESS/HOST>', the 'Protocol' field set to 'HTTPS (UMS WebDAV)' (which is highlighted with a red box), and the 'Port' field with the placeholder '<PUBLIC_WEB_PORT/WEB_PORT>'.

With any other protocol, firmware updates are not synchronized between the HA servers.

Connection Data Used during the Update

When a firmware update is assigned to a device, the connection information of the current server is sent to the device if the firmware update is present in the UMS WebDAV directory of the server. If the firmware update is absent for some reason, the connection information of a server with the firmware update available is sent.

The connection information contains

- a **Public Address** if it is configured for the server under **UMS Administration > UMS Network > Server** > [server's context menu] > **Edit**. Otherwise, the stored hostname is used.



- a **Public Web Port** if it is configured for the server under **UMS Administration > UMS Network > Server > [server's context menu] > Edit**. Otherwise, the stored web port is used.

Attribute	Value
Process ID	2e57d4f6-312d-4ab4-aac4-7c9395e13b49
Cluster ID	UMS-CLUSTER-63482-1602863384736-2-0
Version	6.06.100.mm4
Host	miraculix4
Last Known IP	Not set
Public Address	30002
Device Communication Port	8443
Web Port	Not set
Public Web Port	Windows Server 2019
Operating System	

Since the connection information is dynamically adjusted, **Host** and **Port** data are not editable for the downloaded firmware update (with the HTTP(S) (UMS WebDAV) protocol set):

Firmware Update Settings	
Host	<PUBLIC_ADDRESS/HOST>
Protocol	HTTPS (UMS WebDAV)
Port	<PUBLIC_WEB_PORT/WEB_PORT>
Target URL	/ums_filetransfer/IGEL_OS_11-11.04.200
Snapshot file	

1.7.4 Load Distribution with a Number of Load Balancers

If a UMS Server and Load Balancer are installed on a shared computer, the UMS Server communicates with the endpoint devices via port 30002, otherwise via port 30001 as is customary with a single server installation. The Load Balancer always communicates with the devices via port 30001.

Load distribution to the load balancers can be performed as follows. When booting, the devices attempt to establish contact with the UMS Server in this order:

- Name `igelrmserver` in the DNS (*Record Type A*)
- DHCP tag 224
- Local list of **Remote Management Servers** (in the specified order)

In a UMS High Availability network, the load balancers are automatically specified in the list of remote management servers in the local device configuration.

If the DNS entry `igelrmserver` or DHCP tag 224 is used in an HA network, the IP of a load balancer must be entered.

If neither this DNS entry nor the DHCP tag 224 is used, endpoint devices always connect to the first load balancer in the setup list, i.e. all devices are communicating with a single load balancer. The other load balancers are merely stand-bys and will be used only if the first load balancer in the list is not available.



To achieve load distribution between the load balancers, you can however use the DNS entry `igelrmserver` with a *Round Robin DNS*. To do this, the IP addresses of all load balancers are recorded in the DNS as a *Resource Record Set* for the `igelrmserver` entry (cf. http://en.wikipedia.org/wiki/Round-robin_DNS(see page 162)). The devices then connect randomly to one of the available load balancers, thus distributing the query load of all devices.

1.7.5 License Error Because HA Servers Are out of Sync

⚠ 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

HA servers are out of sync preventing devices from registering in the UMS and throwing a license error.

Environment

- High Availability (HA) environment
- Firmware version: any
- UMS version: 6.01 or higher

Problem

Devices are not able to register in the UMS. Licenses are applied correctly. 2 servers appear in sync and another one is out of sync.

Main UMS Licensing ID	MiIFWjCCA0..dyLq1mAtqI	Export UMS Licensing ID	
UMS Licensing ID status			
Hostname	UMS Licensing ID	UMS Licensing ID status	Server status
XRDCWTTCM/GD01B.hca.corpad.net	MiIFWjCCA0..dyLq1mAtqI	Main UMS Licensing ID	Running
XRDCWTTCM/GD01A.hca.corpad.net	MiIFWjCCA0..fDxCpGzZD	Not in sync, please restart server!	Running



License Type	Available Licenses	Used Licenses	License Status
UMS HA Extension	5	5	Not synchronized

License ID	License registered on	Quantity	Customer	Services	Category	Key	Expiration Date
B8e10a3-94c6-4a63-b3a6-02327a3cf08		5	IGEL built-in HA License	UMS HA Extension			

Solution

Issue is related to the UMS Licensing ID. A workaround / solution is to back up the UMS Licensing ID from the UMS Administrator and restore it to the out-of-sync server. See [Manual Synchronization of the UMS Licensing ID](#)(see page 164).

1.7.6 Manual Synchronization of the UMS Licensing ID

Overview

When the main UMS Licensing ID is not synchronized between the UMS Servers, **UMS Licensing ID status** under **UMS Administration > Global Configuration > Licenses** reads "Not in sync, please restart server", see [UMS Licensing ID](#)(see page 444). However, even when you restart the UMS Server, the UMS Licensing ID sometimes remains unsynchronized. In this case, the manual synchronization is required.

Environment

- UMS 6.01.100 or higher
- High Availability (HA) environment

Instructions

The manual synchronization of the UMS Licensing ID includes the following steps:

1. Locating the server holding the main UMS Licensing ID(see page 165)
2. Creating a backup of the UMS Licensing ID(see page 165) on that server
3. Restoring the created backup on all servers with the UMS Licensing ID unsynchronized(see page 167) and restarting all servers



Locating the Server Holding the Main UMS Licensing ID

To find out which server of the HA installation holds the **Main UMS Licensing ID**:

1. Open **UMS Console** and navigate to **UMS Administration > Global Configuration > Licenses > UMS Licensing ID**.
2. Find the server with **UMS Licensing ID status** saying "Main UMS Licensing ID".

Host name	Server status	UMS Licensing ID status	UMS Licensing ID	UMS Licensing ID fingerprint
DokuW10rd.IGEL.LOCAL	Running	Main UMS Licensing ID	MIIFWJCCA0..K7yZzhB5K	A9:10:D7:E2:9F:94:86:29:6F:9C:06:BA:89:E6:5F:21:4F:F6:98:09:4A:DC:7F:C5:AE:E0:65:84:27:57:17:12

Creating a Backup of the UMS Licensing ID

1. Open the [UMS Administrator](#)(see page 529) on the server with the main UMS Licensing ID you located in the previous step.

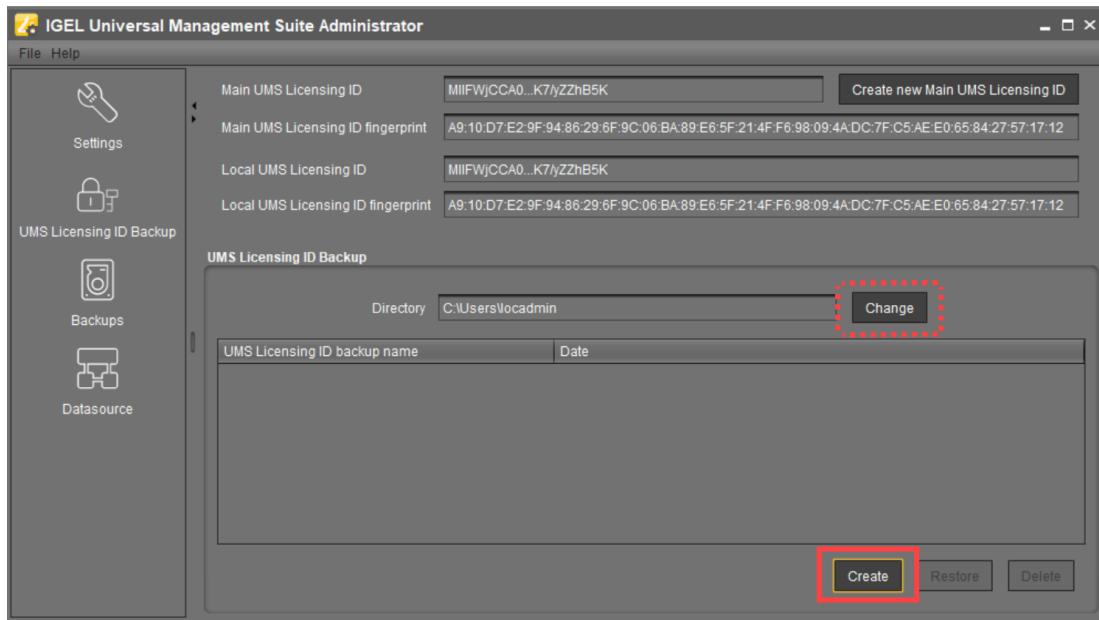
i Default path to the UMS Administrator:
 Linux: /opt/IGEL/RemoteManager/RMAdmin.sh
 Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe

2. Go to **UMS Licensing ID Backup**.

3. Click **Change** if you want to change the directory for storing the backup.

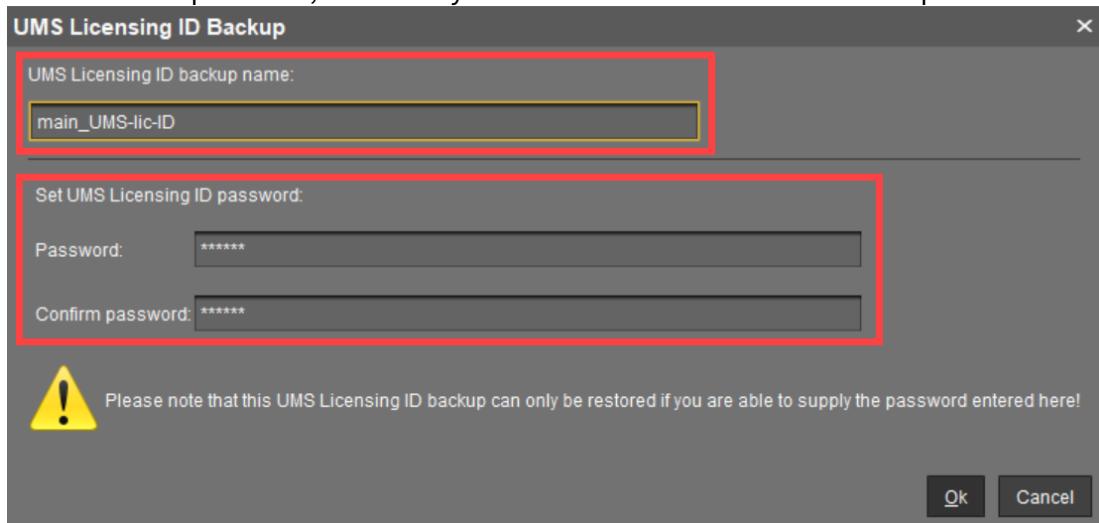


4. Click **Create.**



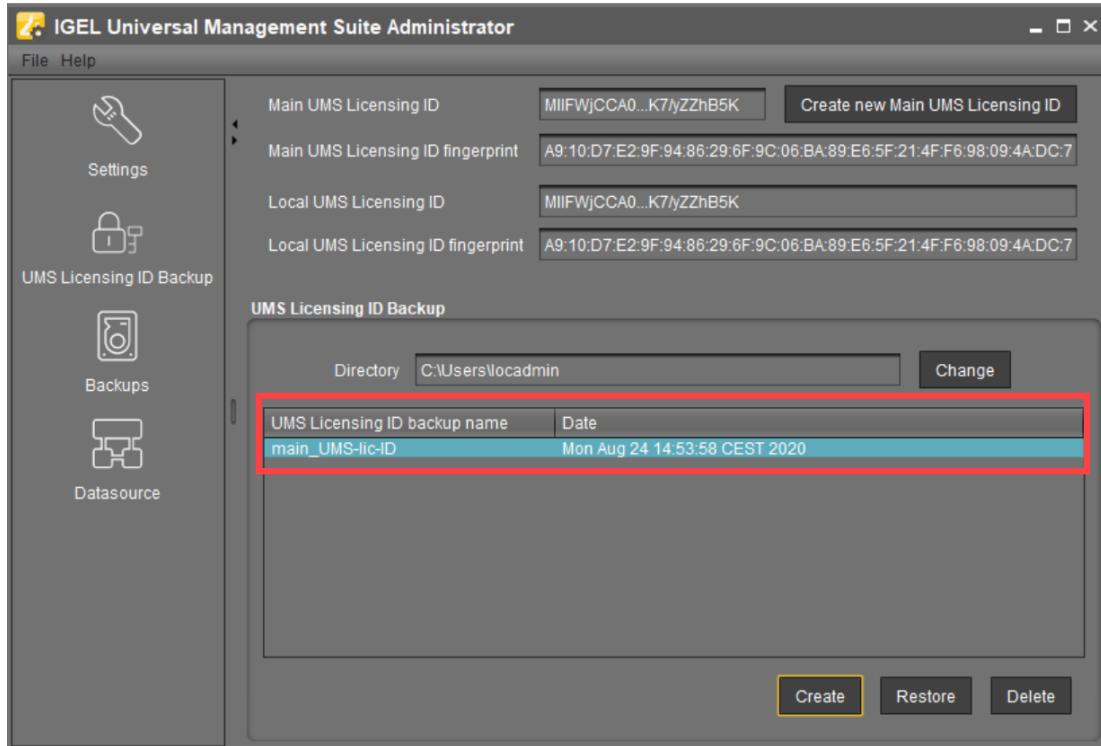
The **UMS Licensing ID Backup** dialog opens.

5. Under **UMS Licensing ID backup name**, specify a name for the backup.
6. Under **Set UMS Licensing ID password**, specify a password for the backup and confirm it. Remember the password, otherwise you won't be able to restore the backup.



7. Click **Ok**.

The backup has been created.



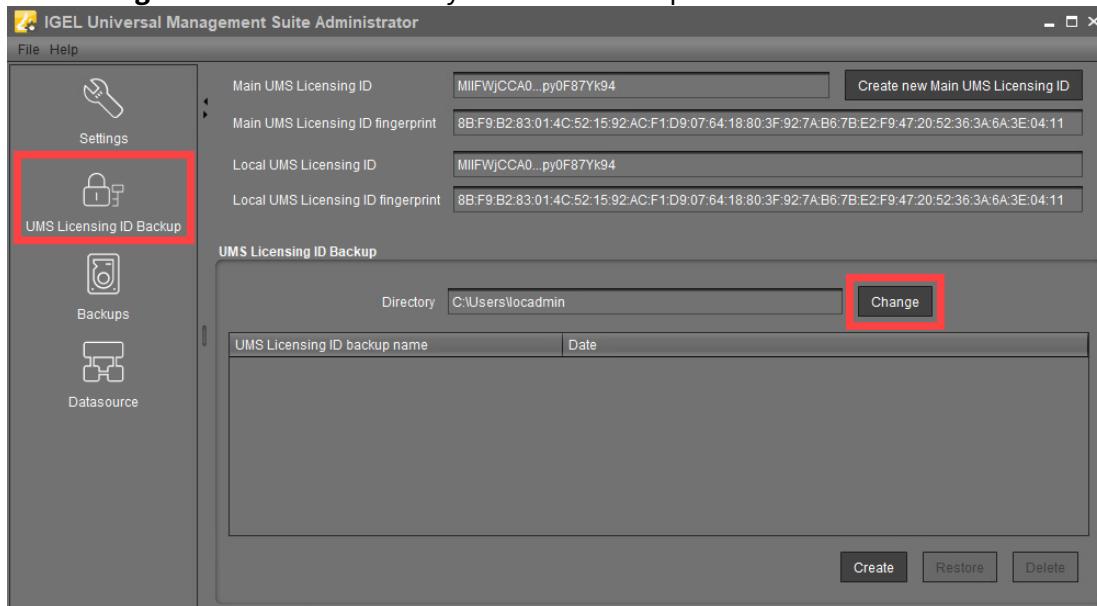
8. Transfer the created backup to every server where the UMS Licensing ID is not in sync.

Restoring the Backup on All Servers with the UMS Licensing ID Unsynchronized

1. Open the UMS Administrator > **UMS Licensing ID Backup** on every server where the UMS Licensing ID is not in sync.

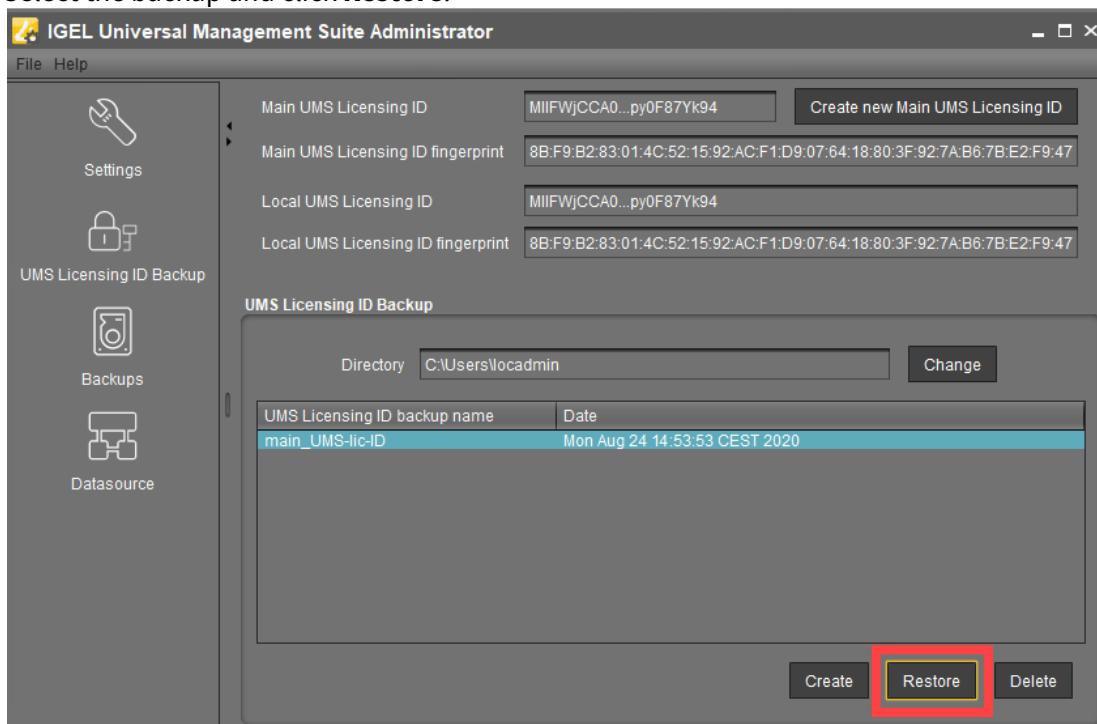


2. Click **Change** and select the directory where the backup was saved.



The backup appears in the list of the available UMS Licensing ID backups.

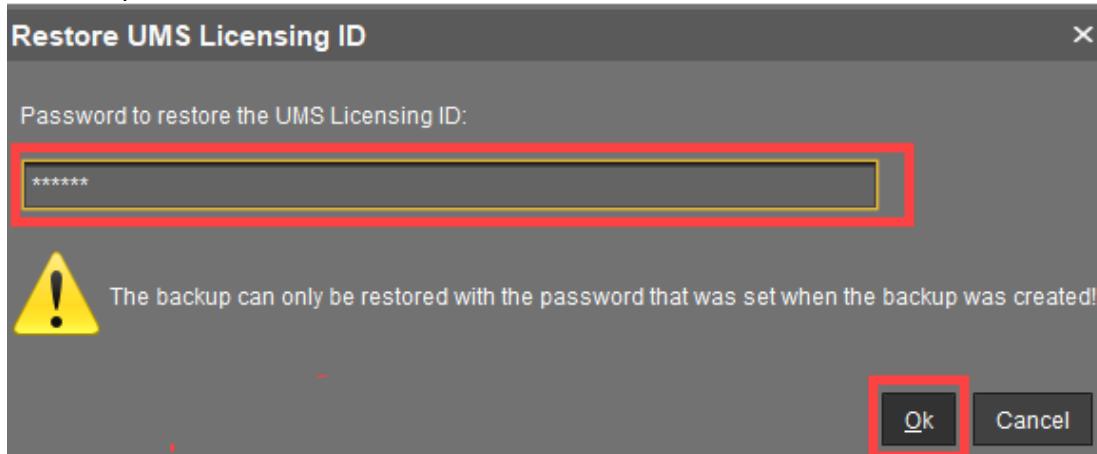
3. Select the backup and click **Restore**.



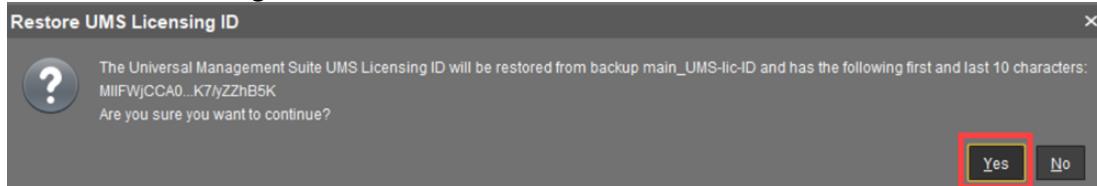
The **Restore UMS Licensing ID** dialog opens.



4. Enter the password and click **OK**.



5. Confirm the restoring.



6. Repeat the procedure for all servers with the UMS Licensing ID unsynchronized.
7. When the backup restoring procedure is complete, restart all servers if you have not yet done so.
In the UMS Console, the **UMS Licensing ID status** under **UMS Administration > Global Configuration > Licenses > UMS Licensing ID** should show that the UMS Licensing ID is now synchronized on all servers.

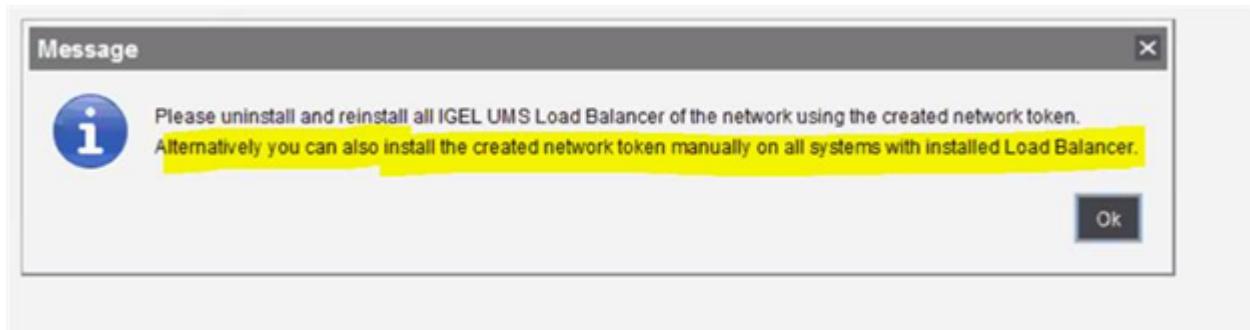
1.7.7 Error Message When Switching Back from an Externally Signed CA to the Internal CA

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

After testing externally signed CA, if switch back to the internal one, an error message will come up:



Environment

- UMS HA; UMS version: any

Solution

1. Run the installer again.
2. Choose **Repair**.
3. Point to the HA 'token' / certificate and install it that way.

1.8 Device

- [Device Scan or Online Check fails](#)(see page 170)
- [Registration of a Device fails](#)(see page 171)
- [Device Registration fails with Error Message: Unexpected end of input stream](#)(see page 172)
- [Device Registration Behind SonicWall Firewall Fails](#)(see page 173)
- [Renaming IGEL OS Devices](#)(see page 173)
- [Changing the Hostname of an Endpoint Device via UMS](#)(see page 176)
- [Monitoring Device Health and Searching for Lost Devices](#)(see page 177)

1.8.1 Device Scan or Online Check fails

Symptom

Although a device responds to a ping command, it does not appear in the UMS Console's list of scanned devices, can not be registered or shows up as offline (red) in the UMS Console's navigation tree.

Problem

The packets for scanning the devices or checking their online status are getting blocked within the network, e.g. by a firewall or VPN.



Solution

Make sure UDP packets on port 30005 are not blocked within your network. Those packets are used for both, scanning for devices as well as checking the status of the clients.

See also [IGEL UMS Communication Ports](#)(see page 48).

1.8.2 Registration of a Device fails

Symptom

Although a device can be scanned from the console, it cannot be registered on the server. One of the following error messages will appear in the UMS console:

- Cannot connect to remote management server
- Protocol state invalid

Problem

This may be caused by

- the server's firewall blocking the process.
- an already existing UMS certificate on the device.
- some database service hanging.
- network transfer delays or losses affecting the registration process.

Solution

Solving the firewall problem:

1. On your system running the UMS console and server add the following port to the Windows firewall as an exception:
 - **Name** = IGEL_RMGUIServer
 - **TCP Port** = 30001

i If you have changed the standard port 30001 in the UMS administrator, open the firewall accordingly for this port.

2. Make sure no other firewall within the network is blocking ports 30001 and 30005.
3. Try to import the device again.

Solving the certificate problem:

- Reset the device to factory defaults and try to import the device again.



Solving the database problem:

- ▶ In UMS Administrator disable the currently active data source and re-activate it again. Try to import the device again.

Checking the network:

- ▶ Check if the network is fine by sending pings from the device console to your UMS server:

```
ping -s -c 10 -M do
```

Start with SIZE =1500 and decrease the size of packages until all packages got transferred without fragmentation or package loss. 1440 / 1400 / 1350 / 1300 are good values to test with.

- ⓘ On a device with IGEL Linux you can use the built-in network tools as well for "pinging" the server (**Starter for Sessions > System > Network Tools**).

See also [UMS Communication Ports](#)²².

1.8.3 Device Registration fails with Error Message: Unexpected end of input stream

Symptom

UMS console shows an error message like "Unexpected end of input stream found at ..." during registration of devices.

Problem

Devices cannot register with UMS over a remote link via VPN gateway, router, firewall or other networking device due to issues with large packets.

The error may occur even if there is no NAT used and the networking device seems to be configured correctly so e.g. pinging is successful in both directions.

Solution

Please consult the documentation for your network device and look up the options for handling large packets. In the case of SonicWall devices the solution is setting the `Ignore Don't Fragment Bit` option.

²² <https://kb.igel.com/display/endpointmgmt601/IGEL+UMS+Communication+Ports>



1.8.4 Device Registration Behind SonicWall Firewall Fails

Symptom

The devices are detected by the UMS during a scan, but registration fails. UMS console shows an error message like "Unexpected end of input stream found at ...".

Possible Causes

The following causes have been reported with firewalls by SonicWall;

- Large packets: See [Thin Client Registration fails with Error Message "Unexpected end of input stream"](#) (see page 172).
- SonicWall DPI-SSL replaces the UMS certificate: If SonicWall DPI-SSL is enabled, it functions as intermediate CA and sends its own certificate to the devices instead of the original UMS certificate. As a consequence, the devices refuse to register because they would only accept the original UMS certificate.

Solution

1. In SonicWall, under **DPI-SSL Status**, add the IP address of the UMS server to the list of DPI-SSL exclusions.
2. Restart the VPN tunnel.

1.8.5 Renaming IGEL OS Devices

By default, if no naming convention is activated and the original hostname of the IGEL OS device has not been changed, the name a device gets upon registration in the UMS is composed of the prefix “ITC” (“TC-”, in the case of import with the serial number) and the MAC address of the device.

Example: ITC00E0C520XXXX; TC-00E0C520XXXX

- i** Before renaming/registering the devices, it is recommended, first of all, to pay attention to the following settings in **UMS Console > UMS Administration > Global Configuration > Device Network Settings > Adjust Names of Devices**. Activate them according to your needs:

UMS Administration

(Additional requests that exceed the queue size should be rejected.)

Adjust Names of Devices

Adjust UMS-internal name if network name has been changed
 Adjust network name if UMS-internal name has been changed

Naming Convention

Enable naming convention for new devices



Renaming upon Registration

Option 1: Via UMS Console > Device Network Settings > Naming Convention

1. Before registering the devices, activate and define **Naming Convention** in the UMS under **UMS Administration > Global Configuration > Device Network Settings**, see [Device Network Settings](#)(see page 457).
2. If the network name, i.e. terminal name, of the device, should be adjusted, enable **Device Network Settings > Adjust network name if UMS-internal name has been changed**.
3. Save the changes.

 **Tip**

If the network name remained unchanged after the device registration is complete, click **Other commands > Settings UMS->Device** from the device's context menu.

Option 2: Via UMS Console > System > Import > Import Devices (Short or Long Format Only) If the Required Names Are Preliminarily Defined in the Import File

If the **Naming Convention** option does not suit your needs, you can import the devices with the names that fulfill your requirements. For the general instruction, see [Importing Devices](#)(see page 308).

1. When preparing the import file, specify the required device names. See [Import with Short Format](#)(see page 309) or [Import with Long Format](#)(see page 309).
2. If the network name, i.e. terminal name, of the devices, should be adjusted, enable **UMS Administration > Global Configuration > Device Network Settings > Adjust network name if UMS-internal name has been changed**.

Option 3: Via IGEL Setup > Accessories > UMS Registration

If the **Naming Convention** is not activated and you need to register only a small number of devices, you can specify the required name when registering the device as follows:

- On the device, open **IGEL Setup > Accessories > UMS Registration** and specify the device name you need under **New host name**. For more information, see [Using UMS Registration Function](#)²³.

Option 4: Via IGEL Setup > Network > LAN Interfaces > Terminal name

If the **Naming Convention** is not activated:

- Before registering the device in the UMS, adjust its name locally under **IGEL Setup > Network > LAN Interfaces > Terminal name**. When the device is registered, this name will also be used in the UMS.

²³ <https://kb.igel.com/display/igelos1105/Using+UMS+Registration+Function>



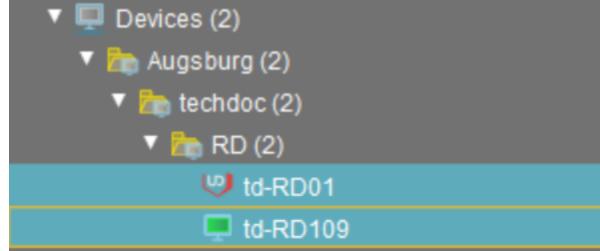
Renaming Already Registered Devices

Option 1: Via UMS Console > Device Network Settings > Naming Convention

1. Activate and define **Naming Convention** in the UMS under **UMS Administration > Global Configuration > Device Network Settings**, see [Device Network Settings](#)(see page 457).
2. If the network name, i.e. terminal name, of the device should be adjusted, enable **Device Network Settings > Adjust network name if UMS-internal name has been changed**.
3. Save the changes.
4. To rename the devices, select one of the following options:

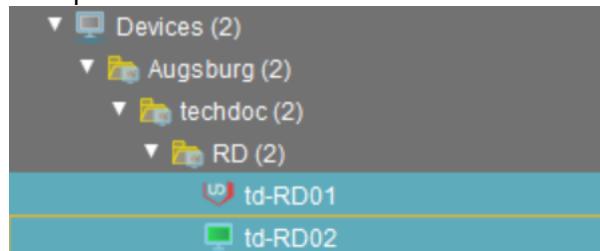
- **Rename all devices:** All devices registered in the UMS will be renamed in accordance with the naming convention using the existing enumeration.

Example:



- **Rename and renumber all devices:** All devices will be renamed in accordance with the naming convention, this will result in continuous, end-to-end numbering. All names will be reallocated. If numbers have become free because devices were taken out of service, these numbers will be used for other devices.

Example:



Tip

If the network name remained unchanged, click **Other commands > Settings UMS->Device** from the device's context menu.

Option 2: Via UMS Console > System > Import > Import Devices (Short or Long Format Only) If the Required Names Are Preliminarily Defined in the Import File

If the **Naming Convention** option does not suit your needs, you can reimport the devices with the names that fulfill your requirements. For the general instruction, see [Importing Devices](#)(see page 308).



1. When preparing the import file, specify the required device names. See [Import with Short Format](#)(see page 309) or [Import with Long Format](#)(see page 309).
2. If the network name, i.e. terminal name, of the devices, should be adjusted, enable **UMS Administration > Global Configuration > Device Network Settings > Adjust network name if UMS-internal name has been changed.**

Option 3: Via UMS Console > [device's context menu] > Rename or via Network > LAN Interfaces > Terminal name

- If you have to rename individual devices, see [Changing the Hostname of an IGEL Device via UMS](#)(see page 176).

Option 4: Via IGEL Management Interface (IMI)

- If you are using [IMI](#)²⁴, you can rename your devices as described under [PUT /v3/thinclients/{tcld}](#)²⁵.

⚠ General Notes

- After renaming via UMS, it may be necessary to reboot the endpoint up to three times before the changed network name is displayed correctly.
- Scripts under **System > Firmware Customization > Custom Commands** as well as some DNS or DHCP infrastructure settings may interfere and obstruct the renaming of devices.

1.8.6 Changing the Hostname of an Endpoint Device via UMS

There are two different ways to change the hostname of an endpoint device via UMS:

Option 1:

If **Adjust UMS-internal name if network name has been changed** is checked under **UMS Administration > Global Configuration > Device Network Settings**:

1. Right-click the device within the UMS structure tree.
2. Choose **Edit Configuration**.
3. Go to **Network > LAN Interfaces**.
4. Change **Terminal name**.
5. Click **Save**.
6. Select that you want the settings to be applied **Now**.
7. Click the **Refresh** button in the UMS in order to see the changed hostname.
8. Reboot the device.

Option 2:

If **Adjust network name if UMS-internal name has been changed** is checked under **UMS Administration > Global Configuration > Device Network Settings**:

²⁴ <https://kb.igel.com/display/igelimi/IMI+Manual>

²⁵ <https://kb.igel.com/pages/viewpage.action?pageId=2723464>



1. Right-click the device within the UMS structure tree.
2. Choose **Rename**.
3. Change the name.
4. Click **OK**.
5. Right-click the device.
6. Choose **Other commands > Settings UMS -> Device**.
7. Reboot the device.

1.8.7 Monitoring Device Health and Searching for Lost Devices

Overview

You have two possibilities of monitoring the devices' health:

- Online check: The UMS initiates a regular poll to all devices.
- Last contact between the UMS and the devices: The UMS is aware of the time and date when it had its last interaction with devices; with IGEL OS 11.05.100 or higher, devices can send periodical heartbeat signals to the UMS.

Both methods can be combined; it is recommended to review the advantages and disadvantages. Generally speaking, a combination makes sense if network load is not an issue.

Environment

- Reportable heartbeat: Endpoint devices with IGEL OS 11.05.100 or higher
- Checking the last contact between the device and the UMS: UMS 6.07 or higher
- UMS and endpoint devices are connected directly or via ICG

Online Check (UMS Polls the Devices)

The UMS Server polls the devices in a configurable time interval. When a device responds to the poll, its icon is green ; when a device does not respond, its icon turns red . (When the online check is disabled, the icon is grey .) For more information on the display of icons, see [Devices](#)(see page 382).

The online check can be enabled or disabled under **Misc > Settings > Online Check**; also, the time interval can be configured there.

Advantages:

- Works with any firmware version (and any UMS version).
- Provides an instant insight into device health by means of colored icons.
- Status updates can be very frequent (max. every 0.1 seconds).

Disadvantages:

- Causes relatively high network load, as all devices are polled at the same time (the overall network load is dependent on the time interval).
- Offline devices cannot be traced systematically, must be looked up manually in the structure tree.



Last Contact between Device and UMS (Devices Send Data to the UMS)

You can search explicitly for devices that did not have any interaction with the UMS for a given time. By creating an appropriate view, you can determine which device last had contact with the UMS at which time. This may be useful for detecting devices that are not operational anymore.

In addition to the previously existing contacts, devices with IGEL OS 11.05.100 or higher can send periodical heartbeat signals to the UMS to indicate that they are still operational.

Advantages:

- Systematic searches for lost devices are possible.
- The search results can be saved and sent by e-mail.
- Low network load, or no additional load at all:
 - When the heartbeat feature is used: The heartbeat signals are sent with random delay times. (Of course, the overall network load is dependent on the time interval).
 - When the heartbeat feature is not used: No additional network load is generated.

Disadvantage:

- Status updates cannot be as frequent as with the online check.

Tracing Devices by Their Last Contact with the UMS

Tracing a Specific Device

1. In the structure tree, go to **Devices** or use the search slot to find the desired device.

The screenshot shows the UMS interface with the search bar containing "cad" highlighted with a red box. The device list shows a single entry: "ITC005056930CAD".

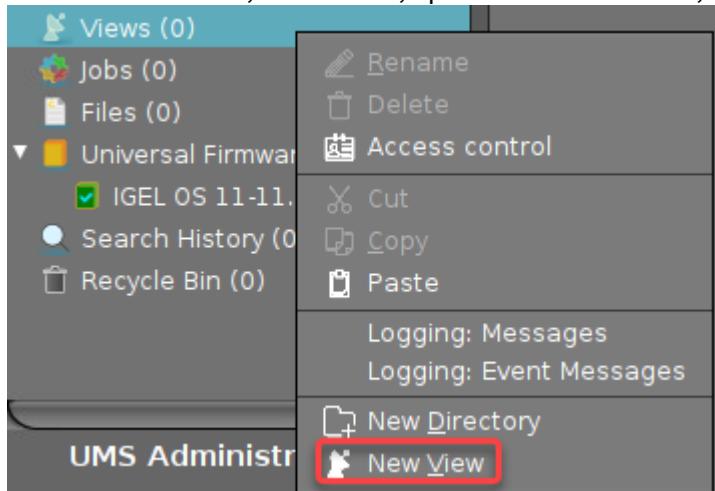
2. In the **Advanced System Information** area, check out the value of the **Last contact**.

Attribute	Value
Unit ID	005056930CAD
MAC address	00:50:56:93:0C:AD
Last IP	192.168.30.106
Product	IGEL OS 11
Product ID	UC1-LX
Version	11.04.240.01
Firmware Description	
IGEL Cloud Gateway	
Expiration date of OS 10 maintenance subscription	
Last contact	Mar 17, 2021 11:42:22 AM
Last Boot Time	Jan 22, 2021 11:22 AM
Network Name (at Boot Time)	ITC005056930CAD
Runtime since last Boot	18:41:50
Total Operating Time	234 days
Battery Level	



Finding Devices That Have Not Shown Up since a Given Time

1. In the structure tree, to to **Views**, open the context menu, and select **New View**.



2. Enter an appropriate **Name**, and, **optionally**, a **Description**, and click **Next**.

A screenshot of the "Create new view" dialog box. It has a "View name" header and a main area with "Name" set to "Last devices" and "Description" set to "Determines the last contacts with devices". A red rectangle highlights the "Name" and "Description" fields. At the bottom, there are "Back", "Next", "Finish", and "Cancel" buttons, with "Next" highlighted by a red rectangle. There is also an "Expert mode" link at the bottom right.



3. In the search field, type "contact" to reduce the number of criteria.

Create new view x

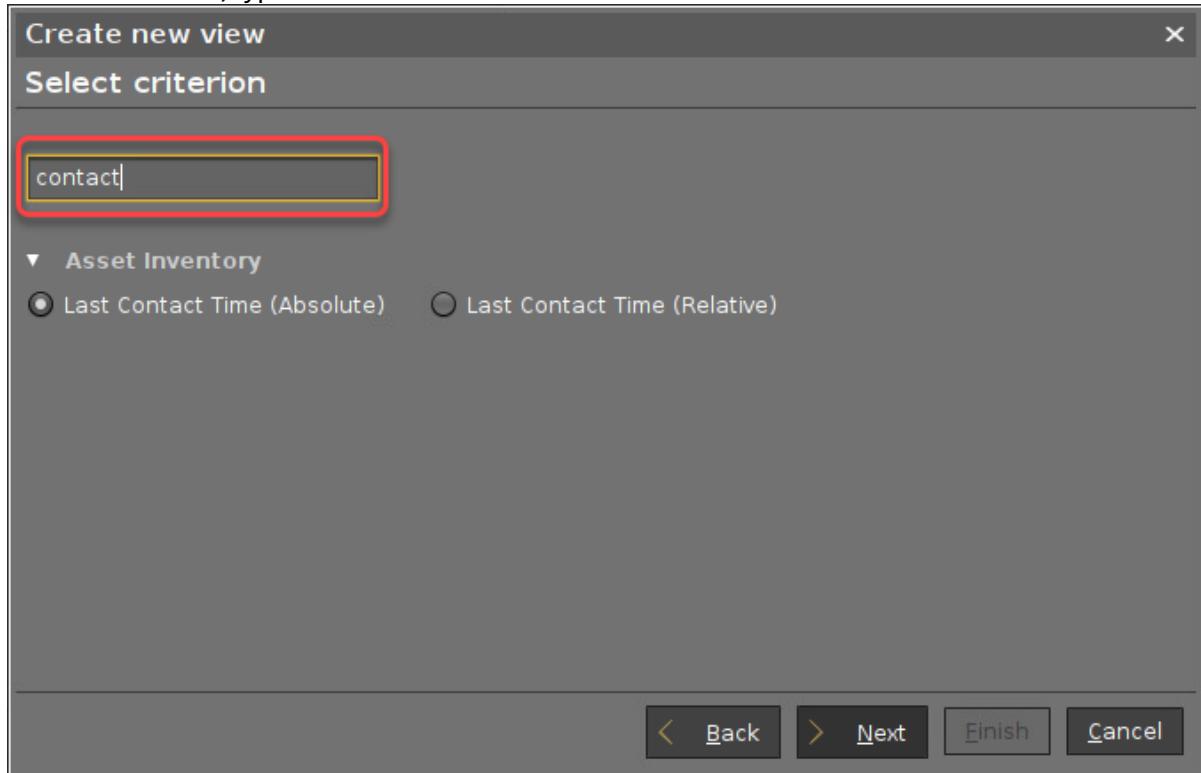
Select criterion

contact

▼ Asset Inventory

Last Contact Time (Absolute) Last Contact Time (Relative)

Back Next Finish Cancel

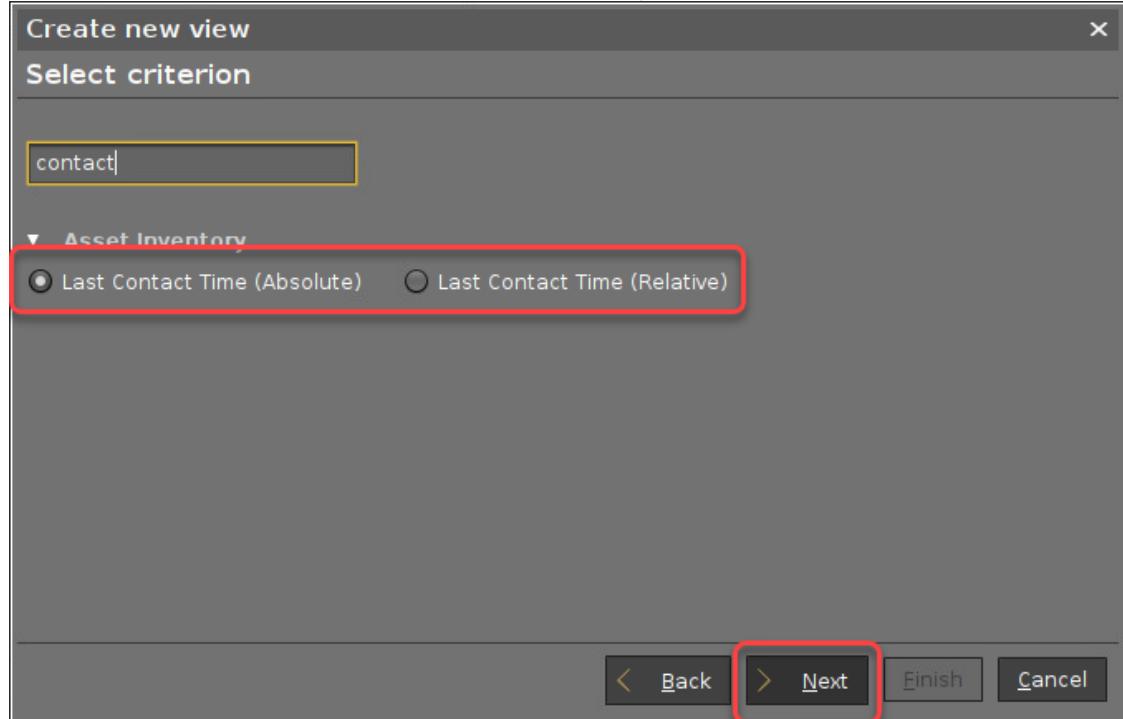


4. Choose one of the following criteria and click **Next**:

- **Last contact time (relative)**: The time interval between the last contact between the UMS and the device and now. This can be the last received heartbeat or any other kind of communication.



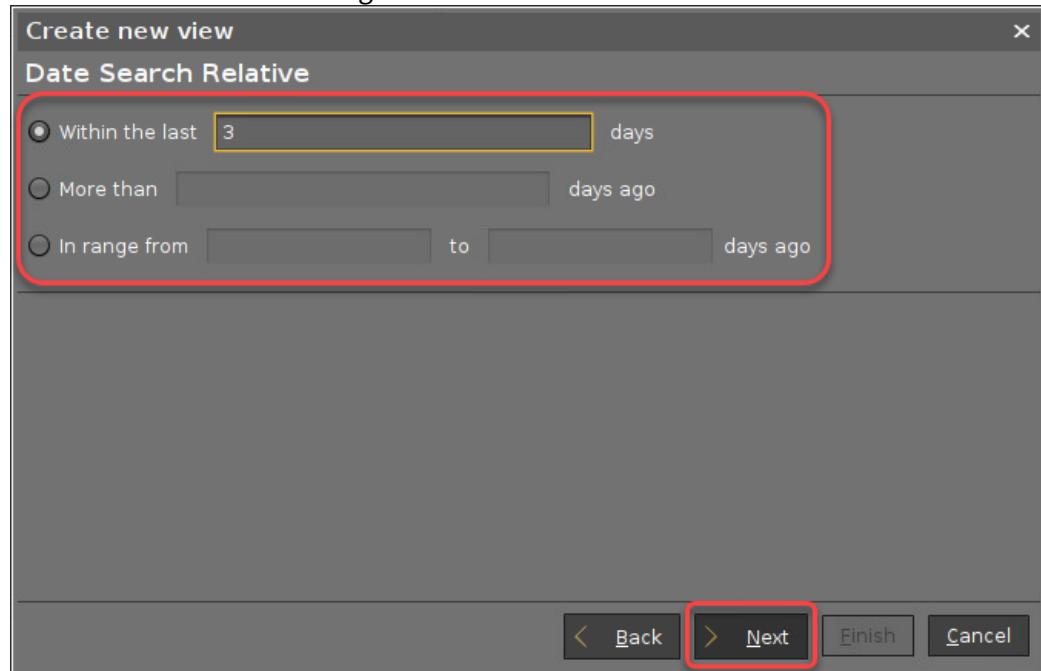
- **Last contact time (absolute):** The date of the last contact between the UMS and the device. This can be the last received heartbeat or any other kind of communication.



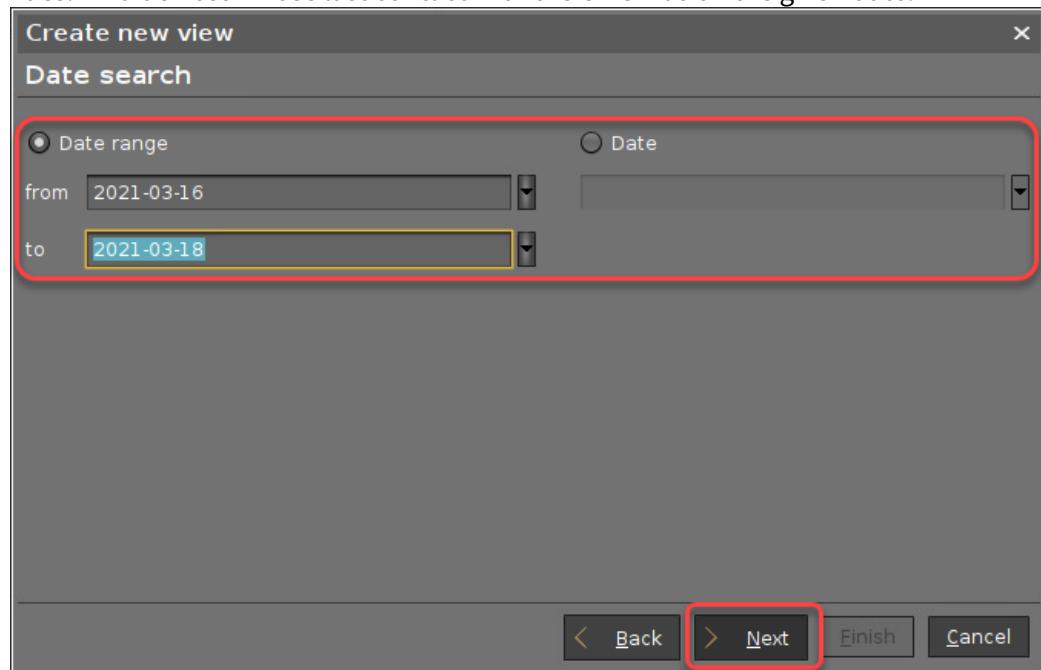
5. Provide the data, depending on whether you chose **Last contact time (relative)** or **Last contact time (absolute)**, and then click **Next**.
 - If you have selected **Last contact time (relative)**:
 - **Within the last [number of] days:** Find devices whose last contact with the UMS was between yesterday and the given number of days ago.
 - **More than [number of] days ago:** Find devices whose last contact with the UMS is more than the given number of days ago.



- **In range from [number] to [number of] days ago:** Find devices whose last contact with the UMS was within the given time interval.



- If you have selected **Last contact time (absolute)**:
 - **Date range:** Find devices whose last contact with the UMS was within the given date range.
 - **Date:** Find devices whose last contact with the UMS was on the given date.



6. Review your settings and click **Finish**.



Create new view

Finish view creation

Name: Lost devices?

Description: No heartbeat received after a given time

View criteria

Boot Time within the last 3 days

Create view
 Narrow search criterion (AND)
 Create additional search criterion (OR)

Finish Back Next Cancel

7. If the devices are not shown immediately, click **Load devices**.

Name: Lost devices

Description: Determines the last contacts with devices

Rule: Last Contact more than 2 days ago

Result list was last updated at 1:18 PM.

Load devices Refresh

6 matching devices found.

Settings

8. To make the **Last contact** column visible, click the icon that is shown underneath and then select **Last contact** in the **Choose visible columns** dialog.

Name: Last contact

Description: Determines the last contacts with devices

Rule: Last Contact within the last 2 days

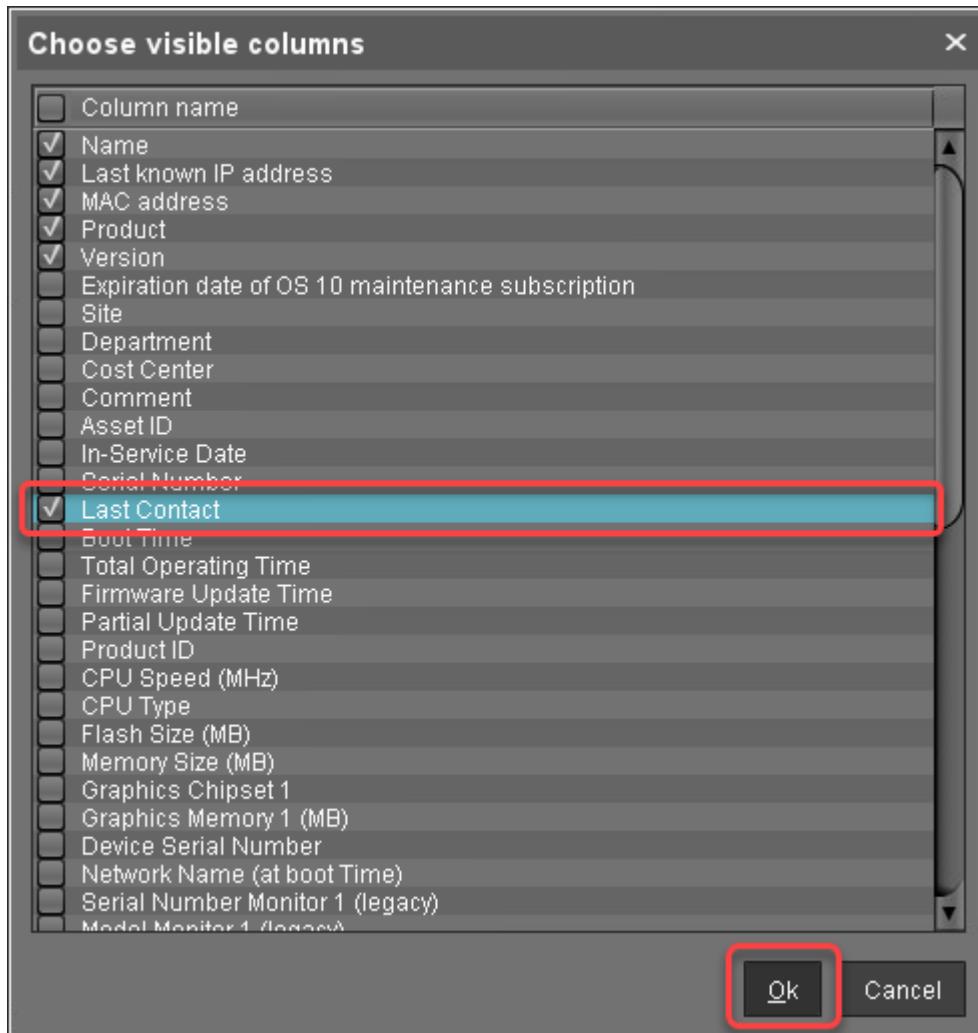
Result list was last updated at 11:58 AM.

Refresh Settings

Matching devices (3 devices)

Name	Last known IP address	MAC address	Product	Version
IGEL OS(RPI4)	192.168.30.103	DCA632C18C3B	IGEL OS(RPI4)	11.01.110
techdoc010	192.168.30.101	005056931508	IGEL Universal Desktop OS 2	5.13.100.01
techdoc08	192.168.30.100	005056938970	IGEL Universal Desktop OS 2	5.13.100.01

▼



The results are shown.

Name	Last contact				
Description	Determines the last contacts with devices				
Rule	Last Contact within the last 2 days				
Result list was last updated at 11:58 AM. Settings					
Refresh					
Matching devices (3 devices)					
Name	Last known IP address	MAC address	Product	Version	Last Contact
IGEL OS(RPI4)	192.168.30.103	DCA632C18C3B	IGEL OS(RPI4)	11.01.110	Mar 22, 2021 11:23:17 AM
techdoc010	192.168.30.101	005056931508	IGEL Universal Desktop OS 2	5.13.100.01	Mar 22, 2021 11:23:02 AM
techdoc08	192.168.30.100	005056938970	IGEL Universal Desktop OS 2	5.13.100.01	Mar 22, 2021 11:22:47 AM

You can save the results in various formats (see [Saving the View Results List](#)(see page 422)) or send them via e-mail (see [Sending a View as Mail](#)(see page 423)).



Configuring Devices to Send a Reportable Heartbeat

1. In the UMS Console, go to **UMS Administration > Device Network Settings** and edit the settings as follows:
 - Activate **Configure devices to send periodic contact signal**
 - Set **Heartbeat interval** to the desired value.

i The heartbeat signal will have a random delay of 0 to 10 minutes. This is to avoid overloads which might occur when large amounts of devices send their heartbeat signals simultaneously.

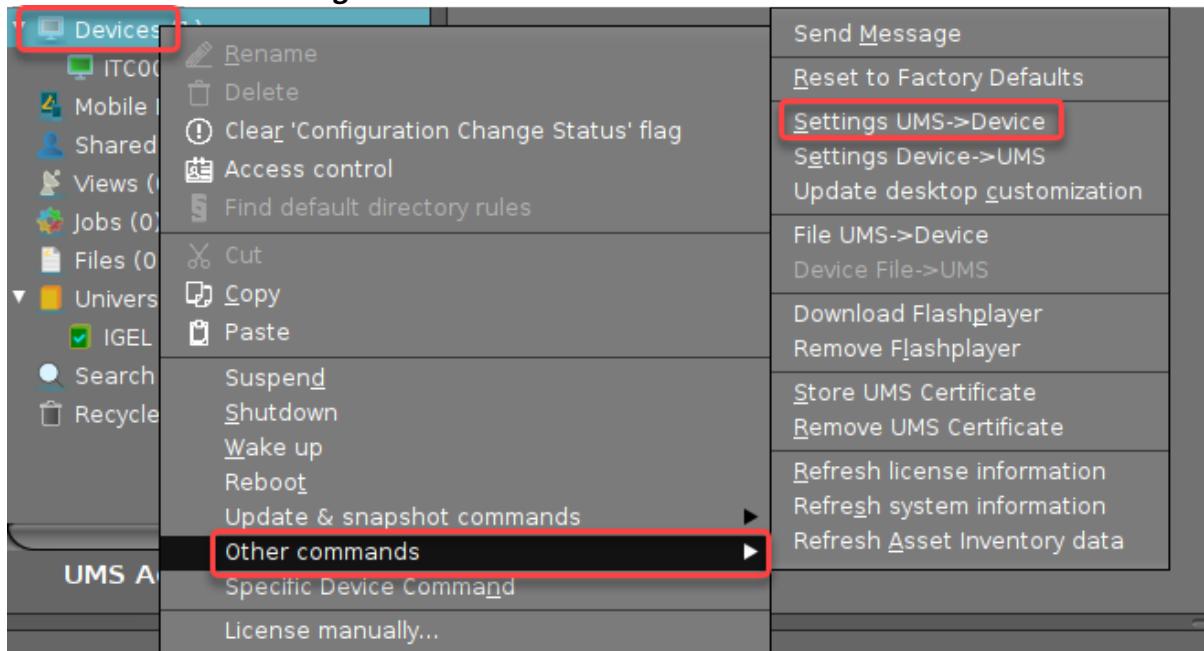
The screenshot shows the 'Device Network Settings' page with the following configuration:

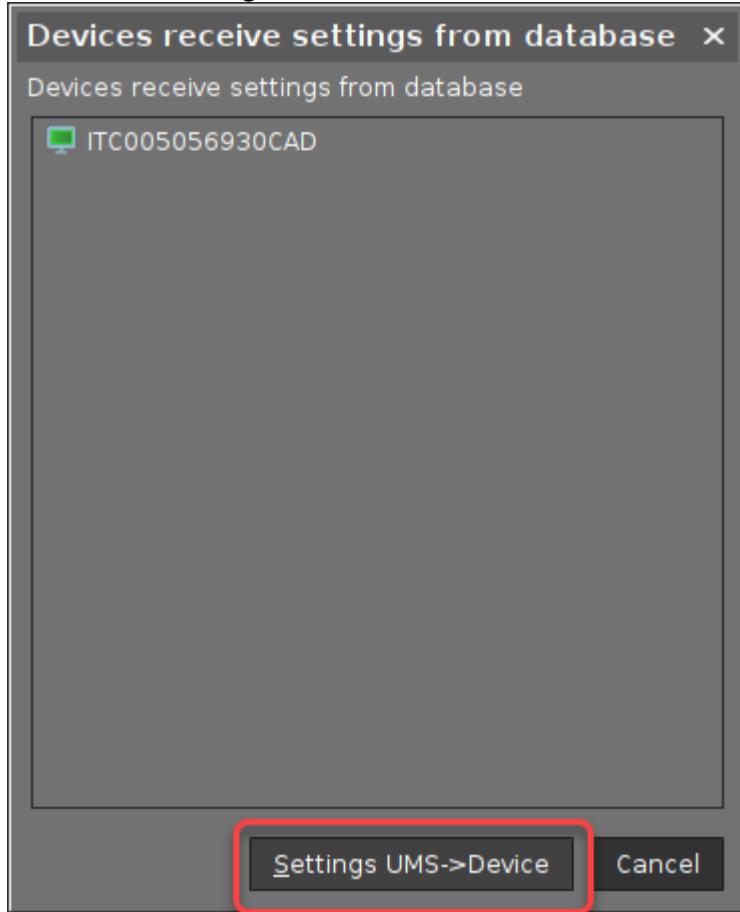
- Configuration of the System Information Update:** Update system information on selection of a device
- Advanced Device's Status Updates:** Devices send updates
- Heartbeat Signal:** Configure devices to send periodic contact signal. The 'Heartbeat interval:' dropdown menu is open, showing options: 3 hours (selected), 1 hour, 2 hours, 3 hours, 4 hours, 5 hours, 6 hours, 12 hours, and 24 hours.
- Automatic Registration:** Enable automatic registration (optional)
- Device Requests:** Maximum number of concurrent threads for device requests: 50

2. Click to save your settings.
The settings will become effective the next time the devices receive their settings from the UMS.



3. To make the new settings effective immediately, go to **Devices**, open the context menu, and select **Other commands > Settings UMS->Device**.



4. Confirm with Settings **UMS->Device**.

1.9 Start of the UMS Console / Web App

- [UMS Web App: The Browser Displays a Security Warning \(Certificate Error\)\(see page 187\)](#)
- [Starting UMS Console Crashes NX Session\(see page 204\)](#)
- [UMS Console doesn't start on Linux System without X11\(see page 205\)](#)
- [UMS Web App: "404 - System Error" Message\(see page 205\)](#)

1.9.1 UMS Web App: The Browser Displays a Security Warning (Certificate Error)

Symptom

When opening the UMS Web App, the browser displays a security warning and/or reports a certificate error.

Environment

- UMS Web App (UMS 6.06 or higher)

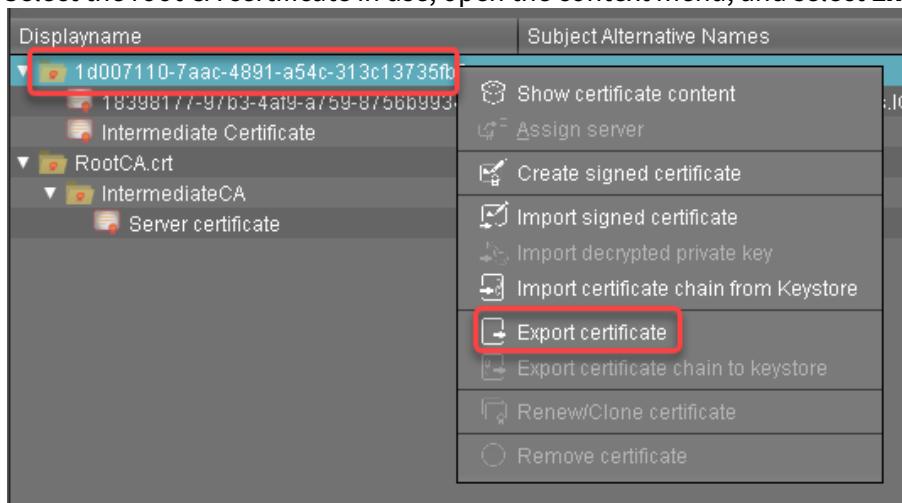
Problem

The customer uses an end certificate from a root CA that is not known to the browser. This is the case for self-signed certs, e.g. the default implementation.

Solution

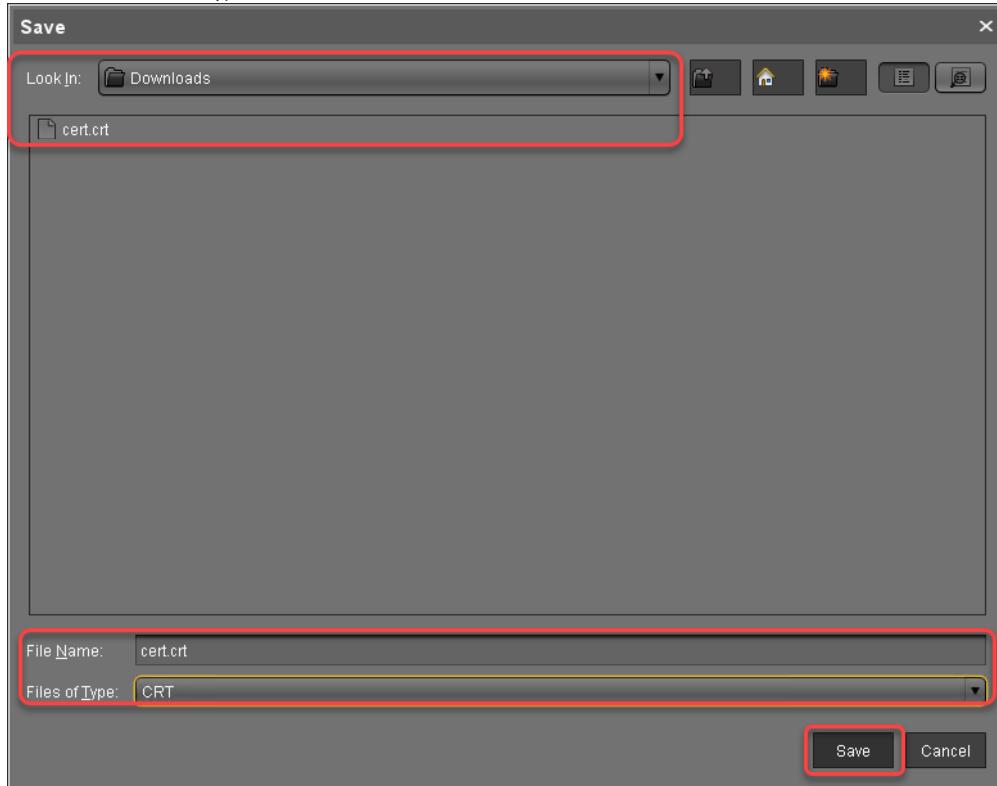
Exporting the Certificate from the UMS

1. In the UMS Console, go to **UMS Administration > Global Configuration > Certificate Management > Web**.
2. Make sure all end certificates in use are derived from the same root CA certificate.
3. Select the root CA certificate in use, open the context menu, and select **Export certificate**.





4. Select an appropriate location, select the correct file extension for your browser (most common: *.crt or *.cert), and click **Save**.



5. Add the certificate to the trusted certificates of your browser. For instructions, see [Importing the Certificate into the Browser](#)(see page 189).

Importing the Certificate into the Browser

⚠ The procedures described here may differ if you have a different browser version.

The following browsers are described here:

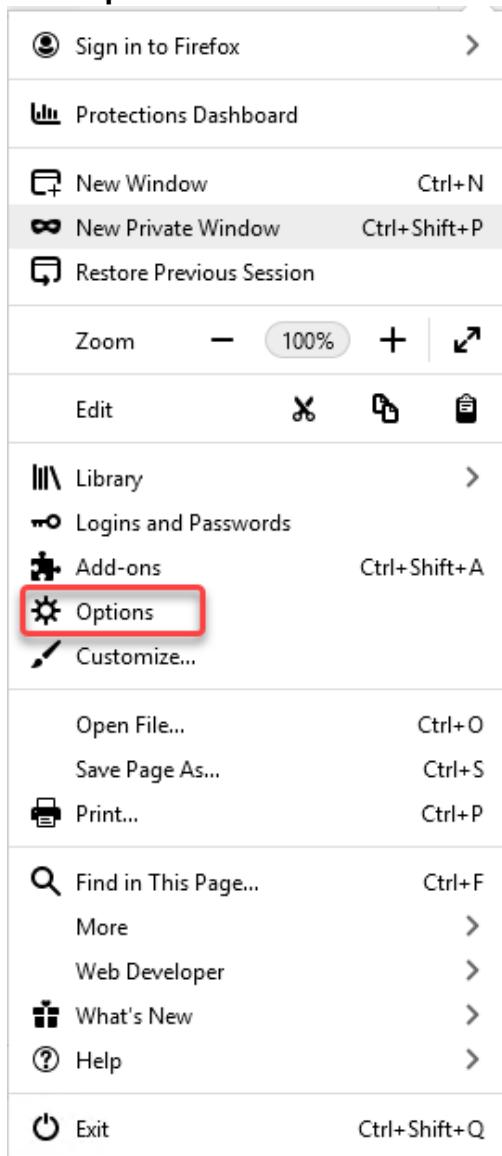
- [Firefox](#)(see page 189)
- [Chrome](#)(see page 193)
- [Microsoft Edge](#)(see page 200)

Firefox

1. Click to open the menu.



2. Select **Options**.





3. Select **Privacy & Security**.

-  General
-  Home
-  Search
-  Privacy & Security
-  Sync

4. Scroll down to Certificates and click **View Certificates**.

Certificates

When a server requests your personal certificate

- Select one automatically
- Ask you every time

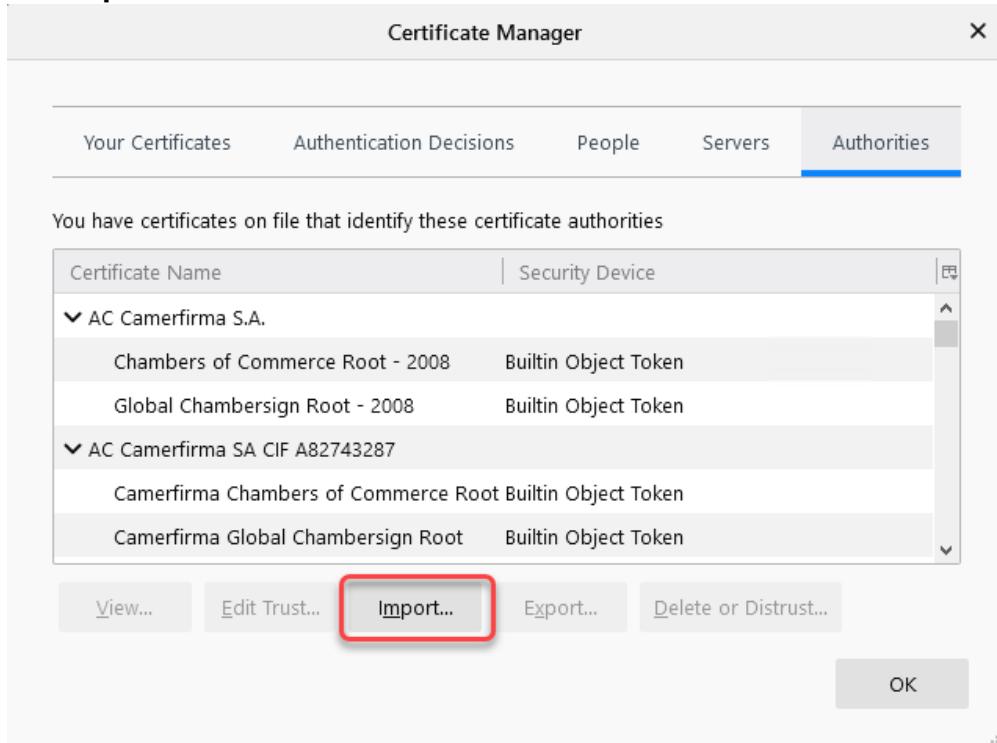
Query OCSP responder servers to confirm the current validity of certificates

[View Certificates...](#)

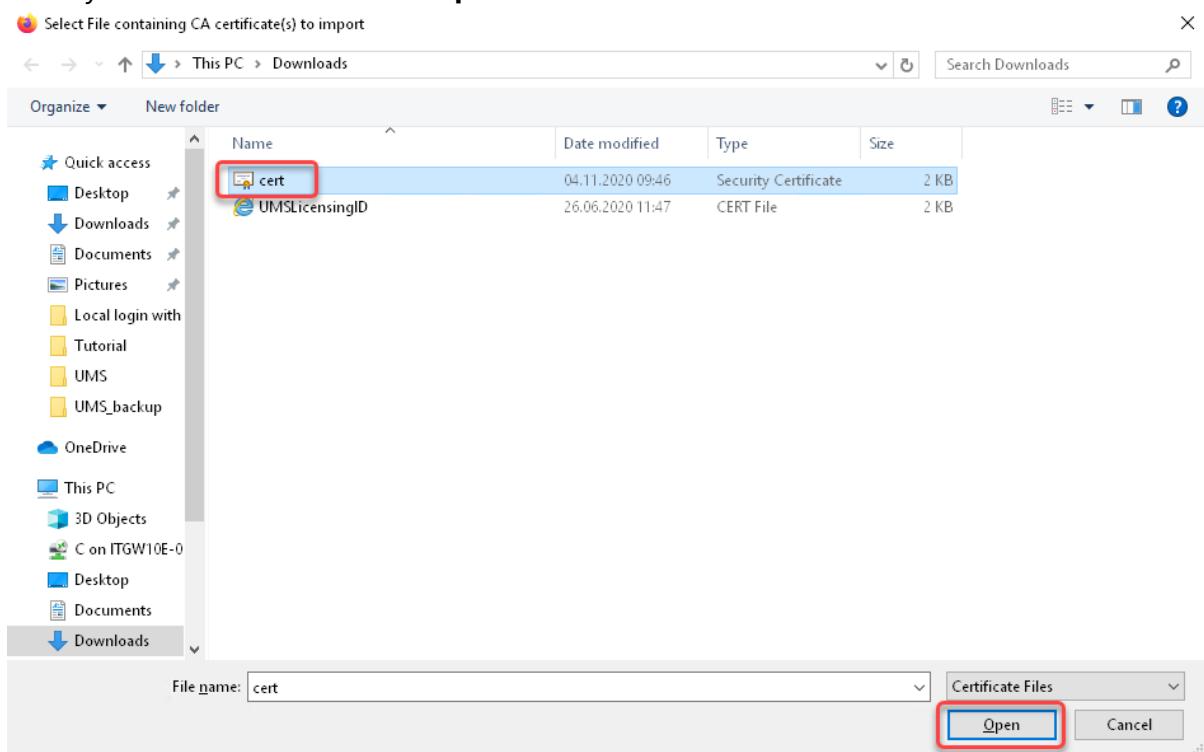
[Security Devices...](#)



5. Click **Import**.

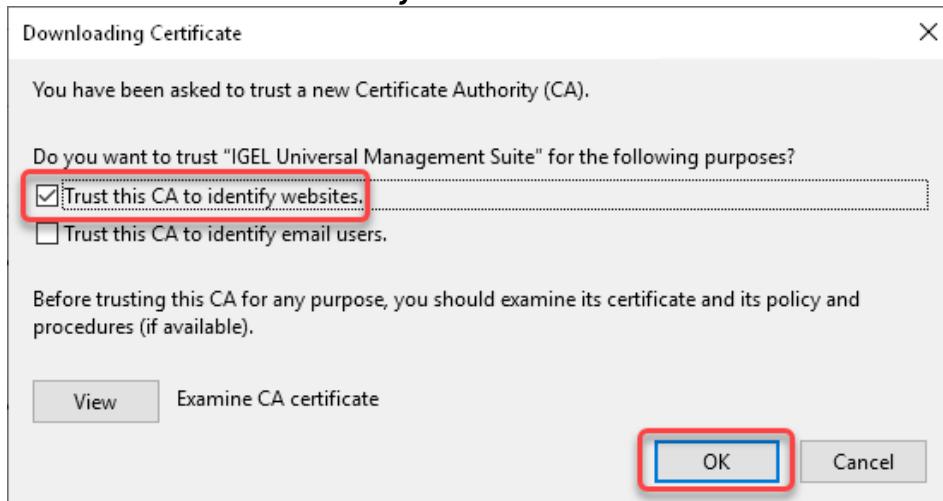


6. Select your certificate file and click **Open**.

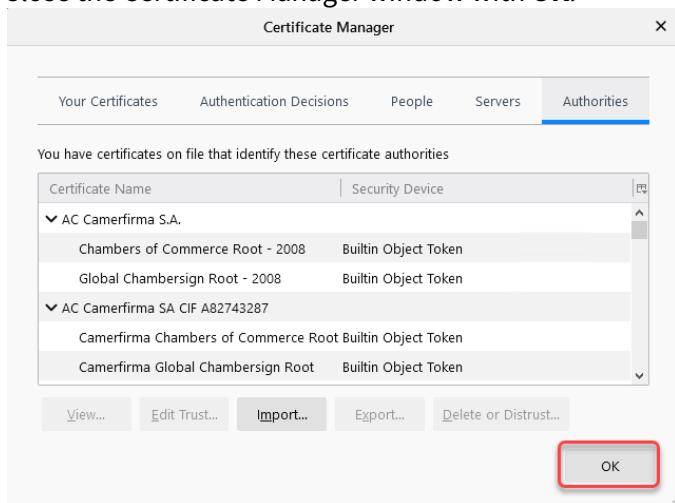




7. Activate **Trust this CA to identify websites** and click **OK**.



8. Close the Certificate Manager window with **OK**.



9. Restart the browser.

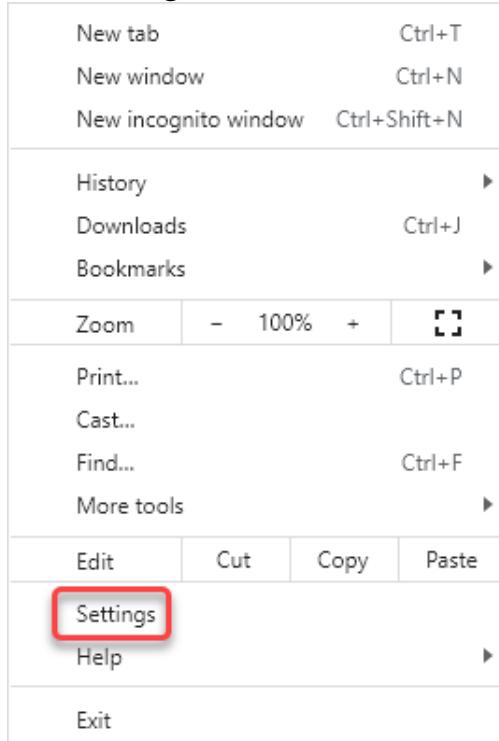
The browser can access the UMS Web App without problems.

Chrome

1. Click to open the menu.



2. Select **Settings.**



3. Go to **Privacy and security and select **Security**.**

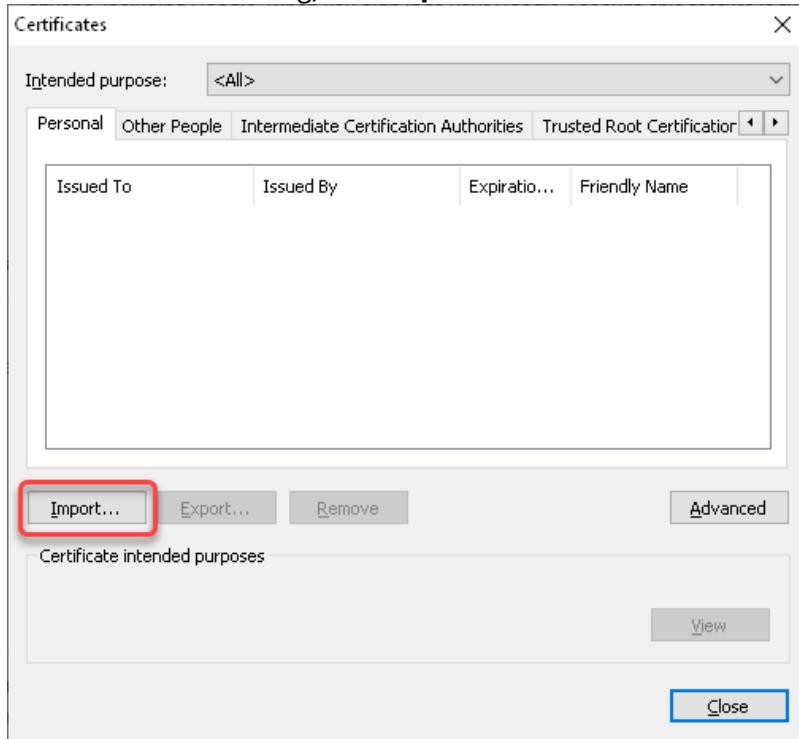
A screenshot of the "Privacy and security" settings page in Google Chrome. On the left, a sidebar lists "You and Google", "Autofill", "Safety check", "Privacy and security" (which is selected and highlighted with a red box), "Appearance", "Search engine", "Default browser", and "On startup". The main content area shows "Clear browsing data", "Cookies and other site data", "Security" (which is highlighted with a red box), and "Site Settings". The "Security" section is described as "Safe Browsing (protection from dangerous sites) and other security settings".

4. Scroll down and click the symbol next to **Manage certificates.**

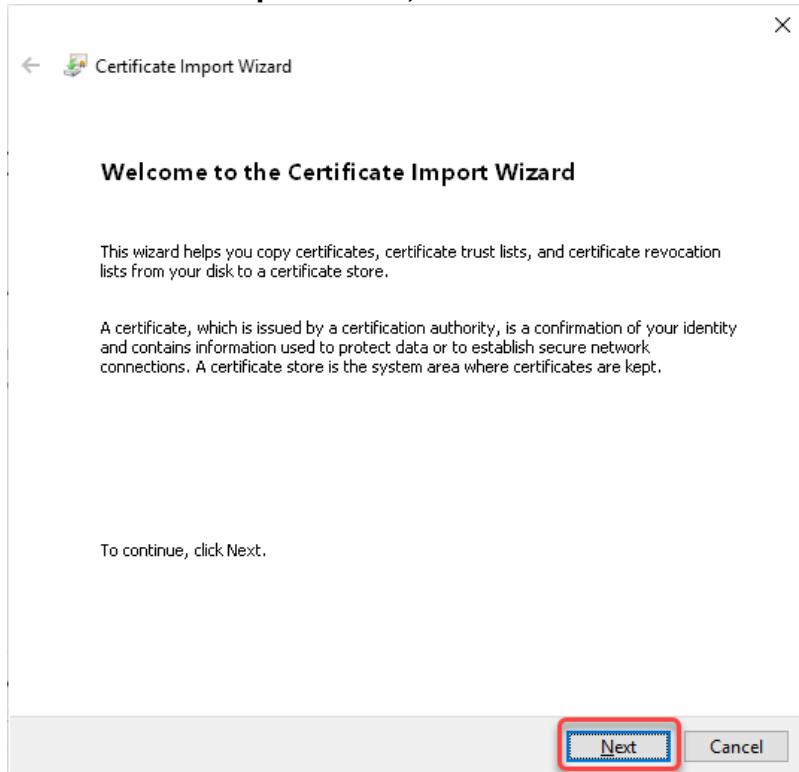
A screenshot of the "Google Advanced Protection Program" settings page. It includes sections for "Manage security keys", "Manage certificates" (which is highlighted with a red box and has a red square icon next to it), and "Google Advanced Protection Program" which describes itself as "Safeguards the personal Google Accounts of anyone at risk of targeted attacks".



5. In the **Certificates** dialog, click **Import**.

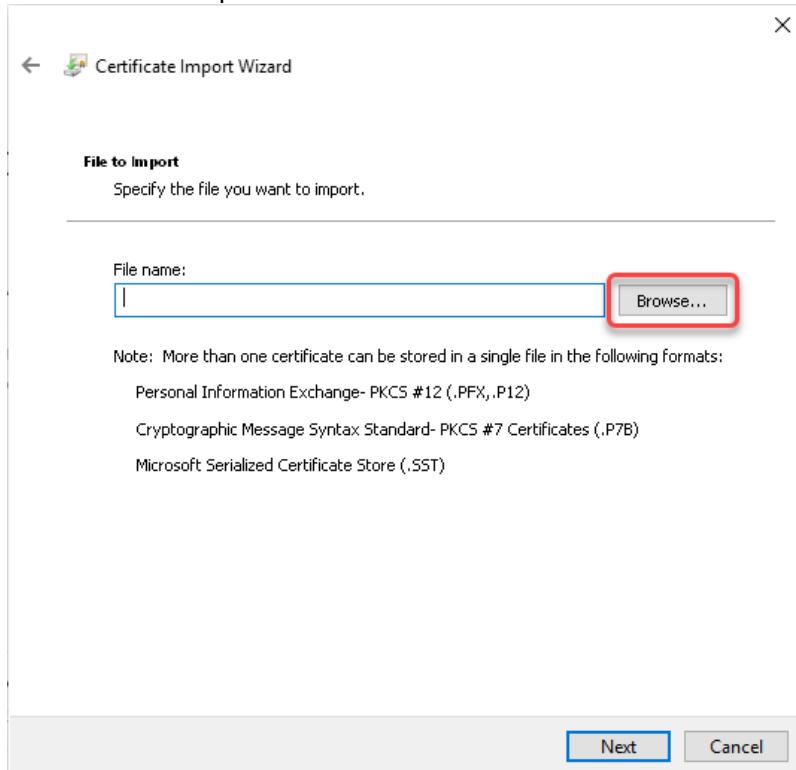


6. In the **Certificate Import Wizard**, click **Next**.

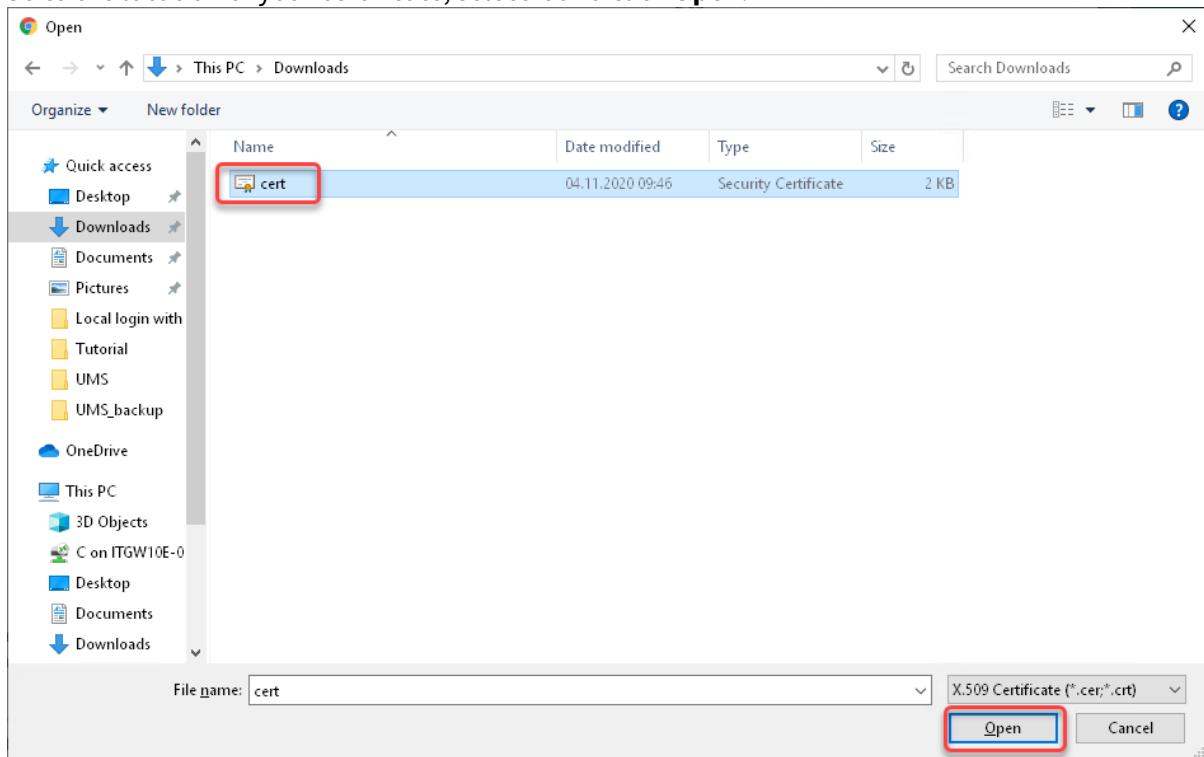




7. Click **Browse** to open the file chooser.

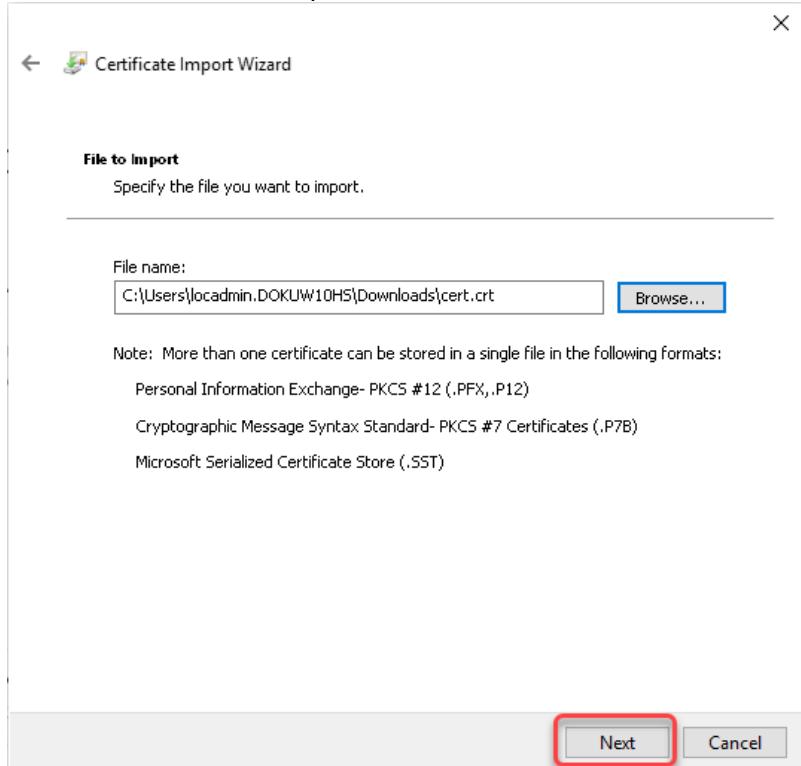


8. Go to the location of your certificate, select it and click **Open**.



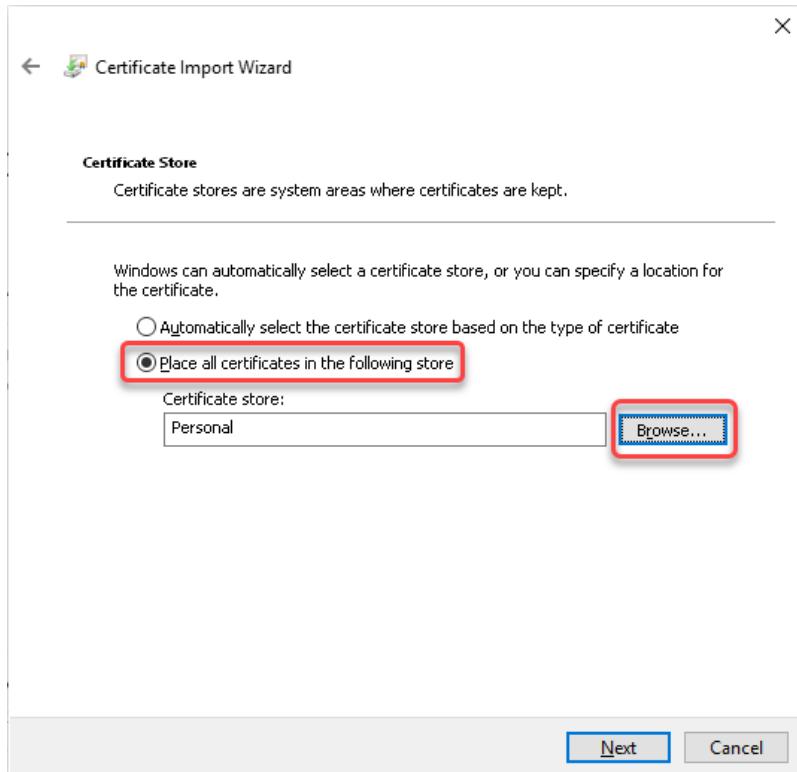


9. Back in the Certificate Import Wizard, click **Next**.

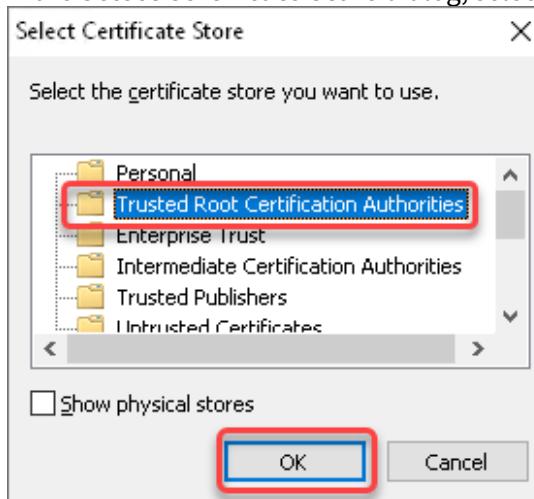




10. Select **Place all certificates in the following store** and click **Browse** to determine the certificate store.

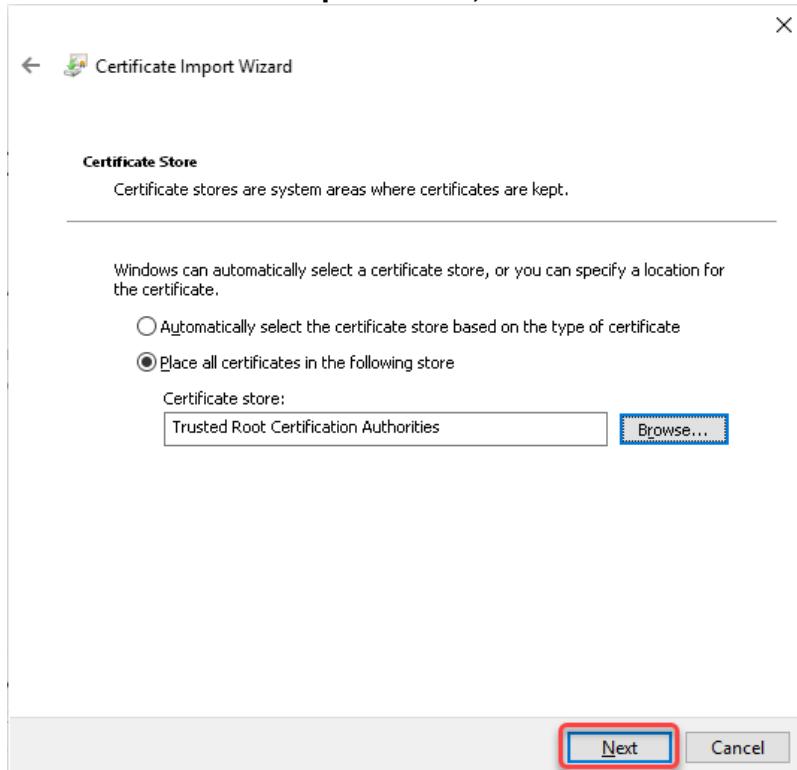


11. In the **Select Certificate Store** dialog, select **Trusted Root Certificate Authorities** and click **OK**.

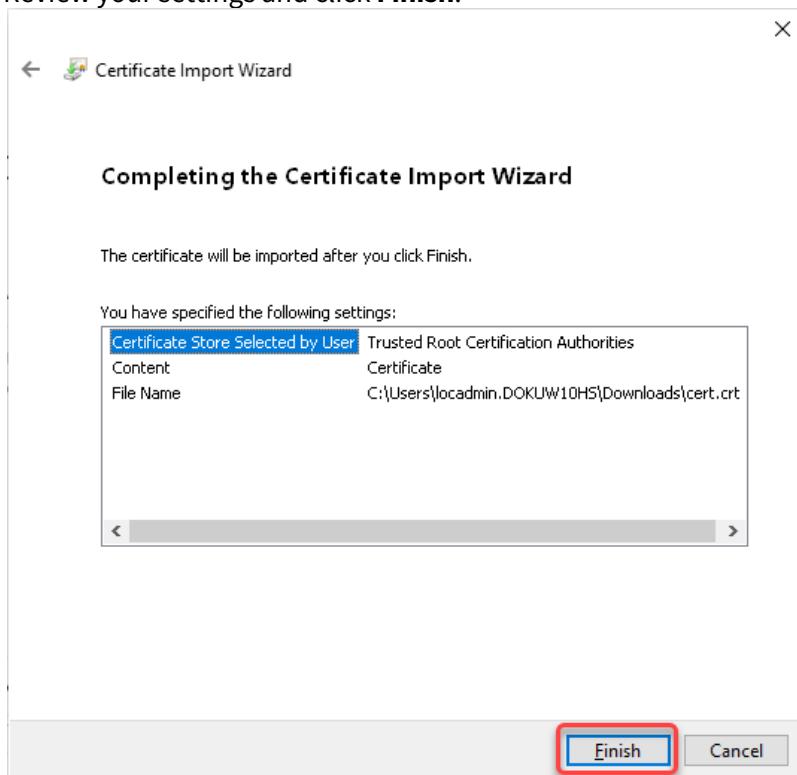




12. Back in the **Certificate Import Wizard**, click **Next**.

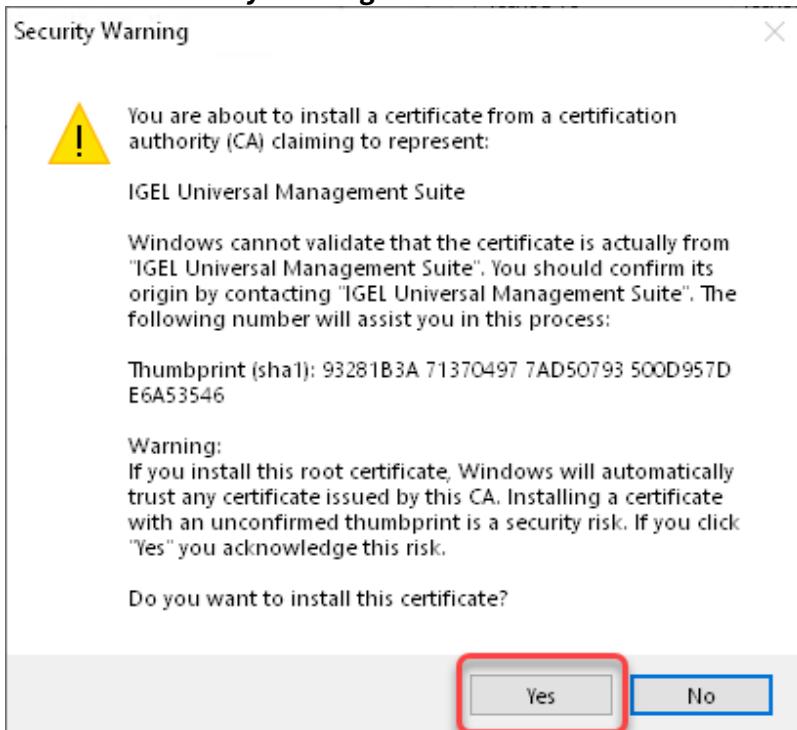


13. Review your settings and click **Finish**.

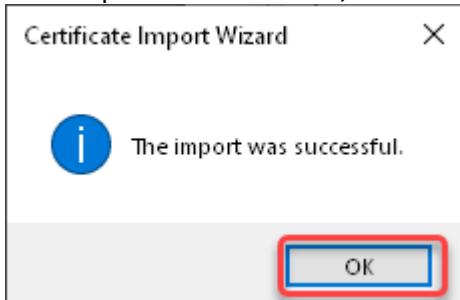




14. Confirm the **Security Warning** with **Yes**.



15. If the import was successful, a success message is displayed.



The certificate is installed on your system.

16. Restart the browser.

The browser can access the UMS Web App without problems.

Microsoft Edge

1. Make sure you have administrator permissions.
2. Go to the location where you have stored the certificate and double-click the certificate file.
The **Certificate** dialog of your Windows system opens.

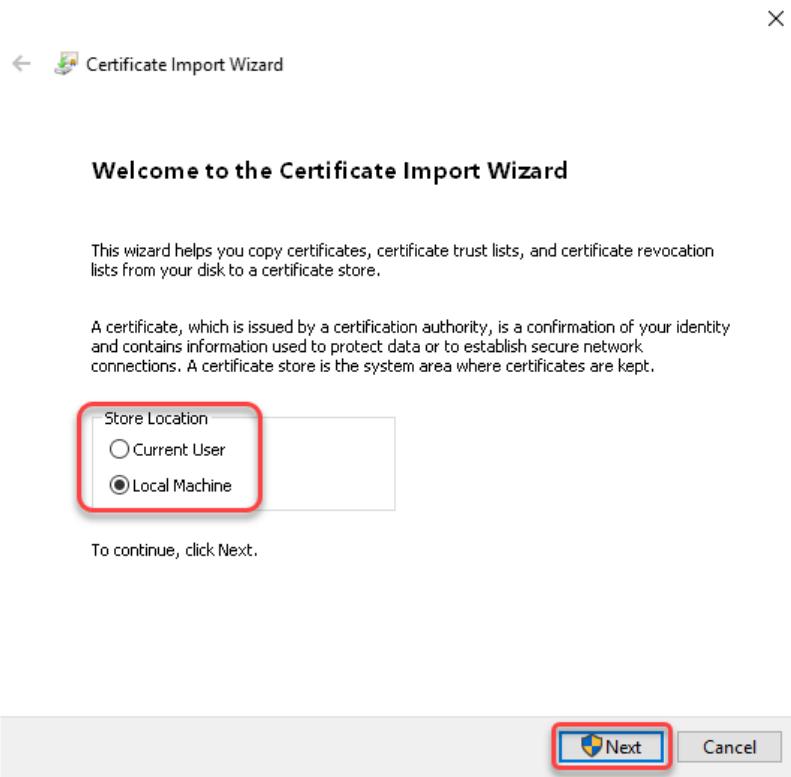


3. Click **Install Certificate...**





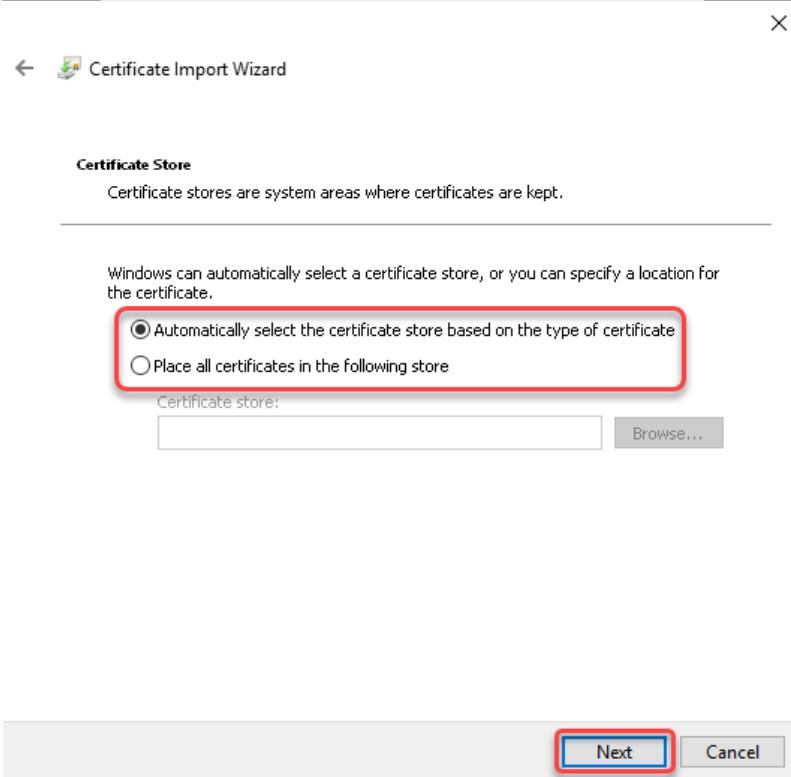
4. Define whether the certificate should be installed for the current user only or for all users (**Local Machine**) and click **Next**.



5. Confirm the **User Account Control** dialog.

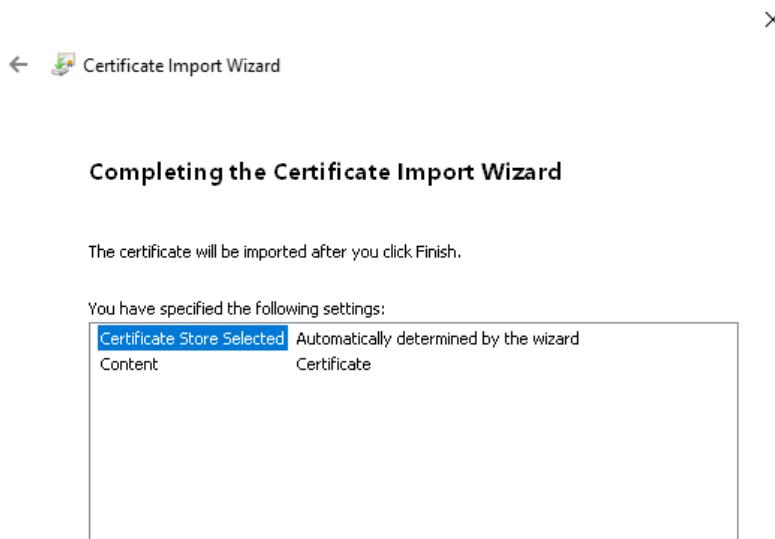


6. Define whether the certificate store should be determined automatically or manually and click **Next.**

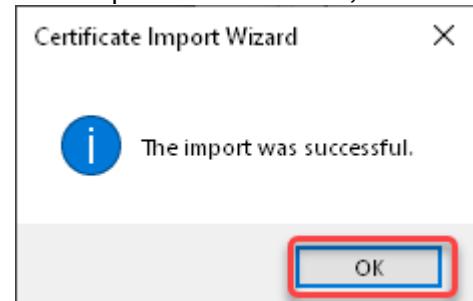




7. Review your settings and click **Finish**.



If the import was successful, a success message is displayed.



The certificate is installed on your system.

8. Restart the browser.
The browser can access the UMS Web App without problems.

1.9.2 Starting UMS Console Crashes NX Session

Symptom

When you are connected to an Ubuntu host via NX, starting the 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 the UMS Console.

1.9.3 UMS Console doesn't start on Linux System without X11

Symptom

IGEL UMS doesn't start on Linux system without X11.

Problem

The UMS console application needs X11 to run.

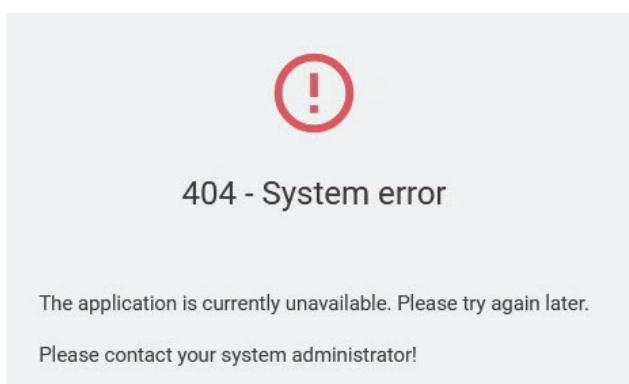
Solution

- ▶ Install X Window System (X11) to run IGEL UMS.

1.9.4 UMS Web App: "404 - System Error" Message

Symptom

After the installation of the Universal Management Suite, the UMS Web App starts with a 404 system error.





Environment

- UMS 6.08.100 or higher with the embedded database
- Microsoft Windows Server 2019

Problem

This might happen at startup when the UMS Web App is starting faster than the UMS Server service.

Solution

- Restart the Windows service `IGEL_RMGUIServer`. Details on how to do this can be found under [HA Services and Processes](#)(see page 691).

1.10 Logon failures

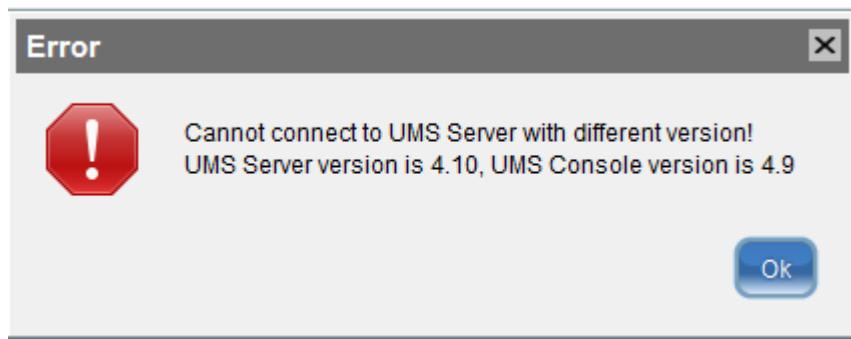
- [UMS Console Logon fails](#)(see page 206)
- [UMS Console Login with AD User Account fails](#)(see page 207)
- [Login to the UMS Fails after the Update](#)(see page 207)

1.10.1 UMS Console Logon fails

Symptom

When you try to log on to the console you get the error message **Unable to load tree**.

More recent UMS versions show the following error message:



Problem

Problems with the connection between the UMS console and the UMS server may be caused by a difference in software versions, e.g. if the UMS server was updated but the console still uses an old version.



Solution

Check the version status:

1. Check the version of the console by selecting **Help > Info** from the UMS console menu.
2. Check the version of the server by selecting **Help > Info** from the UMS administrator menu.
3. If necessary, update the UMS console to the same version as the server or newer.

1.10.2 UMS Console Login with AD User Account fails

Symptom

UMS console login fails for Active Directory user.

Problem

1. Open catalina log file C:\Program Files\IGEL\RemoteManager\rmguiserver\logs\catalina.log
2. Check the log for message KDC has no support for encryption type (14)

Solution

If this happens, the following things needs to be done/checked:

1. Have a look at <http://technet.microsoft.com/en-us/library/cc733991.aspx>.
2. Disable **DES encryption** for the AD user account, this can be done in the account setup of the Windows user administration > Account options.
3. Follow <http://docs.oracle.com/javase/6/docs/technotes/guides/security/jgss/tutorials/Troubleshooting.html>.

1.10.3 Login to the UMS Fails after the Update

Symptom

You cannot log in to the UMS after an update or the installation of the UMS Server.

An error message with the URL `https://[ums_server_host]:8443/info` appears:



Problem

The IGEL RMGUI Server Service has not fully started yet.

Solution

Wait for a few minutes more. After that, try to log in again.

1.11 Active Directory / LDAP

- [Integrating Active Directory](#)(see page 208)
- [Problems When Configuring an Active Directory with LDAP over SSL](#)(see page 218)
- [Import of Administrator Accounts from Active Directory Fails](#)(see page 219)

1.11.1 Integrating Active Directory

Problem

Instead of creating and organizing UMS administrators manually you are looking for an easy way of importing them from your existing Active Directory.

Reason

You would like to import users and user groups from the Active Directory to the UMS, using the same AD group assignments and credentials as already defined in the AD.

Solution

In this paper we explain the best way of importing users from the Active Directory as UMS administrator accounts.

We will import users from the Active Directory to the UMS console in three steps by:

- Configuring the connection to the Active Directory
- Selecting the users to be imported and starting the import
- Assigning permissions

- [Configuring an AD Connection \(see page 209\)](#)
- [Importing Users from AD to UMS \(see page 210\)](#)
- [Assigning Permissions \(see page 213\)](#)
- [Configuring an LDAP Connection \(see page 217\)](#)

Configuring an AD Connection

Perform the following steps to set up the connection between the UMS and the Active Directory of your company:

1. If you have user and group dependencies between different configured domains/subdomains, then you might want to activate **Include all configured AD domains for search and import of AD users / groups**. This option activates the group search for a user within all configured domains. On activation, a confirmation dialog is shown.

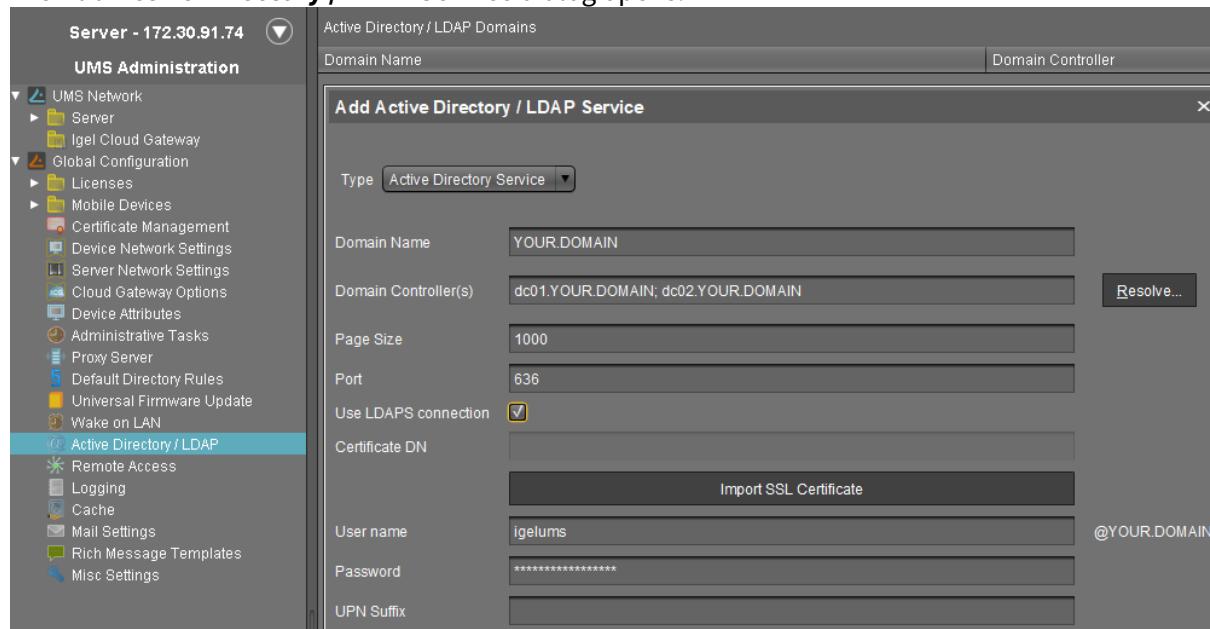
- i** If this option is activated, a user may gain additional permissions. This will be the case if
- the user is in a group that has been discovered due to this option,
 - this group has been imported under **System > Administrator accounts**,
 - and permissions have been assigned to this group i.e. permissions the user would not have otherwise.

Please note that, due to the additional lookups, this option might have an impact on the performance in the following areas:

- UMS login
- Permission dialogs
- Shared Workplace (SWP)

2. Click **Add (+)** under UMS console > **UMS Administration > Global Configuration > Active Directory / LDAP**.

The **Add Active Directory / LDAP Service** dialog opens.



The screenshot shows the UMS Administration interface with the 'Active Directory / LDAP Domains' section selected. The 'Add Active Directory / LDAP Service' dialog is open, showing the configuration for an Active Directory service. The 'Domain Name' field is set to 'YOUR.DOMAIN'. The 'Domain Controller(s)' field contains 'dc01.YOUR.DOMAIN; dc02.YOUR.DOMAIN' with a 'Resolve...' button. The 'Page Size' is set to 1000, 'Port' to 636, and 'Use LDAPS connection' is checked. The 'Certificate DN' field has a 'Import SSL Certificate' button. The 'User name' is 'igelums' and the 'Password' is masked. The 'UPN Suffix' field is empty.



3. Select **Active Directory Service** as Type.

4. Enter the **Domain Name**.

- i Several Active Directories can be linked. You should therefore ensure that you provide the correct domain when logging in (e.g. to the UMS console).

5. Enter the **Domain Controller(s)** manually or click **Resolve...** for the automatic search.

To separate domain controllers, use a semicolon.

- ! If the option **Use LDAPS connection** (see below) is enabled, make sure that a fully qualified name of the **Domain Controller** has been entered. See [Problems When Configuring an Active Directory with LDAP over SSL\(see page 218\)](#).

6. Enter **Page Size**.

The **Page Size** property sets the maximum number of items in each page of results that will be returned by a search. It affects query performance, but not the number of overall results. The standard value is "1000". Change this value in line with your server configuration.

7. Activate **Use LDAPS connection** to secure the connection with the provided certificate.

The **Port** changes automatically to default "636".

8. Click **Import SSL Certificate** to configure the certificate and to verify the **Certificate DN**.

- i Since the name of the **Domain Controller** is checked against the certificate, they must correspond. If more than one domain controller is used, the root certificate of the domain must be configured. See [Problems When Configuring an Active Directory with LDAP over SSL\(see page 218\)](#).

- i The supported certificate formats are .cer, .pem and .der

9. Under **User name and Password**, enter your user credentials.

10. Enter **UPN Suffixes** (aliases) if you have defined any (semicolon separated list). Example:
domain.local;test.local

- i The settings must correspond to the configuration of the Active Directory. If there are registered UPN suffixes in the AD, they should be known also by the UMS.

11. Click on **Test Connection** to check that you have entered a valid configuration.

12. Click **Ok** to confirm your settings.

The Active Directory domain is listed under **Active Directory / LDAP Domains**.

Active Directory / LDAP Domains		
Domain Name	Domain Controller	Page Size
YOUR.DOMAIN	dc01.YOUR.DOMAIN; dc02.YOUR.DOMAIN	1000

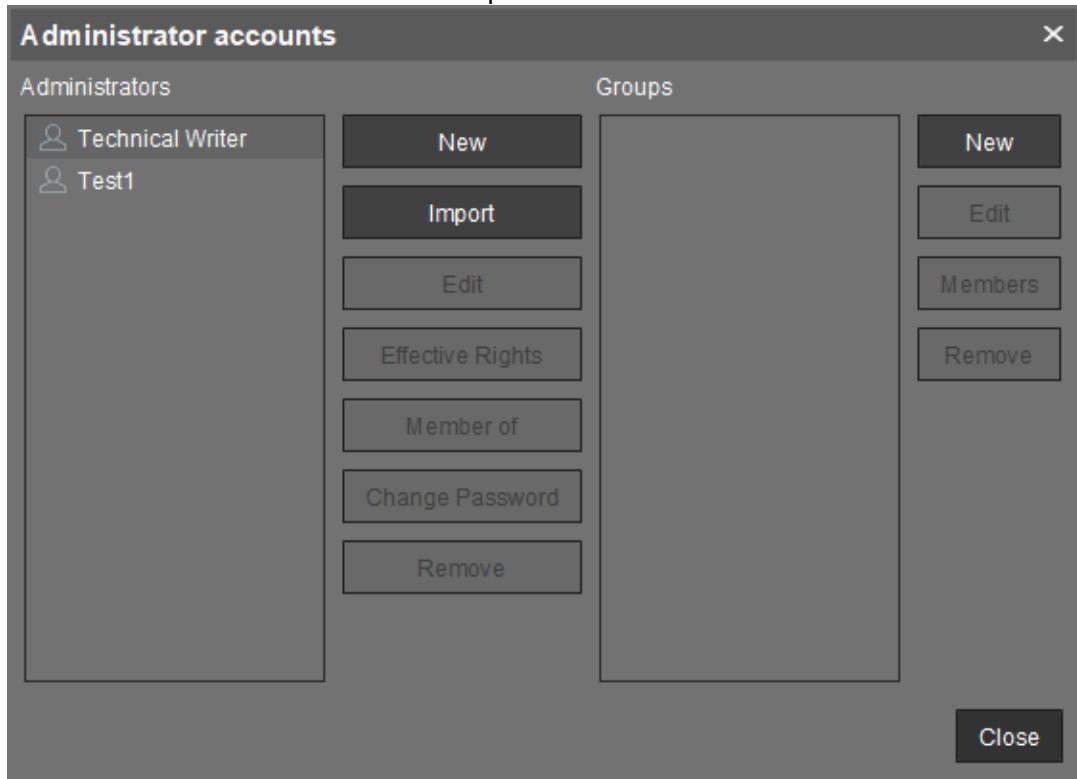
Importing Users from AD to UMS

After connecting the Active Directory you can import users or user groups to the UMS:



1. Click **System > Administrator Accounts**.

The **Administrator Accounts** window opens:



2. Click **Import** to log in to the AD/LDAP service.
3. Select the domain and enter your credentials, if not already defined.
4. Click **Next** to open the Active Directory browser.
5. Select individual users or groups from the structure tree of your AD.
6. Use drag and drop to add your selection to the **Selected Entries** list.



Import Users from AD / LDAP Directory

Search User / Group in the AD / LDAP Directory

▼ ● Users

- Administrator
- Allowed RODC Password
- Cert Publishers
- Denied RODC Password
- DnsAdmins
- DnsUpdateProxy
- Domain Admins
- Domain Computers
- Domain Controllers
- Domain Guests
- Domain Users**
- elch
- Enterprise Admins
- Enterprise Read-only Dom
- Gottschalk2

Search | Details

Account name Starts w... []

Object type Undefined []

Userdefined Filter ne=*)(givenName=*)(sn=*))

Start searching from dc=UMS,dc=TEST

Default Search

Selected entries

Display name	Account name
elch	elch@ums.test
Domain Users	

Back Next Finish Cancel

The screenshot shows the 'Import Users from AD / LDAP Directory' dialog box. On the left, a tree view under the 'Users' category shows various Active Directory groups and users. The 'Domain Users' group is currently selected. To its right is a search interface with fields for 'Account name' (set to 'Starts w...'), 'Object type' (set to 'Undefined'), and a 'Userdefined Filter' field containing the expression 'ne=*)(givenName=*)(sn=*)'. Below these is a search button and a 'Start searching from' field set to 'dc=UMS,dc=TEST'. A 'Selected entries' section contains a table with two rows: 'elch' (Display name) and 'elch@ums.test' (Account name), followed by another row for 'Domain Users'. At the bottom are navigation buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

i As an alternative to navigating in the structure tree, you can also add users or groups to your selection using the Search function.

7. Click **Next** and confirm to start the import.
A result list of imported accounts opens.



8. Click **Finish** to complete the import.

If the result list is either empty or some accounts are missing from the list, see [Import of Administrator Accounts from Active Directory Fails](#)(see page 219).

- i** A UMS administrator set up by mistake must be deleted manually using the dialog 'Administrator accounts'. The IGEL UMS uses the 'User logon name' from the AD as the name of the imported user.

Assigning Permissions

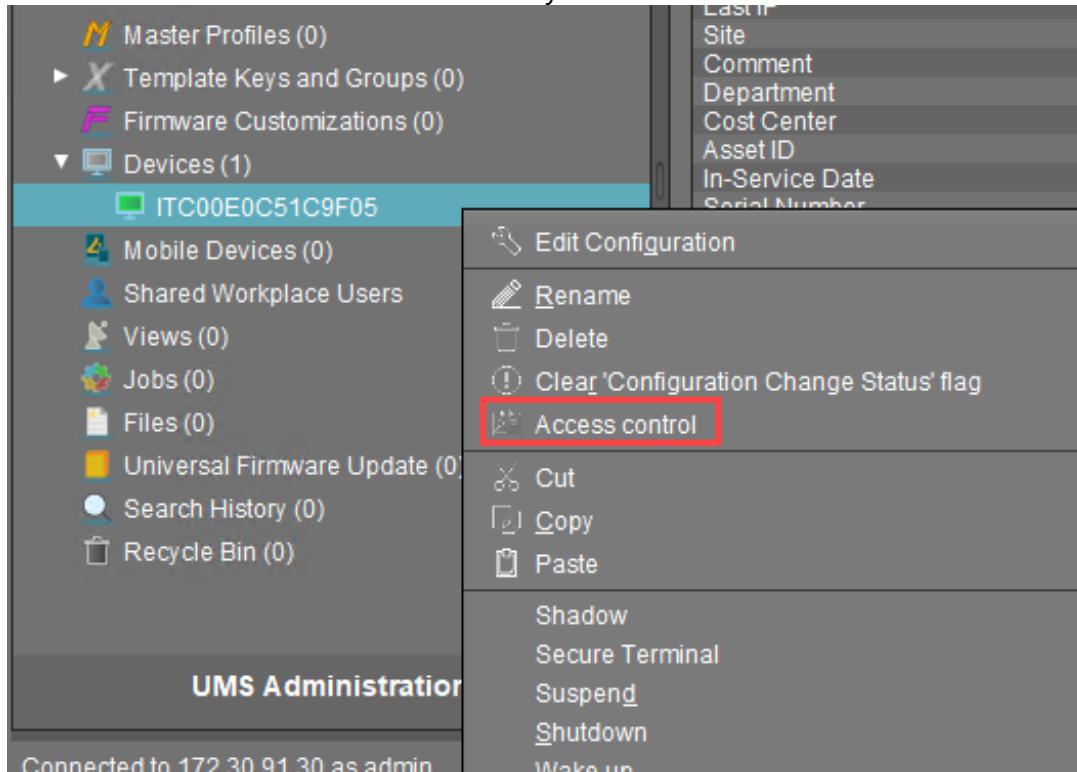
After the AD users have been imported, they can access the UMS with their Active Directory credentials.

As UMS administrators, the users still need individual access rights.

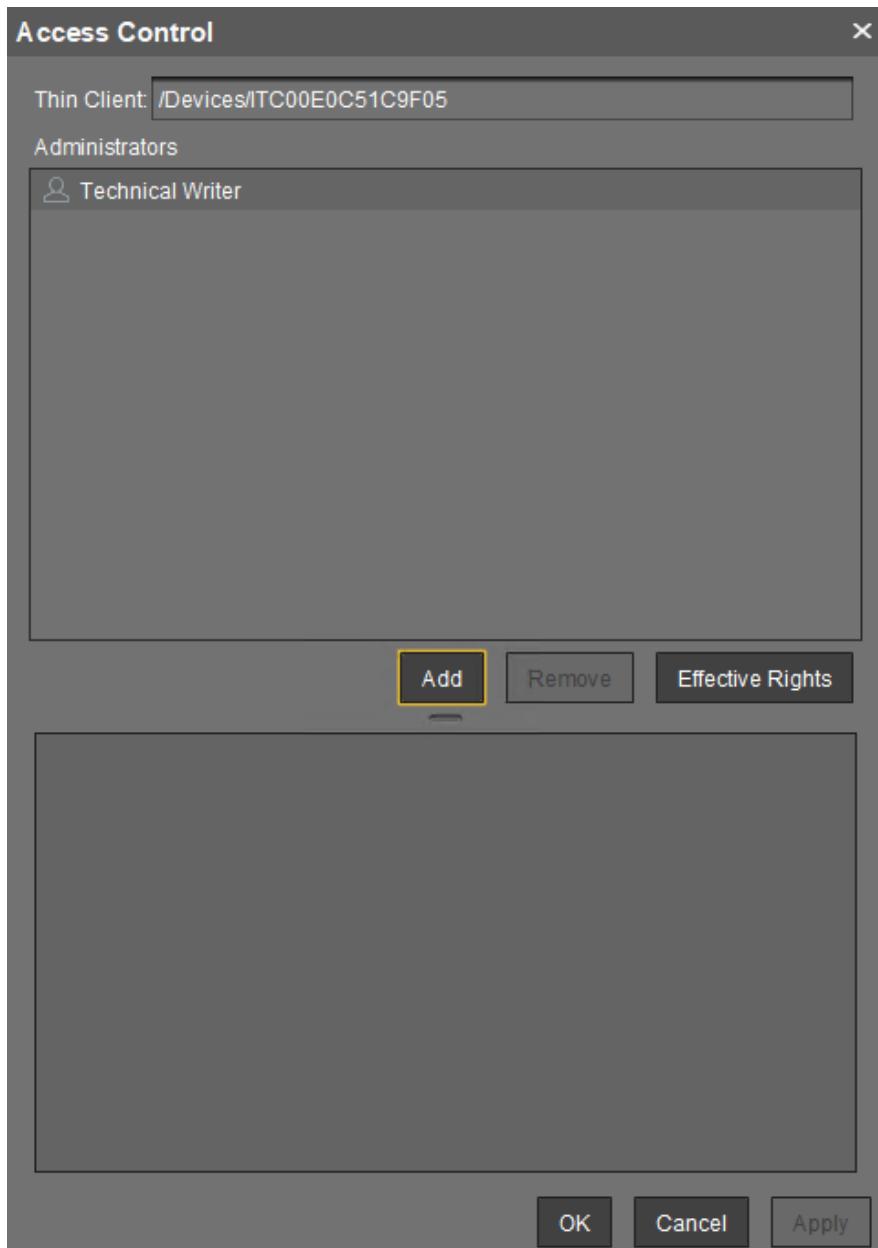
- i** The logon to the UMS is not possible via the 'pre Windows 2000 logon name' ('DOMAIN\logon name'), but only via the format 'logon name@DOMAIN'.
- i** For example, in order to be able to change the configuration of a thin client, a user requires authorization to browse the thin client's directory path and configure the thin client itself.

To assign these rights, proceed as follows:

1. In the structure tree of the UMS console choose the **Devices** node or a subgroup of devices or a single client.
2. Click **Access Control** in the context menu of your selection.



3. The **Access Control** window opens.



4. Click **Add** to select your new user/group.
5. The corresponding **Effective Rights** will be listed in the lower part of the mask.



Access Control

Thin Client: /Devices/ITC00E0C51C9F05

Administrators

Technical Writer
Test1

Add Remove Effective Rights

Permission	Allow	Deny	Effective Rights
Browse	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user Test1
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user Test1
Move	<input type="checkbox"/>	<input type="checkbox"/>	not set
Edit Configuration	<input type="checkbox"/>	<input type="checkbox"/>	not set
Write	<input type="checkbox"/>	<input type="checkbox"/>	not set
Edit System Information	<input type="checkbox"/>	<input type="checkbox"/>	not set
Access Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign	<input type="checkbox"/>	<input type="checkbox"/>	not set
Power Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Firmware Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Settings Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Remote access	<input type="checkbox"/>	<input type="checkbox"/>	not set

OK Cancel Apply

6. **Allow or Deny** the rights of the selected group or user for access to the selected devices
7. Confirm the settings with **OK**.
8. Click the **Refresh** button of the console to apply the changes in the UMS.

i If you have changed the rights of registered users they only take effect after a refresh.

For further details about authorization rules see our How-To [IGEL UMS: User Authorization Rules](#)(see page 91).



- ⓘ Access rights to objects or actions within the IGEL UMS are attached to the administrator accounts and groups. The rights of the database user account cannot be restricted. They are created during installation or when setting up the data source. The account always has full access rights in the UMS.

Configuring an LDAP Connection

As a variant you may connect other LDAP directory services, i.e. Novell eDirectory and OpenLDAP, to the UMS:

1. Click **Active Directory / LDAP** in the **UMS Administration** area of the UMS console.
2. Click **Add (+)** in the **Active Directory / LDAP Domains** mask.
3. The **Add Active Directory / LDAP Service** mask opens.

Add Active Directory / LDAP Service

Type	Other LDAP Service
Base DN	
Host(s)	
Port	636
Certificate DN	
	Import SSL Certificate
LDAP Access UserDN	
LDAP Access Password	
Naming Attribute	
Additional term for LDAP search	
Group attribute	
Page Size	1000
Test connection	
Ok Cancel	

4. Select **Other LDAP Service** as **Type**.
5. Enter the **Base DN** and the **LDAP Access UserDN** in accordance with the LDAP Data Interchange Format.



6. Enter the IP of your device in the **Host(s)** field; for more devices, use a comma separated list.
7. The default **Port** for LDAP over SSL is 636.

i For security reason UMS supports secure LDAP connections only.

8. Under **LDAP Access UserDN/Password** enter the credentials of the LDAP Service access. The user needs to have read rights on the whole directory service, because it will be used for the determination of the structure in the directory service.
9. Under **Naming Attribute** enter the name of the LDAP attributes, which contains the distinct user account name.
10. Optionally, you can add an **Additional term for LDAP search**, which will be attached to the search for users. This way, performance can be optimized.
11. As **Group attribute** enter the name of the LDAP attribute, which contains the group membership of a user.
12. Define the **Page Size**. This property sets the maximum number of items in each page of results that will be returned by a search. It affects query performance, but NOT the number of overall results. The standard value is 1000. Change this value in line with your server configuration.
13. Click **Import SSL Certificate** to verify the **Certificate DN**.

1.11.2 Problems When Configuring an Active Directory with LDAP over SSL

Symptom

You cannot configure an AD Connection under **Active Directory / LDAP** with the option **Use LDAPS connection** activated. When testing the connection, one of the following types of error messages appears:

- "The connection to the LDAP service failed! Check the certificate and server name";
- "simple bind failed".
The log file looks like:
- "2019-05-23 14:13:38,512 ERROR [https-jsse-nio-8443-exec-151] dec: simple bind failed: QA-DC01:636 javax.naming.CommunicationException: simple bind failed: QA-DC01:636 [Root exception is javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: No subject alternative DNS name matching QA-DC01 found.]"
or
- "javax.naming.CommunicationException: simple bind failed:
dc01.your.domain:636
[Root exception is javax.net.ssl.SSLHandshakeException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target]"

Problem

The **Domain Controller(s)** name and the certificate configured under **Import SSL Certificate** do not match.



Solution

1. Check that a *fully qualified name of the domain controller* has been entered, e.g. "dc01.your.domain". An IP address or a short name such as "dc01" will not be accepted when the domain controller name is checked against the certificate.
2. If several domain controllers are used, make sure that the *root certificate* has been configured.

1.11.3 Import of Administrator Accounts from Active Directory Fails

Symptom

The import of UMS administrators from an Active Directory fails, the result list of imported accounts is either empty or some accounts are missing on the list.

Problem

Active Directory user accounts may have an empty User Principal Name (UPN). This occurs when updating an older Active Directory (e.g. on Windows NT 4.0) to a new one migrating the AD user accounts to the new AD.

Solution

1. Set the UPN of each AD account to be imported.
2. Retry the import of AD users in IGEL UMS.

1.12 Profiles

- [Find Out a Profile's Priority](#)(see page 219)
- [Precedence of Profiles and Universal Firmware Updates](#)(see page 220)
- [Assigning Profiles to Devices filtered by Views or Search](#)(see page 221)

1.12.1 Find Out a Profile's Priority

Using profiles is a very powerful method to manage and configure one, ten, or thousands of endpoint devices with the IGEL UMS (Universal Management Suite). However, when you are deploying a great number of profiles, things can get confusing. Some profiles may have overlapping scopes and thus try to set different values for one specific parameter on a device. One profile will always win, but which one is it? Luckily, the UMS can show the order of priorities at a glance.

For a comprehensive reference of profiles, see the [Profiles Chapter](#)(see page 331) in the UMS Manual; the prioritization is covered in [Prioritization of Profiles](#)(see page 350).

The following example shows how to find out a profile's priority:

1. In the structure tree, select the device for which you want to see the order of profile priorities.



2. Take a look at the **Assigned objects** area. All profiles that are assigned to the device are listed by priority, in descending order. The profile with the highest priority is listed first, and so on. In the following screenshot, the profile with the highest priority is a master profile. It is followed by a firmware customization, which has in turn higher priority than a standard profile, see [Firmware Customizations](#)(see page 375). And at the bottom, the object with the lowest priority is displayed – a standard profile with the lower profile ID.

The screenshot shows the 'Assigned objects' section of the IGEL Universal Management Suite. It lists four items in descending order of priority:

- Background(ID: 5567) (highlighted)
- Logo IGEL
- Screensaver
- Browser

1.12.2 Precedence of Profiles and Universal Firmware Updates

This article explains which firmware update settings will be effective when several concurring settings are assigned to your devices. Firmware update settings can be defined locally on the device, by one or more profiles, or by one or more Universal Firmware Update.

General Order of Priority

Generally, the order of priority is as follows, from highest to lowest priority:

- Universal Firmware Update
- Profile
- Local settings

For details, see the following sections.

Universal Firmware Update vs. Profile

If both a Universal Firmware Update and a profile that contains update settings are assigned to your device, the Universal Firmware Update has priority over the profile. This is also valid if the profile is a master profile; for further information, see [Prioritization of Profiles](#)(see page 350).

The following settings under **System > Update > Firmware Update** are overwritten by the Universal Firmware Update:

- **Protocol**
- **Server name**
- **Port**
- **Server path**
- **User**
- **Password**

Profile vs. Local Settings

The settings of a profile always overwrite the local settings.

Universal Firmware Update vs. Universal Firmware Update

If several Universal Firmware Updates are assigned to one device, the rules described below apply.

Assignment to Different Levels in a Hierarchical Order of Folders

If several Universal Firmware Updates are assigned to a device via different folders and subfolders, the one that is closest to the device has priority over all others.

Example: A Universal Firmware Update for IGEL OS 10.05.100 is assigned to a folder named "devices", which contains our device. Another Universal Firmware Update which contains IGEL 10.06.100 is assigned to a folder named "teamA". The folder "teamA", on this part, contains the folder "devices". As a result, the devices will be updated to IGEL OS 10.05.100 (or keep IGEL OS 10.05.100) because the Universal Firmware Update for IGEL OS 10.05.100 is closer to the device in the folder hierarchy.

Assignment on the Same Level

If several Universal Firmware Updates are assigned to a device on the same hierarchical level, the one with the highest ID has priority over the others.

To find the ID of a Universal Firmware Update, move the mouse pointer over the Universal Firmware Update in question and read the tooltip:



In this example, the ID is 7818.

Compatibility

Only those Universal Firmware Updates are effective which are compatible with the device.

1.12.3 Assigning Profiles to Devices filtered by Views or Search

Valid for UMS version 5.02.100 and higher.

If you need to assign a profile to a group of devices which meet a certain criterion, you can proceed in the following way:

1. Define a view which filters the clients with a certain criterion (e. g. all devices which contain a USB storage hotplug).
2. Right-click the view to open the context menu.
3. Click **Assign profiles to the thin clients of the view**.

The **Assign profiles** window opens.



4. Select the relevant profile (e.g. the profile which allows USB storage hotplug).
5. Click to move it from the left to the right column.
6. Confirm the setting with **OK**.

In the same way you can assign profiles to devices of a search result:

1. Right-click the search result to open the context menu.
2. Click **Assign profiles to the thin clients of the search**.
The **Assign profiles** window opens.
3. Select the relevant profiles and click to move them from the left to the right column.
4. Confirm the setting with **OK**.

► To cancel the profile assignment, click **Detach profiles from the device of the view or search**.

You can also assign profiles to views or search results automatically and regularly as an administrative task.

1.13 Java Web Start

- [UMS Console via Java Web Start](#)(see page 222)
- [Error when connecting to UMS via Java Web Start: "received fatal alert: handshake_failure"](#)(see page 223)
- [VNC Connection Error with Java Web Start Console and external VNC Viewer](#)(see page 224)

1.13.1 UMS Console via Java Web Start

Requirements

- Java 1.8.0_212

Starting the UMS Console via Java Web Start

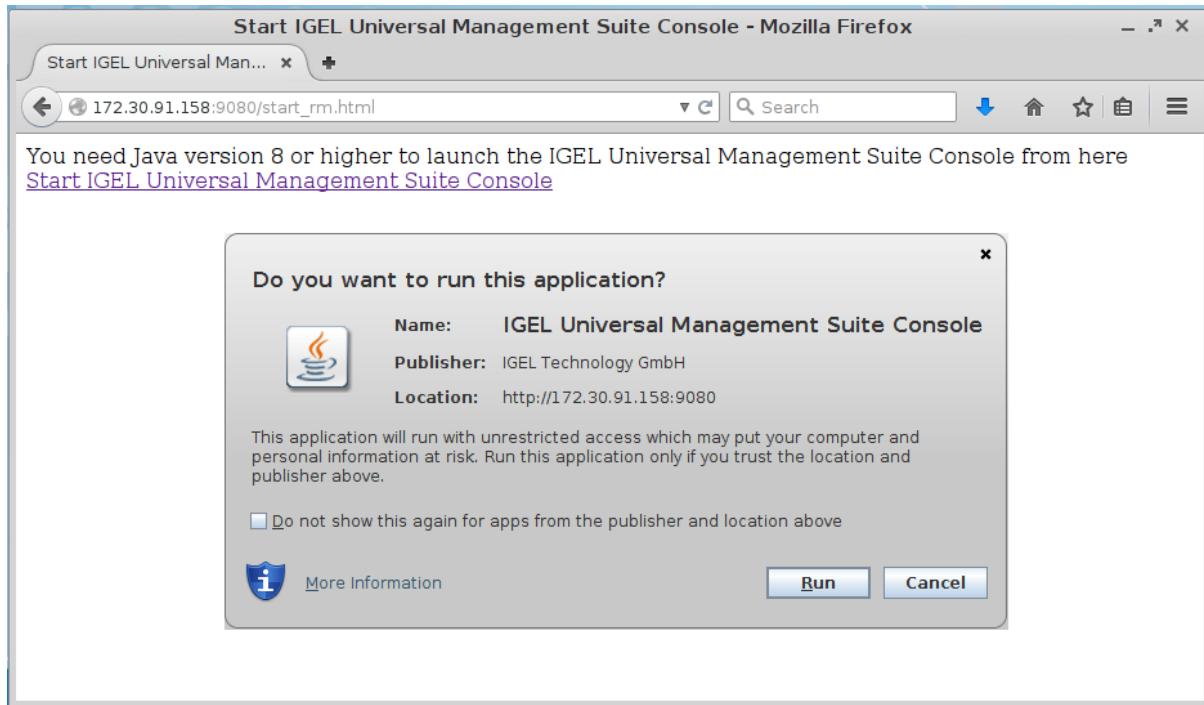
To start the UMS Console via Java Web Start, proceed as follows:

1. In a web browser, open the address
 - [http://\[UMS-Server\]:9080/start_rm.html](http://[UMS-Server]:9080/start_rm.html) if you want to use the HTTP port
or
 - [https://\[UMS-Server\]:8443/start_rm.html](https://[UMS-Server]:8443/start_rm.html) if you want to use the HTTPS port.



- i** If **UMS Administrator > Settings > Allow SSL connections only** is activated, the HTTP port, 9080, will be disabled. See also [Settings for IGEL UMS Administrator](#)(see page 530).

2. Click on the **Start IGEL Universal Management Suite Console** link.



3. Confirm that the downloaded JNLP file will be opened with the **Java Web Start Launcher**.
The application will be downloaded.
4. Allow the application signed by IGEL Technology GmbH to be executed.
The UMS Console will start, and the [login window](#)(see page 306) will appear.

- i** Starting the UMS Console via Java Web Start ensures that the version of the UMS Console matches the version of the UMS Server.

1.13.2 Error when connecting to UMS via Java Web Start: "received fatal alert: handshake_failure"

Symptom

When trying to connect to *UMS* via *Java Web Start*, the connection fails with the error message "received fatal alert: handshake_failure".

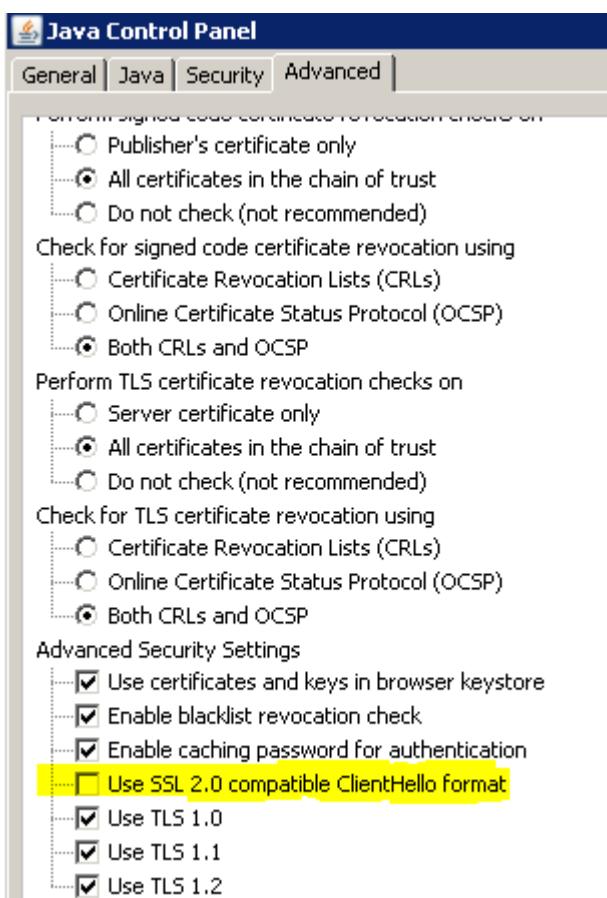


Problem

The old Java Feature "SSL 2.0 compatible ClientHello format" is outdated and not accepted by UMS versions 4.09.100 or newer.

Solution

Disable **Use SSL 2.0 compatible ClientHello format** in the **Advanced Settings** menu of the **Java Control Panel**.



1.13.3 VNC Connection Error with Java Web Start Console and external VNC Viewer

Symptom

You are using IGEL UMS Java Web Start Console with Java SE Runtime Environment 7 or 8 (Java 7 or 8) and you have defined an external VNC viewer program in IGEL UMS Java Web Start Console.

When shadowing a thin client the error message appears: **Cannot run program """: CreateProcess error=2, system cannot find the file.**



Problem

The VNC viewer program's path definition is not correct. Java 6 did accept the path without quotes but Java 7 or 8 will not find the program without quotation. So this problem will most likely occur after upgrading the Java Environment.

Solution

Check the VNC viewer program's path in your UMS Console:

1. Go to **Misc > Settings**
2. Select your **External VNC viewer** program
3. Make sure the path is enclosed in double quotes ("C:\program files\path\program.exe")
4. Save your settings with **OK**

1.14 Misc

- [Where Can I Find the UMS Log Files?\(see page 225\)](#)
- [Clearing up the UMS\(see page 227\)](#)
- [Removing a Certificate\(see page 229\)](#)
- [Notifications - Always Be Informed\(see page 229\)](#)
- [Updating Timezone Information \(Daylight Saving Time, DST\)\(see page 233\)](#)
- [E-Mail Settings for Gmail Accounts\(see page 235\)](#)
- [Searching With Regular Expressions in UMS\(see page 236\)](#)
- [Copy Sessions in Setup or UMS\(see page 237\)](#)
- [Drag & Drop Acceleration for Large Structure Trees\(see page 237\)](#)
- [Which UMS Directories Should Be Scanned for Viruses, Which Can Be Excluded?\(see page 238\)](#)
- [Licensing with Smartcard fails\(see page 239\)](#)
- [Finding UD Devices for PowerTerm Activation using a View\(see page 239\)](#)

1.14.1 Where Can I Find the UMS Log Files?

UMS Server

<code>rmguiserver/logs</code> (<code>rmguiserver/conf/log4j.properties</code> - for configuring the logs)	
<code>catalina.log</code>	Central log file for all logging events
<code>ums-server-msg.log</code>	Logging of the Apache ActiveMQ messaging
<code>communication.log</code>	Logging of communication with UMS Console or devices Edit at # communication logging - define the log levels; refer to Log4j documentation ²⁶

²⁶ <https://logging.apache.org/log4j/2.x/manual/index.html>



<code>license_deployment.log</code>	Logging of licenses Edit at # license deployment logging; refer to Log4j documentation ²⁷
<code>localhost.log</code>	Technical logging of the Apache Tomcat server
<code>stderr.log</code>	Error output of the Apache Tomcat server
<code>stdout.log</code>	Standard output of the Apache Tomcat server
<code>umsthreaddump.log</code>	Periodic logging of the threads Edit with # threaddump logging; refer to Log4j documentation ²⁸
<code>usgcommunication.log</code>	Logging of communication with ICG Edit at # communication logging - define the log levels; refer to Log4j documentation ²⁹
<code>health.log</code>	Logging of the UMS HA Health Check (see page 688)
<code>monitoring.log</code>	Performance logging (see page 501) Edit at # execution monitoring; change INFO to DEBUG to get detailed information on each method call (the server restart is then required)
<code>rogui/server/logs</code> (<code>rogui/server/conf/log4japi.properties</code> - for configuring the logs)	
<code>api.log</code>	Logging of the API service

UMS Load Balancer

<code>umsbroker/etc/work/logs</code> (<code>umsbroker/etc/conf/log4j.properties</code> - for configuring the logs)	
<code>igel-ums-broker.log</code>	Central log file for all logging events
<code>broker-msg.log</code>	Logging of the messages exchanged
<code>broker-health.log</code>	Logging of the UMS HA Health Check (see page 688)
<code>broker-monitoring.log</code>	Performance logging (see page 501) Edit at # monitoring logging; change INFO to DEBUG to get detailed information on each method call (the server restart is then required)

UMS Watchdog

<code>umswatchdog/etc/work/logs</code> (<code>umswatchdog/etc/conf/log4j.properties</code> - for configuring the logs)	
<code>igel-ums-watchdog.log</code>	Central log file for all logging events

²⁷ <https://logging.apache.org/log4j/2.x/manual/index.html>

²⁸ <https://logging.apache.org/log4j/2.x/manual/index.html>

²⁹ <https://logging.apache.org/log4j/2.x/manual/index.html>



<code>watchdog-msg.log</code>	Logging of the messages exchanged
<code>watchdog-health.log</code>	Logging of the UMS HA Health Check (see page 688)

UMS Console

<code>\$HOME/.igel</code>	
<code>RMClient.exe.log</code>	Startup logging
<code>\$HOME/.igel/logs</code> (rmclient/log4j.properties - for configuring the logs)	
<code>igel-ums-console.log</code>	Central log file for all logging events

UMS Administrator

<code>\$HOME/.igel</code>	
<code>RMAadmin.exe.log</code>	Startup logging
<code>rmguiserver/logs</code> (rmadmin/log4j.properties - for configuring the logs)	
<code>igel-ums-admin.log</code>	Central log file for all logging events

For enabling the logging of UMS user actions and actions initiated by a device, see [Logging](#)(see page 500).

If you require UMS log files for IGEL Support, see [Save Support Information / Send Log Files to Support](#)(see page 525).

1.14.2 Clearing up the UMS

Problem

You have several firmware versions in the UMS. Your collection of clients and profiles has become large and confusing. You are losing track of assignments and connections between these elements.

Goal

You want to minimize the variety of firmware and profiles to simplify processes. You just want to see what you need. The firmware, clients, and profiles are interdependent. So, what is the best way to proceed?

Solution

- ⓘ We advise making a back-up of the UMS before deleting any components. You can also use the UMS recycle bin for the deleted objects.

The following are the main steps for reorganizing the UMS:

1. Download the new firmware.
2. Move clients to the new firmware.
3. Move profiles to the new firmware.



4. Delete old firmware, clients, and profiles that are no longer required.

Downloading the new Firmware

1. Check our [download server](#)³⁰ to see whether there are new updates that are relevant for your applications.
2. Download the relevant update files. Install an update directory for the files on the UMS server or on your FTP server.

Moving Clients to the New Firmware

Find out how many different firmware versions you really need.

Upgrading all clients to the same firmware:

1. Create a new **View** to search for all clients using a firmware version older than the current version.
Example:
View Name: Show all UD LX devices with old firmware
Rule: Product name is like (!reg!)(?i).*Universal Desktop LX.* AND Firmware version is less than 5.04.100
2. Assign the update directory to these devices.
3. Start the update process.

Moving Profiles to New Firmware

Examine your profiles and decide which of them are relevant for the new firmware. You have three possibilities you can do now:

- Adjust the firmware version the profiles are based on, to be sure that they will work with the new firmware.
- Leave the profile settings as they are.
If the parameters of the new firmware match the parameters of the old version, a profile will work anyway. If they do not match, these parameters will be ignored.
- Create new profiles.

For more information see UMS Manual: [Creating Profiles](#)³¹.

Deleting old Firmware, Clients and Profiles that are no longer required

To finally clear up the UMS you now should delete obsolete objects.

- Use again Views to select the clients, which are no longer required.
For more Information see UMS Manual: [How to Create a New View in the IGEL UMS](#)(see page 403).
- Select the obsolete profiles. You can do this manually or by using the search option: **Misc > Search > Profiles > Product&Firmware.**

³⁰ <https://www.igel.com/software-downloads/>

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



- Delete old firmware which is not assigned any longer to a client or profile: **Misc > Remove Unused FIRMWARES.**

Do you have also obsolete **Views, Jobs, Template Keys?** Delete them as well.

For **Template Keys** the **Profile Relation** is shown in the setting mask.

1.14.3 Removing a Certificate

UMS also allows you to remove the certificate from devices. This may be necessary

- in order to prepare for moving a device from the test environment to the productive environment
- in order to prepare for replacing the server certificate.

To remove the certificate, proceed as follows:

- ▶ Select **Remove UMS Certificate** under **Devices > Commands > Other device commands**.

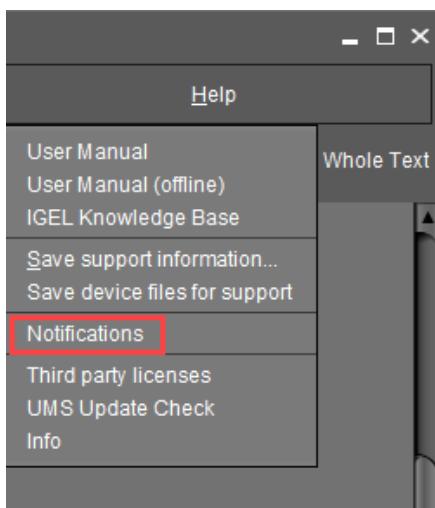
Each *IGEL* UMS Server can now access the device configuration until one of the servers registers the client.

1.14.4 Notifications - Always Be Informed

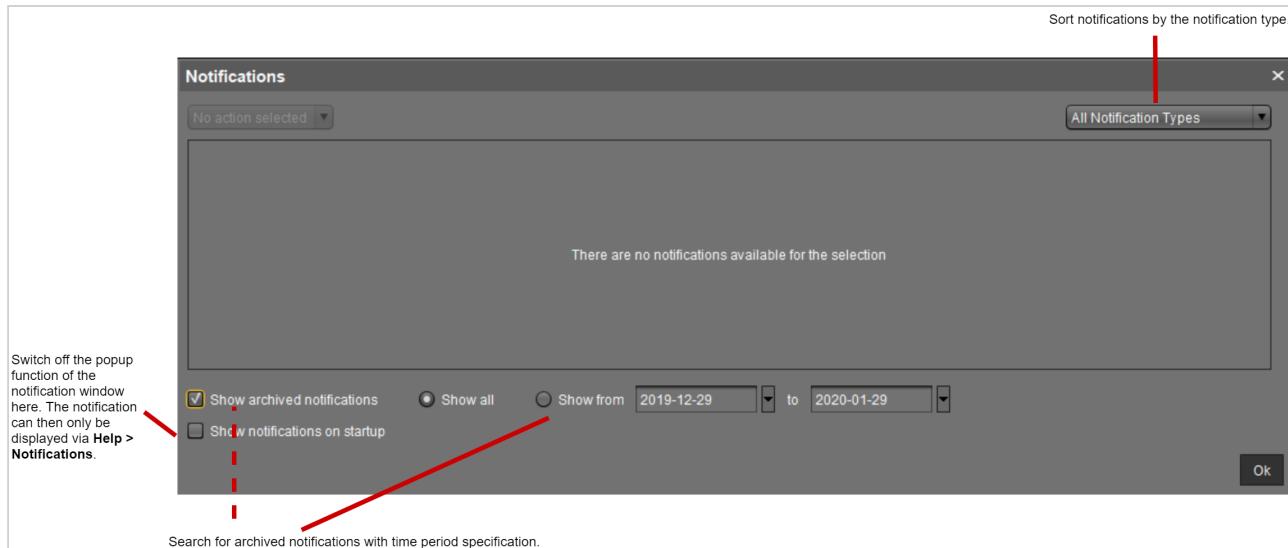
As of UMS 5.09.100, you can get notifications about newly available firmware updates, device licenses, etc. By default, notifications are enabled and pop up when you start the UMS Console. In this article, you will learn how to adapt this feature to your needs.

About Notifications

Basically, all users with read permission can see the notifications. The notifications are displayed after starting the UMS Console. When the dialog is closed, the notifications can still be viewed anytime under **Help > Notifications**.



The Notification Window



Enabling the Notification Function

1. Go to **UMS Administration > Misc Settings**.
2. Activate **Enable notifications**.

The notification feature is active. The notifications can be viewed under **Help > Notifications**.

Exporting Notification and Sending It by Email

The disk usage notifications can be exported and sent via email: **UMS Administration > Administrative Tasks > add > Action: "Send notification information via email"**.

- [Configuring the Notifications Pop-Up\(see page 230\)](#)
- [Disk Usage\(see page 231\)](#)
- [Global Notifications\(see page 232\)](#)
- [Admin Tasks\(see page 232\)](#)

Configuring the Notifications Pop-Up

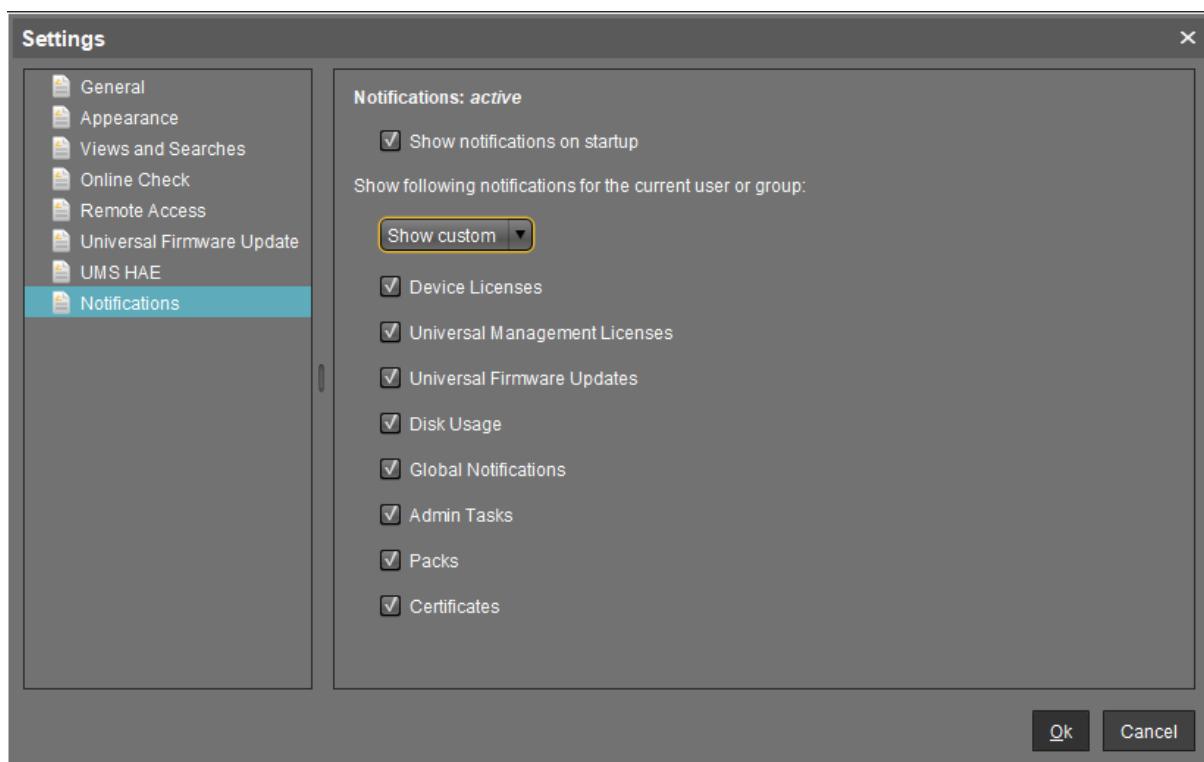
To configure the notifications pop-up:

1. Go to **Misc > Settings > Notifications**.
2. Enable **Show notifications on startup** to display the notification window as a pop-up every time the UMS Console is started.
3. Select **Show custom** under **Show following notification for the current user or group**.
4. Specify which content should be displayed in the notification.
Possible options:
 - **Device Licenses:** Informs about the expiration of device licenses.



- **Universal Management Licenses:** Informs about the expiration of UMS licenses and if the available license amount is exceeded.
- **Universal Firmware Updates:** Informs about the latest firmware updates.
- **Disk Usage:** Informs about a critical value of free disc space. For more details, see [Disk Usage](#)(see page 231).
- **Global Notifications:** Informs about important news like maintenance times and bugfixes. For more details, see [Global Notifications](#)(see page 232).
- **Admin Tasks:** Automatically informs in a set of cases if no administrative task has been defined. For more details, see [Admin Tasks](#)(see page 232).
- **Packs:** Informs if license packs will expire.
- **Certificates:** Informs if certificates will expire.

5. Confirm the settings with **Ok**.



Disk Usage

Menu path: **Misc > Settings > Notifications > Disk Usage**

This notification informs the user when there is not enough free drive space anymore.

- i** The notifications are generated on a daily base. Therefore it might take up to 24 hours until you get a notification after your available disk space has fallen below the configured value.



The individual critical drive space value can be set under **UMS Administration > Global Configuration > Misc Settings > Notifications**.

Types of disk usage notifications:

- Specific notification for each connected server: The server hostname and the available drive space will be shown in the notification message.
- Installation path and database path are on different file systems: Two notifications for each file system will be shown.

Global Notifications

Menu path: **Misc > Settings > Notifications > Global Notifications**

This notification type informs the user about important news, like maintenance times and bugfixes.

Unlike other notification types, the **Global Notifications** message is not automatically generated by the UMS, but is parsed from an XML file, which must be created and uploaded to the [firmware update server](#)³².

Global Notifications can include an additional web link that can provide more information. The web link is displayed as a blue link button next to the global notification.

Global Notification		
Notification Type	Message	Message created
error	This is a global notification of type "error"	Feb 13, 2019
warning	This is a global notification of type "warning".	Feb 13, 2019
info	New feature "global notifications"	Feb 13, 2019
info	Link Read something about the UMS.	Feb 13, 2019

- ▶ Click the link to open the web page in the standard browser.
- ▶ Move the mouse over the link to display the URL.

Admin Tasks

Menu path: **Misc > Settings > Notifications > Admin Tasks**

Admin Tasks: Informs automatically in the following cases if no administrative task has been set:

- enabled **Logging**;
- a new **Scheduled Job** has been set;
- the embedded database is active.

Exporting Notification and Sending It by Email

The disk usage notifications can be exported and sent via email: **UMS Administration > Administration tasks > Add > Action: Send notification information via email**.

³² https://www.igel.com/files/IGEL_UNIVERSAL_MANAGEMENT_SUITE/.properties/global/%20notifications.xml



- ⓘ Each server executes an administrative task every 6 hours to check the available space on the drive and deliver the disk usage information to the notification system. Disk usage admin tasks older than 24 hours are considered expired. In order to display the notification, the server must have been running continuously up to 6 hours within the last 24 hours.

1.14.5 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). This is known to work for

- IGEL Linux version 10.01.100 or newer
- IGEL Linux version 5.04.100 or newer
- IGEL Linux version 4.14.100 or newer
- IGEL Linux ARM version 1.09.100 or newer.

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
 - <http://packages.ubuntu.com/trusty-updates/all/tzdata/download> (for *IGEL Linux* version 5.x)
 - <http://packages.ubuntu.com/precise-updates/all/tzdata/download> (for *IGEL Linux* version 4.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**.
- 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 `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`

i 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
```

1.14.6 E-Mail Settings for Gmail Accounts

Purpose

You want to send views from the IGEL Universal Management Suite by email using a Gmail account.

Solution

- i** In order to allow the UMS to send emails via Gmail, you have to make the following setting in your Google account:
- Log in to Google.
 - Go to **My Account > Sign-in & security > Connected apps & sites**.
 - Set **Allow less secure apps** to ON.

1. Go to **UMS Administration > Global Configuration > Mail Settings**.
2. Enter `smtp.gmail.com` as the **SMTP Host**.
3. Enter your Gmail address under **Sender Address**.
4. Enable **Activate SMTP Auth**.
5. Enter your Gmail address under **SMTP User**.
6. Enter your Gmail password under **SMTP Password**.
7. Enter `465` under **SMTP Port**.
8. Enable **Activate SMTP SSL**.
9. Under **Mail recipient**, enter the email address you want administrative emails from the UMS to be sent to.



Mail Settings

Mail Settings

SMTP Host	smtp.gmail.com
Sender Address	user@gmail.com
<input checked="" type="checkbox"/> Activate SMTP Auth	
SMTP User	user@gmail.com
SMTP Password	*****
SMTP Port	465
<input checked="" type="checkbox"/> Activate SMTP SSL	
<input type="checkbox"/> Activate SMTP Start TLS	
Send Test Mail	Result: <input type="text"/>

Recipient for administrative task result and service mails

Mail recipient	user@example.com
----------------	------------------

10. Click **Send Test Mail** to test your settings.

Additional Information

<https://support.google.com/a/answer/176600?hl=en>

1.14.7 Searching With Regular Expressions in UMS

Universal Management Suite (UMS) can help you manage large thin client installations. Often you will want to search or filter for objects with certain properties, and UMS offers a wide selection. For advanced searches, however, you might need Regular Expressions, a powerful feature built into UMS.

You can use them in:

- Quick Search
- **Misc > Search**
- **Views > New View**
- **Edit > Edit Configuration > System > Registry > Search parameter ...**
- **UMS Administration > Global Configuration >Default Directory Rules**



UMS uses Java Regular Expressions. These are different from the globbing patterns that you may know from the DOS/Windows Command Prompt or the Linux commandline. For example, instead of using * to match any number of characters, in UMS you use:

.*

Here the . matches any character. The * acts as a quantifier, stating how often the preceding pattern may occur, in this case zero or more times.

So, if you want to find something that begins with IGEL, use:

IGEL.*

Something beginning with IGEL and ending with 12:

IGEL.*12

If you want to find something ending with IGEL:

*.IGEL

Find out more about Java Regular Expressions in [Oracle's documentation](#)(see page 236).

1.14.8 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.

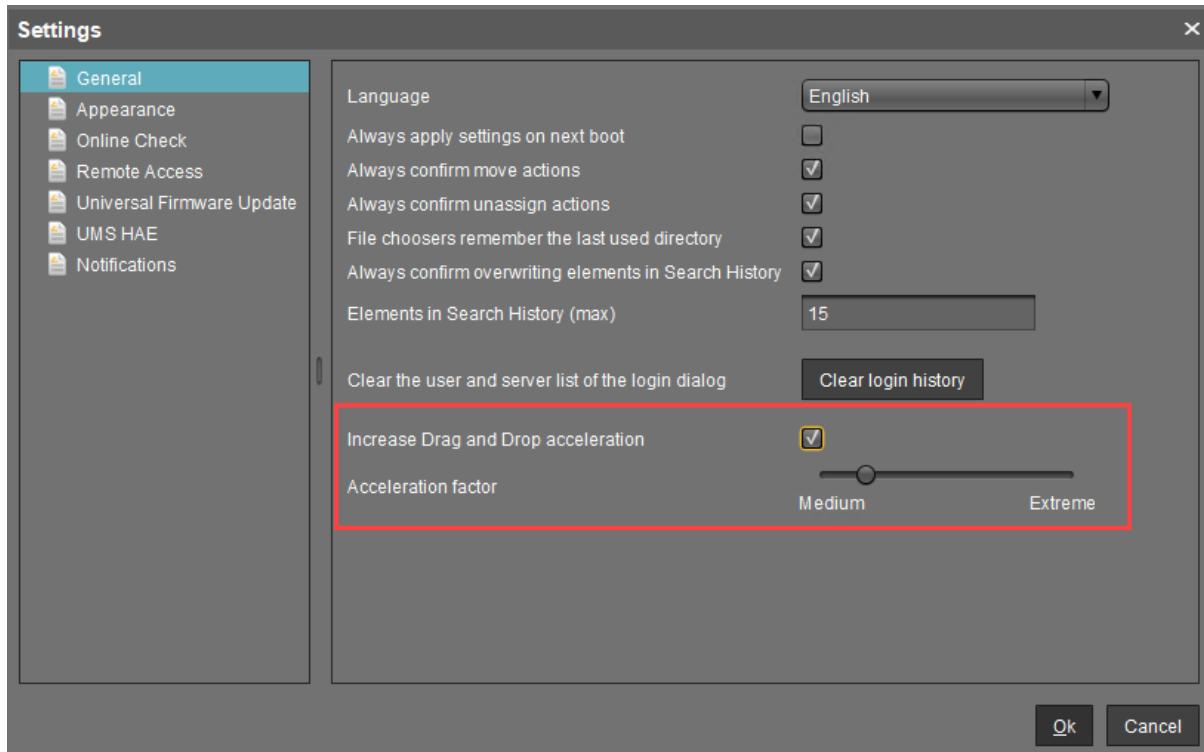
1.14.9 Drag & Drop Acceleration for Large Structure Trees

If you have a really large number of objects in your *IGEL* UMS (Universal Management Suite), it can be tedious to drag and drop an object to a new position if the new position is quite far away from the current position.

But with UMS version 5.03.100 or newer, you can increase your scrolling speed. As soon as the object you are moving touches the bottom edge of the structure tree window, the acceleration starts.

To enable drag and drop acceleration:

1. Open the UMS and go to **Misc > Settings > General**.
2. Activate **Increase Drag and Drop acceleration**.
3. Adjust the **Acceleration factor** according to your needs and click **Ok**.



Drag & drop acceleration is ready.

1.14.10 Which UMS Directories Should Be Scanned for Viruses, Which Can Be Excluded?

Question

Which UMS directories can be excluded from antivirus scanning, which directories should be scanned?

Environment

This article is valid for the following environment:

- UMS 5.08 or higher
- UMS is installed on Microsoft Windows server

Answer

Everything in C:\<Program Files>\IGEL\RemoteManager\ can be excluded.

If your UMS also manages Windows devices, the downloadable files in C:\<Program Files>\IGEL\RemoteManager\rmguiserver\webapps\ums_filetransfer\ should be scanned.



1.14.11 Licensing with Smartcard fails

Symptom

You can not create licenses from smartcard in IGEL UMS (**License Management**) although valid licenses are stored on the SIM / smartcard and the smartcard reader's driver is installed to your system.

- ▶ The smartcard reader shows a problem in the Windows Hardware Manager [!].

Problem

Another smartcard reader (eg. built-in cardreader) overrides the access.

Solution

Deactivate or deinstall all other smartcard readers in the Windows Hardware Manager.

1.14.12 Finding UD Devices for PowerTerm Activation using a View

Symptom

You want to use Ericom PowerTerm terminal emulation with devices running IGEL Universal Desktop Linux v5 (firmware version 5.xx.xxx).

To use your Ericom PowerTerm terminal emulation you need a free license key from IGEL. To get to the activation form please register with our support and ticket system.

After successful registration you have access to free technical support, and to the IGEL Service- and Repair-Center as well as to the license activation form.

Problem

You have to send the MAC addresses of all devices to be activated to IGEL but there is no easy way to identify all devices in UMS that may need the activation license.

Solution

1. Start the IGEL Universal Management Suite that manages all your IGEL UD devices.
2. Create a new View (e. g. named PowerTerm Activation) with selection rule: Product ID matches the following regular expression:
.*LX \d\|\d[^p]*

i This feature uses Java Regular Expressions. Find out more about these from Oracle's documentation.



Create new view

Text search

.LX \d\d[\^p]*

Consider case
 Compare whole text
 Use regular expression
 Not like

3. Go to System > License Management.
4. Click Export MAC list
5. Select option Export all MAC addresses from a view.



6. Click Next.
7. Select the view created before.



8. Click Next
All devices with UD Linux v5 firmware and without PowerTerm license will be listed.
9. Click Export.
10. Select target folder.
11. Define file name.
12. Click Save.
13. Send the exported CSV file to IGEL as requested in the activation form.
14. Import the license file you will receive upon your request later.



2 Installation and Sizing Guidelines for IGEL UMS

The following installation and sizing guidelines are intended to support you with setting up the IGEL Universal Management Suite environment – UMS Server, UMS Console & UMS Web App, database, and, if required, load balancer and ICG instances.

The size and structure of the UMS setup depend mainly on the following criteria:

- Number of devices
- High Availability
- ICG connection for devices outside of your company network

2.1 General Preconditions

The Installation and Sizing Guidelines apply for a standard UMS setup and describe the most common UMS environments. Any individual exceptions or requirements may not be covered by these scenarios.

- System requirements: UMS 6.05 and newer, ICG 2.02 and newer
- All UMS Servers and UMS Load Balancers must reside on **the same VLAN**.
For High Availability (UMS HA), network traffic must be allowed over UDP broadcast port 6155, and TCP traffic and UDP broadcast traffic over port 61616. For further port configuration, see [UMS Communication Ports](#)(see page 48).
- Note: IGEL UMS Server HA is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks.
- UMS Console may be located **inside the same (V)LAN as UMS Servers** (no NAT, no proxies) or **outside the VLAN** with firewalls/routing configured according to [UMS Communication Ports](#)(see page 48).
- Devices **directly connected to the UMS Server** are in **the same (V)LAN as UMS Servers** (no NAT, no proxies). If there is a firewall, it must be configured according to [UMS Communication Ports](#)(see page 48).
- Devices **outside of the internal LAN** are connected **via ICG**.
- Devices are **not booted/rebooted frequently** (once a day on average).
- **A maximum of 10 different firmware versions** is managed via UMS.
- UMS backups and exports are **not permanently stored on the UMS server** host.
- In the case of automatic device registration (see [Registering Devices Automatically](#)(see page 312)): The **DNS** alias `igelrmserver` or the **DHCP** tag can only point to ONE UMS installation.
Therefore, the installation of several separate UMS Servers (without the High Availability Extension) in one network is not recommended.

2.1.1 Recommended Additional Information

[UMS Communication Ports](#)(see page 48): Find a list with all ports that are relevant for the communication with the UMS.

"Supported Environment": Find in this section in the [latest release notes](#)(see page 565), which servers, clients, and backend databases are supported.

[High Availability \(HA\)](#)(see page 657): Find useful how-tos and the reference guide around your HA installation.



IGEL Cloud Gateway³³. Find how-tos, the reference guide, and additional information concerning the management of endpoints outside the company network.

- Installation Types & Diagrams(see page 243)
- Performance Optimizations(see page 251)

2.2 Installation Types & Diagrams

Installation Size	#Devices	#UMS Server Host (+ Load Balancer)	UMS Server	UMS Console Standalone	#Load Balancer Standalone	Load Balancer Standalone	Database* * *	ICG
S	<1 server 5.000	8 GB RAM (UMS Web App + 1 GB) 4 CPUs 25 GB free disk space	Optional* 3 GB RAM 2 CPUs 1 GB HDD				Embedded database	1 ICG instance per 2,500 devices
M	<1 server 15.000	8 GB RAM (UMS Web App + 1 GB) 4 CPUs 25 GB free disk space	Optional* 3 GB RAM 2 CPUs 1 GB HDD				External database 10 GB	Server generally: 8 GB RAM 2 CPUs 20 GB HDD
M / S (HA)	<2 servers 15.000 2 load balancers	9 GB RAM (Web App +1GB) 6 CPUs 25 GB HDD	Optional* 3 GB RAM 2 CPUs 1 GB HDD				External database 10 GB	Only ICG service: 2 GB RAM 2 CPUs 2 GB HDD
L (HA)	<2 servers 50.000 2 load balancers	6 GB RAM*** (Web App +1GB) 4 CPUs 25 GB HDD	Mandatory 3 GB RAM 2 CPUs 1 GB HDD				External database 10 GB	

³³ <https://kb.igel.com/igelicg-2.02/en/igel-cloud-gateway-icg-31600925.html>



Installation Size	#Devices	#UMS Server Host (+ Load Balancer)	UMS Server	UMS Console Standalone	#Load Balancer Standalone	Load Balancer Standalone	Database*	ICG
XL (HA)**	<Up to 300.06 servers**	00 (1 server / 50,000 devices)	9 GB RAM (Web App +1GB) 6 CPUs 25 GB HDD	Mandatory	Up to 3 Load Balancer (1 LB / 3 Server)	4 GB RAM 4 CPUs 2 GB HDD	External database 20 GB	

* UMS Console can be installed on UMS Server host.

** Follow the recommendation of the external database system on RAM and CPU.

*** RAM and CPU requirements are less than in the case of **M / S (HA)** installation since the UMS Console is installed on a separate host machine (**UMS Console Standalone = Mandatory**).

**** General recommendation: 1 UMS Server per 50,000 devices, 1 load balancer for 3 UMS Servers.

- Small Environment: UMS S(see page 244)
- Medium Environment: UMS M(see page 246)
- Small and Medium Environments: UMS M/S (HA)(see page 247)
- Large Environment: UMS L (HA)(see page 249)
- Extra Large Environment: UMS XL (HA)(see page 250)

2.2.1 Small Environment: UMS S

Small Size UMS Installation (<5k Devices) or Demo/POV Environment with an Embedded Database

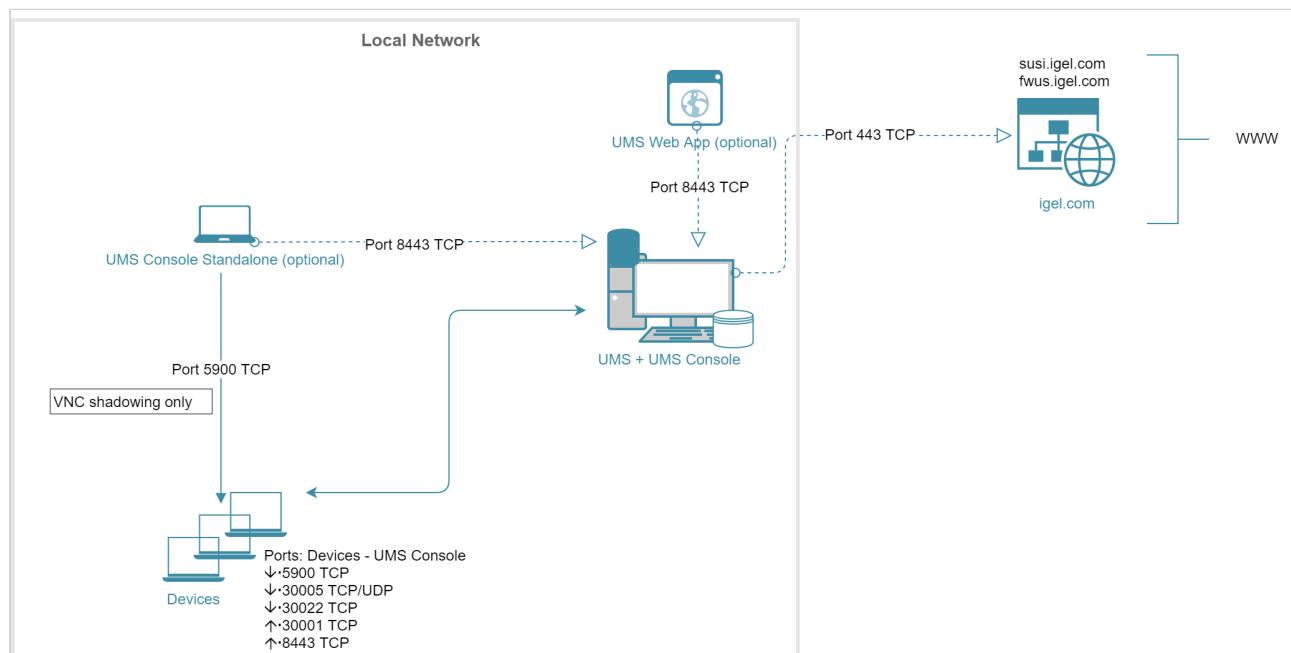
Installation Size	#Devices	#UMS Server Host	UMS Server	UMS Console Standalone	#Load Balancer Standalone	Load Balancer Standalone	Database	ICG
S	<1 server 5.000		8 GB RAM (UMS Web App + 1 GB) 4 CPUs 25 GB free disk space	Optional*			Embedded database	1 ICG instance per 2,500 devices Server generally: 8 GB RAM



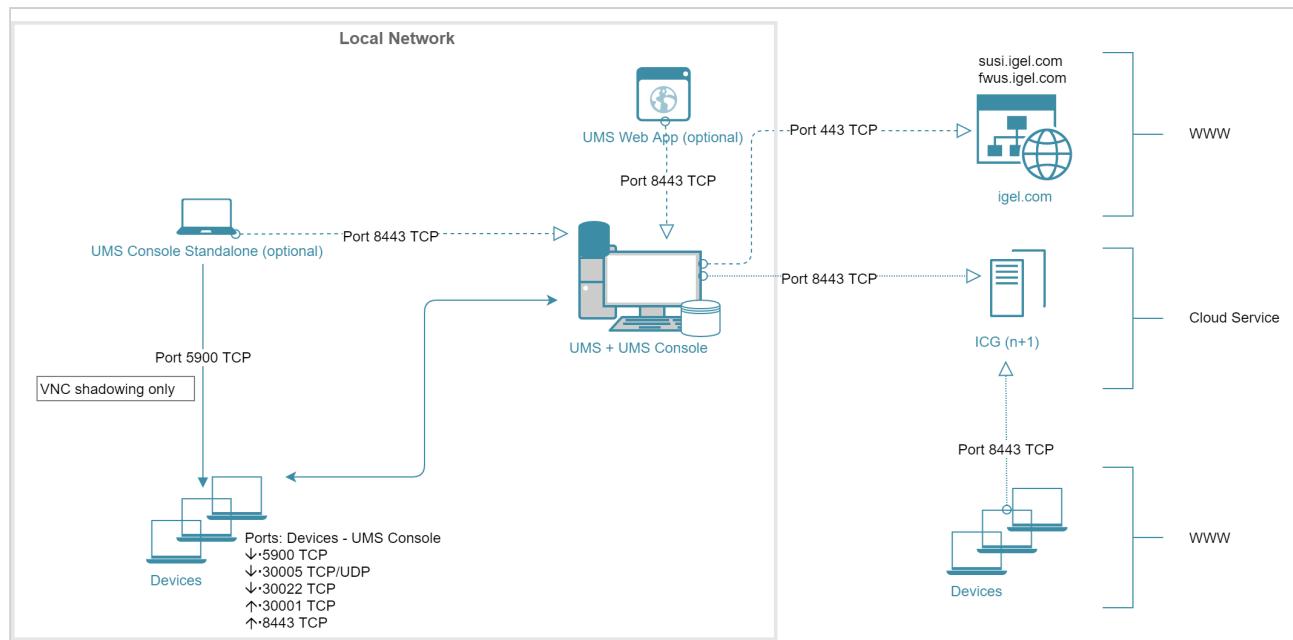
Install Size	#Devices	#UMS Server Host	UMS Console Standalone	#Load Balancer Standalone	Load Balancer Standalone	Database	ICG
							2 CPUs 20 GB HDD Only ICG service: 2 GB RAM 2 CPUs 2 GB HDD

* UMS Console can be installed on UMS Server host.

Architecture: Small Environment



Architecture: Small Environment + ICG in Cloud



2.2.2 Medium Environment: UMS M

Medium Size UMS Installations (up to ~15k Devices); No High Availability

Installation Size	#Devices	#UMS Server Host	UMS Server	UMS Console Standalone	#Load Balancer Standalone	Load Balancer * Standalone	Database* ICG	ICG
M	<1 server 15.000		8 GB RAM (UMS Web App + 1 GB) 4 CPUs 25 GB free disk space	Optional* 3 GB RAM 2 CPUs 1 GB HDD			External database 10 GB	1 ICG instance per 2,500 devices Server generally: 8 GB RAM 2 CPUs 20 GB HDD Only ICG service: 2 GB RAM 2 CPUs 2 GB HDD

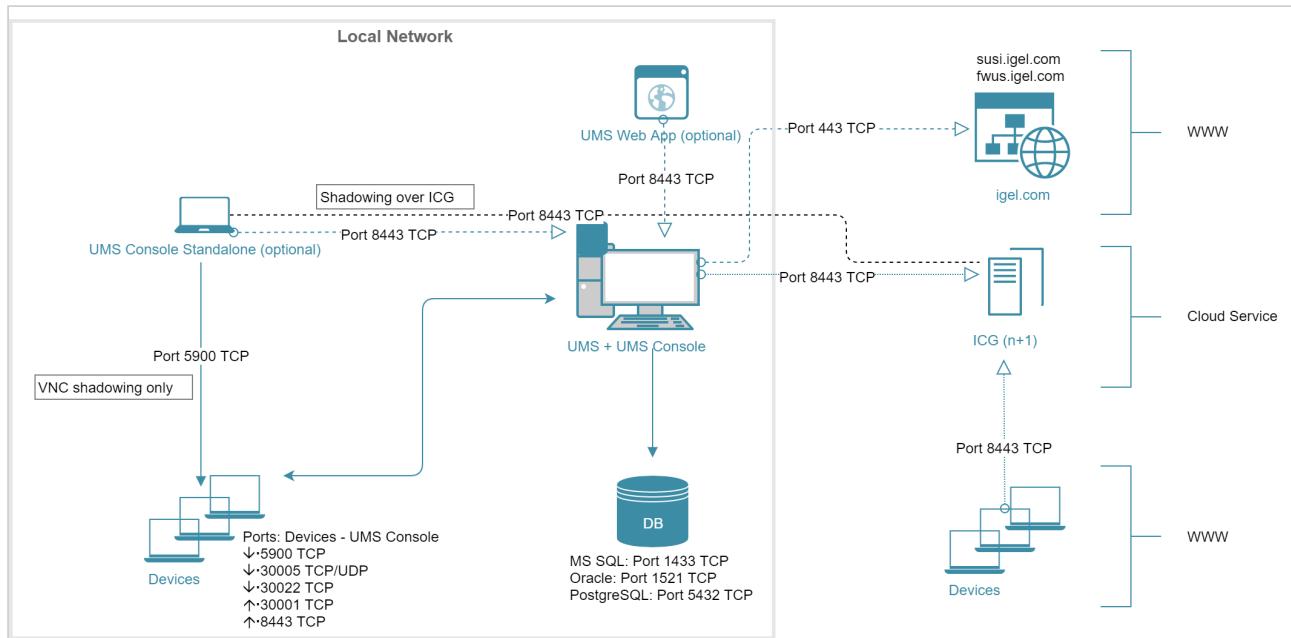


* UMS Console can be installed on UMS Server host.

** Follow the recommendation of the external database system on RAM and CPU.

i For High Availability, see [Small and Medium Environments: UMS M/S \(HA\)](#)(see page 247).

Architecture: Medium Environment + ICG



2.2.3 Small and Medium Environments: UMS M/S (HA)

Small and Medium Size UMS Installations (up to ~15k devices); High Availability

Install ation Size	#Devi ces	#UMS Server Host (+ Load Balancer)	UMS Server	UMS Console Standalon	#Load Balanc er	Load Balanc er	Database*	ICG
M / S (HA)	<2 servers 15.00 2 load balancers	9 GB RAM (Web App +1 GB) 6 CPUs 25 GB HDD	Optional* 3 GB RAM 2 CPUs 1 GB HDD				External database 10 GB	1 ICG instance per 2,500 devices Server generally: 8 GB RAM 2 CPUs

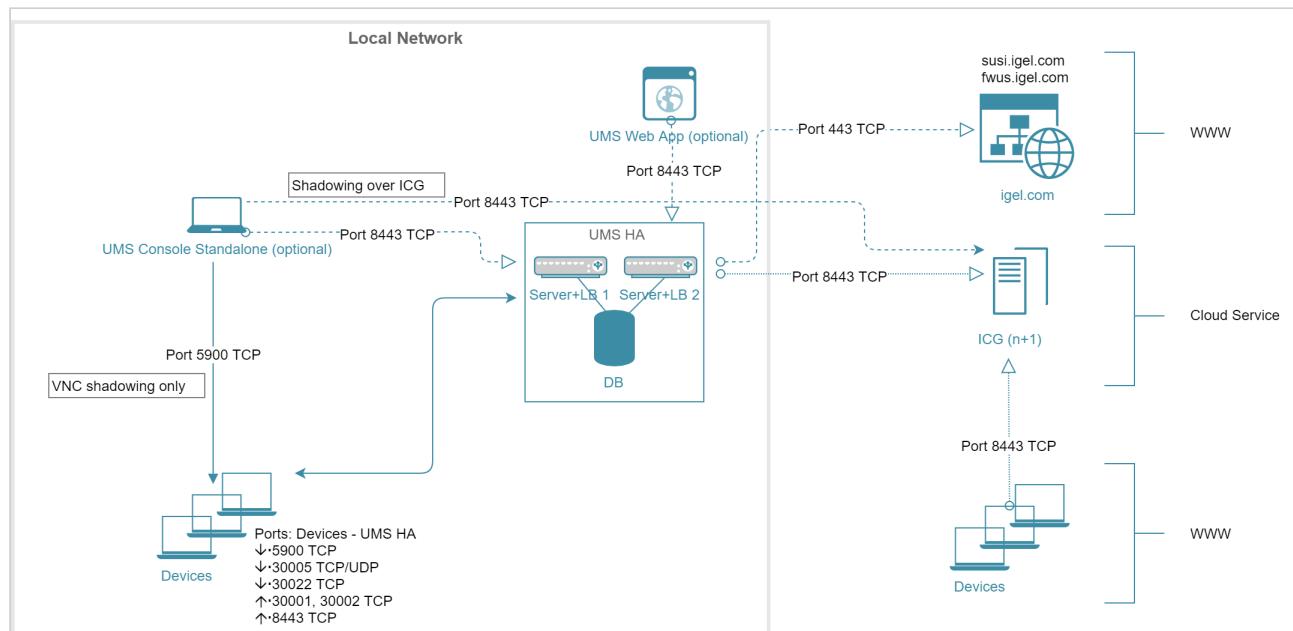


Installation Size	#Devices	#UMS Server Host (+ Load Balancer)	UMS Console Standalone	#Load Balancer Standalone	Load Balancer Standalone	Database*	ICG
						20 GB HDD Only ICG service: 2 GB RAM 2 CPUs 2 GB HDD	

* UMS Console can be installed on UMS Server host.

** Follow the recommendation of the external database system on RAM and CPU.

Architecture: Small and Medium Environment (HA) + ICG





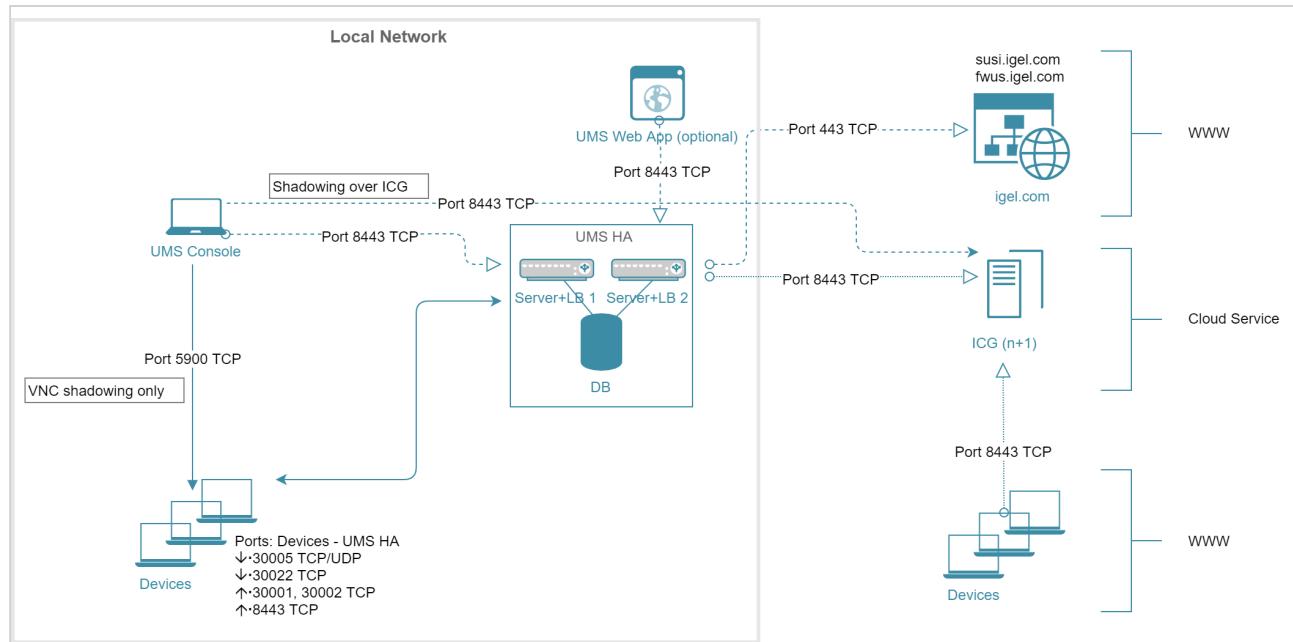
2.2.4 Large Environment: UMS L (HA)

Large UMS Installations with up to 50k Devices; High Availability + ICG

Installation Size	#Devices	#UMS Server Host (+ Load Balancer)	UMS Server	UMS Console Standalone	#Load Balancer Standalone	Load Balancer Standalone	Database*	ICG
L	<2 servers 50.00 0 load balancers	6 GB RAM (Web App +1GB) 4 CPUs 25 GB HDD	Mandatory 3 GB RAM 2 CPUs 1 GB HDD				External database 10 GB	1 ICG instance per 2,500 devices Server generally: 8 GB RAM 2 CPUs 20 GB HDD Only ICG service: 2 GB RAM 2 CPUs 2 GB HDD

* Follow the recommendation of the external database system on RAM and CPU.

Architecture: Large Environment (HA) + ICG



2.2.5 Extra Large Environment: UMS XL (HA)

Extra Large UMS Installations with up to 300k Devices; High Availability + ICG

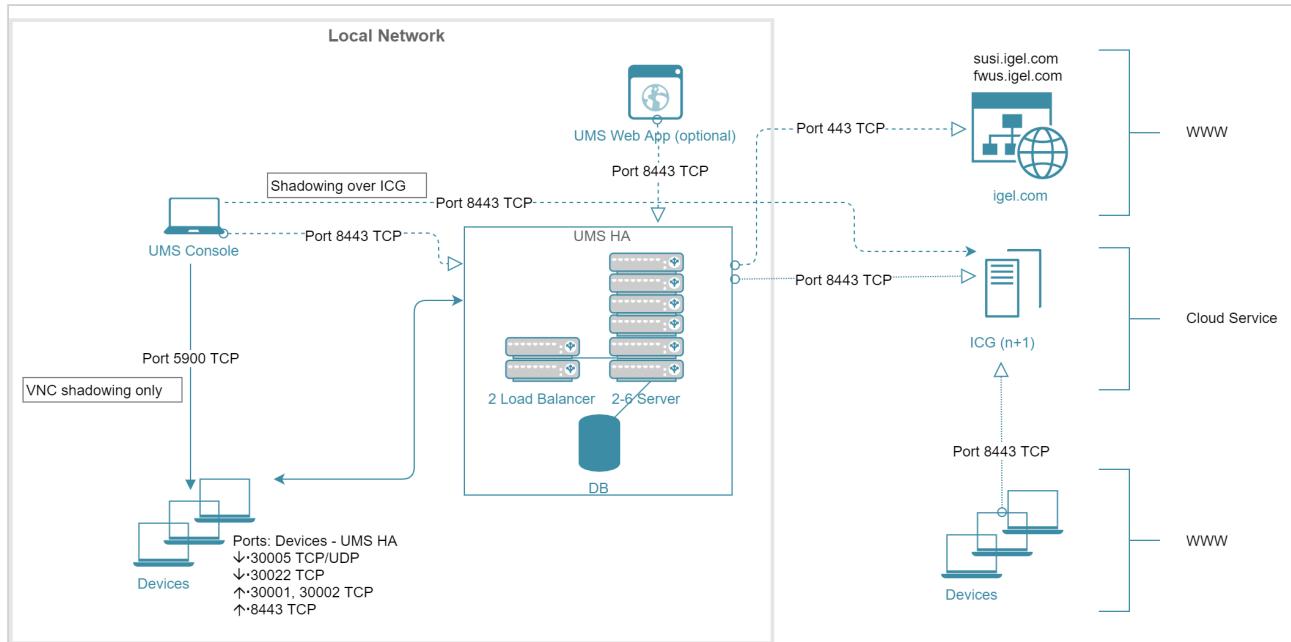
Installation Size	#Devices	#UMS Server Host	UMS Server	UMS Console Standalone	#Load Balancer Standalone	Load Balancer Standalone	Database*ICG
XL (HA)**	<Up to 300.06 servers 00 (1 server / 50,000 devices)	9 GB RAM (Web App +1GB) 6 CPUs 25 GB HDD	Mandatory 6 GB RAM 4 CPUs 1 GB HDD	Up to 3 load balancers (1 load balancer / 3 servers)	4 GB RAM 4 CPUs 2 GB HDD	External database 20 GB	1 ICG instance per 2,500 devices Server generally: 8 GB RAM 2 CPUs 20 GB HDD Only ICG service: 2 GB RAM 2 CPUs 2 GB HDD

* Follow the recommendation of the external database system on RAM and CPU.



**** General recommendation:** 1 UMS Server per 50,000 devices, 1 load balancer for 3 UMS Servers.

Architecture: Extra Large Environment (HA) + ICG



2.3 Performance Optimizations

2.3.1 Data Sizing

- The number of registered firmware versions has the **largest impact** on the size of the database. (Listed in UMS Console under **Misc > Firmware Statistics**)
- The number of devices or profiles has a **minor impact**.
- Average size per...
 - Firmware configuration: ~15 MB
 - Profile (depends on the number of active parameters): ~100 kB
 - Device: ~100 kB
- Reserve 500 MB up to 1 GB for database transaction logs of excessive database calls like **Remove unused Firmware**. Please note that the usage depends on the database system used.

2.3.2 Latencies

If you are struggling with long-distance connections and high latency, please consider the following recommendations:

- Minimize latency between...
 - Database <-> UMS Server: <= 20 ms
 - Several UMS Servers: <= 50 ms



- Load balancer <-> UMS Server: <= 50 ms
- High latency between the database and the UMS Server has a **huge impact** on the performance. The communication between the device and the UMS Console will slow down, the UMS Console itself will become lazy.
- High latency between the device and the UMS Server has **little impact** on overall performance.

2.3.3 Performance Optimizations

- **UMS logs:**

Use administrative tasks to automatically clean up logs (logging data, job execution data, execution data of administrative tasks, process events, asset information history) or remove old UMS log files (/runguiserver/logs) when storage space runs out.

- **Firmware:**

Remove unused firmware regularly.

- **Embedded database only:**

- Optimize database regularly (UMS Administrator application, e.g. once a month)
- Check for free storage space and expand the storage size if necessary (keep at least 1 GB free at all times)

- **Number of devices:**

- If the device count is high (>10k) and overall performance is low, increase UMS Server and UMS Console memory.
- Avoid too many devices (>5k) in one folder.

- **Assignments:**

Keep the number of assignments per device (direct and indirect) at a low level (<25).

- **Default directory rules:**

Do not use default directory rules with the **Apply rule when device boots** option unless they are required.

Concurrent device requests:

If you are experiencing problems with many concurrent device requests (delays in configuration deployment or logging on to the device), open the UMS Console and use the options under **UMS Administration > Global Configuration > Device Network Settings > Device Requests** (thread and queue size) to control the throughput of the device requests. Contact support for recommendations.

2.3.4 Limitations: UMS HA

- Device actions that are manually triggered in the UMS Console are performed by **one UMS Server** (the one the UMS Console is currently connected to); there is no load balancing for these actions.



3 UMS Reference Manual

- [What Is New in IGEL UMS 6.09.100?\(see page 253\)](#)
- [Overview\(see page 254\)](#)
- [UMS Installation and Update\(see page 258\)](#)
- [Connecting the UMS Console to the Server\(see page 306\)](#)
- [Registering Devices on the UMS Server\(see page 306\)](#)
- [UMS Console User Interface\(see page 313\)](#)
- [Profiles\(see page 331\)](#)
- [Master Profiles\(see page 359\)](#)
- [Template Profiles\(see page 361\)](#)
- [Mobile-Device Profiles\(see page 375\)](#)
- [Firmware Customizations\(see page 375\)](#)
- [Devices\(see page 382\)](#)
- [Shared Workplace Users\(see page 402\)](#)
- [Views\(see page 402\)](#)
- [Jobs\(see page 425\)](#)
- [Files\(see page 430\)](#)
- [Universal Firmware Update\(see page 433\)](#)
- [Search History\(see page 435\)](#)
- [Recycle Bin\(see page 436\)](#)
- [UMS Administration\(see page 437\)](#)
- [Importing Active Directory Users\(see page 505\)](#)
- [Create Administrator Accounts\(see page 508\)](#)
- [User Logs\(see page 521\)](#)
- [Save Support Information / Send Log Files to Support\(see page 525\)](#)
- [Save Device Files for Support\(see page 527\)](#)
- [The IGEL UMS Administrator\(see page 529\)](#)

3.1 What Is New in IGEL UMS 6.09.100?

You will find the release notes for IGEL Universal Management Suite 6.09.100 both as a text file in the same folder as the installation programs on our [download server³⁴](#) and in the [Knowledge Base\(see page 565\)](#).

3.1.1 Text Expert Mode of Views: Auto-completion for Operators

When you create or edit a view in the text expert mode and need to enter an operator, you can now use auto-completion for this purpose. Unsupported operators are recognized as syntax errors. See [How to Create a New View in the IGEL UMS\(see page 403\)](#).

³⁴ <https://www.igel.com/software-downloads/workspace-edition/>



3.1.2 Monitoring Endpoint for Requesting the Status of the UMS Server

With the monitoring endpoint, you can check the process / service states for the UMS Server, see [How to Check the Current State of the IGEL UMS Server through Your Existing Monitoring Solution](#)(see page 156).

3.1.3 UMS Administrator Command-Line Interface

The UMS Administrator command-line interface allows you to control the UMS Administrator via a terminal and to automatize UMS Administrator actions via scripting. See [IGEL UMS Administrator Command-Line Interface](#)(see page 547).

3.1.4 ICG Certificates as Part of the Support Information

If the IGEL Cloud Gateway is configured, the basic information on the used ICG certificates will be included in a ZIP file which you send to IGEL support via **Help > Save support information**, see [Support Wizard in the IGEL UMS](#)(see page 525).

3.1.5 UMS Web App: Login Brute-Force Protection

To prevent brute-force attacks, a user account will now be blocked for some time after several failed login attempts, see [How to Log In to the IGEL UMS Web App](#)(see page 732).

3.2 Overview

With the IGEL Universal Management Suite (UMS), you can remotely configure and control IGEL devices.

The UMS supports not only various operating systems but also databases and directory services such as Microsoft® Active Directory.

- ⓘ Each IGEL device comes with a free version of the IGEL Universal Management Suite.

For an overview of devices supported by the IGEL UMS, see [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)(see page 47).

3.2.1 Typical Areas of Use

- Setting up devices automatically;
 - Configuring devices, software clients, tools and local protocols;
 - Distributing updates and firmware images;
 - Diagnostics and support.
-
- [Attributes of the IGEL UMS](#)(see page 255)
 - [IGEL UMS Components](#)(see page 256)



3.2.2 Attributes of the IGEL UMS

Quick installation:

A wizard helps you during the installation procedure. You can connect external database systems as an alternative to the integrated database.

Straightforward management at the click of a mouse:

Most hardware and software settings can be changed with just a few clicks.

Standardized user interface:

The UMS user interface is similar to that for local device configuration. The additional remote management functions give the administrator complete control in the familiar, proven environment.

No scripting:

Although scripting is supported, you will only need it for managing the device configuration in the most exceptional circumstances.

Asset management:

Automatic capturing of all your hardware information, licensed features and installed hotfixes.

Commentary fields:

For various customer-specific information such as location, installation date and inventory number.

Support for numerous operating systems:

The UMS server can run on many common versions of Microsoft® Windows® Server and Linux, see [Installation Requirements for the IGEL UMS](#)(see page 258).

Access independent of the operating system:

The UMS console runs on any device with the Java Runtime Environment. You can also use the UMS console with Java Web Start without a local installation, see [Installation Requirements for the IGEL UMS](#)(see page 258).

Encrypted communication:

Certificate-based TLS/SSL-encrypted communication between remote management servers and clients to prevent unauthorized reconfiguration of the devices.

Failsafe update function:

If a device fails while the update is in progress, e. g. as a result of a power outage or loss of the network connection, it will still remain usable. The update process will then be completed when the device next boots.

Based on standard communication protocols:

There is no need to reconfigure routers and firewalls because the *UMS* uses the standard HTTP and FTP protocols.

Support for extensive environments:

The IGEL Universal Management Suite can be scaled to accommodate several thousand devices.

Group and profile-based administration:

The devices within a given organizational unit can be administered easily via profiles. If members of staff move to another department, the administrator can change the settings with a simple drag-and-drop procedure.

**Trouble-free rollout:**

IGEL devices can be automatically assigned to a group on the basis of either the relevant subnet or a list of MAC addresses provided by *IGEL*. They then automatically receive the configuration settings for the group.

Comprehensive support for all configuration parameters:

Most IGEL device settings, e. g. device or session configurations, can be changed via the *UMS* user interface.

Transferral of administrative rights:

Large organizations can authorize a number of system administrators for different control and authorization areas. These administrative accounts can be imported from an Active Directory.

Planning tasks:

Maintenance tasks can be scheduled to take place during the night so that day-to-day operations are not disrupted.

VNC shadowing:

Members of the IT support team have remote access to devicescreens, enabling them to rapidly identify problems and demonstrate solutions directly to users.

3.2.3 IGEL UMS Components

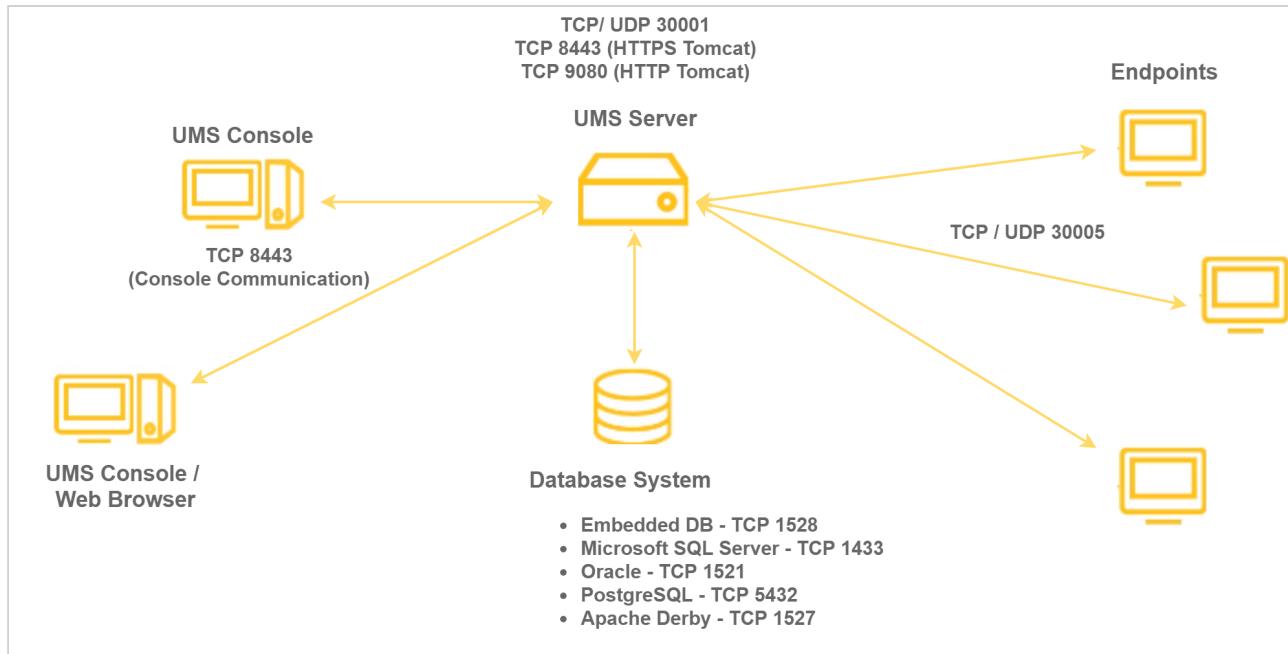
The IGEL Universal Management Suite program (referred to below as the UMS) comprises the following three components:

- [UMS Server](#)(see page 256)
- [UMS Administrator](#)(see page 257)
- [UMS Console / UMS Web App](#)(see page 257)

UMS Server

The UMS Server is a server application which requires a database management system (RDBMS). Information regarding supported database management systems can be found under [Installation Requirements for the IGEL UMS](#)(see page 258). The database can be installed on the server itself or on a remote host.

The UMS Server communicates internally with the database and externally with the registered devices and the UMS Console:



Typically, the UMS Console and UMS Server are installed on different computers. Data transmission between the UMS Server and devices as well as between the UMS Server and Console is encrypted.

All configurations for the managed devices are saved in the database. Changes to a configuration are made in the database and are transferred to the device if necessary. The device can retrieve the information from the database during the booting procedure or you can send the new configuration to the device manually. A scheduled configuration update is also possible.

UMS Administrator

The UMS Administrator is one of the UMS Server's administrative components.

The key parts of the UMS Administrator are as follows:

- Network configuration (ports, WebDAV resources)
- Database configuration (data sources, backups)

Further information regarding the UMS Administrator can be found under [The IGEL UMS Administrator](#)(see page 529).

UMS Console / UMS Web App

UMS Console

The UMS Console is the Java-based user interface to the UMS Server. The devices and their configuration are administered via the GUI of the UMS Console.

The key tasks of the UMS Console are as follows:

- Displaying the devices' configuration parameters
- Setting up profiles and scheduled jobs



- Administering firmware updates

i If you need to start the UMS Console under Linux from the terminal emulator, use the command /[IGEL installation directory]/RemoteManager.sh (if the default installation directory is used: /opt/IGEL/RemoteManager/RemoteManager.sh) It is NOT recommended to execute RemoteManager.sh with sudo. On Red Hat Enterprise Linux 8, RemoteManager.sh can be executed only without sudo.

You will find further information regarding the UMS Console under [UMS Console User Interface](#)(see page 313).

UMS Web App

With UMS version 6.05.100, the UMS Web App, a web-based user interface, has been introduced. The UMS Web App can currently be used only in addition to the UMS Console. For detailed information about the application, see [UMS Web App](#)(see page 720).

3.3 UMS Installation and Update

This chapter describes the requirements for installing the UMS. The standard installation with the embedded database is explained with an example for [Windows](#)(see page 283) and for [Linux](#)(see page 261). You are also told what you need to bear in mind when performing an update and where you can connect external database systems.

- [Installation Requirements for the IGEL UMS](#)(see page 258)
- [Installing a UMS Server](#)(see page 260)
- [Updating UMS](#)(see page 285)
- [Connecting External Database Systems](#)(see page 289)

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=3YJnFiE7y5w>



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:
https://www.youtube.com/watch?v=p52CxtB_0ok

3.3.1 Installation Requirements for the IGEL UMS

You can run the IGEL UMS with Windows and Linux 64-bit systems (x86_64).



- i** For the supported operating systems, see the "Supported Environment" section of the [release notes](#)(see [page 565](#)).

Your hardware and software must meet the following minimum requirements:

Standard UMS (Includes UMS Server and UMS Administrator)

- At least 5 GB of RAM
- At least 2 GB of free disk space

With UMS Console

When the UMS Console is included, the RAM and disk space requirements are increased as follows:

- At least 3 GB of RAM
- At least 1 GB of free disk space

With Embedded Database

When the embedded database is included, the RAM and disk space requirements are increased as follows:

- At least 2 GB of free disk space

UMS with UMS Console and Embedded Database

When both the UMS Console and the embedded database are included, the RAM and disk space requirements are increased as follows:

- At least 8 GB of RAM
- At least 5 GB of free disk space

UMS with UMS Console, Embedded Database, and UMS Web App

When the UMS Console, the embedded database, and the UMS Web App are included, the RAM and disk space requirements are increased as follows:

- At least 9 GB of RAM
- At least 6 GB of free disk space

Only UMS Console

- At least 3 GB of RAM
- At least 1 GB of free disk space

- i** Under Linux, an X11 system is required. It is required by the UMS Administrator application which can only be launched on the same machine as the UMS Server.



- ⓘ As an alternative to a local console installation, you can execute the UMS Console as a Java Web Start application too. The console does not need to be installed here. If necessary, it can be downloaded from the UMS Server and executed. Further information can be found under [UMS Console via Java Web Start](#)(see page 222).

❗ Do not install the UMS Server on a domain controller system!

❗ Manually modifying the Java runtime environment on the UMS Server is not recommended.

❗ Running additional Apache Tomcat web servers together with the UMS Server is likewise not recommended.

Database Systems (DBMS)

- ⓘ For details on the supported database systems, see the "Supported Environment" section of the [release notes](#)(see page 565). Details of the requirements when installing and operating the database can be found in the documentation for the particular DBMS.

High Availability

For installation requirements for [High Availability](#)(see page 657), see [HA: Installation Requirements](#)(see page 660).

- ⓘ The embedded database cannot be used for a High Availability network. You can use the embedded database only for a dedicated test installation with only a single server for the UMS Server and Load Balancer.

⚠ All UMS Servers and UMS Load Balancers must reside on the same VLAN. Network traffic must be allowed over UDP broadcast port 6155, and TCP traffic and UDP broadcast traffic over port 61616. For more information on UMS ports, see [UMS Communication Ports](#)(see page 48).

Note: IGEL UMS Server HA is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks.

3.3.2 Installing a UMS Server

This example describes the complete procedure for installing a UMS Server with an embedded database. If your required installation differs, you can select individual components, e.g. for an individual console installation.

- [IGEL UMS Installation under Linux](#)(see page 261)
- [IGEL UMS Installation under Windows](#)(see page 283)

If you want to install [UMS High Availability \(HA\) Extension](#)(see page 657), see [HA Installation](#)(see page 660).



If you already have a standard UMS installation and want to switch to the UMS HA, see [Switching from a Standard UMS Installation to an HA Installation](#)(see page 680).

IGEL UMS Installation under Linux

- ⓘ For the supported operating systems, see the "Supported Environment" section of the [release notes](#)(see page 565).

The procedure for installing the IGEL Universal Management Suite under Linux is as follows:

1. Download the current version of the IGEL Universal Management Suite from the [IGEL Download Server](#)³⁵.

2. Open a terminal emulator such as xterm and switch to the directory in which the installation file `setup-igel-ums-linux-[Version].bin` is located.

3. Check whether the installation file is executable. If not, it can be made executable with the following command:

```
chmod u+x setup*.bin
```

- ⓘ You will need root/sudo rights to carry out the installation.

4. Execute the installation file as root or with sudo:

```
sudo ./setup-igel-ums-linux-[Version].bin
```

This unzips the files into the `/tmp` directory, starts the included Java Virtual Machine, and removes the temporary files once the installation has been completed.

5. Start the installation procedure by pressing **Enter**.

- ⚠ You can cancel the installation at any time by pressing the [Esc] key twice.

6. Read and confirm the license agreement.

7. Choose whether the installer will install the required dependencies:

- **Now:** Installs the necessary dependencies automatically.
- **Manual:** Skips the installation. You will have to install the required dependencies manually if this has not already been done.
- **Cancel installer:** Aborts the installation procedure.

8. Under **Destination directory**, select the directory in which the UMS is to be installed. (Default: `/opt/IGEL/RemoteManager`)

9. If you are updating an existing UMS installation: Under **Database backup**, select a file for the backup of the embedded database, licenses, and certificates. If you have already created a backup, you can select **No (continue)** in order to skip this step. See also [Updating under Linux](#)(see page 286).

10. Under **Installation type**, select the scope of installation:

- **Complete:** [UMS Server](#)(see page 256) and [UMS Console / UMS Web App](#)(see page 257)
- **Client only:** UMS Console only
- **HA Net:** [High Availability](#)(see page 657) configuration

³⁵ <https://www.igel.com/software-downloads/workspace-edition/>



! Custom file transfer directories are no longer supported. After completing the installation, move the existing files to the `ums_filetransfer/` directory and edit **Files** and **Firmware update** in the UMS Console to bring them online again. You may also need to amend download addresses in the device configurations and profiles.

11. Choose whether the [UMS Web App](#)(see page 720) should be installed.
12. Confirm the **system requirements** dialog if your system fulfills them.
13. Under **Data directory**, select the directory in which Universal Firmware Updates and files are to be saved. (Default: `/opt/IGEL/RemoteManager`)
14. Under **Database selection**, select the desired database system.
 - Internal: The embedded database
 - Other: An external database server

i The embedded database is suitable for most purposes. It is included in the standard installation. If you manage a large network of devices and a dedicated database system is already in use in your company, it is advisable to use this external database system. The same applies if you integrate the High Availability solution.
15. Under **User name**, enter a **user name** and **password** for the database connection.
The credentials for the database connection are created.

i Initially, the credentials entered here are also the credentials of the UMS superuser. After the installation, the credentials for the database user and those for the UMS superuser can be changed independently from each other. For more information about the UMS superuser, see [Changing the UMS Superuser](#)(see page 547).
16. Specify whether you would like to create **shortcuts** for the UMS Console and UMS Administrator on the menu.
17. Check the summary of the installation settings and start the procedure by selecting **Start installation**.
If you have selected the standard installation, the UMS Server along with the embedded database will be installed and started.
18. Once the installation procedure is complete, open the UMS Console via the menu or with the command `/opt/IGEL/RemoteManager/RemoteManager.sh`

i It is generally NOT recommended to execute the command `RemoteManager.sh` with sudo. On Red Hat Enterprise Linux 8, `RemoteManager.sh` can be executed only without sudo.
19. Connect the UMS Console to the UMS Server by entering the login data for the database that you specified during the installation.

- [Preparing Amazon Linux 2 for UMS Installation](#)(see page 263)
- [Installing UMS on Red Hat Enterprise Linux \(RHEL\) 8](#)(see page 263)
- [Installing UMS on Red Hat Enterprise Linux \(RHEL\) 7.3](#)(see page 264)
- [Installing UMS on Oracle Linux Server](#)(see page 265)
- [Installing a UMS Network on Microsoft Azure](#)(see page 267)



Preparing Amazon Linux 2 for UMS Installation

Overview

You can install the UMS on Amazon Linux 2, both in the cloud and on-premises.

If you want to use the UMS Console or the UMS Administrator on your Amazon Linux 2 machine, you must install and set up the Mate desktop environment. The procedure is described in this article.

Environment

This description is valid for the following environment:

- UMS 6.05 or higher
- Amazon Linux 2, cloud or on-premises

Instructions

1. Log in to Amazon Linux 2 as a user with sudo permissions.
 2. Update all package repositories:
`sudo yum update`
 3. Install the Mate desktop environment:
`sudo amazon-linux-extras install mate-desktop-1.x`
 4. Go to /etc/sysconfig/ and create a file named desktop with a text editor.
 5. Enter the following content into the desktop file:
`PREFERRED=/usr/bin/mate-session`
 6. Save the file.
 7. Go to your home directory and create a file named .Xclients
 8. Enter the following content into the .Xclients file:
`/usr/bin/mate-session`
 9. Save the file.
 10. Make the .Xclients file executable:
`chmod +x ~/.Xclients`
- You can now install the UMS; for instructions, see [IGEL UMS Installation under Linux](#)(see page 261).

Installing UMS on Red Hat Enterprise Linux (RHEL) 8

You want to install the UMS on the 64-bit version of Red Hat Enterprise Linux (RHEL) 8.

- (i) The installation of the UMS on RHEL 8 can be done on a plain RHEL 8 system (Server with a GUI).

Before installing the UMS (or UMS HA, see [HA Installation](#)(see page 660)), the following steps have to be done:

1. As root, update the local package database and reboot the server.
`# yum -y update`

The UMS installation will load additional modules if they have not yet been installed: `qt5-qbase`



2. Set the TERM variable as follows, especially if a GUI is installed on the server.

```
# export TERM=xterm
```

3. Make the /root directory writable.

By default, the /root directory has no write flag set. As the default installation of UMS HA creates the network configuration archive in this directory, this directory must get the write flag for the root user.

```
# sudo chmod u+w /root
```

4. Configure the firewall.

RHEL 8 comes with an activated firewall. For the UMS and UMS HA to work properly, the following ports have to be opened in the active profile (see also [UMS Communication Ports](#)(see page 48)):

```
# 8443/tcp 9080/tcp 30001/tcp 30002 tcp 61616/tcp 61616/udp 1528/tcp 6155/udp
```

To open these ports, the following commands must be executed:

```
# sudo firewall-cmd --zone=public --add-port=8443/tcp --permanent
# sudo firewall-cmd --zone=public --add-port=9080/tcp --permanent
# sudo firewall-cmd --zone=public --add-port=30001/tcp --permanent
# sudo firewall-cmd --zone=public --add-port=30002/tcp --permanent
# sudo firewall-cmd --zone=public --add-port= 61616/tcp --permanent
# sudo firewall-cmd --zone=public --add-port= 61616/udp --permanent
# sudo firewall-cmd --zone=public --add-port= 1528/tcp --permanent
# sudo firewall-cmd --zone=public --add-port= 6155/udp --permanent
```

5. Proceed with the UMS installation as described in [IGEL UMS Installation under Linux](#)(see page 261).

Installing UMS on Red Hat Enterprise Linux (RHEL) 7.3

You want to install the UMS on the 64-bit version of Red Hat Enterprise Linux (RHEL) 7.3.

From UMS 5.09

From UMS Version 5.09, the installation of 32-bit libraries is no longer required. The necessary dependencies are automatically installed if the corresponding option has been chosen during the UMS installation procedure.

1. Adjust the RHEL Server firewall settings to allow the network ports used by the UMS, see [UMS Communication Ports](#)(see page 48).
2. Complete the installation as described in [IGEL UMS Installation under Linux](#)(see page 261).



From UMS 5.07.100

From UMS Version 5.07.100, the required 32-bit libraries can automatically be installed by the UMS installer if the corresponding option is chosen during the UMS installation procedure.

1. Adjust the RHEL Server firewall settings to allow the network ports used by the UMS, see [IGEL UMS Communication Ports](#)(see page 48).
2. Complete the installation as described in [IGEL UMS Installation under Linux](#)(see page 261).

Before UMS 5.07.100

To install the UMS on the 64-bit version of RHEL 7.3, proceed as follows:

1. As root, update your 64-bit packages to the latest version:

```
yum update
```
2. Install libraries for 32-bit support:

```
yum install \
glibc.i686 \
libzip.i686 \
ncurses-libs.i686 \
bzip2-libs.i686 \
libXtst.i686 \
libXinerama.i686 \
libXi.i686 \
libXext.i686 \
libXrender.i686 \
libgcc.i686
```
3. Reboot.
4. Adjust the RHEL Server firewall settings to allow the network ports used by the UMS, see [UMS Communication Ports](#)(see page 48).
5. Complete the installation as described in [IGEL UMS Installation under Linux](#)(see page 261).

i There is a bug/glitch on Red Hat Enterprise Linux (RHEL) 7.3 with GNOME desktop version 3.14, when running UMS Console. The main window of the UMS Console is displayed as an empty grey rectangle, because the GUI is rendered incorrectly. As a workaround, the window can be resized by dragging the windows edges or by double-clicking near the top edge (maximizing) where the title bar would be. This triggers a repaint, and the UMS Console window is then displayed correctly. Alternatively, use the KDE desktop environment on RHEL 7.3.

Installing UMS on Oracle Linux Server

⚠ Oracle

For the proper operation of the UMS with Oracle databases, particularly for the upgrade process, the number of open_cursors for the database must be adjusted. `open_cursors` is a system setting.



1. To get the actual value, log in to the database as SYSDBA and execute:
`SQL> select name, value from v$parameter where name = 'open_cursors';`
2. The recommended value for open_cursors is "3000". To set the value, issue the following command as SYSDBA:
`SQL> alter system set open_cursors = 3000 scope=both;`
3. The same command should be added to the SPFILE of the Oracle system in order for the changes to persist on the next reboot.

You want to install the UMS on the 64-bit version of Oracle Linux Server.

From UMS 5.09

From UMS Version 5.09, the installation of 32-bit libraries is no longer required. The necessary dependencies are automatically installed if the corresponding option has been chosen during the UMS installation procedure. See [IGEL UMS Installation under Linux](#)(see page 261).

1. Adjust the Oracle Linux Server firewall settings to allow the network ports used by the UMS, see [UMS Communication Ports](#)(see page 48).
2. Complete the installation as described in [IGEL UMS Installation under Linux](#)(see page 261).

From UMS 5.07.100

From UMS Version 5.07.100, the required 32-bit libraries can automatically be installed by the UMS installer if the corresponding option is chosen during the UMS installation procedure.

1. Adjust the Oracle Linux Server firewall settings to allow the network ports used by the UMS, see [UMS Communication Ports](#)(see page 48).
2. Complete the installation as described in [IGEL UMS Installation under Linux](#)(see page 261).

Before UMS 5.07.100

To install the UMS on the 64-bit version of Oracle Linux Server, proceed as follows:

1. As root, update your 64-bit packages to the latest version:

```
yum update
```

2. Install libraries for 32-bit support:

```
yum install \
glibc.i686 \
libzip.i686 \
ncurses-libs.i686 \
bzip2-libs.i686 \
libXtst.i686 \
libXinerama.i686 \
libXi.i686 \
libXext.i686 \
libXrender.i686 \
libgcc.i686
```

3. Reboot.



4. Adjust the Oracle Linux Server firewall settings to allow the network ports used by the UMS, see [UMS Communication Ports](#)(see page 48).
5. Complete the installation as described in [IGEL UMS Installation under Linux](#)(see page 261).

Installing a UMS Network on Microsoft Azure

Overview

This article describes a standard UMS single server installation (not [High Availability](#)(see page 657) along with IGEL Cloud Gateway (ICG). The database is reachable via Azure or is hosted in Azure.

i **High Availability (HA)**

IGEL UMS Server HA is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks.

Requirements

- Microsoft Azure account
- UMS 6.07.100 or higher

Creating a Virtual Machine for the UMS

1. Log in to Microsoft Azure.
2. Hover over **Resource groups** and select **Create**.

The screenshot shows the Azure services dashboard. On the left, there's a sidebar with 'Create a resource' and 'Recent resources'. The main area is titled 'Resource groups' with a 'Create' button highlighted by a red box. Below it, there's a 'Recent resources' section listing items like 'ICGResourceGroup' and 'dd1fe321-b2ba-406e-af3d-0311e'. On the right, there are sections for 'Free training from Microsoft' and 'Useful links'.

3. Edit the data as follows:
 - **Resource group:** Enter a name for the resource group, e.g. "MyResourceGroup".



- **Region:** Select a region, according to your preferences.

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

Project details

Subscription *	Techdoc Subscription	▼
Resource group *	MyResourceGroup	✓

Resource details

Region *	(Europe) West Europe	▼
----------	----------------------	---

4. Click **Review + create**.
Your resource group is validated.
 5. Click **Create**.
Your resource group is created.
 6. Click **Home** to get to the overview.
 7. Hover over **Virtual machines** and select **Create**.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with a 'Virtual machines' icon and the text 'Virtual machines'. The main area has a title 'Virtual machines' with a star icon. Below it is a 'Create' button with a plus sign, which is highlighted with a red box. To the right of 'Create' is a 'View' link. A horizontal line separates this from a section titled 'Recent resources'. Under 'Recent resources', there are two items: 'VM-ICG' (3 months ago) and 'igel-cloud-gateway' (3 months ago). Another horizontal line separates this from a section titled 'Free training from Microsoft'. This section lists three training modules: 'Introduction to Azure virtual machines' (8 units, 1 hr 7 min), 'Create a Windows virtual machine in Azure' (9 units, 51 min), and 'Create a Linux virtual machine in Azure' (7 units, 1 hr 26 min). At the bottom, there's a 'Useful links' section.

- 8. Edit the data as follows:**



- **Resource group:** Select the resource group you have created before.
- **Virtual machine name:** Enter a name for the virtual machine on which your UMS is to be installed.
- **Image:** Select "Windows Server 2016 Datacenter".
- **Size:** Select the size for your virtual machine. If all components will be running at the same time, we recommend "Standard B4ms" (4cpu/16 GiB). The components and their RAM requirements are as follows:
 - UMS Server: 4 GB
 - UMS Administrator. 2 GB
 - UMS Console: 3 GB
 - UMS Web App: 1 GB
 - Embedded database: 2-3 GB



- **Select inbound ports:** Select "HTTP (80)", "HTTPS (443)", and "RDP (3389)". As an alternative, you can add the ports later on; see [Configuring the Virtual Machine](#)(see page 271).

Subscription * ⓘ Techdoc Subscription

Resource group * ⓘ MyResourceGroup [Create new](#)

Instance details

Virtual machine name * ⓘ MyUmsMachine ✓

Region * ⓘ (Europe) West Europe

Availability options ⓘ Availability zone

Availability zone * ⓘ 1

Image * ⓘ Windows Server 2016 Datacenter - Gen1 [See all images](#)

Azure Spot instance ⓘ

Size * ⓘ Standard_B4ms - 4 vcpus, 16 GiB memory (\$151.84/month) [See all sizes](#)

Administrator account

Username * ⓘ UmsAdmin ✓

Password * ⓘ ✓

Confirm password * ⓘ ✓

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ None Allow selected ports

Select inbound ports * ⓘ HTTP (80), HTTPS (443), RDP (3389)

9. Click **Review + create**.

10. Click **Create**.



Configuring the Virtual Machine

1. In the sidebar menu, go to **Networking**.

A screenshot of the UMS (Endpoint Management) interface. At the top, it says "MyUmsMachine" and "Virtual machine". Below that is a search bar with "Search (Ctrl+/)". The sidebar menu has several options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Networking (which is highlighted with a red box), Connect, Windows Admin Center (previous), Disks, and Size.

2. Click **Add inbound port rule**.
3. Edit the data as follows:
 - Destination port ranges: Enter "8443".
 - Protocol: Select **TCP**.
 - Name: Change to "Port_8443".



4. Click **Add**.

Source ⓘ
Any

Source port ranges * ⓘ
*

Destination ⓘ
Any

Service ⓘ
Custom

Destination port ranges * ⓘ
8443 ✓

Protocol
 Any
 TCP ✓
 UDP
 ICMP

Action
 Allow
 Deny

Priority * ⓘ
370

Name *
Port_8443 ✓

Description

Add **Cancel**

UMS with External Database(see

page 60)

❗ After the installation is complete, do not forget to disable ports 3389 and 22!



5. Select **Outbound port rules**.

Virtual network/subnet: [MyResourceGroup-vnet/default](#) NIC Public IP: **51.124.127.0** NIC Private IP: **10.0.1.4** Accelerated networking: **Disabled**

Inbound port rules	Outbound port rules	Application security groups	Load balancing
🛡 Network security group MyUmsMachine-nsg (attached to network interface: myumsmachine8) Impacts 0 subnets, 1 network interfaces			
Add inbound port rule			
Priority	Name	Port	Protocol
300	⚠ RDP	3389	TCP
320	HTTPS	443	TCP
340	HTTP	80	TCP

6. Click **Add outbound port rule**.

7. Using the procedure described in steps 2 and 3, add the following ports:

- 8443 (TCP)
- 22 (TCP)
- Data base port: The port that will be used for communication with the database. For more information, see [UMS with External Database](#)(see page 60).
- 443 (TCP)

8. Review your settings.

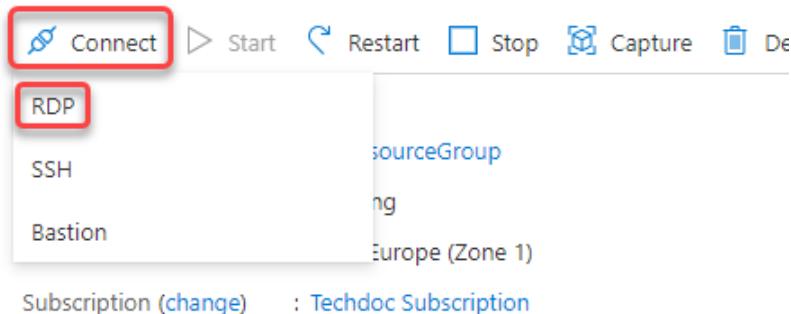
Inbound port rules	Outbound port rules	Application security groups	Load balancing
🛡 Network security group MyUmsMachine-nsg (attached to network interface: myumsmachine8) Impacts 0 subnets, 1 network interfaces			
Add outbound port rule			
Priority	Name	Port	Protocol
100	Port_out_8443	8443	TCP
110	Port_out_22	22	TCP
120	Port_out_1433	1433	TCP
130	Port_out_443	443	TCP
65000	AllowVnetOutBound	Any	Any
65001	AllowInternetOutBound	Any	Any
65500	DenyAllOutBound	Any	Any

Installing the UMS

1. Ensure that your virtual machine is running.



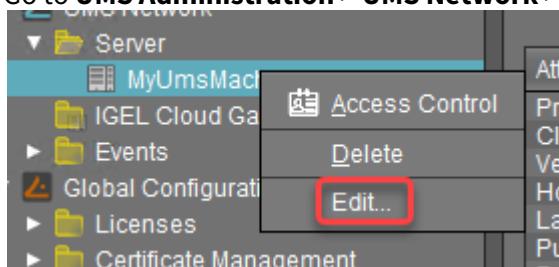
2. Click **Connect** and then select **RDP**.



3. Enter the displayed data in your RDP client or click **Download RDP File** and use the RDP file.
4. With a web browser, download the UMS installer from <https://www.igel.com/software-downloads/workspace-edition/> > **UNIVERSAL MANAGEMENT SUITE > WINDOWS**. (Example: setup-igel-ums-windows_6.07.100.exe)
5. Install the UMS as described in [IGEL UMS Installation under Windows](#)(see page 283) with the following settings:
 - Activate **Standard UMS**.
 - Activate **with UMS Console**.
 - Deactivate **with Embedded Database**.
 - Deactivate **Only UMS Console**.
 - Activate **Web App (early feature set)**.
6. When the installation is finished, open the UMS Administrator and follow the instructions under [How to Set Up a Data Source in the IGEL UMS Administrator](#)(see page 543).

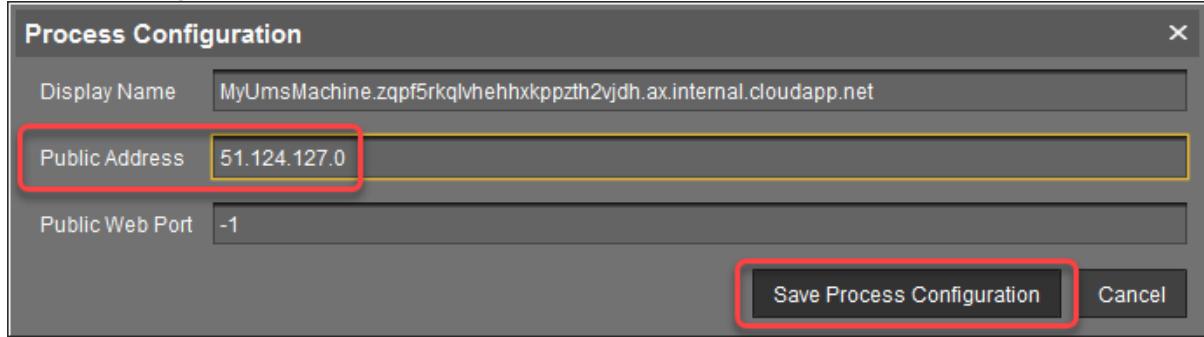
Setting the Public Address on the UMS Server

1. Start the UMS Console and log in.
2. Go to **UMS Administration > UMS Network > Server**, open the context menu and select **Edit**.



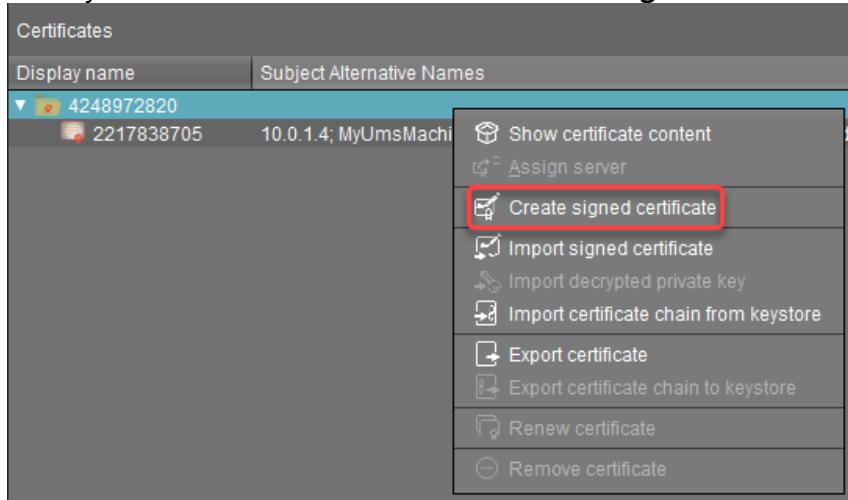


3. Enter the public ID of your virtual machine (displayed on the overview page) and click **Save process configuration**.

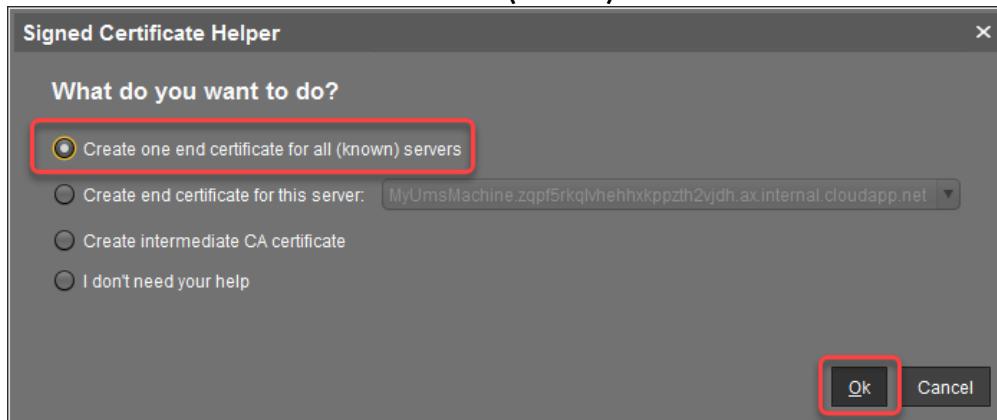


Create Web Certificates

1. In the UMS Console, go to **UMS Administration > Global Configuration > Certificate Management > Web**.
2. Select your root certificate and then select **Create signed certificate** from the context menu.



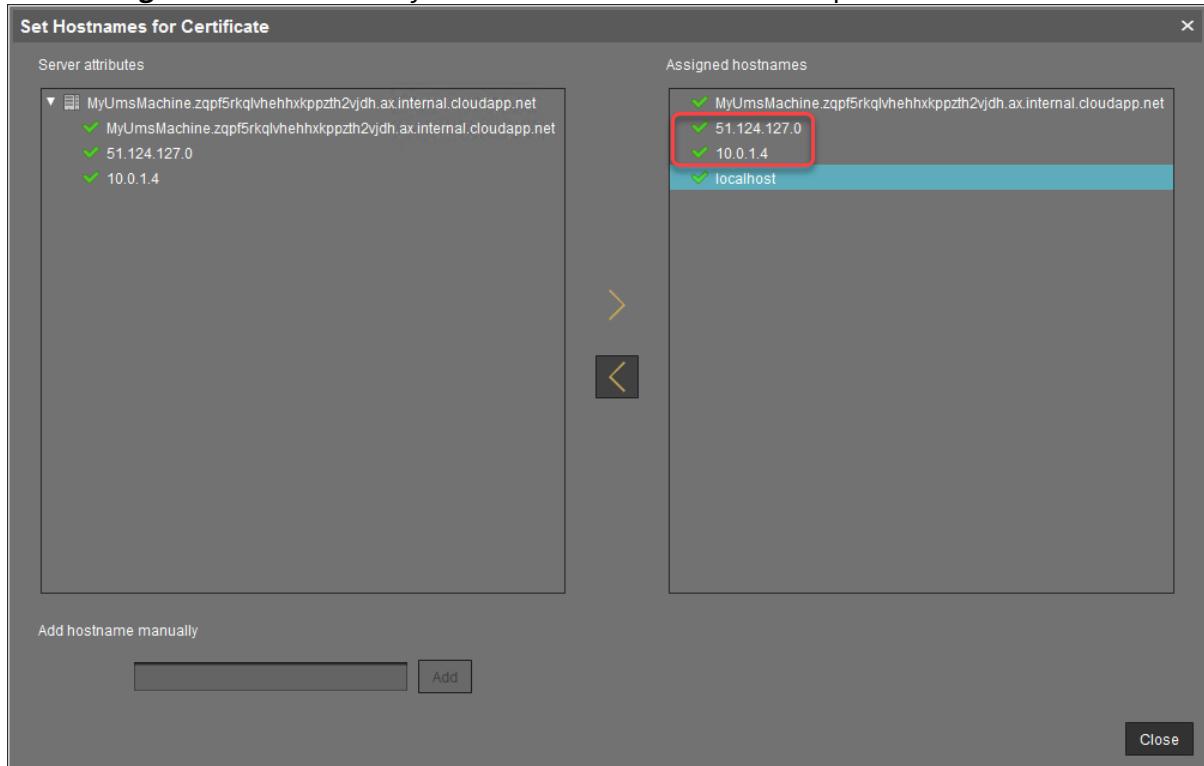
3. Select **Create one end certificate for all (known) servers** and then confirm with **Ok**.



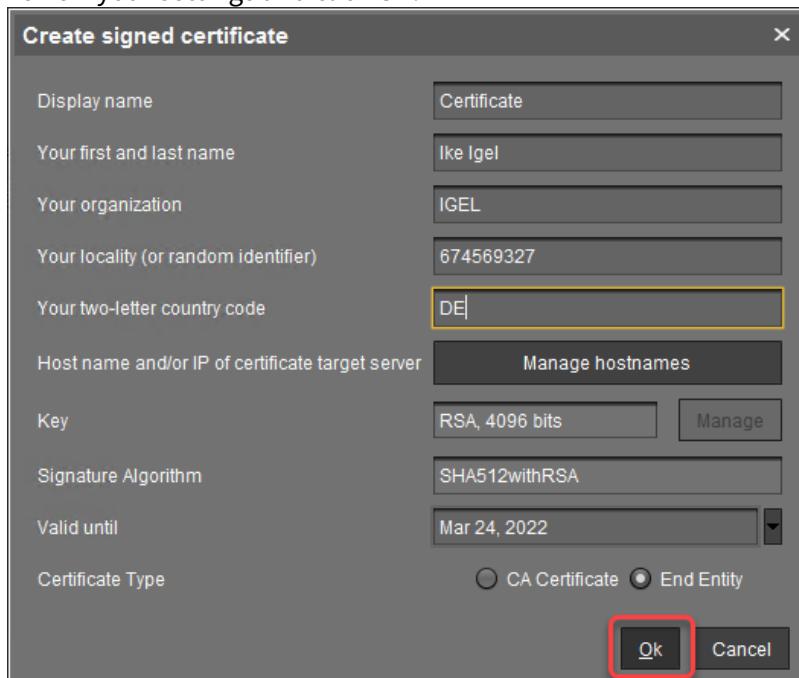
4. Fill in the details as appropriate.



5. Click **Manage hostnames** to verify if the internal IP Address and the public IP address are included.

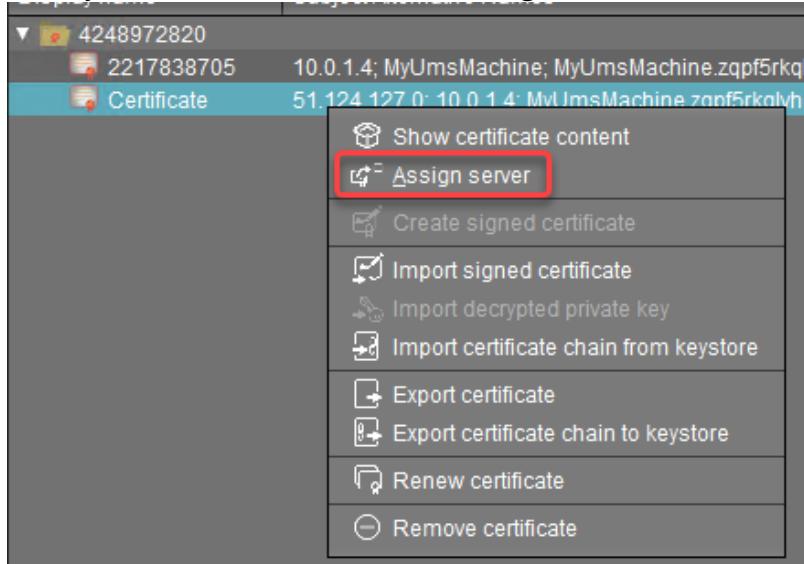


6. Review your settings and click **Ok**.

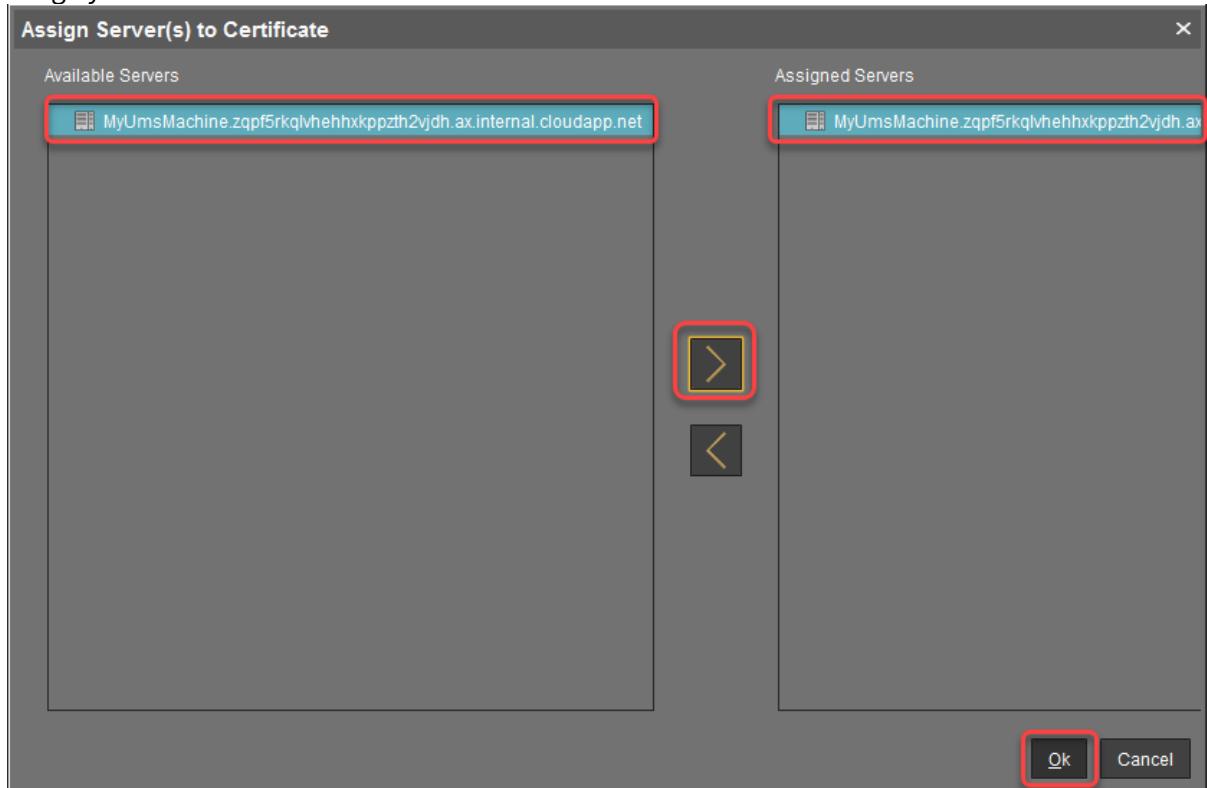




7. Select your certificate and then select **Assign server** from the context menu.

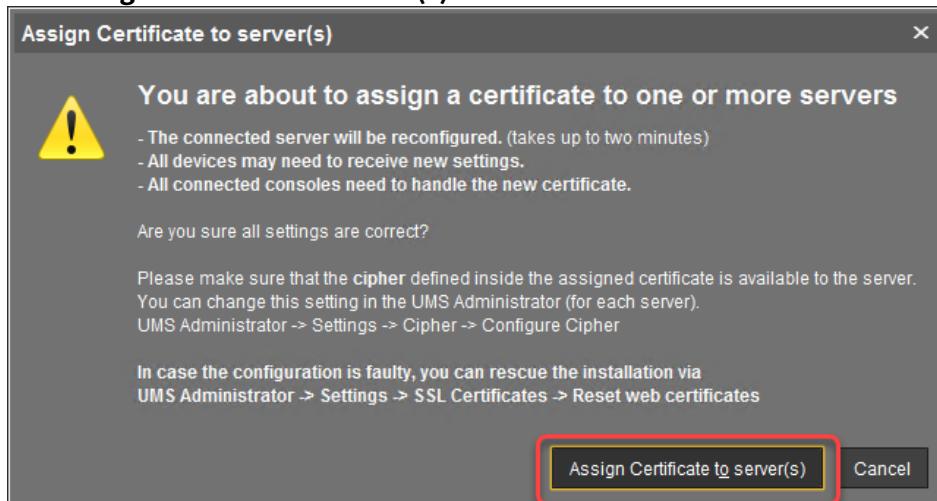


8. Assign your server to the certificate and confirm with **Ok**.





9. Click **Assign Certificate to server(s)** to confirm.



10. Check if the certificate is marked as **Used**.

Certificates						
Display name	Subject Alternative Names	Expiring date	Key Specificat...	Signature	Used	Priv...
4248972800		Mar 24, 2041	RSA (4096 bits)	SHA512withR...	<input checked="" type="checkbox"/>	
2217838705 10.0.1.4; MyUmsMachine; MyUmsMachine.zqpf5rkqlvhehxkppzth2vjdh.ax.internal.cl...		Mar 24, 2022	RSA (4096 bits)	SHA512withR...	<input checked="" type="checkbox"/>	
Certificate 51.124.127.0; 10.0.1.4; MyUmsMachine.zqpf5rkqlvhehxkppzth2vjdh.ax.internal.clou...		Mar 24, 2022	RSA (4096 bits)	SHA512withR...	<input checked="" type="checkbox"/>	

At this point, you can safely connect to your UMS from a local machine as well as from remotely installed UMS Consoles. For clarity purposes, we will still use the UMS Console on Azure.

Downloading the Installer for IGEL Cloud Gateway (ICG)

- With a web browser, download the ICG installer from <https://www.igel.com/software-downloads/enterprise-management-pack/> > **IGEL CLOUD GATEWAY (ICG)**. (Example: `installer-2.02.110.bin`) You can do this on the virtual machine or use your local machine and then copy the file to your virtual machine via RDP (clipboard).

Creating a Virtual Machine for IGEL Cloud Gateway (ICG)

- In your Azure portal, go to your resource group (in our example: `MyResourceGroup`) and add a new **Ubuntu Server 18.04 LTS**.



New ...

A screenshot of the Azure Marketplace interface. At the top, there's a search bar labeled "Search the Marketplace". Below it, a navigation bar includes "Azure Marketplace" with a "See all" link and a "Popular" section. On the left, a sidebar lists categories: Get started, Recently created, AI + Machine Learning, Analytics, Blockchain, Compute, Containers, Databases, Developer Tools, DevOps, Identity, and Integration. In the main area, there are several cards representing different services. One card for "Ubuntu Server 18.04 LTS" has a red box drawn around its icon and text. Other visible cards include "Windows Server 2016 Datacenter", "Web App", "SQL Database", "Function App", and "Azure Cosmos DB". Each card includes a small icon, the service name, and a "Quickstarts + tutorials" link.

2. Edit the settings as follows:

- **Resource group:** This must be set to the resource group we have created before (in our example: MyResourceGroup).
- **Virtual machine name:** Enter a name for the virtual machine.
- **Size:** “D2s v3” (2 CPUs/8 GiB RAM) or higher is recommended.
- **Authentication type:** Select **Password**.
- **Username:** Enter a username for SSH access. This user account will be used for ICG installation by the UMS.

⚠️ For security reasons, the username should be long (20 to 30 characters) and cryptic.

ⓘ Username "icg" Is Reserved

Do not use "icg" as a username for the remote installer; this is the username under which the Tomcat server is running.



- Under **Password** and **Confirm password**, enter a strong password (20 to 30 characters are recommended)

Create a virtual machine

Instance details

Virtual machine name *	MyIcg
Region *	(Europe) Germany West Central
Availability options	Availability zone
Availability zone *	1
Image *	Ubuntu Server 18.04 LTS - Gen1
See all images	
Azure Spot instance	<input type="checkbox"/>
Size *	Standard_D2s_v3 - 2 vcpus, 8 GiB memory (\$83.95/month)
See all sizes	

Administrator account

Authentication type	<input type="radio"/> SSH public key <input checked="" type="radio"/> Password
Username *	cryptic-icg-admin
Password *	*****
Confirm password *	*****

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports *	<input type="radio"/> None <input checked="" type="radio"/> Allow selected ports
Select inbound ports *	SSH (22)

⚠️ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab.

[Review + create](#) [< Previous](#) [Next : Disks >](#)

- Click **Review + create** and review the settings.
- Click **Create**.

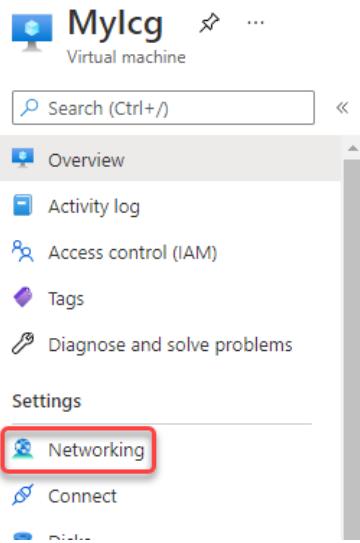


5. Click **Go to resource** and note the **Public IP address**.

Essentials			
Resource group (change)	: MyResourceGroup	Operating system	: Linux (ubuntu 18.04)
Status	: Running	Size	: Standard D2s v3 (2 vcpus, 8 GiB memory)
Location	: Germany West Central (Zone 1)	Public IP address	20.52.18.90
Subscription (change)	: Techdoc Subscription	Virtual network/subnet	: MyResourceGroupvnet118/default
Subscription ID	: dd1fe321-b2ba-406e-af3d-0311ed84e035	DNS name	: Configure
Availability zone	: 1		
Tags (change)	: Click here to add tags		

Configuring the ICG Server

1. In the sidebar menu, go to **Networking**.



2. Click **Add inbound port rule**.
 3. Edit the data as follows:
 • Destination port ranges: Enter "8443".
 • Protocol: Select **TCP**.
 • Name: Change to "Port_8443".



4. Click **Add**.

Source ⓘ
Any

Source port ranges * ⓘ
*

Destination ⓘ
Any

Service ⓘ
Custom

Destination port ranges * ⓘ
8443

Protocol
 Any
 TCP
 UDP
 ICMP

Action
 Allow
 Deny

Priority * ⓘ
310

Name *
Port_8443

Description

Add Cancel

Installing the ICG

1. Follow the instructions under [Providing the Certificates](#)³⁶.
2. Follow the instructions under [Installing the IGEL Cloud Gateway](#)³⁷.

³⁶ <https://kb.igel.com/display/igelicg202/Providing+the+Certificates>

³⁷ <https://kb.igel.com/display/igelicg202/Installing+the+IGEL+Cloud+Gateway>



Connecting the Devices

- ▶ Follow the instructions under [Connecting the Devices³⁸](#).

IGEL UMS Installation under Windows

- i** For the supported operating systems, see the "Supported Environment" section of the [release notes\(see page 565\)](#).

Standard Installation

To install the IGEL Universal Management Suite under Windows, proceed as follows:

1. Download the current version of the IGEL Universal Management Suite from the [IGEL Download Server³⁹](#).
 2. Launch the installer.
- i** You will need administrator rights in order to install the UMS.
3. Read and confirm the **License Agreement**.
 4. Read the **Information** regarding the installation process and click **Next**.
 5. Only if this is an update installation: If you already have a UMS installation, select the file name for the **backup** of your embedded database. If you do not choose a file name and click on **Next**, no backup will be created. See also [Updating under Windows\(see page 288\)](#).
 6. Only if this is a new installation: Select the folder for the installation under **Select Destination Location**. (Default: C:\Program Files\IGEL\RemoteManager)
 7. Choose the components to be installed under **Select Components**.
 - **Standard UMS**
 - **with UMS Console**
 - **with Embedded Database**
 - **Only UMS Console**
 - **UMS High Availability Network**
 - **UMS Server**
 - **UMS Load Balancer**
 - **UMS Web App (early feature set)**

i The embedded database is suitable for most purposes. If not disabled, the embedded database will automatically be installed if you select **Standard UMS**.
The use of an external database system is recommended in the following cases:

 - You manage a large network of devices.
 - A dedicated database system is already in use in your company.
 - You integrate the High Availability solution.
 8. Read the **Memory (RAM) requirements** and click **Next** if your system fulfills them.

³⁸ <https://kb.igel.com/display/igelicg202/Connecting+the+Devices>

³⁹ <https://www.igel.com/software-downloads/workspace-edition/>



9. Select the **UMS data directory**. (Default: C:\Program Files\IGEL\RemoteManager)
10. Under **User Credentials for DB-connect**, enter the user name and password for the database connection – unless you are planning to connect the UMS to an MS SQL Server via Active Directory. For more information on connecting via AD, see [Connecting the UMS to an SQL Server via Active Directory](#)(see page 292).

The credentials for the database connection are created.

- i** Initially, the credentials entered here are also the credentials of the UMS superuser. After the installation, the credentials for the database user and those for the UMS superuser can be changed independently from each other. For more information about the UMS superuser, see [Changing the UMS Superuser](#)(see page 547).

11. If the internal Windows firewall is active on your host: Review the settings under **Windows firewall settings** and change them where necessary. Each port that is activated here will be set as rule in the Windows firewall. For more information about the usage of ports, see [UMS Communication Ports](#)(see page 48).
12. Choose a folder name under **Select Start Menu Folder**.
13. Read the summary and start the installation process.
The installer will install the UMS, create entries in the Windows software directory, and in the start menu, and will place a shortcut for the UMS Console on the desktop.
14. Close the program after completing the installation by clicking on **Finish**.
If you have chosen the standard installation, the UMS Server will run with the embedded database.
15. Start the UMS Console.
16. Connect the UMS Console to the UMS Server using the access data for the database that you entered during the installation.
You will find information regarding the use of the UMS with external databases under [Connecting External Database Systems](#)(see page 289).

Silent Installation of the UMS Console

You can carry out the installation silently by first creating an .inf file and then launching the installation using a command line.

- i** Silent installation is only possible for the UMS Console. It is not possible for the UMS Server, the UMS Administrator, or the UMS Web App.

For further information, see [Unattended/Silent Installation of UMS Console](#)(see page 284).

Unattended/Silent Installation of UMS Console

Issue

After a UMS Server update, an update of the UMS Console on client machines is needed.

Solution

Perform the following steps for an unattended/silent installation of the UMS Console:

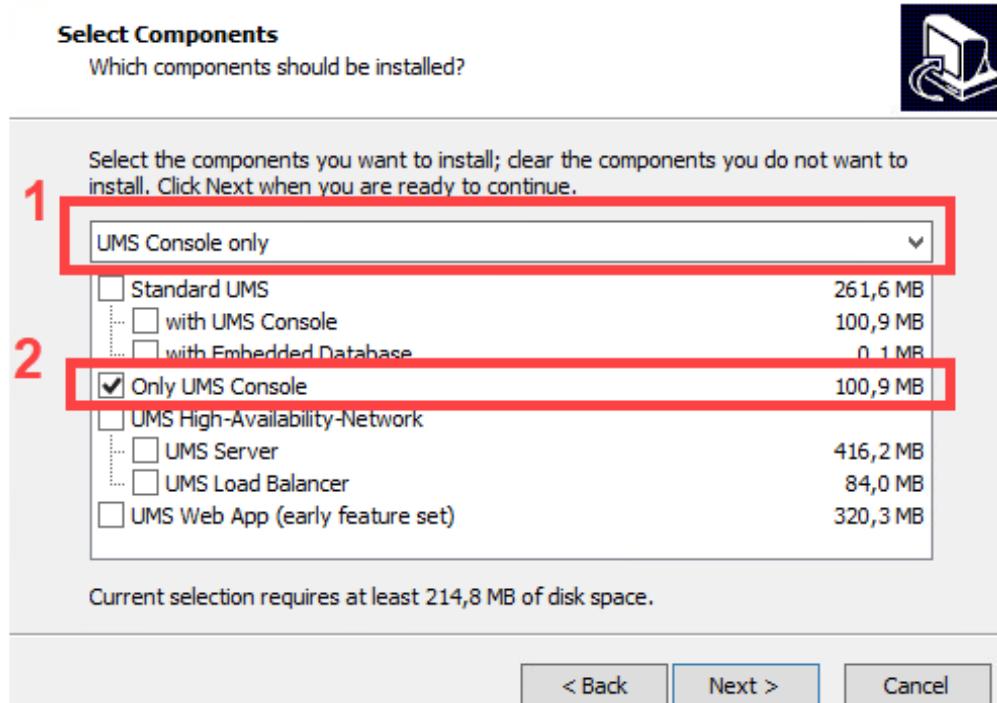


1. Create a config file:

In cmd or powershell:

```
C:\[download directory]\setup-igel-ums-windows_x.y.z.exe /saveinf="[config-file]"
```

2. Use the wizard displayed to complete the installation while recording it to the config file. Under **Select Components**, make the following selection:



3. Install:

```
C:\[download-directory]\setup-igel-ums-windows_x.y.z.exe /loadinf="[config-file]" /silent
```

An installer window prompting the user may appear, but the installation will complete in the background, regardless.

i This applies only to the UMS installer for Windows.

i Silent installation is only possible for the UMS Console. It is not possible for the UMS Administrator, the UMS Server, or the UMS Web App.

3.3.3 Updating UMS

Here you will find how to update a UMS installation under Windows or Linux.

Update instructions for the UMS High Availability (HA) installation can be found under [Updating the Installation of an HA Network](#)(see page 671).

If you want to switch to the UMS HA from the standard UMS installation, see [Switching from a Standard UMS Installation to an HA Installation](#)(see page 680).



- [Updating under Linux](#)(see page 286)
- [Updating under Windows](#)(see page 288)

⚠ Before the installation, check that your hardware and software fulfill the [installation requirements](#)(see page 258). See also [Devices Supported by IGEL Universal Management Suite](#)(see page 47).

⚠ Create a backup of the database before updating a previously installed version of the UMS. Otherwise, you risk losing all database content. See [Backups](#)(see page 536) and [Creating a Backup](#)(see page 536).

✓ We recommend that you install the new version of the UMS on a test system before installing it on the productive system. Once you have checked the functions of the new version on the test system, you can install the new version on the productive system. This also applies to hotfixes, patches etc. for the server system and database.

⚠ Installing a version of the UMS which is older than the one currently used is only possible if you have a backup of the database with the corresponding older schema. You can only switch from an older database schema to a newer one, not the other way around. You should therefore create a backup of your existing system before you start the update.

⚠ If the version of the UMS Console is older than the version of the UMS Server, you will not be able to establish a connection to the UMS Server (Unable to load tree error message). In this case, you will need to update the installation of the UMS Console.

✓ If you use an older version of the IGEL Remote Manager with SAP DB, we recommend that you switch to the embedded database before updating the UMS. For a more detailed description of this switch, please contact [IGEL Support](#)⁴⁰.

i From UMS 5.01.100, you can only use the directory `ums_filetransfer` or subdirectories created in it for WebDAV downloads. The installer offers you the option of moving existing directories to this new default folder.

i During a UMS upgrade, e.g. from 6.06 to 6.07, the database schema is changed by the installer. With large production databases, this process can last up to 2 hours. Do not abort the installation during this time.

Updating under Linux

Before starting the update procedure, read [Updating UMS](#)(see page 285).

⚠ Create a [backup of the database](#)(see page 536) before updating a previously installed version of the UMS. Otherwise, you risk losing all database content.

⁴⁰ <https://www.igel.com/submit-a-ticket/>



⚠ Oracle

For the proper operation of the UMS with Oracle databases, particularly for the upgrade process, the number of open_cursors for the database must be adjusted. open_cursors is a system setting.

1. To get the actual value, log in to the database as SYSDBA and execute:
`SQL> select name, value from v$parameter where name = 'open_cursors';`
2. The recommended value for open_cursors is "3000". To set the value, issue the following command as SYSDBA:
`SQL> alter system set open_cursors = 3000 scope=both;`
3. The same command should be added to the SPFILE of the Oracle system in order for the changes to persist on the next reboot.

To perform an update under Linux, proceed as follows:

1. Download the current version of the IGEL Universal Management Suite from the IGEL [Download Server](#)⁴¹.
2. Log in as root.
3. Open a terminal emulator such as xterm and switch to the directory in which the installation file `setup-igel-ums-linux-[Version].bin` is located.
4. Check whether the installation file is executable. If not, it can be made executable with the following command:
`chmod u+x setup*.bin`
5. Execute the installation file.

The installer unzips the files into the `/tmp` directory, starts the included Java Virtual Machine and removes the temporary files once the installation has been completed.

i You can cancel the installation at any time by pressing the [Esc] key twice.

6. Read and confirm the license agreement.
7. Read the explanation of the installation process.
8. Under **Destination directory**, select the directory in which the UMS is to be installed. (Default: `/opt/IGEL/RemoteManager`)
9. Under **Database backup**, select a file for the backup of the existing embedded database. If you have already created a backup, you can select **No (continue)** in order to skip this step.
10. Under **Installation type**, select the scope of installation:
 - **Complete:** [UMS Server](#)(see page 256) and [UMS Console / UMS Web App](#)(see page 257)
 - Client only: UMS Console only
 - HA net: [High Availability](#)(see page 657) configuration
11. Choose whether the [UMS Web App](#)(see page 720) should be installed.
12. Confirm the **system requirements** dialog if your system fulfills them.
13. Specify whether you would like to create **shortcuts** for the UMS Console and UMS Administrator in the menu.
14. Check the summary of the installation settings and start the procedure by selecting **Start installation**.

⁴¹ <https://www.igel.com/software-downloads/workspace-edition/>



- i** During a UMS upgrade, e.g. from 6.06 to 6.07, the database schema is changed by the installer. With large production databases, this process can last up to 2 hours. Do not abort the installation during this time.
15. Once the installation procedure is complete, open the UMS Console via the menu or with the command `/opt/IGEL/RemoteManager/RemoteManager.sh`

i It is generally NOT recommended to execute the command `RemoteManager.sh` with sudo. On Red Hat Enterprise Linux 8, `RemoteManager.sh` can be executed only without sudo.
 16. Connect the UMS Console to the UMS Server with the help of the existing access data.

Updating under Windows

Before starting the update procedure, read [Updating UMS\(see page 285\)](#).

- ⚠** Create a [backup of the database\(see page 536\)](#) before updating a previously installed version of the UMS. Otherwise, you risk losing all database content.

To perform an update under Windows, proceed as follows:

1. Download the current version of the IGEL Universal Management Suite from the IGEL [Download Server](#)⁴².
2. Close any other applications and launch the installer.

i You will need administrator rights in order to install the UMS.
3. Read and confirm the **License Agreement**.
4. Read the **Information** regarding the installation process and click **Next**.
5. Under **Database backup**, select a file for the backup of the existing embedded database. If you do not choose a file name and click on **Next**, no backup will be created.
6. Choose the components to be installed under **Select Components**.
 - **Standard UMS**
 - **with UMS Console**
 - **with Embedded Database**
 - **Only UMS Console**
 - **UMS High Availability Network**
 - **UMS Server**
 - **UMS Load Balancer**
 - **UMS Web App (early feature set)**
7. Read the **Memory (RAM) requirements** and click **Next** if your system fulfills them.
8. If the internal Windows firewall is active on your host: Review the settings under **Windows firewall settings** and change them where necessary. Each port that is activated here will be set as rule in the Windows firewall. For more information about the usage of ports, see [UMS Communication Ports\(see page 48\)](#).

⁴² <https://www.igel.com/software-downloads/workspace-edition/>



9. Read the summary and start the installation process.

The installer will install a new version of the UMS, create entries in the Windows software directory and in the start menu and will place a shortcut for the UMS Console on the desktop.

- (i) During a UMS upgrade, e.g. from 6.06 to 6.07, the database schema is changed by the installer. With large production databases, this process can last up to 2 hours. Do not abort the installation during this time.

10. Close the program once the installation is complete by clicking on **Finish**.

11. Start the UMS Console.

12. Connect the UMS Console to the UMS Server with the help of the existing access data.

For information on the silent installation of the UMS Console, see [Unattended/Silent Installation of UMS Console](#)(see page 284).

- (i) If you use an external database, check the database connection in the [UMS Administrator](#)(see page 529) > [Datasource](#)(see page 543). If [SQL Server AD Native](#)(see page 292) is used, you must also set the correct startup type and logon settings for the "IGEL RMGUIServer" service and restart the service. For details, see "[Configuring the UMS Server Windows Service](#)" under "[Setting Up the UMS for SQL Server AD Native](#)"(see page 299).

3.3.4 Connecting External Database Systems

- (i) The use of an external database system is recommended in the following cases:
 - You manage a large network of devices.
 - A dedicated database system is already in use in your company.
 - You integrate the [High Availability](#)(see page 657) solution.

In other cases, the use of the embedded database is suitable. It is included in the standard UMS installation, see [IGEL UMS Installation under Windows](#)(see page 283) or [IGEL UMS Installation under Linux](#)(see page 261).

- (i) For details on the supported database systems, see the "Supported Environment" section of the [release notes](#)(see page 565). Details of the requirements when installing and operating the database can be found in the documentation for the particular DBMS.

- To configure the database, use the relevant DBMS management program.
- To configure the data source and to connect the UMS to the database, use the [UMS Administrator](#)(see page 529) > [Datasource](#)(see page 543).

! Be aware not to use special characters in your schema name or database user name!

! All UMS Servers must work with the same database.

(i) For large High Availability environments, cluster databases are recommended.



For the backup procedure for UMS installations with the external database, see [Creating a Backup](#)(see page 536).

See also [Migrating a UMS Database From Embedded DB to Microsoft SQL Server](#)(see page 112).

- [Oracle](#)(see page 290)
- [Oracle RAC](#)(see page 290)
- [Microsoft SQL Server](#)(see page 291)
- [Microsoft SQL Server Cluster](#)(see page 291)
- [Connecting the UMS to an SQL Server via Active Directory](#)(see page 292)
- [PostgreSQL](#)(see page 304)
- [Apache Derby](#)(see page 305)

Oracle

To integrate Oracle, proceed as follows:

1. Set up a new database user with Resource role in the Oracle Database Administration.

i A number of Oracle versions set up the Resource role without Create View authorization. Please ensure that this authorization is set for the role.

⚠ Oracle

For the proper operation of the UMS with Oracle databases, particularly for the upgrade process, the number of open_cursors for the database must be adjusted. open_cursors is a system setting.

1. To get the actual value, log in to the database as SYSDBA and execute:
SQL> select name, value from v\$parameter where name = 'open_cursors';
2. The recommended value for open_cursors is "3000". To set the value, issue the following command as SYSDBA:
SQL> alter system set open_cursors = 3000 scope=both;
3. The same command should be added to the SPFILE of the Oracle system in order for the changes to persist on the next reboot.

2. In the [UMS Administrator](#)(see page 529), set up a new **Oracle** type data source.

Oracle RAC

1. Set up a new database user with Resource role in the Oracle Database Administration.

i A number of Oracle versions set up the Resource role without Create View authorization. Please ensure that this authorization is set for the role.

⚠ Oracle

For the proper operation of the UMS with Oracle databases, particularly for the upgrade process, the number of open_cursors for the database must be adjusted. open_cursors is a system setting.



1. To get the actual value, log in to the database as SYSDBA and execute:

```
SQL> select name, value from v$parameter where name = 'open_cursors';
```
 2. The recommended value for open_cursors is "3000". To set the value, issue the following command as SYSDBA:

```
SQL> alter system set open_cursors = 3000 scope=both;
```
 3. The same command should be added to the SPFILE of the Oracle system in order for the changes to persist on the next reboot.
2. Use the [UMS Administrator](#)(see page 529) to set up a new **Oracle RAC** type data source for each server.

Microsoft SQL Server

To connect the Microsoft SQL Server, proceed as follows:

1. Open the SQL Console of the SQL Server by selecting "New Query" in SQL Server Management Studio.
2. Use the following script as a template, customize it (password), and then execute it.

i To avoid problems when enabling the data source, ensure that LOGIN, USER, and SCHEMA have the same name.

```
CREATE DATABASE rmdb
GO
USE rmdb
GO
CREATE LOGIN igelums with PASSWORD = 'setyourpasswordhere',
DEFAULT_DATABASE=rmdb
GO
CREATE USER igelums with DEFAULT_SCHEMA = igelums
GO
CREATE SCHEMA igelums AUTHORIZATION igelums GRANT CONTROL to igelums
GO
```

3. In the [UMS Administrator](#)(see page 529), set up a new **SQL Server** type data source.
4. Ensure that the **port** of the SQL Server in the data source is configured correctly. (Default: 1433)

i The Microsoft SQL Server should allow Windows and SQL authentication.

i If you deploy MS SQL Server Always On Availability Groups, use **SQL Server** as a **DB type** and specify under **Host** the domain name of the Always On Availability Group listener.

Microsoft SQL Server Cluster

1. Open the SQL console of the SQL server by selecting "New Query" in SQL Server Management Studio.
2. Use the following script as a template, customize it (password) and execute it.



- ⓘ To avoid problems when activating the data source, ensure that LOGIN, USER, and SCHEMA have the same name.

```

CREATE DATABASE rmdb
GO
USE rmdb
GO
CREATE LOGIN igelums with PASSWORD = 'setyourpasswordhere',
DEFAULT_DATABASE=rmdb
GO
CREATE USER igelums with DEFAULT_SCHEMA = igelums
GO
CREATE SCHEMA igelums AUTHORIZATION igelums GRANT CONTROL to igelums
GO
  
```

3. Use the [UMS Administrator](#)(see page 529) to set up a new **SQL Server Cluster** type data source for each server.

- ⓘ The Microsoft SQL Server Cluster should allow Windows and SQL authentication.

Connecting the UMS to an SQL Server via Active Directory

With UMS 6.05 or higher, you can connect to a Microsoft SQL server database using Microsoft Active Directory (AD).

Two modes are available:

- AD native
- AD over Kerberos

AD Native (Windows only)

The UMS does not know the database credentials; instead, the credentials are taken from the underlying system user. A Windows API is used to connect to the database.

This mode is only available if both the UMS Server and the UMS Administrator are running in a Windows domain. Also, the domain user account under which the UMS Server and the UMS Administrator are running must have access to the database.

AD over Kerberos

The credentials of the database user must be entered into the UMS. The database connection is handled by the Kerberos protocol.

This mode can be used on Windows and Linux operating systems. The underlying system must provide the access data to connect to the domain controller for Kerberos. The UMS Administrator and the UMS Server can run with the normal users.

-
- [Prerequisites](#)(see page 293)
 - [Adding Users and a Group to the Windows Domain](#)(see page 293)



- Configuring the SQL Server (see page 294)
- Setting Up the UMS (see page 298)

Prerequisites

The following components must be available

- A Windows domain server
- A Microsoft SQL Server database running on a server in the Windows domain
- The UMS Server and the UMS Administrator are located in the Windows domain (AD native mode) or have access to the Windows domain (AD Kerberos mode).

Next Step

>> [Adding Users and a Group to the Windows Domain \(see page 293\)](#)

Adding Users and a Group to the Windows Domain

- Make sure that your windows domain contains users who have the following permissions:

- Log in to the database server
- Log in to the database that is connected the UMS
- Log in to the server with the UMS components (AD native mode only)
- Run the UMS Server as a Windows service (AD native mode only)

- i** It is recommended to create a group in the domain that will contain the users for the database ("UMSdb" in our example) and put the users ("Ike" and "Tina") for the UMS into this group. This group will become the owner of the UMS database, allowing all users in the group to work with the database.

Name	Type	Description
Enterprise Read-only Domain Controllers	Security Group...	Members of this group
Key Admins	Security Group...	Members of this group
Enterprise Key Admins	Security Group...	Members of this group
Cloneable Domain Controllers	Security Group...	Members of this group
RAS and IAS Servers	Security Group...	Servers in this group can
UMSdb	Security Group...	UMS database group
Ike	User	UMS user
Tina	User	UMS user

UMSdb Properties

Members:

Name	Active Directory Domain Services Folder
Ike	HEXlocal/Users
Tina	HEXlocal/Users

Check List

- ✓** The users or the group with the required permissions have been set up.

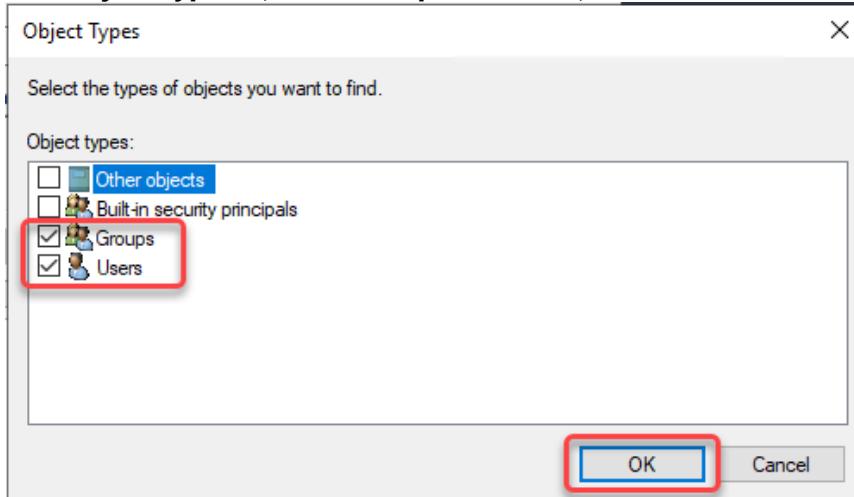
Next Step

>> [Configuring the SQL Server \(see page 294\)](#)

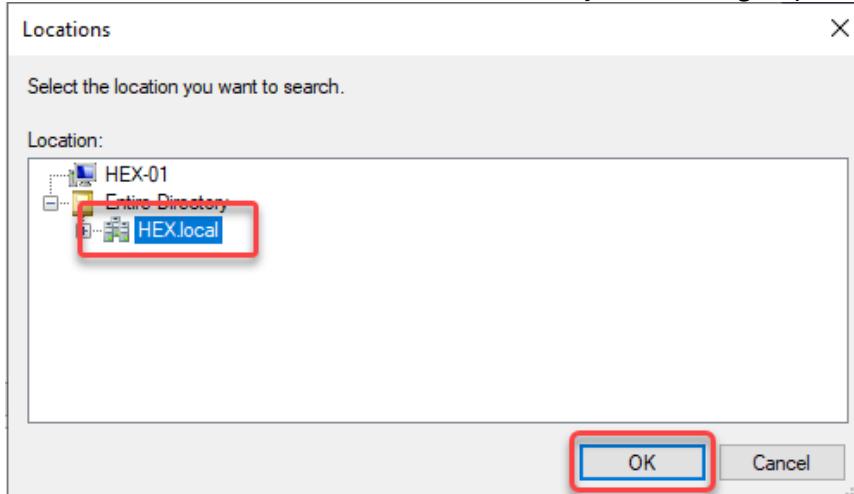
Configuring the SQL Server

Adding the User or Group

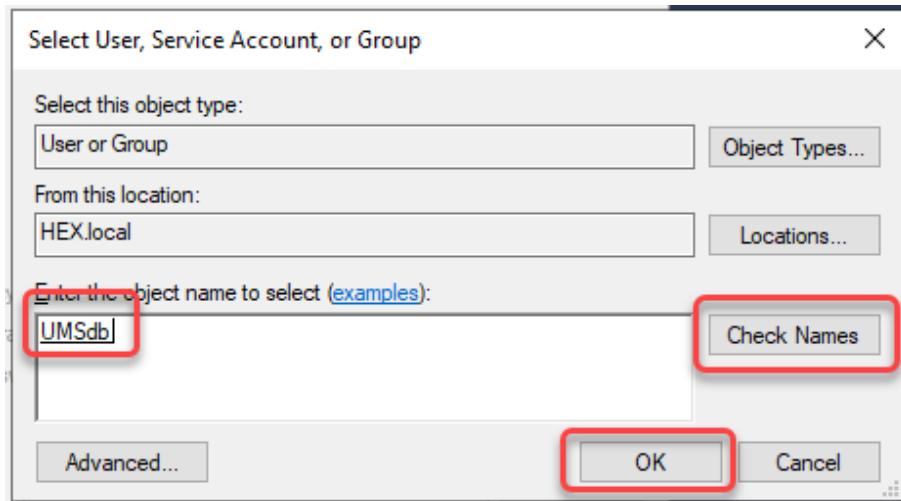
1. Connect to the database with the SQL Server Management Studio.
2. Open the **Security** branch, right-click on **Logins** and select **New Login**.
3. Choose **Windows Authentication** for the login, and click **Search**.
4. Click **Object Types...**, select **Groups** and **Users**, and click **OK**.



5. Click **Locations...**, choose the location wherein your user or group is residing, and click **OK**.



6. Enter the name of the group or user, click **Check Names**, select the name of your user or group, and click **OK**.



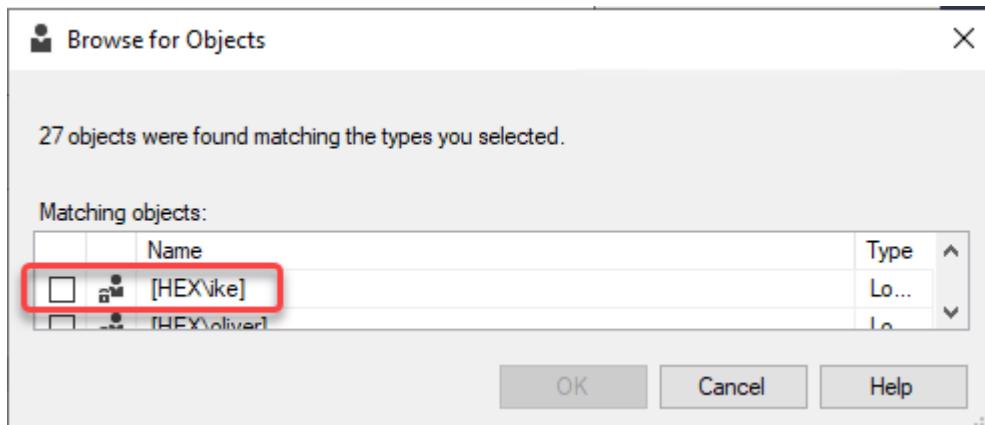
If you selected a group, all users in this group will be able to access the databases where this group is defined as the database owner. Also, if you selected a group, you should add at least one user which will become the main database owner.

Setting up the Database

The database that will be used by the UMS either needs to have a domain user as the database owner or grant a domain user or group the necessary access rights.

Setting the Domain User as Owner

1. Open the **Create database** dialog.
2. Set a **Database name**.
3. For the **Owner** of the database, click ... on the right side to browse for a user.
4. Select the user that will be the database owner.



Check and Grant Access Rights to the Domain User or a Domain Group

1. Go to the **Security** branch of the database server.
2. Select the user or group that is to be used for database login and open **Properties**. The dialog **Login Properties - [Location]** opens.
3. Click **User mapping** to map your UMS database to the user or group.



4. In the **Users mapped to this login** area, select your database.

For the database owner defined before, all settings (**User:** "dbo" and **Default Schema:** "dbo") are valid.

Login Properties - HEX\ike

Select a page

- General
- Server Roles
- User Mapping
- Securables
- Status

Connection

Server: HEX-01
Connection: sa
[View connection properties](#)

Progress

Ready

Script **Help**

Users mapped to this login:

Map	Database	User	Default Schema
<input type="checkbox"/>	rmdbADa		
<input type="checkbox"/>	rmdbADb		
<input type="checkbox"/>	rmdbADc		
<input type="checkbox"/>	rmdbADd		
<input type="checkbox"/>	rmdbADgrp		
<input type="checkbox"/>	rmdbH1		
<input type="checkbox"/>	rmdbH4		
<input type="checkbox"/>	rmdbha		
<input type="checkbox"/>	rmdbKBR		
<input type="checkbox"/>	tempdb		
<input checked="" type="checkbox"/>	umsdb	dbo	dbo

Guest account enabled for: umsdb

Database role membership for: umsdb

<input type="checkbox"/> db_accessadmin
<input type="checkbox"/> db_backupoperator
<input type="checkbox"/> db_datareader
<input type="checkbox"/> db_datawriter
<input type="checkbox"/> db_ddladmin
<input type="checkbox"/> db_denydatareader
<input type="checkbox"/> db_denydatawriter
<input checked="" type="checkbox"/> db_owner
<input type="checkbox"/> db_securityadmin
<input checked="" type="checkbox"/> public

OK **Cancel**

A red box highlights the "Users mapped to this login" table, specifically the row for "umsdb". The "User" and "Default Schema" columns for this row are both set to "dbo". The "db_owner" checkbox under "Database role membership for: umsdb" is also highlighted with a blue bar.



For a group, your group name is appropriate. The **Default Schema** must be set to "dbo".

Login Properties - HEX\UMSdb

Select a page: General, Server Roles, User Mapping, Securables, Status

Connection: Server: HEX-01, Connection: sa, View connection properties

Progress: Ready

Script Help

Users mapped to this login:

Map	Database	User	Default Schema
<input type="checkbox"/>	mdbADA		
<input type="checkbox"/>	mdbADb		
<input type="checkbox"/>	mdbADc		
<input type="checkbox"/>	mdbADD		
<input type="checkbox"/>	mdbADgrp		
<input type="checkbox"/>	mdbH1		
<input type="checkbox"/>	mdbH4		
<input type="checkbox"/>	mdbha		
<input type="checkbox"/>	mdbKBR		
<input type="checkbox"/>	tempdb		
<input checked="" type="checkbox"/>	umsdb	HEX\UMSdb	dbo

Guest account enabled for: umsdb

Database role membership for: umsdb

<input type="checkbox"/> db_accessadmin
<input type="checkbox"/> db_backupoperator
<input type="checkbox"/> db_datareader
<input type="checkbox"/> db_datawriter
<input type="checkbox"/> db_ddladmin
<input type="checkbox"/> db_denydatareader
<input type="checkbox"/> db_denydatawriter
<input checked="" type="checkbox"/> db_owner
<input type="checkbox"/> db_securityadmin
<input checked="" type="checkbox"/> public

OK Cancel

A red rounded rectangle highlights the "Default Schema" column in the "Users mapped to this login" table, specifically around the row for the "umsdb" user.



5. In the area **Database role membership for: [your UMS database]**, activate **db_owner**.

The screenshot shows the 'Login Properties' dialog box for the 'umsdb' login. The 'Connection' section indicates the server is 'HEX-01' and the connection is 'sa'. The 'Progress' section shows 'Ready'. In the main area, under 'Database role membership for: umsdb', the 'db_owner' checkbox is checked and highlighted with a red box. Other checkboxes available but unchecked include: db_accessadmin, db_backupoperator, db_datareader, db_datawriter, db_ddladmin, db_denydatareader, db_denydatawriter, db_securityadmin, and public.

6. Click **OK** to confirm the changes.

Check List

- The database that will be used by the UMS Server is created.
- A user or group with access to this database is defined.

Next Step

>> [Setting Up the UMS](#)(see page 298)

Setting Up the UMS

Select the procedure according to the desired authentication method:



- [Setting Up the UMS for SQL Server AD Native](#)(see page 299)
- [Setting Up the UMS for SQL Server Kerberos](#)(see page 302)

Setting Up the UMS for SQL Server AD Native

⚠ Password Policy - Regular Password Changes

If your password policy involves regular password changes, be aware that changing the AD password requires updating the run options of the Windows Service.

Configuring the UMS Server Windows Service

The Windows service for the UMS Server must run as a domain user that has read and write access to the UMS database.

If this was not changed by the installation, the administrator must do it manually before the SQL Server database is activated in the UMS Administrator. You can use the Windows app **Services** or the command line.

ⓘ High Availability

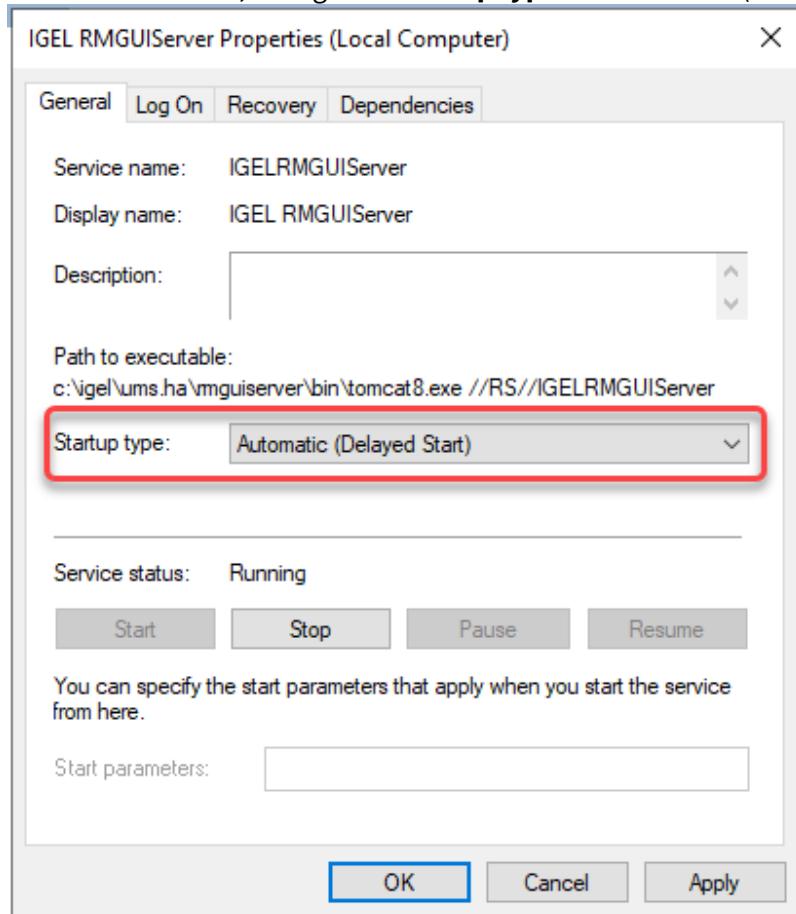
In case of an HA installation or update, this must be done on ALL UMS Server hosts.

Using the "Services" App

1. Start the "Services" app of Windows and select **Properties** for the service **IGEL RMGUIServer**.



2. On the **General** tab, change the **Startup type** to "Automatic (Delayed Start)".

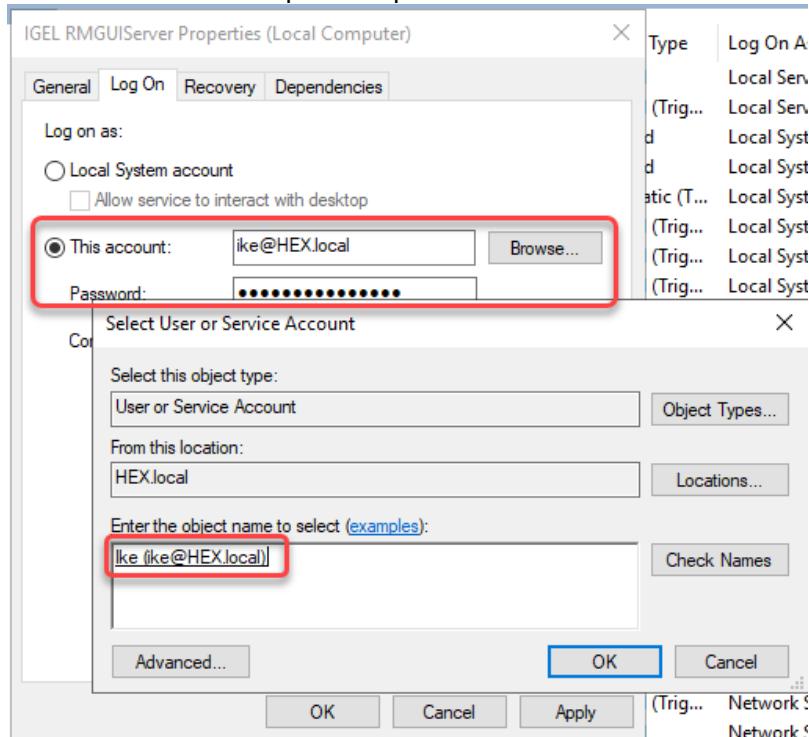


3. Switch to the **Log On** tab and edit the settings as follows:

- **This account:** Set this to the domain user with database access and local windows administrator rights.
- **Password:** Enter the password for the domain user.



- **Confirm Password:** Repeat the password for the domain user.



4. Restart the service.

Using the Command Line

1. Enter the following command: `sc config IGELRMGUIServer obj=[domain]\[username] password=[password] start=delayed-auto`
2. Enter the following commands to restart the service:
`sc stop IGELRMGUIServer`
`sc start IGELRMGUIServer`

Activating the Database

The activation of an SQL Server database is done with the UMS Administrator as usual. The native connection uses the credentials of the domain user that started the UMS Administrator to access the database. This user must have database access and local Windows admin rights. No additional credentials must be defined.

To activate the database:

1. In the UMS Administrator, select **Datasource** and then click **Add....**
2. In the **New Datasource** dialog, edit the settings as follows:
 - **DB type:** Select "SQL Server AD Native".
 - **Host:** Enter the name of the host on which the MS SQL database is running.
 - **Port:** Enter the port on which the MS SQL database service is listening.
 - **Schema:** Enter "dbo".



- **Database / SID:** Enter the name of the database.

Configure Datasource

DB type	SQL Server AD Native
Host	hex-01.hex.local
Domain	
Port	1433
User	
Schema	dbo
Database / SID	umsdb
Instance	

Ok Cancel

3. Click **Activate**.

The **Define UMS superuser username and password** dialog opens.

4. Enter the username and the password of the UMS superuser and click **Ok**.

Define UMS superuser username and password

User name	ums.admin.user
Password	
Confirm password	

Ok Cancel

Your UMS is set up for connecting to the Microsoft SQL Server database via Active Directory.

Setting Up the UMS for SQL Server Kerberos

⚠ Password Policy - Regular Password Changes

If your password policy involves regular password changes, be aware that changing the AD password requires updating the UMS Server database configuration.

Setting Up Kerberos

The UMS can use an SQL Server database with domain login on Windows systems and Linux systems even if they are not part of the domain. In this case, the **DB type** "SQL Server AD Kerberos" must be used and the system must be configured before the database is activated.

Creating a Kerberos Configuration File



The Kerberos configuration file contains the data needed for the system to access the domain information.

To learn how a Kerberos configuration file looks, see the following example:

```
[libdefaults]
default_realm = HEX.LOCAL
ticket_lifetime = 24h
[realms]
HEX.LOCAL = { kdc = 111.111.111.111 default_domain = HEX.LOCAL }
[domain_realm]
.hex.local = HEX.LOCAL
[appdefaults]
```

For a detailed description of the content, see https://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/krb5_conf.html.

- i** The domain does not have to be identical to the domain of the server where the UMS is installed.

Saving the Kerberos Configuration File

- Save the Kerberos configuration file in the directory <UMS installation directory>/rmguiserver/conf with the name krb5.conf

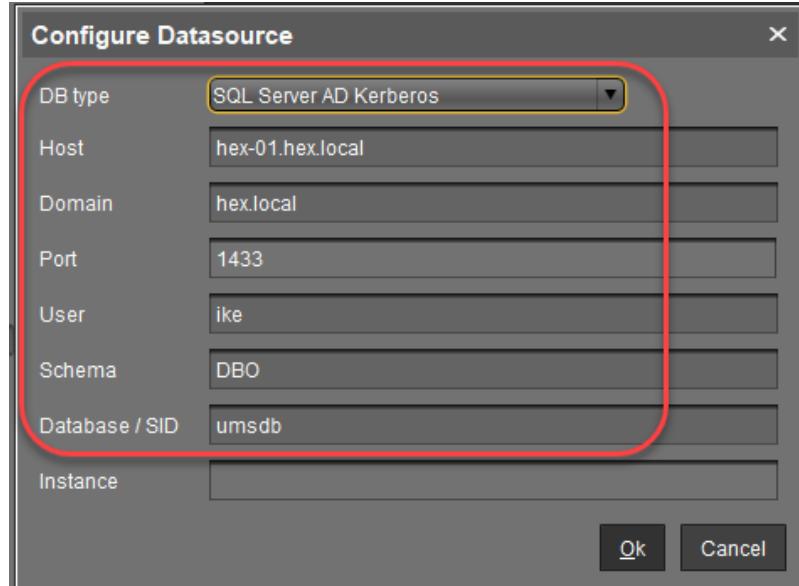
Activating the Database

The activation of the SQL Server database is done as normally in the UMS Administrator. The Kerberos connection needs a domain user and password for access to the database.

To activate the database:

1. In the UMS Administrator, select **Datasource** and then click **Add...**
2. In the **New Datasource** dialog, edit the settings as follows:
 - **DB type:** Select "SQL Server AD Kerberos".
 - **Host:** Enter the fully qualified name of the host on which the MS SQL database is running.
 - **Domain:** Enter the domain of the user which logs into the database.
 - **User:** Enter the username for connecting to the database, without the domain.
 - **Port:** Enter the port on which the MS SQL database service is listening.
 - **Schema:** Enter "dbo".

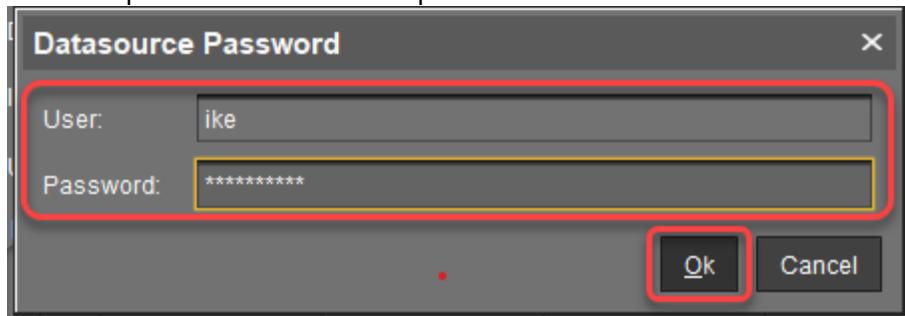
- **Database / SID:** Enter the name of the database.



3. Click **Activate**.

The **Datasource Password** dialog opens.

4. Enter the domain password of the database user and click **Ok**. This password will also be used as the initial password of the UMS superuser.



PostgreSQL

- i** For details on the supported database systems, see the "Supported Environment" section of the [release notes](#)(see page 565). Details of the requirements when installing and operating the database can be found in the documentation for the particular DBMS.

When installing a new instance of the PostgreSQL database, set the following parameters:

1. Install the database cluster with UTF-8 **coding**.
2. Accept the conditions for all **addresses**, not just localhost.
3. Activate **Procedural Language** PL/pgsql in the default database.



For further information regarding installation of the PostgreSQL database, see <http://www.postgresql.org>⁴³.

Once installation is complete, carry out the following configuration procedure:

1. Change the server parameters: The parameter `listen_addresses` in the file `postgresql.conf` must contain the host name of the IGEL UMS Server or '*' in order to allow connections to each host.
2. Set up a host parameter in the file `pg_hba.conf` in order to give the UMS Server the authorization to log in using the user data defined there.

i If the IGEL UMS Server is installed on the same machine as the PostgreSQL Server, no changes to these files are needed.
3. Launch the administration tool pgAdmin.
4. Create a new login role with the name `rmlogin`.
5. Create a new database with


```
name = rmdb
owner = rmlogin
encoding = UTF-8
```
6. Set up a new schema within the `rmdb` database with


```
name = rmlogin
```
7. Check whether the language `plpgsql` is available in the `rmdb` database. If not, set it up.
8. In the [UMS Administrator](#)(see page 529), create a new data source with the following parameters:
DB type: PostgreSQL
Host: Name of the PostgreSQL Server
Port: Port of the PostgreSQL Server. (Default: [5432](#))
User: `rmlogin`
Database / SID: `rmdb`

Apache Derby

- i** For details on the supported database systems, see the "Supported Environment" section of the [release notes](#)(see page 565). Details of the requirements when installing and operating the database can be found in the documentation for the particular DBMS.

As with other external databases, we recommend that you create a new database instance for use by the IGEL UMS.

Perform the following steps to create a new database instance and define the instance as a data source in the **UMS Administrator**:

1. For security purposes, enable **User Authentication** in the Derby DB.
2. Launch the `ij Utility` (in `[derby-installation-dir]/bin`).
3. To create the `rmdb` instance, execute the following command:

```
connect
'jdbc:derby:rmdb;user=dbm;password=dbmpw;create=true';
```

⁴³ <http://www.postgresql.org/>



4. Define the UMS database user `rmlogin` with password `rmpassword`
`CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.user.rmlogin', 'rmpassword');`
5. Exit *ij* and launch the *Derby Network Server*.
6. In the [UMS Administrator](#)(see page 529), create a new data source with the following parameters:
DB type: Derby
Host: Name of the Derby Server
Port: Port of the Derby Server. (Default: [1527](#))
User: `rmlogin`
Database / SID: `rmdb`

For further information regarding installation of the Derby database, see <http://db.apache.org/derby>.

3.4 Connecting the UMS Console to the Server

The procedure for connecting the UMS Console to the UMS Server is described below.

To establish a connection to the UMS Server, proceed as follows:

1. Start the UMS Console.
2. Enter the access data:
 - **Server:** Host name of the UMS Server. If you are logging on to the UMS Console of the server, enter `localhost`.
 - **Port:** Port on which the GUI server of the UMS receives UMS Console queries. Default: [8443](#). You can change the port using the UMS Administrator; see [Settings for IGEL UMS Administrator](#)(see page 530).
 - **User name:** User name for the connection between the UMS Console and database. When setting up the UMS for the first time, this is the user name of the database user account which was created while the UMS Server was being installed. If you belong to a domain configured in the UMS, enter `@`.
 - **Password:** Password for the connection between the UMS Console and database. When setting up the UMS for the first time, this is the password of the database user account which was created while the UMS Server was being installed.
3. Click on **Connect**.

The data entered under **Server**, **Port**, and **User name** will be saved for subsequent connection procedures. The next time you establish a connection, you will only need to enter the password. The server and user information last used is also stored. You can delete stored logon data under **Misc > Settings > General > Clear login history**.

3.5 Registering Devices on the UMS Server

You can register devices on the UMS Server in the following ways:

- [Searching for Devices](#)(see page 307)
- [Registering Devices](#)(see page 307)
- [Importing Devices](#)(see page 308)
- [Registering Devices Automatically](#)(see page 312)
- [Setting up Devices Manually](#)(see page 313)



- Registering manually on the device; see "[Using UMS registration](#)" function⁴⁴ in the IGEL OS reference manual.

3.5.1 Searching for Devices

In order to find devices in the network, the following requirements must be met:

- The devices must be switched on and functioning.
- The firmware for the devices must support the *UMS*. This is the case with the following devices:
 - IGEL devices with original firmware
 - Devices converted with IGEL OS Creator (OSC)
 - Devices on which IGEL OS was booted via a UD Pocket
 - Devices on which IGEL OS was installed using IGEL Universal Desktop Converter 2/3 (UDC2/UDC3)
 - Devices on which the UMA (Universal Management Agent) is running

To search for devices in the network and register them in the UMS, proceed as follows:

1. Log in to the UMS Console.
The content panel of the console will be displayed.
2. Click on .
The **Scanning for devices** window will open.
3. Specify the search area:
 - **Local Network of the UMS Server:** The UMS Server will send a broadcast message to the network.

Info: If there are a number of network interfaces, you should bear in mind that the broadcast message is only sent via the first network interface. If you use Windows, this is under the first item in the list of network connections.

 - **IP Range:** The UMS Server contacts each device in the given range.
 - **List of IP Ranges:** With **Edit list**, you can specify the IP ranges in which the UMS will search for devices.
 - **Use TCP for scanning:** If this option is enabled, communication with the devices will take place via TCP. If this option is disabled, UDP will be used.

Info: If TCP is used for searching, the search procedure will take longer.
4. Click on **Scan**.
The search results will be shown in the **Found devices** window. The devices can now be registered; see [Registering devices](#)(see page 307).

3.5.2 Registering Devices

As soon as you have obtained the search result you can register new devices.

⁴⁴ <https://kb.igel.com/display/igelos1104/Using+UMS+Registration+Function>



1. If you only want to see devices with a specific feature in the **Certificate stored, Unit ID, MAC Address, Name, IP Address or Product** column, enter the corresponding character string in the **Filter** field.
2. Select the devices that are to be registered. You have the following options:
 - Manual selection: In the **Include** column, highlight the devices that are to be registered.
 - Selecting all devices that are not yet registered: Click on **Select new Ones**. This will highlight all devices that have not yet received a server certificate from the UMS.
3. Click on **OK**.

The devices will now be registered in the UMS database. This may take some time.

- i** During registration, the UMS server certificate is saved on the device. Further access to the devices will now be validated on the basis of this certificate. Only the owner of the certificate can manage the device.

The result of the procedure and any error messages will be displayed in a new window.

The devices will be placed in the **Devices** directory in the structure tree.

3.5.3 Importing Devices

You can make devices known to the UMS before the devices are physically available in the network. This allows you to specify editable attributes such as department or cost center. To do this, import the devices' data from a CSV file.

- i** In order for devices to be registered fully, the devices' firmware data must be available in the UMS. Further information can be found under [Import Firmwares](#)(see page 393).

To import devices, proceed as follows:

1. Configure your DHCP and DNS server as described in [Registering Devices Automatically](#)(see page 312), step 2.
2. Select **System > Import > Import Devices**.
3. Click on **Open File** and select the file.
4. Select the relevant format, i.e. the format of the data.
 - **Short Format:** See [Import with Short Format](#)(see page 309)
 - **Long Format:** See [Import with Long Format](#)(see page 309)
 - **IGEL Serial Number Format:** See [Import with IGEL Serial Number](#)(see page 311)
5. If entries are flagged as erroneous, click on **Clear** to delete all messages from the window.
6. Click on **Import devices** to launch the import procedure.

To correct erroneous entries, proceed as follows:

- Change the entries highlighted in red with the following editing functions:
- [Ctrl-C] and [Ctrl-V] for copying and pasting a highlighted row
 - [Del/Ctrl-X] for deleting a highlighted row
 - [Return/Enter] inserts an additional row under a field.



Import with Short Format

The short format provides the information required for the import and assignment to a profile. The import file should be UTF-8 encoded.

- **Unit ID:** If the device is an IGEL device or a device converted with UDC3 or IGEL OS Creator (OSC), the unit ID is identical to the MAC address of the device. If the device is a UD Pocket, the unit ID is hard-wired into the UD Pocket's USB flash drive.
- **Name:** Device name.



- The maximal length of the device name is restricted to 15 characters if **Adjust network name if UMS-internal name has been changed** is enabled under **UMS Administration > Global Configuration > Device Network Settings**.
- The length of the device name is not restricted if **Adjust network name if UMS-internal name has been changed** and **Naming Convention** are not activated under **UMS Administration > Global Configuration > Device Network Settings**.
- Each device name will be automatically overwritten in compliance with the naming convention, even if **Adjust network name if UMS-internal name has been changed** is enabled, in case **Enable naming convention** is activated under **UMS Administration > Global Configuration > Device Network Settings**.

See also [Device Network Settings](#)(see page 457).

- **Firmware ID:** ID of the firmware installed on the device.



The ID of a firmware version already registered can be found via **Misc > Firmware Statistics**.

- **Profile Assignments:** ID of the assigned profile or a list of IDs separated by commas if a number of profiles are to be assigned to the device.



You can remove a profile assignment already made by placing an exclamation mark in front of the profile ID. Example: !12



The ID of a profile is shown in the **description data** and in the **tooltip** for the profile.

Code Example

```
00E0C5540B8B;IGEL-Office15-2;111;26
00E0C5540B8C;IGEL-Office15-3;111;12,26,27
00E0C5540B8D;IGEL-Office16-1;111;12
```

Import with Long Format

The long format provides detailed data as described in the following. The import file should be UTF-8 encoded.



- **Directory:** Storage directory in the UMS structure tree. This directory must exist before the devices are imported.
- **Unit ID:** If the device is an IGEL device or a device converted with UDC3 or IGEL OS Creator (OSC), the unit ID is identical to the MAC address of the device. If the device is a UD Pocket, the unit ID is hard-wired into the UD Pocket's USB flash drive.
- **Product and Version:** Product name and firmware version of the device (separated with a semicolon)
- **Name:** Name of the device



- The maximal length of the device name is restricted to 15 characters if **Adjust network name if UMS-internal name has been changed** is enabled under UMS Console > **UMS Administration > Global Configuration > Device Network Settings**.
- The length of the device name is not restricted if **Adjust network name if UMS-internal name has been changed** and **Naming Convention** are not activated under **UMS Administration > Global Configuration > Device Network Settings**.
- Each device name will be automatically overwritten in compliance with the naming convention, even if **Adjust network name if UMS-internal name has been changed** is enabled, in case **Enable naming convention** is activated under **UMS Administration > Global Configuration > Device Network Settings**.

See also [Device Network Settings](#)(see page 457).

- **Site:** Location of the device
- **Department:** Department to which the device is assigned
- **Comment:** Comment regarding the device
- **Asset ID:** Inventory number of the device
- **In-Service Date:** Date on which the device was commissioned
- **Serial Number:** Serial number of the device
- **Profile Assignments:** ID of the assigned profile or a list of IDs separated by commas if a number of profiles are to be assigned to the device

You can remove a profile assignment already made by placing an exclamation mark in front of the profile ID. Example: !12

The ID of a profile is shown in the description data and in the tooltip for the profile.

- **Cost Center:** Cost center to which the device is assigned

Code example

```
/Import;00E0C5540B9A;IGEL OS
11;11.01.100.01;IGEL-1;Büro1;EDV;Meier;0815;01.06.2019;F44M;26;01

/Import;00E0C5540B9B;IGEL OS
11;11.01.100.01;IGEL-2;Büro2;EDV;Müller;4711;01.06.2019;F45M;26;01

/Import;00E0C5540B9C;IGEL OS
11;11.01.100.01;IGEL-2;Büro3;EDV;Schulz;42;01.06.2019;F46M;26;01
```



- ⓘ A slash "/" means that the devices will be placed in the root directory. In the above examples, the devices are thus placed in the folder "Import" under root (the folder "Import" must exist).

Import with IGEL Serial Number

When ordering your IGEL devices, you can request an import file from IGEL. Alternatively, you can create your own import file using an alternative format. Both formats are based on CSV.

- ⓘ This import method works only for IGEL UD devices.

Both the format of an import file that is sent by IGEL and the alternative format specify the fields **Serial Number** and **MAC Address**.

Serial Number Format as Sent by IGEL

In an import file that is sent by IGEL, the serial number format consists of 5 fields. However, only the **Serial Number** (2nd field) and **MAC Address** (3rd field) are specified in the file.

Example:

```
;14D3F5002B290902DD ;00E0C521B4E4 ; ;  
;14D3F5002B29090441 ;00E0C521B648 ; ;  
;14D3F5002B2909056F ;00E0C521B776 ; ;  
;14D3F5002B29090648 ;00E0C521B84F ; ;  
;14D3F5002B2909070B ;00E0C521B912 ; ;
```

Alternative Serial Number Format

The alternative format has 2 fields. The field sequence is random.

Example:

Sequence MAC address - serial number:

00E0C51B37F8;14D3D3C03B174120D0

Sequence serial number - MAC address:

14D3D3C03B174120D0;00E0C51B37F8

Import Fields

For both import formats, the UMS fills in the fields **Name** and **Version** by itself. In the following, all fields predefined for imported devices are described.

MAC Address: MAC address of the device.

Name: Device name.



- !** The maximal length of the device name is restricted to 15 characters if **Adjust network name if UMS-internal name has been changed** is enabled under UMS Console > **UMS Administration > Global Configuration > Device Network Settings**.
 The length of the device name is not restricted if **Adjust network name if UMS-internal name has been changed** and **Naming Convention** are not activated under **UMS Administration > Global Configuration > Device Network Settings**.
 Each device name will be automatically overwritten in compliance with the naming convention, even if **Adjust network name if UMS-internal name has been changed** is enabled, in case **Enable naming convention** is activated under **UMS Administration > Global Configuration > Device Network Settings**. See also [Device Network Settings](#)(see page 457).

Version: Firmware version of the device, assigned by the UMS. The firmware with the highest ID will be assigned to the device. The IDs for firmware versions already registered can be found via **Misc > Firmware Statistics**.

Serial Number: Serial number of the device.

3.5.4 Registering Devices Automatically

You can configure the UMS server so that all devices on the server's network are automatically registered at startup. To do this, the devices must be given the address of the UMS server via **DHCP or DNS**.

- i** We recommend automatic registration when registering new devices for the first time during the rollout. Disable automatic registration as soon as all devices have been registered, so that no unknown devices can obtain sensitive settings.

To configure UMS servers and devices for automatic registration, proceed as follows:

- Under **UMS Administration > Global Configuration > Device Network Settings**, select the **Enable automatic registration (without MAC address import)** checkbox.

i If this option is enabled, each device without a UMS certificate (is distributed to the clients during registration) in the network will be added to the UMS database. If you reset a device to the factory settings and reboot it, it will immediately be registered on the server again.

- Configuration of the network environment for an automatic UMS registration:

- Via DNS:**

Create a DNS entry `igelrmserver` (entry type A) on your DNS server which points to the UMS server.

- Via DHCP:**

Change the DHCP server configuration depending on the IGEL OS version of your endpoints as follows:

- IGEL OS 11.03.500 or lower:** Set `igelrmserver` as DHCP option 224. Set the DHCP option 224 as a string - not as a DWORD - to the IP address of the server. For the default Linux DHCP server, add the following in the `dhcpd.conf` file in the appropriate section, e.g. in the global section: `option igelrmserver code 224 = text option igelrmserver ""`



- **IGEL OS 11.04.100 or higher:** Alternatively you can use DHCP option 43 (vendor-specific options) to send DHCP option 224 (name: igelrmserver) to the correct endpoints. An end device with IGEL OS 11.04.100 or higher sends the option 60 (vendor class identifier) with igel-dhcp-1 as value.

i An IGEL specific DHCP option that is sent in DHCP option 43 overrides a corresponding DHCP option that is sent in the global namespace. The DHCP options 1, 224, and 226 can be embedded in option 43.
You can prevent a DHCP option 224 that has been sent in the global namespace from being interpreted. To achieve this, you must add option 1 (called "exclusive", type Byte, value 1) to DHCP option 43.

3.5.5 Setting up Devices Manually

You can create the data sets for devices manually.

- i** The firmware for the devices must be available in the database. To ensure that this is the case, it can be imported or provided by devices that have already been registered. This method is therefore not always appropriate when setting up the UMS for the first time.

To create an entry for a device in the database manually, proceed as follows:

1. In the context menu of a device directory, select the **New Device** option.
2. Give the **MAC address**, the **name** and the **firmware** of the device and, optionally, select a **directory** for the device.
3. Enter the following data:
 - **MAC address:** MAC address of the device
 - **Version:** Firmware version of the device
 - **Name:** Device name (A maximum of 15 characters is allowed.)
 - **Directory** (optional): Directory in which the device is to be displayed

3.6 UMS Console User Interface

The program's graphical user interface and the tools available are described in detail below.

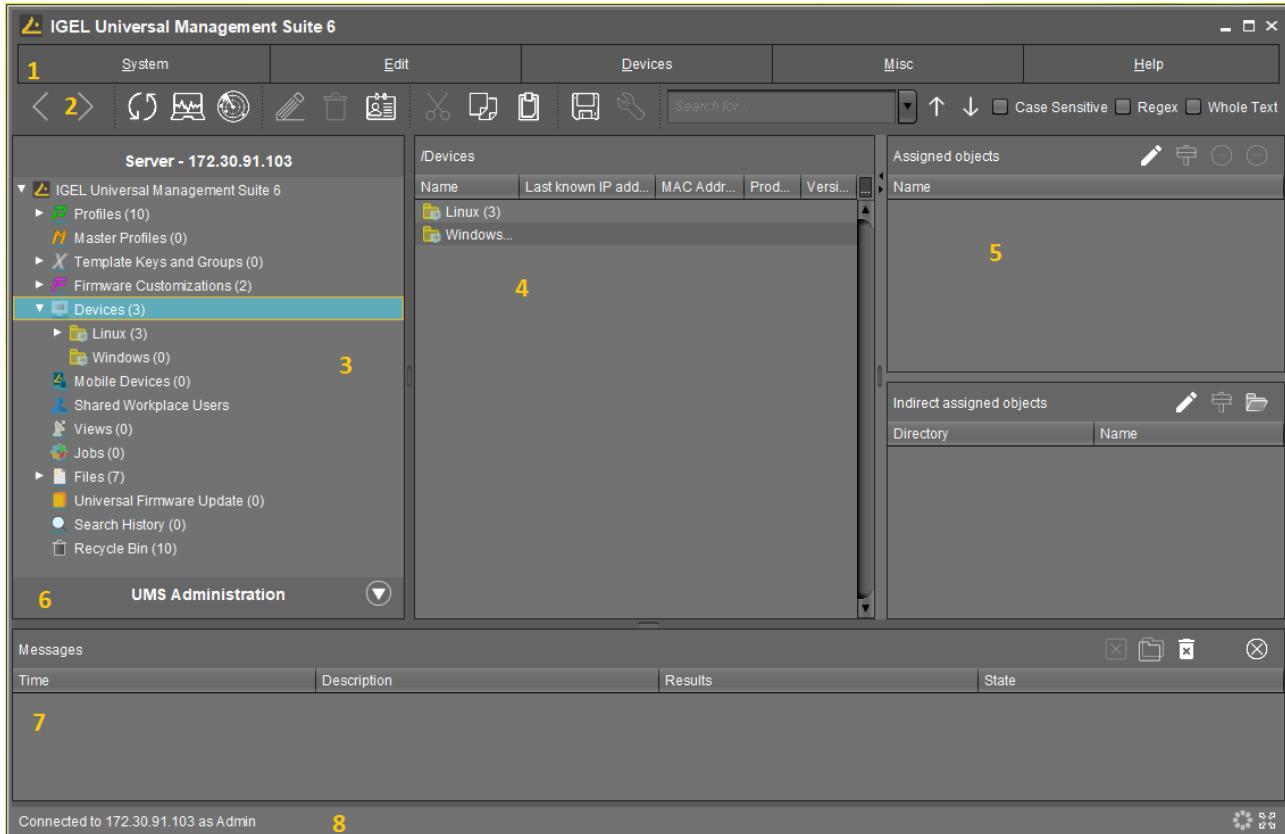
- [The Console Window](#)(see page 314)
- [Menu Bar](#)(see page 315)
- [Structure Tree](#)(see page 324)
- [Symbol Bar](#)(see page 325)
- [Content Panel](#)(see page 326)
- [UMS Administration](#)(see page 327)
- [Messages](#)(see page 327)
- [Status Bar](#)(see page 328)
- [Assigned Objects](#)(see page 328)
- [Context Menu](#)(see page 329)
- [Search for Objects in the UMS](#)(see page 329)



- Deleting Objects in UMS / Recycle Bin(see page 330)

3.6.1 The Console Window

The UMS Console contains the following areas:



1	Menu Bar ⁴⁵	All commands and actions can be executed from the menu. You can use shortcuts ([Alt] + underlined character in the menu element) to access the menu bar via the keyboard.
2	Symbol Bar (see page 325)	Frequently used commands relating to objects in the navigation tree.
3	Structure Tree (see page 324)	Provides access to all UMS Objects such as devices registered on the UMS Server, Directories, Profiles, Views, Scheduled tasks etc.
4	Content Panel ⁴⁶	Information regarding the selected object. Many entry fields can be edited directly.

⁴⁵ <https://kb.igel.com/display/endpointmgmt601/Menu+bar>

⁴⁶ <https://kb.igel.com/display/endpointmgmt601/Content+panel>



5	Assigned Objects⁴⁷	Objects assigned to the devices or folders.
6	UMS Administration (see page 327)	Administrative tasks, e. g. configuring domains, Universal Firmware Updates and the scheduled backup of the UMS Database (only Embedded DB)
7	Messages⁴⁸	Messages regarding actions launched in the UMS Console. Messages regarding successful procedures will be shown in green. Messages regarding problems when executing procedures will be shown in red.
8	Status row⁴⁹	Status messages from the console, e. g. the server currently connected and the user name.

- i** You can change the vertical and horizontal limits between the navigation tree/UMS Administration, content panel and messages in order to adjust the size of the areas to suit your needs. From UMS Version 5.02.100, the changes are saved so that they will be available again the next time that you log on.

3.6.2 Menu Bar

The menu bar comprises the following menus:

- [System](#)(see page 315)
- [Edit](#)(see page 316)
- [Devices](#)(see page 316)
- [Misc](#)(see page 317)
- [Help](#)(see page 323)

System

Menu path: **Menu Bar > System**

In this menu, you will find options for actions relating to the UMS:

- **Connect to:** Allows you to establish the UMS server connection
 - **Server:** IP or host name of the UMS server
 - **Port:** Port number, default: 8443
 - **User name:** User name, "@" for LDAP users
 - **Password:** User password
- **Refresh:** Allows you to refresh the view
- **Disconnect:** Allows you to disconnect the UMS server connection
- **New:** Allows you to create new UMS objects such as directories, profiles, tasks etc.
- **Import:** Allows you to import objects such as firmware, profiles, devices

⁴⁷ <https://kb.igel.com/display/endpointmgmt601/Assigned+objects>

⁴⁸ <https://kb.igel.com/display/endpointmgmt601/Messages>

⁴⁹ <https://kb.igel.com/display/endpointmgmt601/Status+bar>



- **Export:** Allows you to export objects such as firmware, profiles, devices
- **Administrator accounts:** Allows you to set up and manage UMS user accounts and user groups
- **Logging:** Allows you to display and export recordings of messages, events and VNC log entries.
- **License management:** Allows you to create and assign firmware licenses to devices and export device lists.

i From UMS Version 5.07.100, the license management for device licenses can be found under **UMS Administration > Global Configuration > Device Licenses**(see page 446).

- **VNC viewer:** Allows you to shadow a device
- **Open Customization Builder:** if licensed: Allows you to launch the Universal Customization Builder (UCB), see the [UCB manual](#)⁵⁰.
- **Exit:** Allows you to close the UMS console application

Edit

Menu path: **Menu bar > Edit**

In this menu, you will find options for editing highlighted objects:

- **Save description:** Allows you to save changes to the data in the content panel
- **Edit Configuration:** Allows you to edit configuration parameters for the selected device or profile
- **Rename:** Allows you to rename an object in the navigation tree
- **Delete:** Allows you to delete an object in the navigation tree
- **Access control:** Allows you to manage user and group rights for the selected object
- **Cut:** Allows you to cut a data object and copy it to the clipboard.
- **Copy:** Allows you to copy data objects to the clipboard.
- **Paste:** Allows you to paste data objects from the clipboard.

Devices

Menu path: **Menu Bar > Devices**

In this menu, you will find all commands that can be sent to the selected devices.

i Most of these commands can also be accessed from the context menu, i.e. by right-clicking on a single device or a device directory.

Suspend: Puts the highlighted devices into suspend mode.

Shut down: Shuts down the highlighted devices.

Wake up: Starts the highlighted devices via the network (Wake-on-LAN).

Reboot: Restarts the highlighted devices.

Update: Carries out a firmware update on the highlighted IGEL OS devices.

Update when shutting down: Updates the firmware when the highlighted IGEL OS devices are shut down.

⁵⁰ <https://kb.igel.com/display/endpointmgmt/UCB+Manual>



Download firmware snapshot: Downloads the firmware snapshot for the highlighted Windows clients.

Partial update: Carries out a partial update on the highlighted Windows clients.

Create firmware snapshot: Creates a firmware snapshot on the highlighted Windows clients.

Reset to factory defaults: Resets the highlighted devices to the factory defaults.

i See also [Reset to Factory Defaults⁵¹](#) (IGEL OS) or [Reset to Factory Defaults⁵²](#) (Windows).

Send message: Sends a message to the highlighted devices.

Other device commands:

- **Reset to factory defaults:** Resets the highlighted devices to the factory defaults.
- **Settings UMS ->Device:** Sends the configuration of the UMS to the highlighted devices.
- **Settings Device ->UMS:** Reads the local configuration of the highlighted devices to the UMS.
- **Update desktop customization:** Updates the set desktop background and the boot logo on the highlighted IGEL OS devices.
- **File UMS ->Device:** Defines a file which is sent to the highlighted devices.
- **Device File ->UMS:** Defines a file which is sent from the highlighted devices to the UMS.
- **Download Flash Player:** Downloads the Flash Player plugin for Firefox on the highlighted IGEL OS devices.
- **Remove Flash Player:** Removes the Flash Player plugin for Firefox from the highlighted IGEL OS devices.
- **Store UMS certificate:** Stores the UMS certificate on highlighted devices.
- **Remove UMS certificate:** Removes the UMS certificate from the highlighted devices.
- **Refresh license information:** The license information will be refreshed.
- **Refresh system information:** The system information will be refreshed.
- **Refresh asset inventory data:** Asset inventory data will be refreshed.

Specific device command: Executes the following commands:

- **Deploy Jabra Xpress package:** Installs a [Jabra Xpress package⁵³](#) (IGEL OS).
- **Start Login Enterprise launcher:** Starts Login Enterprise Launcher if it has been configured, see [Login Enterprise Launcher in IGEL OS⁵⁴](#).

Take over settings from....: Sends profile settings to the device on a one-off basis.

Clear 'Configuration Change Status' flag: Resets configuration change flags (blue dot next to the symbols for the devices).

Check template definitions: Checks the assignment of template values.

Scan for devices: Searches for devices in the network of the UMS Server.

Misc

Menu path: Menu Bar > **Misc**

⁵¹ <https://kb.igel.com/display/igelos1103/Reset+to+Factory+Defaults>

⁵² <https://kb.igel.com/display/w10iot404/Reset+to+Factory+Defaults>

⁵³ <https://kb.igel.com/display/igelos1104/Jabra+Xpress>

⁵⁴ <https://kb.igel.com/display/igelos1104/Login+Enterprise+Launcher+in+IGEL+OS>



Search: Allows you to search for objects - the search is listed in the structure tree under **Search History** and can be changed again there.

Scheduled Jobs: Allows you to manage public holiday lists and assign tasks to hosts.

- **Host Assignment:** Allows you to assign virtual hosts to selected devices.
 - **Universal Management Suite Host:** Host name of the UMS.
 - **Last Scheduler Run:** Date and time when the Scheduler last ran.
 - **Available devices:** Restricts the available devices displayed.
 - **Assigned devices:** Tree or list view of the available devices on the selected host.
- **Manage Public Holidays:** Allows you to establish public holiday lists which you can use when creating new tasks.
 - **Date lists:** Allows you to set up lists for public holidays.
 - **Days:** Allows you to specify the date of the public holidays in a public holiday list.

Change Password: Allows the password of a logged-in user to be changed.

SQL Console: Direct access to the database with SQL commands.

- ! The SQL console is intended solely for administrative purposes. You can destroy the database through operations on the SQL console.

Firmware Statistics: A list of firmware versions registered in the database with filter function.

Remove Unused Firmwares: Opens a dialog which lists unused firmwares and allows you to delete them individually or collectively.

Settings([see page 318](#)): Allows you to change configuration parameters such as language and appearance of the UMS Console, types of notifications, etc.

-
- [Settings\(see page 318\)](#)

Settings

Menu path: **Menu Bar > Misc > Settings**

Here you can change the following parameters:

- [General\(see page 319\)](#)
- [Appearance\(see page 319\)](#)
- [Views and Searches\(see page 320\)](#)
- [Online Check\(see page 321\)](#)
- [Remote Access\(see page 322\)](#)
- [Universal Firmware Update\(see page 322\)](#)
- [UMS HAE\(see page 322\)](#)
- [Notifications\(see page 322\)](#)



General

Menu path: Menu Bar > **Misc > Settings > General**

Language: Language selection for the graphical user interface. For the changes to be applied, you must close the UMS Console and start it again.

- Always apply settings on next boot** (Default)
- Always confirm move actions** (Default)
- Always confirm unassign actions** (Default)
- File choosers remember the last used directory** (Default)
- Always confirm overwriting of elements in Search History** (Default)

Elements in Search History (max): Maximum number of elements that the search history will show. (Default: [15](#))

Clear the user and server list of the login dialog: Allows you to clear the login history.

- Increase Drag and Drop acceleration** (Default)

Acceleration factor: Can only be set if the checkbox above has been enabled.

Appearance

Menu path: Menu Bar > **Misc > Settings > Appearance**

Skin: Selection of possible themes/color combinations in which the GUI is displayed.

Possible options:

- "Workspace"
- "Smart contrast"
- "Pewter"
- "Cinder grey"
- "Ocean"

Device commands always in background

- In the background. (Default)
- Not in the background

Open message area automatically on new messages

- The message area in the lower part of the UMS Console window will open automatically when incoming messages are received. (Default)
- Will not open automatically

Show content amount of directories

- Will be shown. (Default)



- Will not be shown

Load collapsed/uncollapsed tree status at login

- The structure tree will be restored to how it was at the last login. (Default)
- Will not be restored

Show category root icon

- Show icons as symbols for the main categories in the structure tree. (Default)
- Show folder symbols for the main categories in the structure tree.

Use Advanced Health Status Icons

- Icons displaying the status of the device will be shown in the UMS Console; see [Devices](#)(see page 382). (Default)
- The status icons will not be shown.

Directory tooltip contains directory tree path

- Will be shown. (Default)
- Will not be shown

Directory tooltip contains directory and content amount

- The number of directories and the objects in the directory will be shown in the tooltip. (Default)
- The number of directories and the objects in the directory will not be shown in the tooltip.

Views and Searches

Menu path: Menu Bar > **Misc > Settings > Views and Searches**

You can configure the display of view and search results.

Lifetime for views: Defines how long the results of views are cached.

Possible options:

- "Amount and items are never stored": The view results are not cached. Thus, they must be loaded anew each time the view is selected in the structure tree (under **Views**).
- "Amount and items are kept for [time span)": The view results are cached for the selected time span. When the time span has expired, the view results must be loaded anew when the view is selected in the structure tree (under **Views**). The option "Amount and items are kept for 30 minutes" is recommended for most cases.

Lifetime for searches: Defines how long the results of searches are cached.

- "Amount and items are never stored": The search results are not cached. Thus, they must be loaded anew each time the search is selected in the structure tree (under **Search History**).
- "Amount and items are kept for [time span)": The search results are cached for the selected time span. When the time span has expired, the search results must be loaded anew when the search is



selected in the structure tree (under **Search History**). The option "Amount and items are kept for 30 minutes" is recommended for most cases.

When opening a view result...

Possible options:

- "Automatically load amount and items": The devices are loaded immediately when a view is selected in the structure tree (under **Views**). With large amounts of devices, this may result in high loading times. You can refresh the display by clicking **Refresh**.
- "Automatically load amount": The amount of devices is loaded immediately when you select a view in the structure tree (under **Views**). You can load the devices by clicking **Load devices**.
- "Show parameters only": Nothing is loaded immediately when a view is selected in the structure tree (under **Views**). You can load the devices by clicking **Search for hits > Load devices**.

When opening a search result...

- "Automatically load amount and items": The devices / profiles / views are loaded immediately when a search is selected in the structure tree (under **Search History**). With large amounts of devices / profiles / views, this may result in high loading times. You can refresh the display by clicking **Refresh**.
- "Automatically load amount": The amount of devices / profiles / views is loaded immediately when a search is selected in the structure tree (under **Search History**). You can load the devices / profiles / views by clicking **Search for hits > Load device / Load profile / Load view**.
- "Show parameters only": Nothing is loaded immediately when a search is selected in the structure tree (under **Search History**). You can load the devices / profiles / views by clicking **Search for hits > Load device / Load profile / Load view**.

Show amount of views in tree

- The amount of devices is shown in the structure tree, provided that the amount has been loaded at least once.
- The amount of devices is not shown.

Show amount of hidden devices in view

- The amount of hidden devices is shown in the structure tree.
- The amount of hidden devices is not shown.

Online Check

Menu path: Menu Bar > **Misc > Settings > Online Check**

Here you can define how often the UMS polls the devices to check if they are online.

Every: The online check is executed in the given interval in milliseconds. (Default: 3000)

Never: No check is executed.

Check now: The online check is executed when this button is clicked.



Remote Access

Menu path: Menu Bar > **Misc > Settings > Remote Access**

External VNC viewer: Allows you to configure an external VNC viewer by entering or selecting the path to the executable file.

External terminal client: Allows you to select an external terminal client by entering or selecting the path to the executable file (currently supported: Putty).

Show end dialog if two or more sessions are open

- The end dialog will be shown. (Default)

Show warning dialog for sessions that end unexpectedly

- The warning dialog will be shown. (Default)

Universal Firmware Update

Menu path: Menu Bar > **Misc > Settings > Universal Firmware Update**

Activate automatic status refresh

- The registration status of the firmware update will be refreshed automatically. (Default)

Automatic status refresh interval: Interval in seconds.

UMS HAE

Menu path: Menu Bar > **Misc > Settings > UMS HAE**

Here you can configure the High Availability Extension status update.

Activate automatic process status refresh

- The process status will be refreshed automatically. (Default)

Automatic process status refresh interval: Interval in seconds. (Default: 30)

- (i)** You will see the status in the content panel if you click on a server or load balancer under **UMS Administrator > Server**.

Notifications

Menu path: Menu Bar > **Misc > Settings > Notifications**

Show notifications on startup

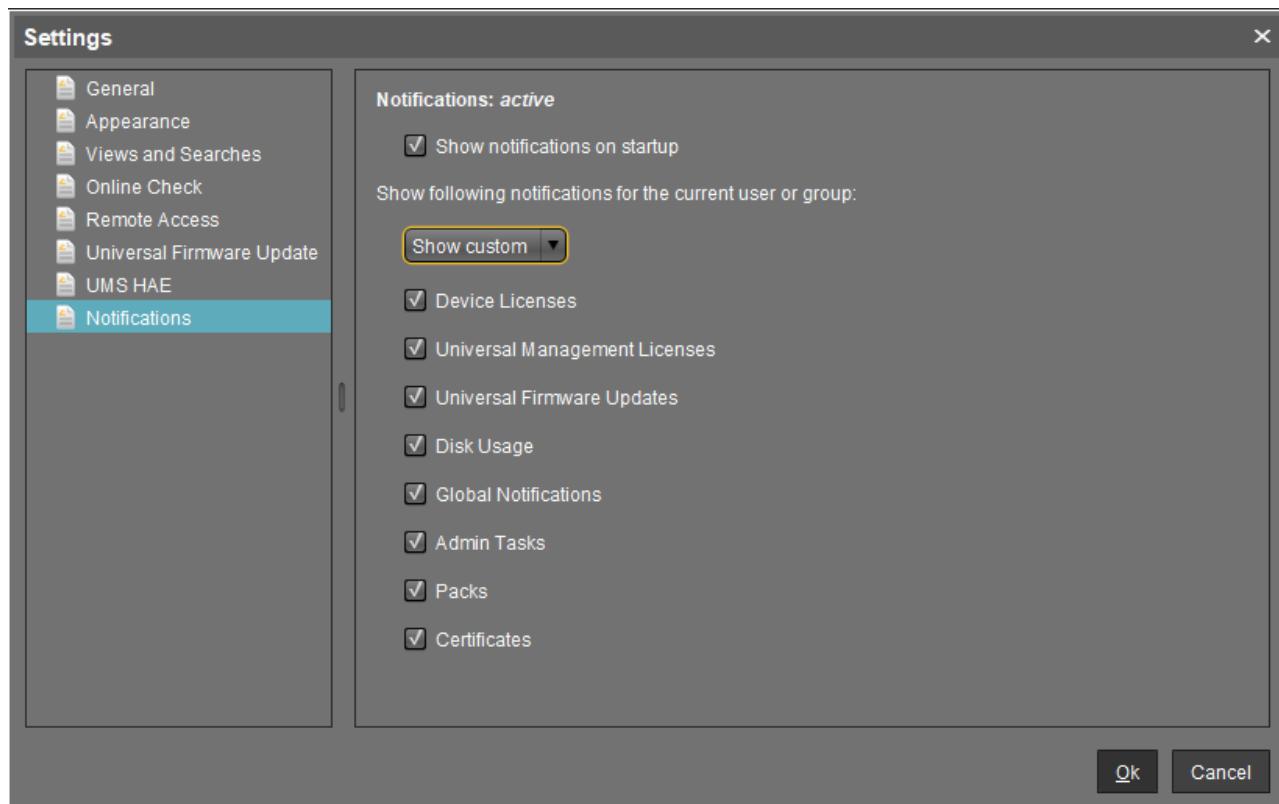
- The notification will pop up automatically on each connection to the UMS Console.
- The notification will not pop up automatically. To see the notification, go to **Help > Notifications**.



Show following notifications for the current user or group

Possible options:

- "Show all"
- "Show nothing"
- "Show custom"
 - "Device Licenses"
 - "Universal Management Licenses"
 - "Universal Firmware Updates"
 - "[Disk Usage](#)(see page 231)"
 - "[Global Notifications](#)(see page 232)"
 - "[Admin Tasks](#)(see page 232)"
 - "Packs"
 - "Certificates"



Help

Menu path: Menu Bar > **Help**

In this area, you will find information that may help you when using the UMS.

User Manual: Link to the manual on kb.igel.com

User Manual (offline): Opens the user manual in PDF format.



IGEL Knowledge Base: Link to further online documentation on kb.igel.com

Legend: Icons used in the UMS and their meanings.

Save support information...: Saves log files from the UMS Server and UMS Console as well as profiles and associated firmware information for the selected devices in a ZIP file and also stores log files from the connected ICGs. If the IGEL Management Interface (IMI) extension is being used, its API log file will be saved too. Further information can be found under [Support Wizard in the IGEL UMS](#)(see page 525).

Save device files for support: Saves log and configuration files for a device, for example setup.ini and group.ini, in a ZIP file.

UMS HA Health Check: Checks whether the interaction between the components of the High Availability system is working properly, in particular, whether the components can exchange messages and data. Further information can be found under [UMS HA Health Check](#)(see page 688).

Notifications: List of all notifications

Third party licenses: A list of licenses for third-party software and libraries used in the UMS.

UMS Update Check: Checks whether a newer version of the UMS is available for downloading.

Info: Shows details of the current version of the UMS Console and Java environment as well as the logged-in user.

3.6.3 Structure Tree

You can highlight or select objects in the structure tree by clicking on them. Multiple selections are possible using the [Shift] or [Ctrl] key.

From UMS Version 5.01.100, you can specify whether the UMS Console should remember the open areas in the structure tree and show them open the next time that it starts. With extensive structures, however, this can result in longer starting times. You will find the **Load collapsed/uncollapsed tree status at login** setting under **Misc > Settings > Appearance**.

From UMS Version 5.03.100, you can increase the speed when scrolling for drag & drop actions. Acceleration starts as soon as the object moved touches the bottom edge of the structure tree window. Acceleration is helpful if the structure tree contains a very large number of objects. To change the scroll speed, enable **Extras > Settings > General > Increase drag and drop acceleration** and set the **Acceleration factor** to a suitable value.

The number of elements contained including elements in sub-folders is shown after each folder. You can change this setting under **Misc > Settings > Appearance > Show content amount of directories**.

The structure tree is subdivided into the following areas:

- [Profiles](#)(see page 331): Create and organize standard profiles.
- [Master Profiles](#)(see page 359): Create and organize master profiles.
- [Template Keys and Groups](#)(see page 361): Keys and values for use in template profiles.
- [Firmware Customizations](#)(see page 375): Customize the user interface to suit your corporate design.
- [Devices](#)(see page 382): Organize managed devices.
- [Mobile Devices](#)(see page 451): Organize managed mobile devices.
- [Shared Workplace users](#)(see page 402): Assign specific profiles to AD users.
- [Views](#)(see page 402): Create configurable list views for devices.
- [Jobs](#)(see page 425): Define scheduled tasks, e.g. firmware updates.
- [Files](#)(see page 430): Registering Files for transfer to devices.
- [Universal Firmware Update](#)(see page 433): Allows you to download the current firmware versions for distribution to devices.



- **Search History**(see page 435): Saved search queries.
- **Recycle Bin**(see page 436): Deleted and restorable objects.

3.6.4 Symbol Bar

In the **symbol bar**, you will find buttons for frequently used commands:

	Navigate one step forwards or backwards in the console history. This only relates to the view; actions cannot be undone.
	Refresh the view and status of the devices
	Online check of the devices
	Search for devices within the network
	Change object names in the structure tree
	Delete objects in the structure tree
	Specify access rights for selected objects
	Cut a tree element
	Copy a tree element into the clipboard
	Paste a tree element from the clipboard
	Save the edited description data for devices or profiles
	Edit configuration parameters for devices or profiles
	Open the UMS Web App (see page 720) if it has been activated during the UMS installation (see page 260)/ update (see page 285)procedure.
	Find objects in the structure tree using a name, MAC, IP, or ID. Regular expressions (Regex) can be used, the user's last 20 search queries are saved.



	Navigate one step forwards or backwards in the search results
Case sensitive	Specify whether upper and lowercase letters are taken into account when searching
Regex	Specify whether regular expressions are used when searching
Whole text	Specify whether the search expression needs to match the entire text or only part of it

3.6.5 Content Panel

The content panel shows the properties of the particular object highlighted in the structure tree. This can be the contents of a directory, e.g. the profiles, devices, sub-folders, tasks etc. contained therein, or detailed information relating to an object such as a device's system information, the basic data for a profile, the hit list for a view etc.

Illustrative List of Details Shown in the Content Panel for Some Objects from the UMS Structure Tree

Server - [IP Address]

- **Profiles**(see page 331): Name, description, profile ID, etc.
- **Master Profiles**(see page 359): Name, description, profile ID, etc.
- **Template Profiles**: (see page 361) Name and description of template keys and value groups.
- **Firmware Customizations**(see page 375): Name, use case and configuration parameters of a firmware customization.
- **Devices**(see page 382): System information, license and monitor information, features, etc.

With a **Copy to Clipboard (ASCII)** button at the bottom of the content panel, you can copy the device information in ASCII format.

- **Mobile Devices**(see page 704): System information, network details, etc. of the connected mobile devices.
- **Shared Workplace Users**(see page 402): Name, email addresses of the users from Active Directory, etc.
- **Views**(see page 402): Name, rule, matching devices, etc.
- **Jobs**(see page 425): Job info, schedule, execution results, etc.
- **Files**(see page 430): Source URL, classification, device file location, access rights, etc.
- **Universal Firmware Update**(see page 433): Firmware update settings and version, download status, etc.
- **Search History**(see page 435): Name, rule, matching devices, etc.
- **Recycle Bin**(see page 436): Name and type of the deleted object, its deletion date, etc.

UMS Administration

- **Server - View Your IGEL UMS Server Information**(see page 437): Information regarding the service executed, requests, failed and waiting requests



- [Load Balancer - View Your IGEL UMS Load Balancer Information](#)(see page 439): Information regarding the service executed, requests, failed and waiting requests
- [Licenses](#)(see page 443): License summary, registered licenses
- [Certificate Management](#)(see page 453): Signature algorithm, key, status of the certificates, etc.
- [Device Attributes](#)(see page 463): Device attributes such as name, type, etc.
- [Administrative Tasks](#)(see page 464): List with tasks, execution history
- [Proxy Server](#)(see page 484): Name, host, port, etc.
- [Universal Firmware Update](#)(see page 493): Settings for the Universal Firmware Update, settings for the FTP servers to which the files are copied (optional)
- [Wake-on-LAN](#)(see page 495): Wake-on-LAN configuration parameters
- [Active Directory / LDAP](#)(see page 497): Active Directory / LDAP domains
- [Remote Access](#)(see page 498): Secure VNC connection, graphics settings, etc.
- [Logging](#)(see page 500): Log message settings, logging event settings
- [Mail Settings](#)(see page 501): Mail settings, recipient for administrative task result and service emails
- [Misc Settings](#)(see page 503): Recycle bin, template profiles, master profiles

3.6.6 UMS Administration

- [UMS Network](#)(see page 437)
- [Global Configuration](#)(see page 442)

3.6.7 Messages

The **Messages** window area contains information regarding the successful or unsuccessful execution of commands.

An unsuccessfully executed command will be marked in the message list with a warning symbol and a red **State** symbol . A warning symbol will also flash in the status bar of the UMS Console until the user selects the message.

Messages			
Time	Description	Results	State
1/21/20 12:30 PM	Wake up devices	The action ended successfully.	Finished
1/21/20 12:29 PM	Reboot devices	The action failed.	Failed

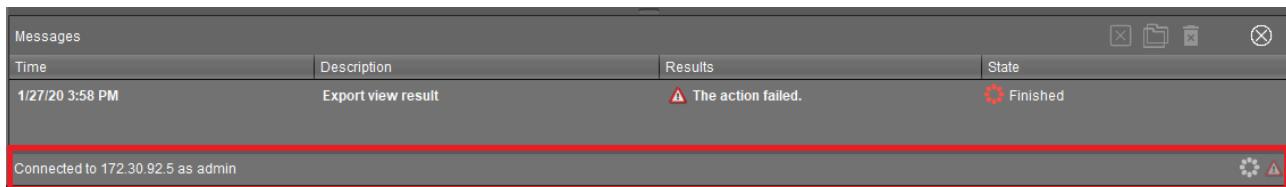
- ▶ Click or double-click the message in order to view the relevant details.
- ▶ Click to delete messages you have already dealt with or wait until the message window is automatically reset when you close the UMS Console.
- ▶ You can change the size of the message window using the middle slider or hide it altogether with a button .

To open the **Messages** window area again, click in the status bar of the UMS Console (or if messages about the unsuccessful command execution have not yet been selected).



3.6.8 Status Bar

The **status bar** shows the name of the UMS Server currently connected and the user who is logged in to the UMS Console. The symbol at the bottom right indicates the status of the message window. For example, it signals when new warning messages are present. These can be seen here even if the message area is hidden.



3.6.9 Assigned Objects

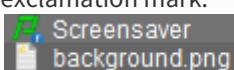
To ensure that you can quickly tell directly and indirectly assigned objects apart, the **Assigned objects** area is subdivided into two parts:

- Directly assigned objects have been assigned to an individual device, folder or profile.
- Indirectly assigned objects have been "inherited" via the file structure.

The screenshot shows two main sections: 'Assigned objects' and 'Indirect assigned objects'.
Assigned objects: This section has a table with columns 'Name' and 'Icon'. It lists two items: 'Screensaver' (with a green checkmark icon) and 'background.png' (with a white document icon).
Indirect assigned objects: This section has two tabs: 'Directory' and 'Name'. The 'Directory' tab is selected, showing a list with 'Augsburg' (with a folder icon). The 'Name' tab is also shown, listing 'French' (with a yellow person icon).

- Double-click an object in the assignment area in order to directly edit it.

- i** Assigned objects with configuration changes not yet transferred to the device are marked with an exclamation mark:





3.6.10 Context Menu

You will be given an object-dependent **context menu** by right-clicking on the corresponding object. Depending on your selection, actions for folders, devices, Shared Workplace users etc. will be available. The chosen command will be carried out for all objects previously marked in the tree.

- ⓘ Certain commands can only be executed for individual objects, not for directories with objects. These options are then disabled in the menu. Example: The command **File Device > UMS** can only be executed for an individual device. In contrast, the command **File UMS > Device** can be executed for all devices in a directory.

For details on some of the device commands, see [Devices](#)(see page 316).

3.6.11 Search for Objects in the UMS

Objects within the UMS structure tree can be found using the following functions:

- **Quick Search**
- **Search function**
- **View**

Quick Search

The **Quick Search**  in the [symbol bar](#)(see page 325) provides the quickest access to the search function. The entry mask is always visible in the console window. The key combination [Shift-Ctrl-F] places the cursor in the entry field. The **Quick Search** search queries are restricted to a small number of object properties, e.g. object name, object ID, MAC address, and IP address. These data are buffered locally when the UMS Console is launched and can therefore be searched very quickly without having to access the database. The user's last 20 search queries are saved to allow quick access. They are saved in the console user's system user data (Windows Registry) rather than in the UMS database.

Search Function

The normal UMS search function (**Misc > Search** or [Ctrl-F] key combination) provides additional options for searching the UMS database. In addition to the Quick Search data (see above), all other device, profile or view data can be selected here, e.g. an individual inventory number or the monitor model connected. Various criteria can be logically linked (AND / OR). The user's search queries are recorded under [Search History](#)(see page 435) in the structure tree and can therefore be processed or reused easily.



Create new Search

Select criterion

Basic Information

- Comment
- Device License
- Expiration Date of OS10-Maint..
- Keystore Alias
- Name
- Serial Number
- Unit ID
- Cost Center
- Device Serial Number
- IGEL Cloud Gateway
- Last Known IP Address
- Online
- Site
- Department
- Directory
- In-Service Date
- MAC Address
- Profile Assignment
- Structure Tag

Asset Inventory

- Asset ID
- BIOS Version
- CPU Speed
- Duplex Mode
- Firmware Version
- Flash Size
- Graphics Memory Size 1
- Last Boot Time (Relative)
- Network Speed
- Partial Update (Relative)
- Product ID
- BIOS Date
- Battery Level
- CPU Type
- Firmware Description
- Flash Player
- Graphics Chipset 1
- Graphics Memory Size 2
- Memory Size
- OS Type
- Partial Update (Version)
- Total Operating Time
- BIOS Vendor
- Boot Mode
- Device Type
- Firmware Update (Relative)
- Flash Player Version
- Graphics Chipset 2
- Last Boot Time (Absolute)
- Network Name
- Partial Update (Name)
- Product

Monitor Information

- Monitor Date of Production
- Monitor Serial Number
- Monitor Model
- Monitor Size
- Monitor Native Resolution
- Monitor Vendor

Monitor Information (legacy)

- Monitor 1 Date of Production
- Monitor 1 Serial Number
- Monitor 2 Date of Production
- Monitor 2 Serial Number
- Monitor 1 Model
- Monitor 1 Size
- Monitor 2 Model
- Monitor 2 Size
- Monitor 1 Native Resolution
- Monitor 1 Vendor
- Monitor 2 Native Resolution
- Monitor 2 Vendor

Buttons: Back, Next, Finish, Cancel

Views

Views(see page 402) function very similarly to search queries. Here too, various criteria can be linked and the query saved. In contrast to search queries, however, views are available to all UMS administrators together – depending on their authorizations. Views can also be taken into account when defining scheduled tasks(see page 425).

From UMS Version 5.02.100, both search results and views can be assigned to profiles. See also Assigning Objects to a View(see page 424) and Assign Objects to the Devices of Views(see page 480).

3.6.12 Deleting Objects in UMS / Recycle Bin

In the IGEL Universal Management Suite, you can move objects to the **Recycle Bin** instead of permanently deleting them straight away. The **Recycle Bin** is enabled or disabled globally for all UMS users.

- Enable the recycle bin under **UMS Administration > UMS Features > Enable recycle bin**.



If an object in the structure tree is deleted (**Delete** function in the symbol bar, in the context menu or the [Del] key), it will be moved to the **Recycle Bin** following confirmation.

- i If the recycle bin is active, objects can also be deleted directly and permanently by pressing [Shift-Del].

Directories are moved to the **Recycle Bin** along with their sub-folders and all elements and can therefore be restored again as a complete structure. You will find the UMS **Recycle Bin** as the lowest node in the UMS Console structure tree. Elements in the **Recycle Bin** can be permanently deleted there or restored. To do this, bring up the context menu for an element in the **Recycle Bin**.

- i If you cannot bring up the context menu for elements in the **Recycle Bin**, the recycle bin is probably inactive. Check the status of the recycle bin as described above.

Virtually all elements from the UMS structure tree can be moved to the **Recycle Bin**: Devices, profiles, views, tasks, files and their directories. Shared Workplace users cannot be deleted, while administrator accounts (in account management) and search history elements can only be deleted permanently (with [Shift-Del]). The highest nodes in the structure tree cannot be deleted either. However, this procedure will affect all deletable elements beneath this node!

- Objects in the **Recycle Bin** cannot be found via the search function or views and cannot be addressed by scheduled tasks.
- Devices in the **Recycle Bin** will not receive any new settings from the UMS but will remain registered in the UMS and can be restored again from the **Recycle Bin** along with all assigned profiles.
- The fact that profiles in the **Recycle Bin** are no longer effective means that the settings for devices may change. Profiles previously assigned to devices will be reactivated if they are restored again.
- Planned tasks, views and search queries in the **Recycle Bin** will not be executed.
- At the same time, assigned profiles, files, views and firmware updates in the **Recycle Bin** are not active.

3.7 Profiles

Menu path: Structure tree > **Profiles**

In this area, you can manage profiles. **Profiles** are predefined configurations that can be assigned globally to managed devices via the Universal Management Suite.

3.7.1 When Is It a Good Idea to Use Profiles?

You can achieve the following using profiles:

- Setting identical configurations for a number of devices
- Defining different usage scenarios for devices (or groups of devices) in an abstract manner.
- Significantly reducing administrative outlay.
- Reducing configuration options on the device.



You have the option of creating directories for saving profiles and can add, delete, and change the profiles in this part of the structure.

Information on a profile is shown in the content panel.

- ⓘ UMS profiles can be compared with policies in the structure of Microsoft Active Directory (AD). The directories that are grouped and managed via the devices correspond to the organizational units in the AD.

The following profile types exist:

	Standard profiles can be assigned to devices directly or indirectly via directories. A device can receive its settings from a number of directly or indirectly assigned profiles. During the assignment process, the profile settings overwrite the settings configured directly on the device. See Effectiveness of Settings (see page 334). If you use Shared Workplace (see page 693), you have the option of assigning profiles to users. Profiles assigned to users have a higher priority than profiles assigned to devices. See Order of Effectiveness of Profiles in Shared Workplace (see page 353) and Prioritization of Profiles (see page 350).
	Template profiles are profiles where one or more settings are set via variables. These values are determined dynamically. Standard and master profiles can thus be used and combined even more flexibly. See the Template Profiles (see page 361) chapter. If you deploy Shared Workplace (see page 693), notice that template profiles cannot be used.
	Master profiles can overwrite the settings of standard profiles and have their own authorizations, see Master Profiles (see page 359). The order of effectiveness is exactly the opposite of what it is for the standard profiles. See Order of Effectiveness of Master Profiles (see page 354).
	Mobile-device profiles are used for configuring mobile devices with the UMS add-on Mobile Device Management (see page 704) Essentials. See Creating Mobile Device Profiles (see page 718).

This chapter describes

- [Choosing the Right Profile](#)(see page 333)
- [Configuration Levels](#)(see page 334)



- Effectiveness of Settings(see page 334)
- Using Profiles(see page 335)
- Prioritization of Profiles(see page 350)

3.7.2 Managing Profiles



Sorry, the widget is not supported in this export.

But you can reach it using the following URL:

<https://www.youtube.com/watch?v=MI522x3qqn0>

3.7.3 Choosing the Right Profile

Standard Profiles

In most cases, **standard profiles** are sufficient to define configuration settings globally and transfer them to devices via profiles. You can use several profiles at the same time. With the help of the priority rule, the effectiveness of the parameter values specified by a profile can be managed.

In the [Using profiles\(see page 335\)](#) chapter, you can find out how to set up and assign profiles.

In the [Template profiles\(see page 361\)](#) chapter, you can also find out how to create profiles with variable values.

In the [Priority of profiles\(see page 350\)](#) chapter, the priority rule is explained.

Master Profiles

The use of one or two **master profiles** can be helpful in a hierarchical structure with various administrators and complex rights management. With a master profile, a higher-ranking administrator can influence other administrators' profile settings without withdrawing their management rights.

Read the [Master profiles\(see page 359\)](#) chapter very carefully before you use this profile type.



Use **master profiles** very sparingly and only in specific cases. If they are used incorrectly, you can unintentionally disable all other profiles.

User-Specific Profiles

When using *IGEL Shared Workplace (SWP)*, it is a good idea to manage user-specific configurations via profiles. User-specific SWP profiles differ from device profiles in terms of the way in which they work.

For more information, read [IGEL Shared Workplace - Assigning a User Profile\(see page 695\)](#).

3.7.4 Configuration Levels

Profiles allow you to globally manage configuration parameters on devices.

It is important to understand that there are parameters for different types of instances, normal parameters and parameters for fixed and free instances.

Normal Parameters and Fixed Instances

Fixed instances refer to settings options which are fixed, i.e. integrated within the system. These fixed instances include language settings, monitor settings, firmware update settings, user interface settings etc. These options cannot be added or deleted – only changed.

Parameter settings for fixed instances that are configured on the device itself can be overwritten if other values are specified in an assigned profile. If fixed instances are managed via various profiles, very specific [priority rules](#)⁵⁵ apply.

Free Instances

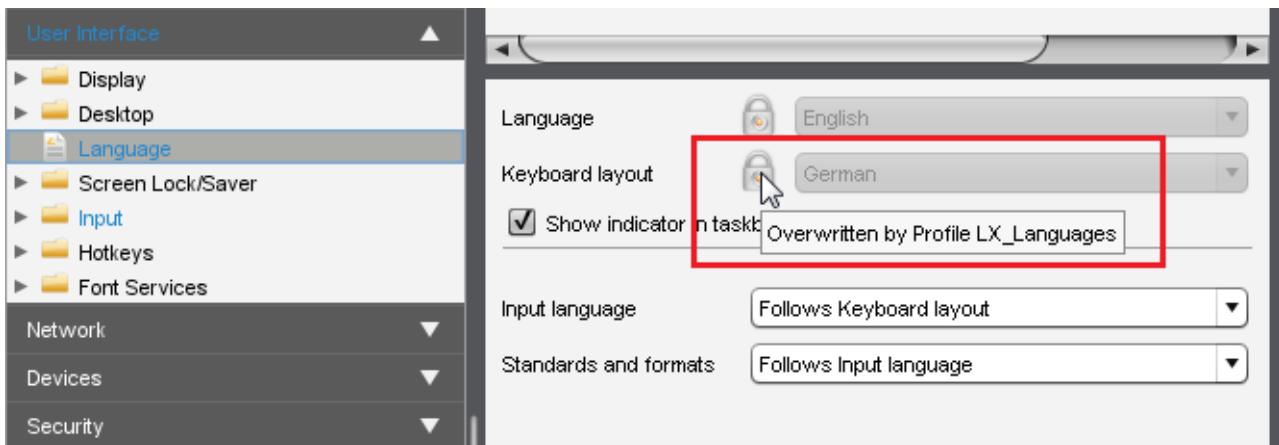
These are the instances that the user can add or delete via . These include sessions, USB devices, printers, accessories, VPN connections and everything that can be selected in device lists.

Parameter values of free instances cannot be overwritten. If several free instances (e.g. printers) are assigned to a device, they are added together. Therefor there are no priorities for the parameter values of free instances.

- ⓘ You can break this rule if you enable **Overwrite sessions** when setting up a profile, see [Create profiles\(see page 335\)](#).

3.7.5 Effectiveness of Settings

Parameters set via a profile are blocked in the configuration dialog and indicated by a lock symbol.



⁵⁵ <https://kb.igel.com/display/endpointmgmt601/Prioritization+of+Profiles>



They can only be edited in the profile. The name of the profile responsible for the locked status will be shown if you move the mouse pointer over the lock symbol.

Each parameter has two value types:

- values determined by the device and
- value determined by the profiles.

These values exist alongside each other, although there is a rule whereby profile settings always take precedence.

- i** If you have set a value for a parameter in a profile and then remove the assignment to a device, the value of the parameter will be changed back to its previous device value. The profile value will not be copied to the device settings.

3.7.6 Using Profiles

In this chapter, you can learn about the procedure for

- [Creating Profiles](#)(see page 335)
- [Copy Profile](#)(see page 340)
- [Copy Profile Directory](#)(see page 341)
- [Exporting and Importing Profiles](#)(see page 341)
- [How to Allocate IGEL UMS Profiles](#)(see page 344)
- [Checking Profiles](#)(see page 346)
- [Removing Assigned Profiles from a Device](#)(see page 347)
- [Deleting Profiles](#)(see page 348)
- [Comparing Profiles](#)(see page 348)

Managing Profiles



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

<https://www.youtube.com/watch?v=MI522x3qqn0>

Creating Profiles

Menu path: Structure tree > **Profiles**

With the new knowledge about profiles, you can start to apply this feature.

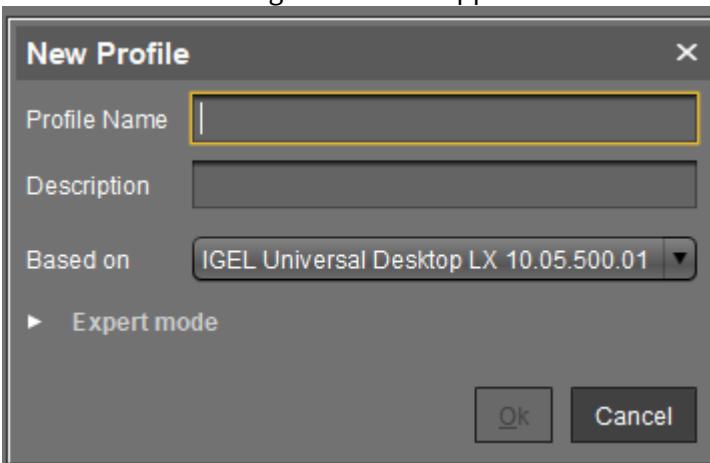
- ⚠** To ensure that you can use all new features of IGEL OS:
- ▶ Update your UMS to the current version.



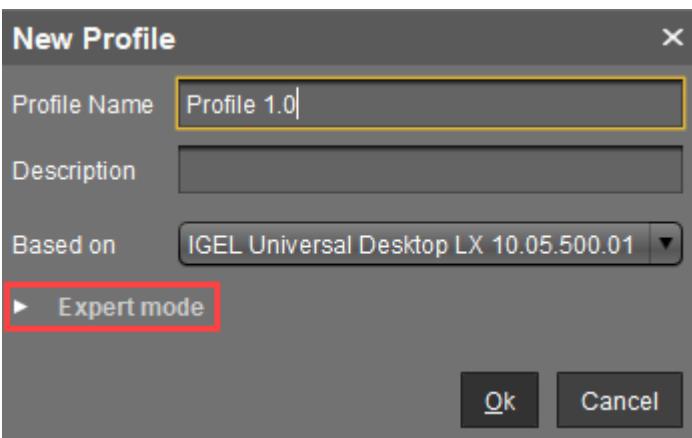
- ▶ For all relevant profiles, set **Based on** to the appropriate firmware version.

To create a new profile in the UMS:

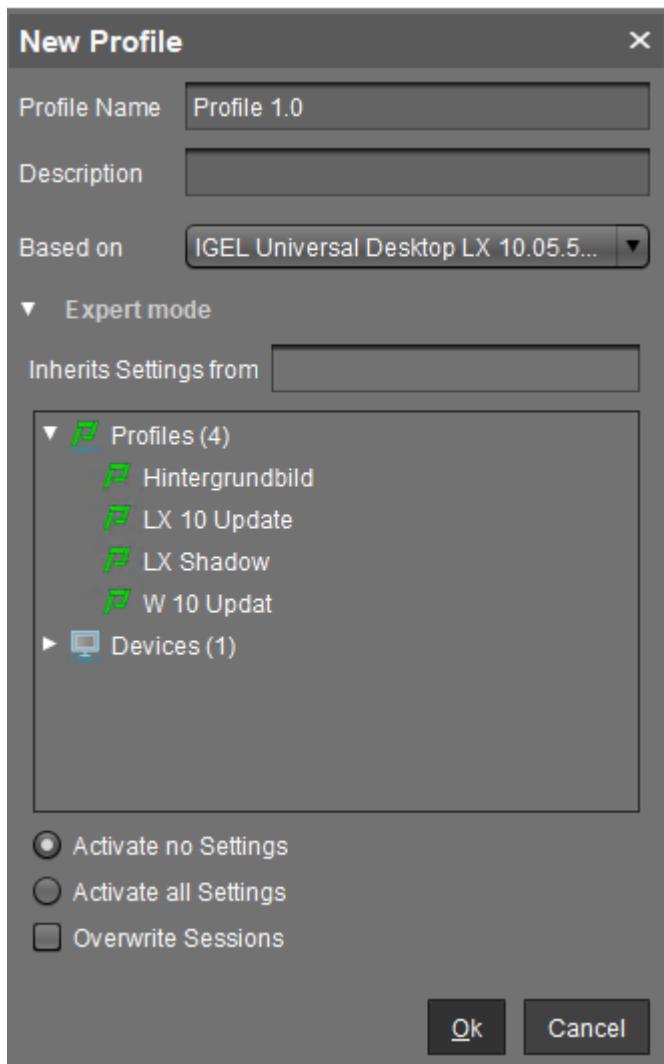
1. Select **New Profile** under **System > New** or in the context menu of the corresponding option in the structure tree
OR
import a previously created profile. See [Exporting and Importing Profiles](#)(see page 341).
The **New Profile** dialog window will appear.



2. Enter a **Name** and a **Description** for the profile.
3. For an "empty" profile that will not use any existing settings, you must select a firmware version for the new profile.
4. Click **Expert mode** if you want to use a profile with existing settings.



5. Now you can specify whether the new profile **Inherits Settings from** an existing profile or device.



6. Select the appropriate firmware under **Based on**.
7. Select one of the possible options:
 - **Activate no settings:** Initially there are no active parameters.
 - **Activate all settings:** All available parameters of the profile will be active.
 - **Overwrite Sessions:** All free instances will be overwritten by the profile.

i Attention! Before changing the default settings in this option, inform yourself about the consequences of other options in [New Profile - Options](#)(see page 338). Activating all settings will block all settings in the local setup! **Overwrite Sessions** should be activated only in exceptional cases. With this option, you can override free instances of all other profiles.

8. Click **OK** to set up and save the profile.

- i** The new profile will be placed in the selected profile directory. If no directory is selected, the new profile will be put directly in the directory **Profiles**.

9. Make your settings.
10. Click **Apply** to save the settings without quitting the profile.
11. Click **Save** to save the settings and quit the profile.

- i** For a better overview, it is recommended to organize profiles using subdirectories.

Video



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

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

New Profile - Options

The options in the **New Profile** window have the following meanings:

- **Do not enable any settings:** No parameters are initially active.
- **Enable all settings:** All available parameters for the profile are enabled. Please note that all settings are locked on the device with a lock symbol. A profile with this setting prevents settings being changed locally on the device. This option makes sense only if you would like to have all settings for a device managed on the basis of this profile.

- i** In many cases, profiles which contain all parameters for an item of firmware take up space in databases and backup files unnecessarily. You should therefore use this option only if it seems necessary. In the majority of cases, it is advisable to configure a device on the basis of several profiles with specific configuration parts.

- **Overwrite sessions:**

- Overwrites the free instances defined for the device or assigned via other other profiles with those of this profile.
- The free instances defined in the profile are added to the free instances that were defined previously on the device or by the assignment of other profiles.

- i** In this case, **sessions** mean both the applications that can be selected via **Sessions** in the menu tree and all other **free instances** that can be created or deleted. See [Parameter Levels](#)⁵⁶.

⁵⁶ <https://kb.igel.com/display/endpointmgmt601/Configuration+Levels>



The **Overwrite sessions** option ensures that only the free instances for this profile are created on the device. Free instances created in other profiles or directly in the device configuration are disabled.

If a number of profiles with the **Overwrite sessions** option enabled are assigned to a device (or Shared Workplace user), the profile with the highest priority is effective, i.e. only the free instances for this profile are available on the device.

- ⓘ Exception: If the profile is a standard profile and a [master profile](#)(see page 359) with session settings is also assigned to the device or user, the settings are added: The device receives all sessions for the standard profile and the master profile. Sessions in master profiles can only be overwritten by a master profile.

New Profile - Configuration

The properties of a profile consist of so-called description data and the profile configuration.

Description data consist of the name of the profile, a descriptive text, the firmware version and the overwrite flag for sessions.

Click on **Edit > Save Description Data** or in the toolbar in order to save these data.

The data are now updated in the database.

- ⓘ When changing the firmware version, remember that profile settings will be lost if they are not supported in the new firmware.

To edit the profile configuration, proceed as follows:

1. Double-click on a profile or select a profile from the navigation tree.
2. Click on **Edit > Edit Configuration**.

The setup will open.

- ⓘ Paths highlighted in blue in the configuration tree lead to settings that have already been set via the profile.

- ⓘ Keys in the Registry (settings) that have been set via a profile are highlighted with a color. The same colors as for highlighting paths in the configuration tree of the UMS are used.

3. To change settings, click on the activation symbol in front of the parameter until the desired function is active.

	The parameter is inactive and will not be configured by the profile.
	<p>The parameter is active and will be configured by the profile.</p> <p>Template keys are inactive.</p>



	The parameter is active and will be configured by the profile.
	Template keys are active. The parameter is active and will be configured by the profile using a template key.
	Reset to default value.

When saving the profile, you can determine when your changes will take effect:

1. Make the required changes.
2. Click on Save.
3. Decide whether the new settings are to take effect immediately or when the relevant devices next boot.

Bear in mind that users who are working may be disturbed if changes take effect immediately.

Assigned profiles with configuration changes not yet transferred to the device are flagged with an exclamation mark in the list of Assigned Objects.

Copy Profile

Menu path: Navigation Tree > **Profiles** > [Name of the profile] > Context Menu > **Copy**

You can copy a profile and paste it in any profile directory.

Copying and pasting are also possible between standard profile directories and master profile directories. If you copy a standard profile and paste it into a master profile directory, the copy of the standard profile will be defined as a master profile. If you copy a master profile and paste it into a standard profile directory, the copy will be defined as a standard profile. Information regarding master profiles can be found in the [Master Profiles](#)(see page 359) chapter.

To copy a profile, proceed as follows:

1. Click on the profile that you want to copy.
2. Open the context menu for the profile and select **Copy**.
3. Click on the profile directory in which you would like to paste the copy of the profile. This can also be the directory of the original profile.
4. Open the context menu for the directory and select **Paste**.

A new profile which has the same name and settings as the original profile will be created. The new profile is not yet assigned to a device, irrespective of the assignments of the original profile.



Copy Profile Directory

Menu path: Navigation Tree > **Profiles** > [Name of the profile directory] > Context Menu > **Copy**

You can copy a profile directory and paste it in any directory.

- i** Copying and pasting are also possible between standard profile directories and master profile directories. If you copy a standard profile directory and paste it into a master profile directory, the copies of the standard profiles will be defined as master profiles. If you copy a master profile directory and paste it into a standard profile directory, the copies of the master profiles will be defined as standard profiles. Information regarding master profiles can be found in the [Master Profiles](#)(see page 359) chapter.

To copy a profile directory, proceed as follows:

1. Click on the profile directory that you want to copy.
2. Open the context menu for the profile directory and select **Copy**.
3. Click on the directory in which you would like to paste the copy of the profile directory. This can also be the directory in which the original profile directory is located.
4. Open the context menu for the directory and select **Paste**.
A new profile directory which has the same name as the original profile directory will be created. The new profile directory will contain newly created copies of the profiles contained in the original profile directory as well as copies of the sub-directories. The copies of the profiles are not yet assigned to a device, irrespective of the assignments of the original profiles.

Exporting and Importing Profiles

Profiles can be exported from the database together with their directory structure. This can be helpful for backup purposes or when importing the profile data from one UMS installation to another.

Alternatively, device settings can be imported as profiles; see [Importing devices as profiles](#)(see page 394).

- [Exporting a Profile and Firmware](#)(see page 341)
- [Importing a Profile and Firmware](#)(see page 342)

Exporting a Profile and Firmware

To export an individual profile, proceed as follows:

1. Right-click the profile.
2. Select the command **Export Profile**.

To export a number of profiles in one file (ZIP archive), proceed as follows:

1. Highlight the desired profiles using the [Ctrl] and [Shift] keys.
2. Select **System>Export>Export Profile**.
The **Export Profiles** window will open.



3. Select the requested profiles in the column **Include**.
4. Confirm by clicking **OK**.
5. Select the destination file.

The firmware information can be exported to an archive along with the profile data. This allows importing to a *UMS* installation without the relevant firmware being registered. This can now be imported together with the profile.

- ⓘ The profiles are converted into the XML format. Make sure that you do not make these files public if the source profiles contain passwords or other confidential data!

Importing a Profile and Firmware

To import an individual profile, proceed as follows:

1. Click **System > Import > Import Profiles**.
2. Select the XML file or archive containing your profile(s).
The **Import Profiles** dialog window will appear. This shows the name and firmware version of each profile configuration contained in the file you have selected.
3. Uncheck one of the boxes in the left row of the table to exclude the relevant profile from the import process.

- ⓘ During the import, you can retain the original directory path of the profile. Alternatively, the profile can be placed in the main directory.

A dialog window shows whether all the selected profiles were imported.

An item of firmware from an archive which was previously not present in the database will automatically be imported together with the corresponding profile.



- Importing Profiles with Unknown Firmware (see page 343)
- Editing profiles (see page 343)

Importing Profiles with Unknown Firmware

Profiles whose underlying firmware is not contained in the database or the import file cannot be imported and will be highlighted in red in the import view.

Such profiles can contain settings which do not feature in any of the registered firmware versions.

To import profiles with unknown firmware, proceed as follows:

1. Click the firmware field that is highlighted in red.
2. Select any firmware version that is known to the system.
3. Import the profile.

If you select an item of firmware that is known to the system, the version will be implicitly converted. Normally, this has only a negligible effect on the profile settings if you select a similar firmware version or a newer version of the same model. However, unknown firmware settings will be lost in the process.

Editing profiles

The properties of a profile consist of so-called description data and the profile configuration.

Description data consist of the name of the profile, a descriptive text, the firmware version and the overwrite flag for sessions. Example:

/Profiles/Universal Desktop LX/Hardware/Disable USB Memory

Name	Disable USB Memory
Description	No USB drive available
Based on	IGEL Universal Desktop LX-FTC 4.06.500.01
Overwrite Sessions	<input type="checkbox"/>

► Click on **Edit > Save Description Data** or in the toolbar in order to save these data.
The data are now updated in the database.

- i** When changing the firmware version, remember that profile settings will be lost if they are not supported in the new firmware.

To edit the **profile configuration**, proceed as follows:

1. Double-click on a **profile** or select a profile from the navigation tree.



2. Click on **Edit > Edit Configuration**.

The set up will open.

- i** Paths highlighted in blue in the configuration tree lead to settings that have already been set via the profile.

3. To change settings, click on the activation symbol in front of the parameter until the desired function is active.

	The parameter is inactive and will not be configured by the profile.
	The parameter is active and the set value will be configured by the profile.

When saving the profile, you can determine when your changes will take effect:

1. Make the required changes.
2. Click on **Save**.
3. Decide whether the new settings are to take effect immediately or when the relevant devices next boot.

- i** Bear in mind that users who are working may be disturbed if changes take effect immediately.

Assigned profiles with configuration changes not yet transferred to the device are flagged with an exclamation mark in the list of **Assigned Objects**:

Name
LX_Screensaver
LX_Languages
LX_Shadow
LX_Update

How to Allocate IGEL UMS Profiles

In the IGEL Universal Management Suite (UMS), you can assign a profile to a device or a device directory.

i Direct and Indirect Assignment of Objects in the IGEL UMS

Objects in the IGEL UMS can be assigned directly or indirectly:

- Directly assigned objects have been assigned to an individual device or directory.



- Indirectly assigned objects have been "inherited" via the directory structure.

Whether a profile is assigned directly or indirectly influences the priority of a profile, see [Order of Effectiveness of Profiles](#)(see page 351).

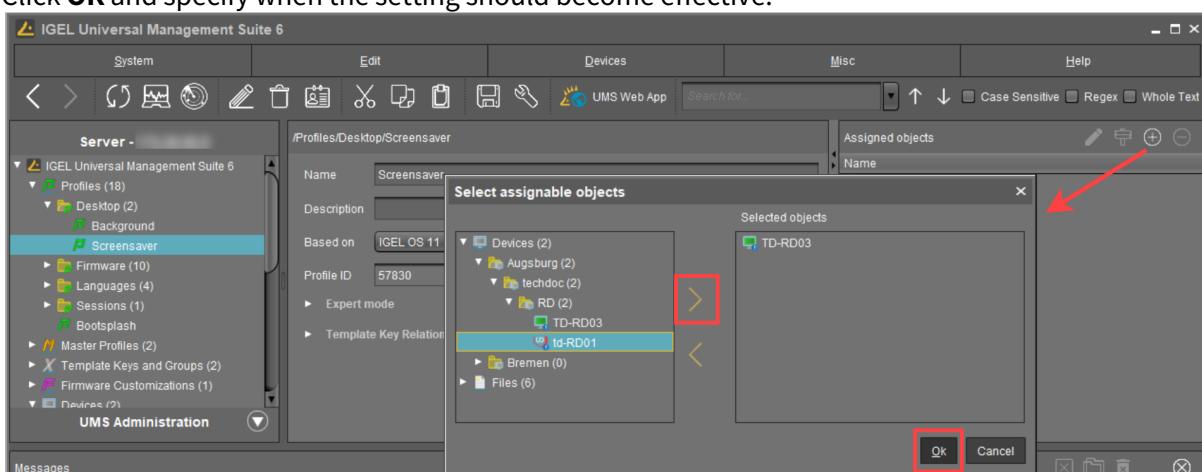
Note also the following:

- If you assign a profile to a directory, it is **indirectly** assigned to each device in this directory including the subdirectories.
- If you subsequently move a device to this directory, the directory profiles will affect this device too.
- If you remove a device from this directory, the profile will no longer influence this device and the local settings for the device will be restored.

You can assign a profile to a device or a device directory per drag & drop or under **Assigned objects** in the **Profiles** or **Devices** tree nodes.

How to Assign a Profile: Starting from the Profile

- In the UMS Console, go to **Profiles** and select the required profile.
- Under **Assigned objects**, click . The **Select assignable objects** window will open.
- Highlight the required device or device directory and click .
- Click **OK** and specify when the setting should become effective.

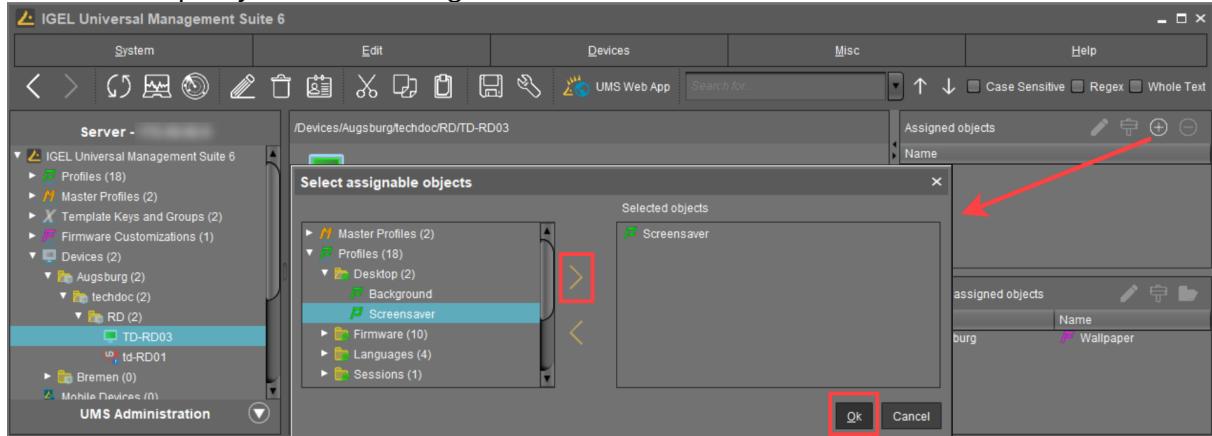


How to Assign a Profile: Starting from the Device / Device Directory

- In the UMS Console, go to **Devices** and select the required device or device directory.
- Under **Assigned objects**, click . The **Select assignable objects** window will open.



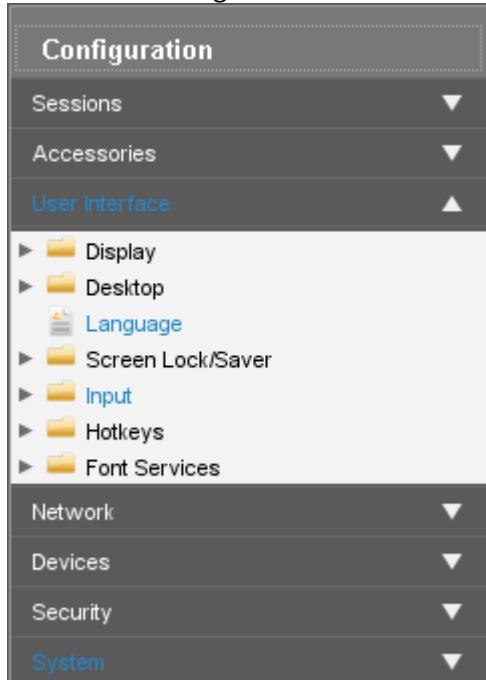
3. Highlight the required profile and click .
4. Click **OK** and specify when the setting should become effective.



Checking Profiles

If you have assigned a profile to a device, check the results:

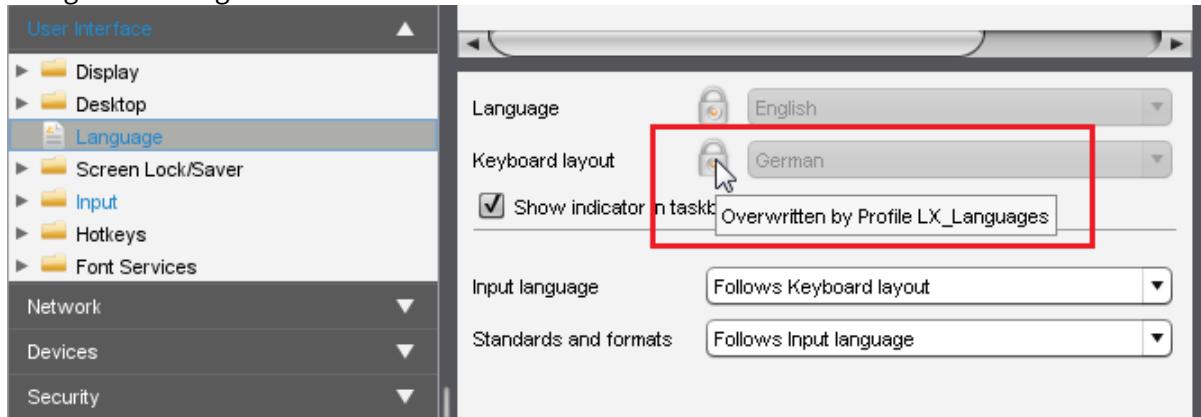
1. Select a device and click **Edit >Edit Configuration**.
The current configuration for the device will be displayed.



A lock symbol will be shown in front of each overwritten setting, i.e. in front of an active setting for



an assigned profile. The value that you have specified in the profile will be shown. You cannot change the setting here.



- Move the mouse over the lock symbol .

A tool tip will show the profile from which the parameter value was taken. This is useful if you have assigned more than one profile to the device. If a setting is active in a number of assigned profiles, the value in the most up-to-date profile will apply.

In the **Assigned Objects** area, you can navigate to an assigned device, profile or assigned file, or edit the configuration.

Name
LX_Screensaver
LX_Update

- Select an object.
- Click  to edit the object.
- Click  to navigate to this object in the tree structure.
- Double-click an assigned object to jump straight to it.

Removing Assigned Profiles from a Device

You can remove assigned profiles from a device or a device directory:

Starting from the profile

- Select a profile in the navigation tree.
- Select an object in the **Assigned Objects** area.
- Click .



Starting from the device

1. Select a device or a device directory in the navigation tree.
2. Select an assigned profile from the list in the **Assigned Objects** area.
3. Click .

This profile will now no longer affect the individual device(s) in the directory. The overwritten value for the settings is reset to the value which was valid before the profile was assigned.

-  Only directly assigned profiles can be removed. Indirectly assigned profiles can only be removed where they are assigned directly, that is the directory.

Deleting Profiles

If you would like to delete a profile, select it in the UMS navigation tree and perform one of the following options:



- ▶ In the symbol bar, click on **Delete**.
- ▶ Press the [Del] button on your keyboard.
- ▶ Right-click on the profile and select the **Delete** option from the context menu.

The same applies to directories too. These are deleted along with all sub-directories and profiles.

-  If you delete a profile, it will be removed for every device or every device directory to which it was assigned. The profile values no longer affect the device settings. In addition, all settings for the profile from the database will be deleted.

If the recycle bin is active, the deleted profile will be stored there and you may recover it if you need to.

Comparing Profiles

In the *IGEL Universal Management Suite 5*, a new function which makes it easy to compare profiles with each other was introduced.

To compare two profiles, proceed as follows:

1. Highlight two profiles using the [Ctrl] key.
2. Right-click on one of these profiles.
3. Select **Compare Profile Settings...** from the context menu .
The **Compare Profile Settings** mask will open.



Compare Profile Settings

Profile 1 Filter Profile 2

Name	Session Name "Bootlogo"	Value "Bootlogo"	Status	Session Name "Wallpaper"	Value "Wallpaper"
system.customization....		true	only in profile "Bootlogo"		
system.customization....		Admin	only in profile "Bootlogo"		
system.customization....		false	only in profile "Bootlogo"		
userinterface.languag...		English	equal		English
system.customization....	ums_filetransfer/MyPic...	igelstart.jpg	only in profile "Bootlogo"		
system.customization....		0007433305240b2101	only in profile "Bootlogo"		
system.customization....		9080	only in profile "Bootlogo"		
system.customization....		172.30.91.90	only in profile "Bootlogo"		
system.customization....		HTTP	only in profile "Bootlogo"		
userinterface.keyboard...		English(US)	changed		French
windowmanager.cust...			only in profile "Wallpaper"		Admin
windowmanager.cust...			only in profile "Wallpaper"	ums_filetransfer/MyPic...	
windowmanager.cust...			only in profile "Wallpaper"	172.30.91.90	
windowmanager.cust...			only in profile "Wallpaper"	true	
windowmanager.cust...			only in profile "Wallpaper"	9080	
windowmanager.cust...			only in profile "Wallpaper"	HTTP	
windowmanager.cust...			only in profile "Wallpaper"	0007433305240b2101	
windowmanager.cust...			only in profile "Wallpaper"	Wald...	

20 / 20 visible Export Close

All settings configured in the two profiles are listed one after another in the standard view. You can use specific comparative operators by clicking on the following buttons:

	Settings that are the same in both profiles are shown or hidden.
	Settings that are different in the profiles are shown or hidden.
	Settings that are only found in profile 1 are shown or hidden.
	Settings that are only found in profile 2 are shown or hidden.

- ▶ Click on one of these buttons in order to disable the relevant comparative operator.
- ▶ Click on it again to enable the operator once more.



inactive active

- ▶ Enable or disable a number of comparative operators.
- ▶ Click on **Export** to save the comparison list locally as a csv, html or xml file.

3.7.7 Prioritization of Profiles

Profiles can be assigned to devices directly or indirectly via directories. A device can receive its settings from a number of directly or indirectly assigned profiles. During the assignment process, the profile settings overwrite the settings configured directly on the device.

If you use *Shared Workplace*, you have the option of assigning profiles to users. Profiles assigned to users have more weight than those assigned to devices. See [Order of effectiveness of profiles in Shared Workplace](#)(see page 353).

The procedure for setting up and configuring profiles is described in [Use profiles](#)(see page 335). This chapter mainly looks at priorities - which profile overrides which one and when.

Order of Effectiveness

The priority of profiles is symbolized by "LEDs" below:



Lowest Priority



Highest Priority

The more red lights, the higher the priority of the profile.

-
- [Order of Effectiveness of Profiles](#)(see page 351)
 - [Order of Effectiveness of Profiles in Shared Workplace](#)(see page 353)
 - [Order of Effectiveness of Master Profiles](#)(see page 354)
 - [Order of Effectiveness of All Profiles](#)(see page 358)
 - [Summary](#)(see page 358)

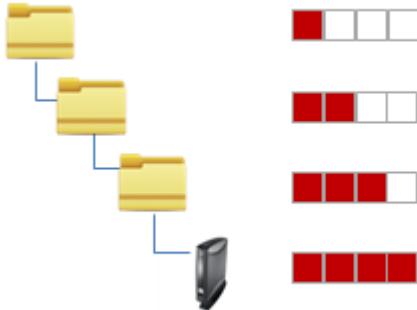
Order of Effectiveness of Profiles

In order to be able to manage the effectiveness of different profile types, you need to understand the order of priority. Various profiles that overlap like stencils can be assigned to a device. What happens if two profiles specify a different value for a setting? Which one has more weight?

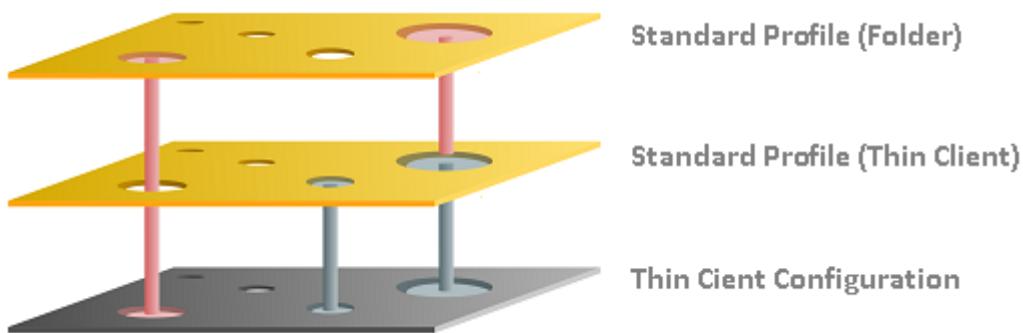
- ❖ Avoid competing settings in a number of profiles. If possible, set up one profile per setting, e.g. a profile for language settings, one for a left-handed mouse, etc.

The following rules apply to competing settings in various profiles:

Rule: The closer the standard profile is to the device in the directory tree, the higher its priority.



The priority rule only plays a role if the same parameter value is different in two profiles. The following graphic shows that there are specified values in both profiles which have an effect on the device. Only the parameter on the right is set by both profiles. In this case, the value of the bottom profile has priority because it is closer to the device.



Rule: In the event that the same settings are specified a number of times, the profiles with higher priority override other profiles. The effectiveness of settings which are specified in one profile only does not change.

See the following [example](#)(see page 352).

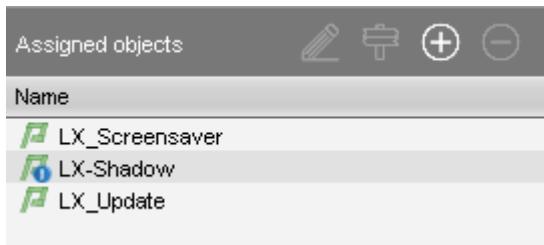
Rule: If several profiles are assigned on an equal basis, the newer profile with the higher profile ID has priority.

- ⓘ In order to read out the ID of a profile, point to a profile in the list of assigned profiles with the mouse pointer. A tooltip with the profile ID will be shown.

Rule: The priority rule only applies to general settings. If a number of sessions are set up, they will not be overridden. They will exist alongside each other because free instances are added.

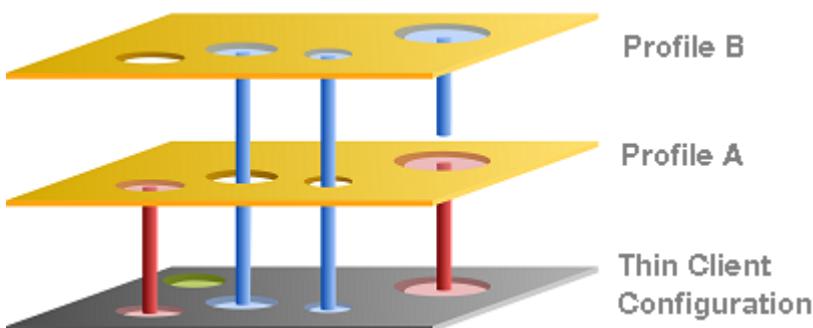
The lists of directly or indirectly assigned profiles are sorted according to the order of priority. Within a directory level, the profile which is higher up in the list thus has a higher priority.

In this example, the "screen saver" profile has the highest priority.



Example – Standard Profiles

We will create three profiles which we assign directly and indirectly to a client:



- **Device Configuration:** You specify the mouse settings on the device itself. In this case (green), the left-handed mouse is specified.
- **Profile A:** You assign to the device a language profile in which (red) the language and the keyboard layout are set to German.
- **Profile B:** You assign to a higher-level directory a profile with screen configuration. This specifies the resolution and the dual screen settings and the language is set to English (blue).

The settings that arrive at the client are:

- Green: Left-handed mouse (TC configuration)
- Red: Language and keyboard German (Profile A)
- Blue: Resolution and dual screen setting (Profile B)

The "English" language setting from Profile B has no effect on the device because Profile A has set the language parameter to German. Because Profile A is closer to the client, it has priority.

Order of Effectiveness of Profiles in Shared Workplace

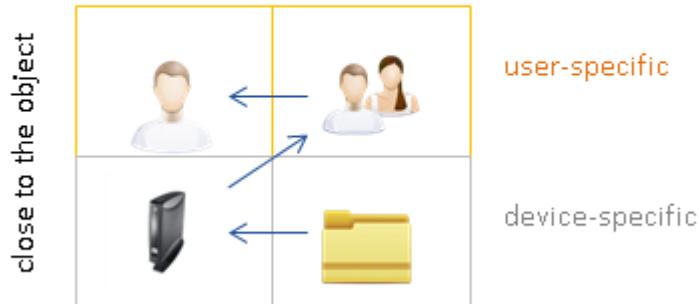
In [IGEL Shared Workplace](#)(see page 693), you can use profiles to configure user settings. For further information, see the guide [IGEL Shared Workplace - Assigning a User Profile](#)(see page 695).

⚠ Template profiles and template keys(see page 361) cannot be used if Shared Workplace is deployed.

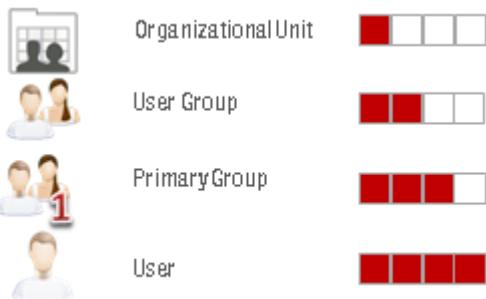
Rule: Profiles that are assigned to users have a higher priority than those that are assigned to devices. This applies to standard profiles and master profiles.

If you allocate a number of profiles, it may be that specific user or client settings are made a number of times. In this case, the following **priority of standard profiles** applies:

Standard Profile



Higher priority	than...
user-specific profiles	device-specific profiles
closer to the user/device	further away from the user/device



Higher priority	than...
primary groups	other groups
other groups	organizational unit



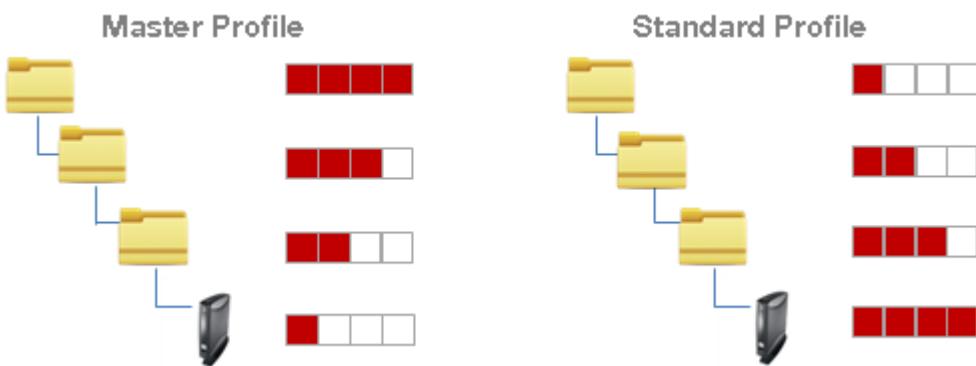
Rule: Profiles that are assigned to an object are prioritized in descending order according to profile ID (highest ID = highest priority).

Rule: Groups within a level are prioritized in alphabetical order.

Order of Effectiveness of Master Profiles

Master profiles allow more flexible access rights within the *IGEL UMS* as they can override the settings for standard profiles and have their own authorizations.

Master profiles are prioritized **the other way around** compared to the standard profiles. This means that a competing profile setting has higher priority the further away from the object the profile is:

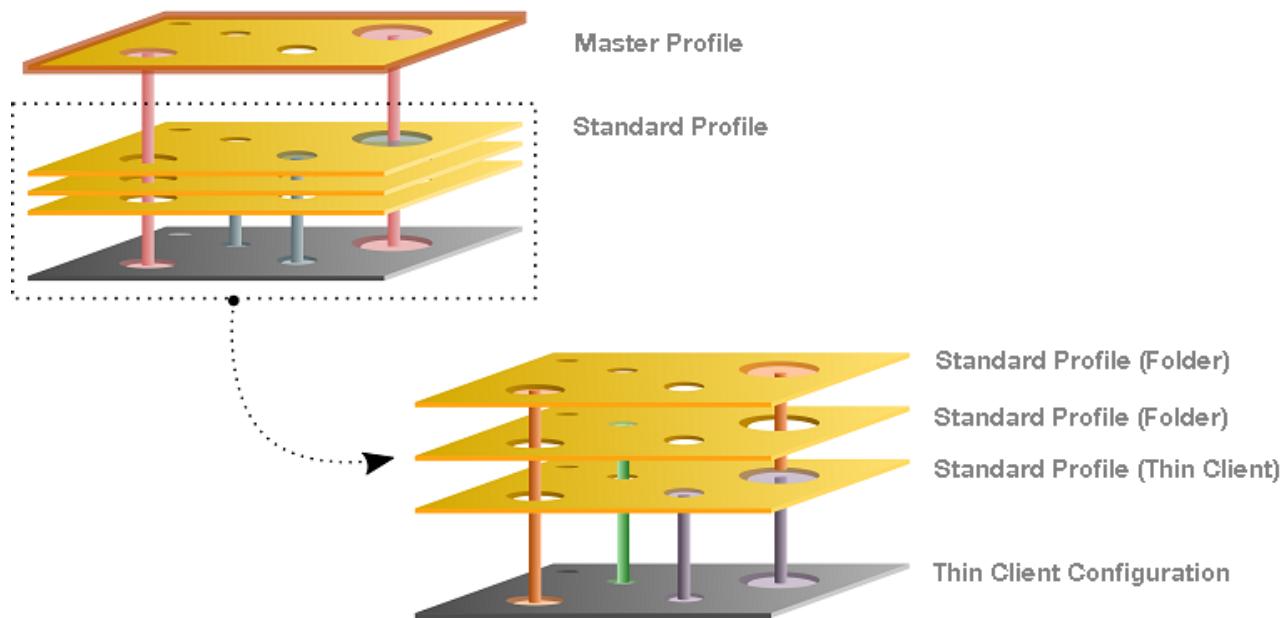


The following applies to master profiles:

Higher priority	than...
further away from the device	closer to the device
higher-level directory	sub-directory

Rule: Master profiles override all standard profiles.

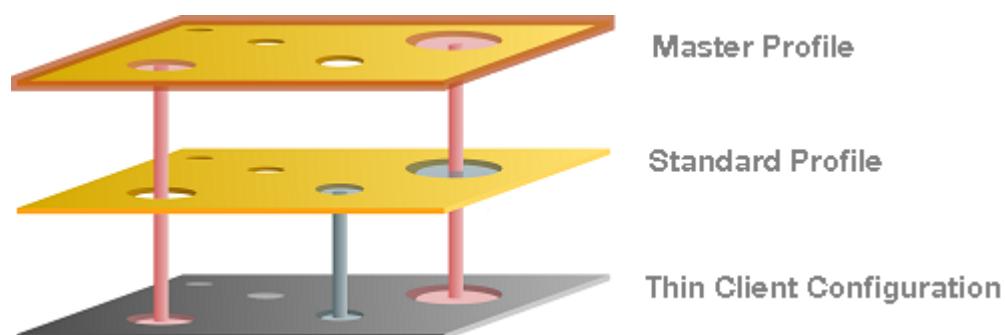
The following graphic shows that the master profile setting overrides that of the standard profiles if the same parameter is pre-populated. Settings that are not double-populated are effective without restriction.



- Example – Master Profiles(see page 355)
- Example – Master and Various Standard Profiles(see page 356)
- Master Profiles in Shared Workplace(see page 356)

Example – Master Profiles

We will create a standard profile and a master profile which we assign to a device.

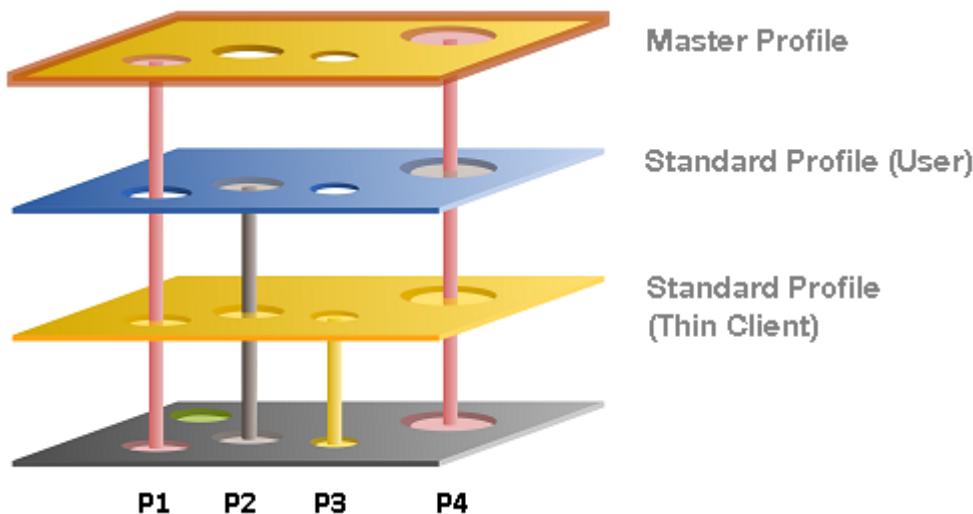


- **Standard profile:** You assign to the device a standard profile in which (gray) the language and the keyboard layout are set to German.
 - **Master profile:** You assign to a higher-level directory a master profile. This specifies the background image and the language is set to English (red).
- The settings that arrive at the client are:
- Gray: Keyboard German (standard profile)
 - Red: Background image and language setting English (master profile)

The "German" language setting from the standard profile has no effect on the device because the master profile has set the language parameter to English. If the parameter settings are the same, the master profile overwrites the values of standard profiles.

Example – Master and Various Standard Profiles

We will create a master profile, a user-specific standard profile and a device-specific standard profile.



- **Standard profile (device):** You assign to the device a standard profile with which you define the mouse settings. In this case the left-handed mouse (**P2**) is specified, the speed of the mouse pointer (**P4**) is set to slow, the double-click interval (**P1**) is set to slow and the keyboard layout is set to German (**P3**).
- **Standard profile (User):** You assign to a higher-level directory a user-specific standard profile in which the right-handed mouse (**P2**) is specified and the mouse speed (**P4**) is set to quick.
- **Master Profile:** You assign to a higher-level directory a master profile. In this case, the mouse pointer speed (**P4**) and the double-click interval (**P1**) are set to medium.

The settings that arrive at the client are:

- Yellow: (**P3**) Keyboard layout German (standard profile green)
- Grey: (**P2**) Right-handed mouse (standard profile blue)
- Red: (**P4, P1**) Mouse speed and double-click interval (master profile)

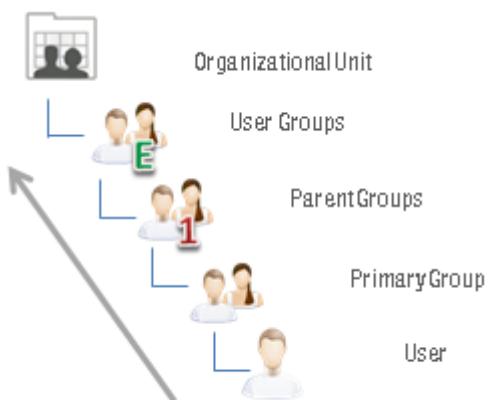
Master Profiles in Shared Workplace

Profiles assigned to users have a higher priority than profiles assigned to devices. In the case of the master profiles, the relevant group rather than the individual client or user is prioritized. This means:

Rule: Master profiles assigned to user groups have a higher priority than those assigned to individual users. These have higher priority than master profiles assigned to device directories. Master profiles assigned to an individual client have the lowest priority.

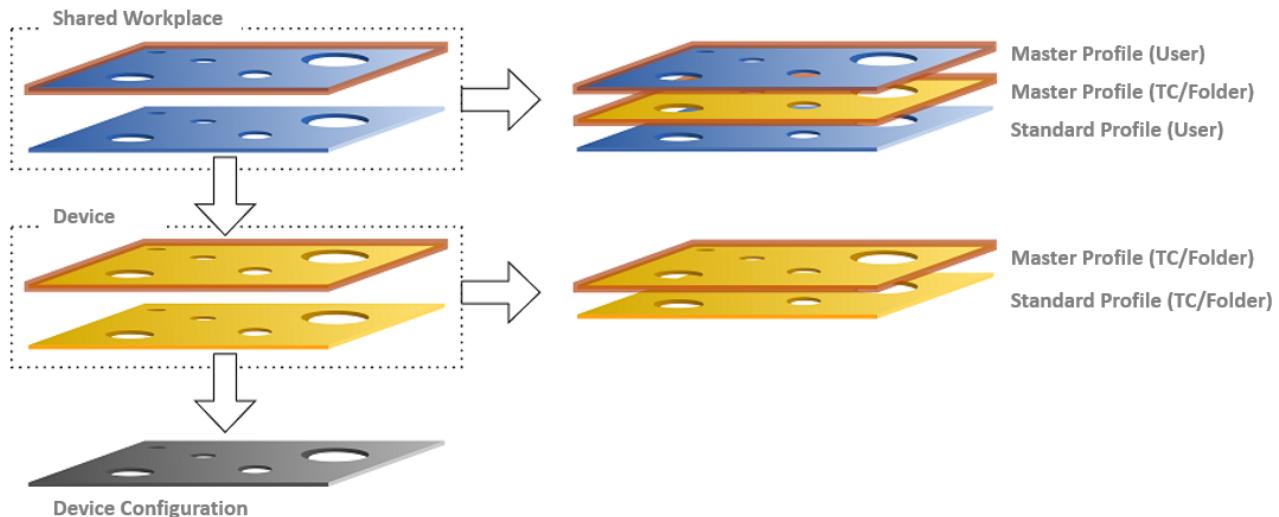


Higher priority	than...
user-specific profiles	device-specific profiles
further away from the user/device	closer to the user/device



Higher priority	than...
organizational unit	other groups
other groups	primary group

Order of Effectiveness of All Profiles



Parameters on the profile level (device and Shared Workplace)

- are specified by profiles or master profiles,
- can be configured exclusively via the UMS,
- overwrite parameter values that were configured on the device itself,
- take effect through assignment to a device or directories,
- can be enabled individually.

Parameters for the device configuration

- can be configured on the device itself or via the UMS,
- always contain ALL parameters,
- ALWAYS exist, even without the UMS.

Summary

The following overview summarizes all rules relating to the priority of profiles:

A - Basic rule

- In the event that the same settings are specified a number of times, the profiles with higher priority override other profiles. See the graphic in the [example](#)(see page 352).
- Settings which are specified in one profile only are not overridden.
- The priority rule only applies to general settings and fixed instances. If for example a number of [free instances](#)(see page 334) are set up, they will not be overridden – they will exist alongside each other.
- If several profiles are assigned on an equal basis, the newer profile with the higher profile ID has priority.

B - Standard profiles

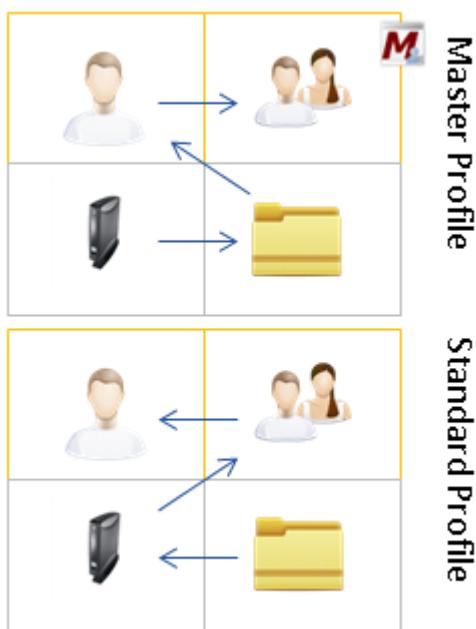
- The closer the standard profile is to the device, the higher its priority.

C - Shared Workplace

- The closer the standard profile is to the user, the higher its priority.
- Profiles assigned to users have a higher priority than profiles assigned to devices.
- Groups within a level are prioritized in alphabetical order.

D - Master profiles

- Master profiles override all standard profiles.
- Settings in master profiles can only be overwritten by master profiles.
- Master profiles are prioritized the other way around compared to the standard profiles.
- Master profiles which are closer to the object have lower priority.
- Master profiles assigned to user groups have a higher priority than those assigned to individual users. These have higher priority than master profiles assigned to device directories. Master profiles assigned to an individual client have the lowest priority.



3.8 Master Profiles

Menu path: Structure tree > **Master Profiles**



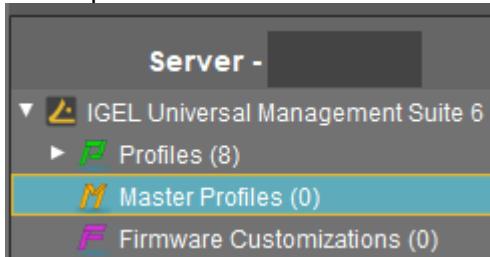
- ⓘ Master profiles have to be first enabled under **UMS Administration > Global Configuration > UMS Features**, see [Enabling Master Profiles\(see page 360\)](#).

The aim of introducing master profiles is to be able to reproduce the more complex system of rights management for UMS administrators in very large or distributed environments.

Important profile configurations can now be assigned to all registered devices on a priority basis without having to revoke the rights of other administrators to manage other settings or profiles.

3.8.1 Most Important Features of Master Profiles

- Master profiles are identical to standard profiles in terms of their effects, but are prioritized differently. For more information, see [Order of Effectiveness of Master Profiles\(see page 354\)](#).
- Master profiles are profiles whose settings override all standard profiles.
- Master profiles cannot be overwritten by standard profiles.
- Master profiles have their own section in the IGEL UMS structure tree.



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=FZFPpdSe0IM>

- [Enabling Master Profiles\(see page 360\)](#)

3.8.2 Enabling Master Profiles

You can specify whether or not you would like to use master profiles. By default, they are disabled.

To enable the master profiles function, proceed as follows:

1. In the UMS structure tree, select **UMS Administration > Global Configuration > UMS Features**.



2. Activate **Enable master profiles**.

The node **Master Profiles** appears in the structure tree.

3.9 Template Profiles

Menu path: Structure tree > **Template Profiles**

- i Template profiles have to be enabled first under **UMS Administration > Global Configuration > UMS Features**, see [Activating Template Profiles](#)(see page 363).

A template profile allows you to add variables for individual parameters in the profile and to assign their values to objects.



- i** Both **standard profiles** and **master profiles** can become template profiles through the use of variables.

Template profiles are used if you would like to avoid having to set up numerous sessions which differ only in terms of a few points.

- ⚠** Template profiles and template keys cannot be used if [Shared Workplace](#)(see page 693) is deployed.

3.9.1 Example

A company's devices are spread across a number of sites. All devices are to receive a browser session with the same settings via a profile, but a different start page is to be configured in the global settings for each site. It should also be possible to choose an individual session name for each site.

3.9.2 Previous Solution

A dedicated profile with global settings and session data was created for each site.

3.9.3 Problem

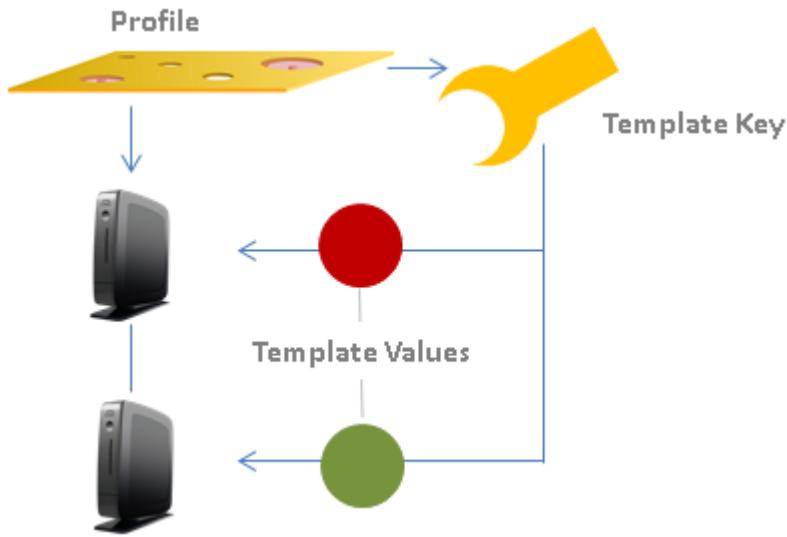
In many cases, the desired settings cannot be combined via various profiles, see [free instances](#)(see page 334). The unnecessarily large number of profiles is also difficult to manage in the long term.

3.9.4 Solution

The use of a single template profile offers greater flexibility. This contains all data for the browser session which are common to the devices as well as placeholders, so-called [template keys](#)(see page 364). The template keys contain parameters that are to receive divergent values for different devices at different sites. In addition, there are static template keys that receive their values from the device.

The template profile is assigned to all devices. The site-relevant template values are assigned to the particular devices that are to receive this value.

The device thus receives a profile whose settings are made up of fixed parameter values updated in the profile and the template values assigned to it that are referenced by template keys in the profile.



Rules:

- Template keys are used in one or more profiles.
- A template key has a number of values.
- The template profile is assigned directly or indirectly to a number of devices.
- A value from the key can be assigned to one or more devices directly or indirectly.

A device thus receives not only general profile settings but also the template value assigned to it for the configuration parameter which is represented in the profile by the associated template key as a placeholder.

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=uJnIK5u688c>

-
- [Activating Template Profiles](#)(see page 363)
 - [Creating Template Keys and Values](#)(see page 364)
 - [Using Template Keys in Profiles](#)(see page 370)
 - [Assigning Template Profiles and Values to the Devices](#)(see page 371)
 - [Value Groups](#)(see page 373)
 - [Export Template Keys and Value Groups](#)(see page 374)
 - [Import Template Keys and Value Groups](#)(see page 375)

3.9.5 Activating Template Profiles

If you would like to use the template profiles function, you must enable it first:

1. In the UMS Console, go to **UMS Administration > Global Configuration > UMS Features**.



2. Activate **Enable template profiles**.

The screenshot shows the 'Server' tab selected in the navigation bar. Under 'UMS Administration', the 'Global Configuration' section is expanded, showing various sub-options like 'Licenses', 'Mobile Devices', and 'Template Profiles'. The 'Template Profiles' option has a red box drawn around it. To its right, under 'UMS Features', there is a 'Recycle Bin' section with a checkbox for 'Enable recycle bin'. Below that is a 'Template Profiles' section containing a checked checkbox for 'Enable template profiles' with a link to 'Show section 'Template profiles' in User Manual'. Further down are sections for 'Master Profiles' (unchecked checkbox) and 'Shared Workplace' (checked checkbox).

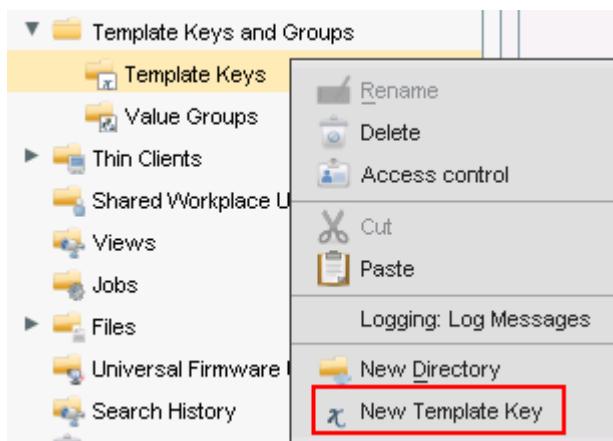
The **Template Keys and Groups** node appears in the UMS structure tree.

The screenshot shows the 'Server' tab selected in the navigation bar. The 'IGEL Universal Management Suite 6' node is expanded, showing 'Profiles (8)', 'Template Keys and Groups (0)' (which is highlighted with a red box), 'Template Keys (0)', 'Value Groups (0)', and 'Firmware Customizations (0)'.

3.9.6 Creating Template Keys and Values

To create template keys and values, proceed as follows:

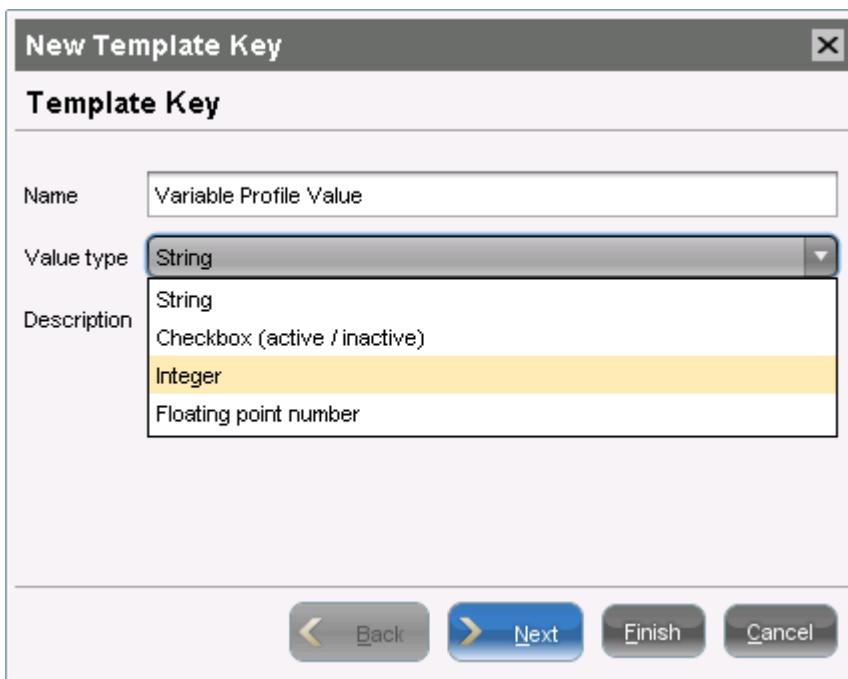
1. Open the context menu for the **Template Keys** folder.
2. Click on **New Template Key**.



- i** Alternatively, this function is also accessible via the menu **System>New>New Template Key**, the focus must be on the **Template Keys** node.

An assistant will guide you through the steps for creating a new template key:

3. Define a **name** for the key.
4. Select a **value type** for the key (String, Checkbox, Integer or Floating point number).
5. Optionally, give a **description** of the key.
6. Click on **Next**.



Name	Variable Profile Value
Value type	String
Description	<input type="checkbox"/> String <input type="checkbox"/> Checkbox (active / inactive) <input checked="" type="checkbox"/> Integer <input type="checkbox"/> Floating point number
<input type="button" value="Back"/> <input type="button" value="Next"/> <input type="button" value="Finish"/> <input type="button" value="Cancel"/>	



To specify the first value of the key, proceed as follows:

1. Enter the desired parameter value in the **Value** field.
2. Optionally, add a **description** of the value.
3. Click on **Create Value**.

The screenshot shows the 'New Template Key' dialog box with the title 'Create Values'. At the top, there is a 'Template Key Name' field containing 'Variable Profile Value'. Below it is a 'Specified Values' table with two columns: 'Value' and 'Description'. A single row is present, but its content is not clearly legible. To the right of the table are icons for edit and delete. Below the table is a 'New Value' section. It contains a 'Value' field with 'Value-1' and a 'Description' field with 'First value of the key'. A 'Create Value' button is located to the right of the description field. At the bottom of the dialog are four buttons: 'Back' (disabled), 'Next', 'Finish', and 'Cancel'.

To specify further values for the key, proceed as follows:

1. Change the entries under **Value** and **Description**.
2. Click again on **Create Value**.
3. Click on **Finish** to save the key with its values once you have created all desired values.



New Template Key

Create Values

Template Key Name

Specified Values

Value	Description
↳ Value-1	First value of the key
↳ Value-2	Second value of the key
↳ Value-3	Third value of the key

New Value

Value

Description

The key with its values will be shown in the tree:

- ▼ Template Keys and Groups
- ▼ Template Keys (4)
 - Landessprache
 - Startscreen TemplateKey
 - Startuppage for country
 - ▼ Variable Profile Value
 - ↳ Value-1
 - ↳ Value-2
 - ↳ Value-3
- Value Groups (0)

- ⓘ The recommended workflow is to create template keys and values from the [profile configuration](#)(see page 367).

Creating Keys and Values in the Profile

In profiles, specific parameters with a template key can be configured. To do this, combine the following steps to form a workflow:



- Create template keys and values⁵⁷
- Use template keys in profiles⁵⁸

To use template keys when configuring a profile, proceed as follows:

1. Open an existing profile or create a new profile.
2. Click on **Edit Configuration** in order to bring up the parameters to be updated.
3. Select a parameter which is to obtain a client-specific value from a template key.
4. Click the activation symbol in front of the parameter until the desired function is active (here:



	The parameter is inactive and will not be configured by the profile.
	The parameter is active and the set value will be configured by the profile, template keys are not available for the parameter.
	The parameter is active and the set value will be configured by the profile, template keys are available for the parameter.
	Template keys are active for this parameter, the profile receives a value from the key later on.

- i** Certain parameters cannot be configured with template keys and only offer the option *inactive* or *active*. This applies for example to passwords or parameters which depend on other configuration settings.

5. Click on the **selection symbol**
 6. Click on **Add**
 - An assistant will guide you through the steps for creating a new template key:
 7. Give a **name** for the key.
- i** The **value type** for the key is stipulated by the parameter.
8. Optionally, give a **description** of the key.

⁵⁷ <https://kb.igel.com/display/endpointmgmt509/Creating+Template+Keys+and+Values>
⁵⁸ <https://kb.igel.com/display/endpointmgmt509/Using+Template+Keys+in+Profiles>



New Template Key

Template Key

Name	New Key
Value type	String
Description	optional

9. Click on **Next**.

To enter the first value of the key, proceed as follows:

1. Define the desired parameter value in the **Value** field.
2. Optionally, add a **description** of the value.
3. Click on **Create Value**.

i In the case of parameters with a fixed value range such as selection menu or checkbox, the available options will be provided for selection. Click on **Add all** to create values for each entry in the value range or **Create Value** to add selected entries only.

New Value

Value	<input type="text"/>
Description	<input type="text"/> Create Value

< Back **Next >** **Finish** **Cancel**

4. Click on **Finish** to save the key with its values.

5. Click on **OK** to return to the profile.

The key will be shown in the profile parameter:



6. **Save** the template profile.

Profiles which use at least one template key in the configuration are labeled with a special symbol in the navigation tree:

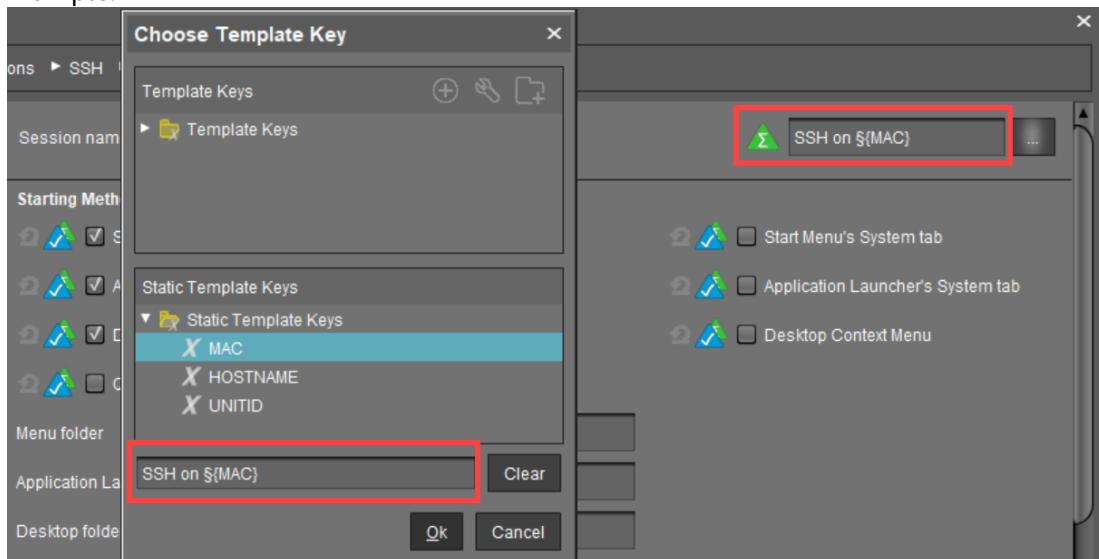
3.9.7 Using Template Keys in Profiles

Template keys are listed in the **Template Keys and Groups / Template Keys** node in the structure tree. They can be moved to their own sub-folders.

Static template keys are not visible in the structure tree; their values are received directly from the device. Static template keys are marked with the $\$$ symbol. The following static template keys are available:

- **MAC**: MAC address of the device
- **HOSTNAME**: Host name of the device
- **UNITID**: Unit ID of the device

Example:



To use a template key in the profile, proceed as follows:

1. Open an existing **profile** or create a new profile.
2. In the profile configuration, bring up the parameters to be updated.
3. Now select a parameter which is to be supplied with client-specific values from a **template key**.
4. Click the **activation symbol** in front of the parameter until the desired function is active – 

	The parameter is inactive and will not be configured by the profile.
	The parameter is active and the set value will be configured by the profile, template keys are not available for the parameter.
	The parameter is active and the set value will be configured by the profile, template keys are available for the parameter.



Template keys are active for this parameter, the profile receives a value from the key later on.



Reset to the default value.

- i These and other icons and their meanings can be found under **UMS Console > Help > Legend**.

- i Certain parameters cannot be configured with template keys and only offer the option *inactive* or *active*. This applies for example to passwords or parameters which depend on other configuration settings.

5. Click on the selection symbol  to choose a template key.
6. Double-click on the desired template key or static template key. Alternatively, you can create a new key, see [Create template keys and values in the profile](#)(see page 367).
7. Click on **OK**.
8. **Save** the template profile.
9. You can also combine template keys:



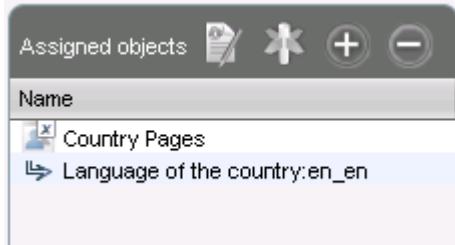
Profiles which use at least one template key in the configuration are labeled with a special symbol in the structure tree: .

3.9.8 Assigning Template Profiles and Values to the Devices

Once you have created the **template keys** and **values** and configured **profiles** using the template keys, you will need to bring together the keys and values again on the device.

To assign to a device a template profile and the values needed to replace the keys, proceed as follows:

1. Select a **template profile** and assign it in the usual manner to a group of devices or a device directory.
2. Select a **value** for each **template key** used in the profile.
3. Assign the relevant values to the corresponding devices.





4. Assign further key values to further devices. Several values for various keys can also be assigned collectively ([Shift] and [Ctrl] keys).

Each device must then have an assigned value for each key in the assigned profiles.

To check that template profiles and values have been assigned correctly, proceed as follows:

1. Click on **Devices** in the top menu bar.
2. Select **Check the Template Definitions**.

The selected and checked devices are flagged according to the result:

	all template keys are defined
	missing template keys

3. Double-click on the message in the message window to open the error log for the check function:

Check the template definitions				
Thin Client	Profile	Template Expression	Description	X
Doku-1-LX (00E0C53627...)	Template Profile	\$(New key)	Missing value for template key "New key"	
Prod-1 (00E0C5111111)	Template Profile	\$(New key)	Missing value for template key "New key"	
Prod-2 (00E0C5222222)	Template Profile	\$(New key)	Missing value for template key "New key"	
Prod-0 (00E0C5000000)	Template Profile	\$(New key)	Missing value for template key "New key"	

Or click on a device and the results of the check will be shown immediately:

Missing Template Values

▶ **System Information**

▼ **Template Definition Check Results**

Severity	Profile	Template Expression	Description
Error	Browser	www.\${Domain}\${C...	Missing value for te...
Information	Browser	www.\${Domain}\${C...	value for template ke...

▶ **Monitor Information**

▶ **Features**

As soon as the devices receive their updated profile settings (e.g. automatically after restarting the devices), the keys contained in the profile for each device will be replaced by the corresponding value from their assignment to the device and then transferred to the device. The local device setup thus receives only the usual parameter values and no more keys.



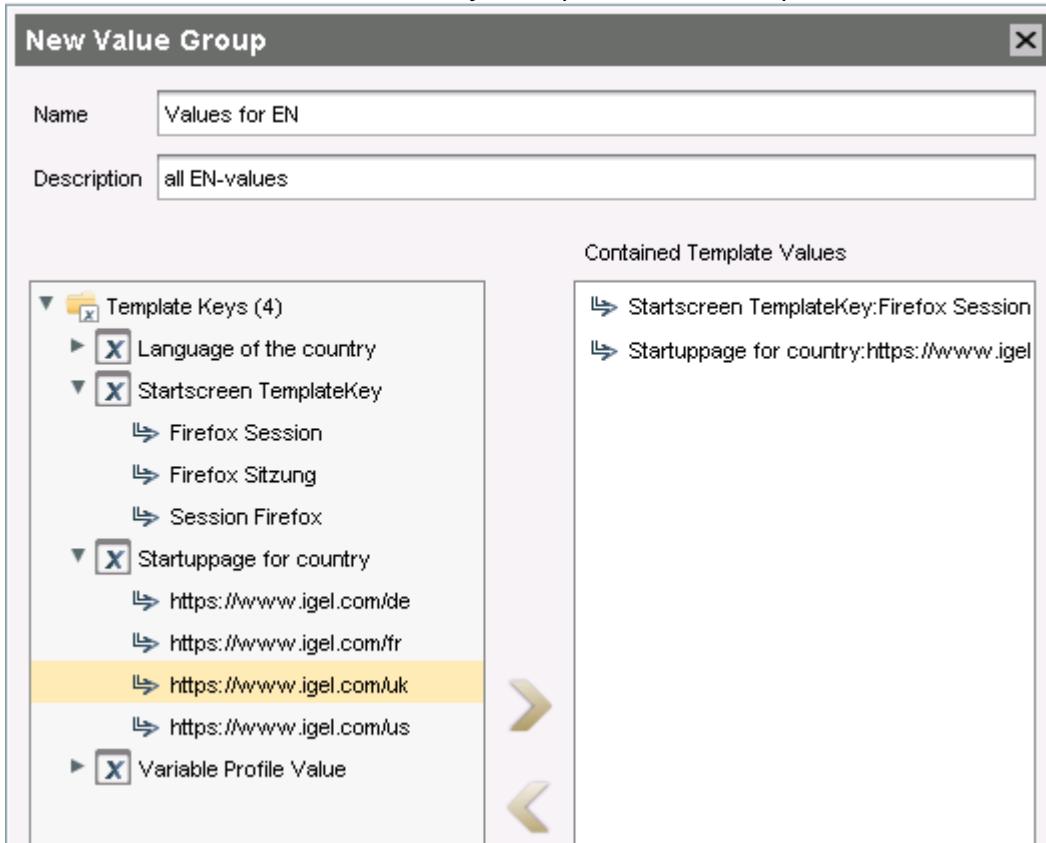
3.9.9 Value Groups

In value groups, logically associated values from various template keys can be brought together and assigned together to devices.

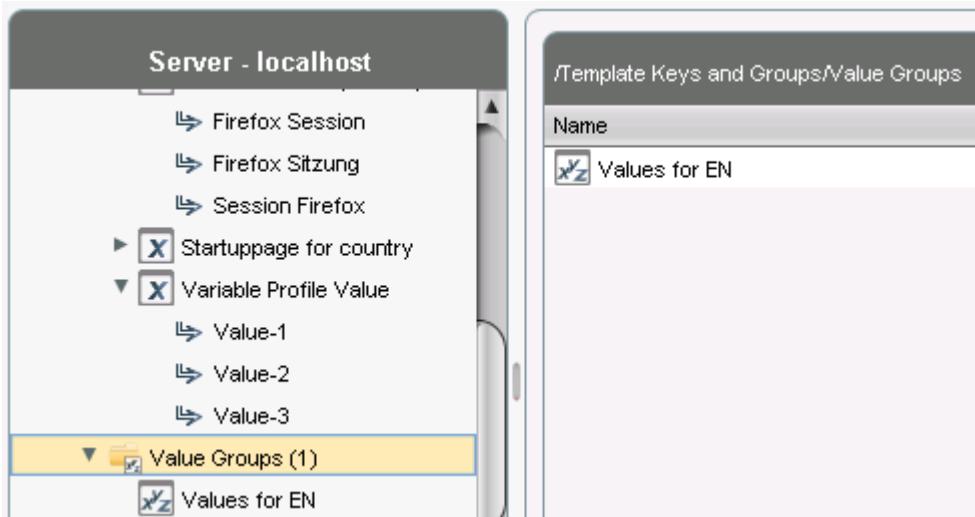
If for example you have various profiles which are to receive country-specific settings via template keys and value assignments, all values for a country / a language can be grouped in a value group. When such a group is assigned, a device also receives all values for its country / its language contained in it.

To create a group, proceed as follows:

1. Create a **template profile** with keys and values.
2. Click on **System>New>New Value Group** in order to create a new value group.
3. Enter a **name** and description for the group.
4. Select the desired values from each key, multiple selections are possible.



5. Confirm your settings by clicking on **OK**.
6. Create further groups.



The screenshot shows the UMS interface with the navigation tree on the left and a details panel on the right.

Navigation Tree (Server - localhost):

- Firefox Session
- Firefox Sitzung
- Session Firefox
- Startpage for country** (selected)
- Variable Profile Value** (selected)
 - Value-1
 - Value-2
 - Value-3
- Value Groups (1)** (highlighted)
 - Values for EN** (selected)

Details Panel (/Template Keys and Groups/Value Groups):

Name
<input checked="" type="checkbox"/> Values for EN

7. Assign the template profile to all devices.
8. Assign the appropriate group in each case to the devices.
9. Highlight the **Devices** tree node.
10. Click on **Devices>Check the Template Definitions** in order to check the definitions.
The result is shown in the message window.

After the next restart or a manual transfer, the devices will receive the new session data with shared and country-specific profile settings.

- i** The advantage of this method is that you only need to add further key values to the relevant value group in the future in order to assign these to the site's devices. In addition, a better overview is possible if there are a large number of template keys and values.

3.9.10 Export Template Keys and Value Groups

Menu path: **System > Export > Export Template Keys and Value Groups**

You can export template keys and value groups in the UMS database in order to import them to another UMS installation.

To export template keys and value groups, proceed as follows:

1. If you would like to preselect template keys, value groups or directories, highlight the desired items in the navigation tree.
2. Go to **System > Export > Export Template Keys and Groups**.
In the **Export Template Keys and Groups** window, the template keys and value groups previously selected or all available template keys and value groups will be shown.
3. In the **Export** column, select the template keys and value groups that you want to export.
4. Click on **Next** and select a save location.
5. Click on **Done**.
The template keys and value groups will be saved in a ZIP archive.



3.9.11 Import Template Keys and Value Groups

Menu path: **System > Export > Import Template Keys and Value Groups**

You can import template keys and value groups. In order for this to be possible, the template keys which are to be imported must not yet exist in the UMS database. Each template key has a unique name which may only be used once in a UMS database.

To import template keys and value groups, proceed as follows:

1. In the navigation tree, highlight the directory in which the template keys and value groups are to be placed.

i If you would like to import template keys and value groups in a single step, please note the following: If a directory below **Template Keys** is selected, the template keys will be placed in the selected directory and the value groups in the **Value Groups** directory. If a directory below **Value Groups** is selected, the value groups will be placed in the selected directory and the template keys in the **Template Keys** directory.

2. Go to **System > Import > Import Template Keys and Value Groups**.
3. Select the file with the template keys and value groups and click on **Open**.
The **Template keys and value groups** window will open.
4. In the **Import** column, select the template keys and value groups that are to be imported.
5. With the **Create path relative to the directory currently selected** option, specify whether the directory structure of the imported template keys and value groups is to be retained:
 - The directory structure of the imported template keys and value groups will be retained, i.e. the exported subdirectories will be restored. (default)
 - The directory structure of the imported template keys and value groups will be ignored, i.e. all template keys and value groups will be placed on the highest directory level.
6. Click on **OK**.
Once all template keys and value groups have been imported, a confirmation will be shown.
If not all template keys and value groups could be imported, the template keys and value groups for which the import failed will be shown.

3.10 Mobile-Device Profiles

With UMS 5.09.100, as part of the UMS extension IGEL Mobile Device Management Essentials (MDM), **mobile-device profiles** were introduced, see the [MDM Manual \(see page 706\)](#) for detailed information on this profile type.

3.11 Firmware Customizations

Menu path: **Structure Tree > Firmware Customizations**

From UMS Version 5.05.100, you can customize the user interface of your IGEL OS devices to suit your CD (corporate design) through firmware customization. The configuration takes place in a dedicated wizard; for a minimal configuration, only a name and a file object need to be specified.



3.11.1 Mode of Action

A firmware customization can be assigned to a device or a directory.

Firmware customizations override normal profiles but in turn can be overridden by master profiles. They are therefore between master profiles and standard profiles in terms of their priority.

Further information regarding the prioritization of profiles can be found under [Prioritization of Profiles](#)(see page 350).

If several applications cases of the same type are assigned to a device, e.g. a background image, only the Use case with the highest priority will be effective. The priority is determined by how direct or indirect the assignment to the device is: A firmware customization assigned directly to the device has a higher priority than one which is assigned to the directory of the device. If both firmware customizations have the same priority, the firmware customization with the higher ID will be effective.

- ⓘ In order to obtain the ID of a firmware customization, move the mouse pointer over the relevant object in the structure tree.

-
- [Create Firmware Customization](#)(see page 376)
 - [Export Firmware Customizations](#)(see page 381)
 - [Import Firmware Customizations](#)(see page 381)

3.11.2 Create Firmware Customization

To create a **Firmware Customization**, proceed as follows:

1. Move the cursor to **Firmware Customization** in the structure tree.
2. Select **Create New Firmware Customization** in the context menu.
The **Firmware Customization Details** dialog window will appear.
3. Give a **Name** for this firmware customization.
4. Select an **Use case**. The following can be selected:
 - [Start Button](#)(see page 377)
 - [Start Menu](#)(see page 377)
 - [Taskbar Background](#)(see page 378)
 - [Screensaver](#)(see page 378)
 - [Screensaver \(Custom Partition\)](#)(see page 379)
 - [Bootsplash](#)(see page 380)
 - [Background Image](#)(see page 381)
5. Click on **Next**.
The **Firmware customization assignment** dialog window will appear.
6. Highlight one or more directories or devices and click on in order to assign the firmware customization.
7. Click on **Done**.

The firmware customizations created are listed in the structure tree under the **Firmware customizations** node. If you click on a firmware customization, the associated files and assigned objects will be shown.



The files used in a firmware customization are marked with a .

- If you want to delete a file marked with , you must first remove it from the associated firmware customization.

The settings for an Use case can be enabled or disabled for a firmware customization as you will already know from the [profiles](#)⁵⁹:

	The parameter is inactive and will not be configured by the firmware customization.
	The parameter is active and the set value will be configured by the firmware customization.

- Exception: The file path for screensaver (custom partition) cannot be disabled.

Start Button

Firmware Customization Details

- **Name:** Name of the firmware customization
- **Use case:** “Start button”
- **Image:** Name of the selected image file
 - **Choose file:** All files registered in the UMS in a suitable format (*.png, *.ico) and for which you have authorizations are shown here.
 - **Upload file:** Select a file from a local directory or from the UMS Server.
 - **Clear:** Deletes the image file shown under **Image**.

Firmware Customization Assignments

Assignment of the devices for which the customizations are to apply.

Start Menu

Firmware Customization Details

- **Name:** Name of the firmware customization
- **Use case:** “Start menu”
- **Image:** Name of the selected image file

⁵⁹ <https://kb.igel.com/display/endpointmgmt601/Editing+profiles>



- **Select file:** All files registered in the UMS in a suitable format (*.jpg, *.bmp, *.png) and for which your have authorizations are shown here.
- **Upload file:** Select a file from a local directory or from the UMS server.
- **Delete:** Deletes the image file shown under **Image**.

Firmware Customization Assignment

Assignment of the devices for which the customizations are to apply.

Taskbar Background

Firmware Customization Details

- **Name:** Name of the firmware customization
- **Use case:** “Taskbar background”
- **Image:** Name of the selected image file
 - **Choose file:** All files registered in the UMS in a suitable format (*.jpg, *.bmp, *.png) and for which your have authorizations are shown here.
 - **Upload file:** Select a file from a local directory or from the UMS server.
 - **Clear:** Deletes the image file shown under **Image**.

Firmware Customization Assignment

Assignment of the device for which the customizations are to apply.

Screensaver

Firmware Customization Details

- **Name:** Name of the firmware customization
- **Use case:** “Screensaver”
- **Image:** Name of the selected image files
 - **Choose file:** All files registered in the UMS in a suitable format (*.jpg, *.bmp, *.png) and for which your have authorizations are shown here.
 - **Upload file:** Select a file from a local directory or from the UMS server.
 - **Clear:** Deletes the image file shown under **Image**.
- **Display mode:** Type of display.
Possible options:
 - next to each other small
 - next to each other medium
 - centered in the middle
 - cut
- **Screen mode:**
 - One image per monitor
 - One image for all monitors (stretched if necessary)
- **Display time:** Time in seconds that an image is shown before it switches. (default: 10)



- **Start**

Possible options:

- [Start screensaver automatically](#)
- Do not start screensaver automatically

- **Start time:** Time in minutes until the screensaver starts. (default: 5)

- **Background color:** (default: black)

- **Choose color:** Color selection according to color spaces

Possible color spaces:

[Swatches](#)

HSV

HSL

RGB

CMYK

Firmware Customization Assignment

Assignment of the devices for which the customizations are to apply.

Screensaver (Custom Partition)

Firmware Customization Details

- **Name:** Name of the firmware customization
- **Use case:** “Screensaver (custom partition)”
- **Images:** Names of the selected image files
 - **Choose file:** All files registered in the UMS in a suitable format (*.jpg, *.bmp, *.png) and for which you have authorizations are shown here. You can select a number of images here.
 - **Upload file:** Select a file from a local directory or from the UMS server.
 - **Remove file:** Deletes the selected image files.

File path (custom partition + folder): File path of a folder on the custom partition (example: /custom/screensaver).

- ⓘ The custom partition must be created beforehand so that the images can be added to it. If no custom partition has been created, the images will be saved in the RAM and will be reloaded each time that the system boots. The folder does not need to be created beforehand, it will be created if necessary. Ensure that the path begins with a /.

- **Display mode:** Type of display. The following can be selected:

- Small, jumping
- Medium, jumping
- Filled
- Fit in

- **Image mode:**

- [One image per monitor](#)
- One image for all monitors (stretched if necessary)

- **Display time:** Time in seconds that an image is shown before it switches. (default: 10)



- **Start**

Possible options:

- Start screensaver automatically
- Do not start screensaver automatically

• **Start time:** Time in minutes until the screensaver starts. (default: 5)

• **Background color:** (default: black)

- **Choose color:** Color selection according to color spaces

Possible color spaces:

Swatches

HSV

HSL

RGB

CMYK

Firmware Customization Assignment

Assignment of the devices for which the customizations are to apply.

Bootsplash

Firmware Customization Details

- **Name:** Name of the firmware customization
- **Use case:** "Bootsplash"
- **Image:** Name of the selected image file
 - **Choose file:** All files registered in the UMS in a suitable format (*.jpg, *.bmp, *.png) and for which you have authorizations are shown here.
 - **Upload file:** Select a file from a local directory or from the UMS server.

i For the bootsplash, the device obtains the selected file from the UMS via HTTPS as soon as it is required.

- **Clear:** Deletes the image file shown under **Image**.
- **Horizontal position:** Horizontal position of the bootsplash. (default: 50%)
- **Vertical position:** Vertical position of the bootsplash. (default: 50%)
- **Progress horizontal position:** Horizontal position of the progress bar. (default: 90%)
- **Progress vertical position:** Vertical position of the progress bar. (default: 90%)

Firmware Customization Assignment

Assignment of the devices for which the customizations are to apply.



Background Image

Firmware Customization Details

- **Name:** “Background image”
 - **Use case:** “Background image”
 - **Background monitor 1-8:** Name of an image file for up to 8 monitors
 - **Choose file:** All files registered in the UMS in a suitable format (*.jpg, *bmp, *png) and for which your have authorizations are shown here.
 - **Upload file:** Select a file from a local directory or from the UMS server.
- i** For the background image, the device obtains the selected file from the UMS via HTTPS as soon as it is required.
- **Clear:** Deletes the image file shown under **Background monitor 1-8**.

Firmware Customization Assignment

Assignment of the devices for which the customizations are to apply.

3.11.3 Export Firmware Customizations

Menu path: **System > Export > Export Firmware Customizations**

You can export firmware customizations. The data exported contain all necessary settings and files.

To export firmware customizations, proceed as follows:

1. If you would like to preselect firmware customizations, highlight the desired firmware customizations or directories in the navigation tree.
2. Go to **System > Export > Export Firmware Customizations**.
In the **Export Firmware Customizations** window, the previously selected firmware customizations or all available firmware customizations will be shown.
3. In the **Export** column, select the firmware customizations that you want to export.
4. Click on **Next** and select a save location.
5. Click on **Finish**.
The firmware data will be saved in a ZIP archive.

3.11.4 Import Firmware Customizations

Menu path: **System > Import > Import Firmware Customizations**

You can import firmware customizations. The imported data contain not only the settings but also all required files.

To import firmware customizations, proceed as follows:

1. Highlight the directory where the firmware customizations are to be placed.
2. Go to **System > Import > Import Firmware Customizations**.



3. Select the file with the firmware customizations and click on **Open**.
The **Import firmware customizations** window will open.
4. In the **Import** column, select the firmware customizations that are to be imported.
5. With the **Create path relative to the directory currently selected** option, specify whether the directory structure of the imported firmware customizations is to be retained:
 - The directory structure of the imported firmware customizations will be retained, i.e. the exported subdirectories will be restored. (default)
 - The directory structure of the imported firmware customizations will be ignored, i.e. all firmware customizations will be placed on the highest directory level.
6. Click on **OK**.
Once all firmware customizations have been imported, a confirmation will be shown.
If not all firmware customizations could be imported, the firmware customizations for which the import failed will be shown.

3.12 Devices

Menu path: Structure tree > **Devices**

In the **Devices** area, you can manage end devices registered on the UMS Server. All devices registered on the UMS Server are shown.

The name of a device shown in the structure tree is used for identification in the UMS and does not need to be identical to the name of the device in the network. The name shown in the structure tree does not need to be unique and can be used a number of times.

The unit ID serves as a unique identifier. With IGEL devices, IGEL zero clients, devices converted with the IGEL UDC/OSC, and devices with the IGEL UMA, the unit ID is set to the MAC address of the device.

You can structure the **Devices** area by creating directories and, possibly, sub-directories. When doing so, you should bear in mind that each device can only be shown once in the structure tree. You can move a device by dragging and dropping it from one directory to another.

3.12.1 Icons for an IGEL OS Device

The following icons in the structure tree show the status of an IGEL OS device:

	When the device is connected via IGEL Cloud Gateway (ICG), a cloud symbol icon is added to the device.
	The device is online. Please note that Misc > Settings > Online Check must be activated for indicating the online status.
	The device is offline. Please note that Misc > Settings > Online Check must be activated for indicating the online status.
	Changes have not yet been transferred to the device (possible with all statuses).



- i** As of IGEL OS 10.03.100, the following status displays are offered. In order to make them visible, the **Devices send updates** option must be enabled (default). To do this, go to **UMS Administration > Global Configuration > Device Network Settings > Advanced Device's Status Updates**.

	The device is showing the login screen (if configured).
	The device is being updated.
	The UMS has no license for the device.
	The device has never been registered.

The UMS monitors the status of the devices by regularly sending UDP packets. In accordance with the preset, this occurs every 3 seconds. You can specify the interval for the online check in the **Misc > Settings > Online Check** menu. You can also update the status manually.

3.12.2 Icons for a UD Pocket

The following icons in the structure tree show the status of a UD Pocket:

	The registered UD Pocket (no further information is available at the moment).
	The UD Pocket is online. Please note that Misc > Settings > Online Check must be activated for indicating the online status.
	The UD Pocket is offline. Please note that Misc > Settings > Online Check must be activated for indicating the online status.
	The UD Pocket is showing the login screen (if configured).
	The UD Pocket is being updated.
	The UD Pocket is not licensed.

- i** These and more icons and their meanings can be found under **UMS Console > Help > Legend**.

For status displays used in the [UMS Web App](#)(see page 720), see [Devices](#)(see page 737).

- [Device](#)(see page 384)
- [Managing Devices](#)(see page 387)
- [Configuring Devices](#)(see page 391)
- [Exporting and Importing Data](#)(see page 392)
- [Send Message](#)(see page 394)
- [View Asset Information](#)(see page 395)
- [Secure Terminal \(Secure Shell\)](#)(see page 397)



- **Shadowing (VNC)**(see page 399)

3.12.3 Device

Menu path: Structure Tree > **Devices** > [Directories] > **[Name of the device]**

This area shows up-to-date information regarding the selected device.

System Information

- **Name**
- **Last IP**
- **Location**
- **Comment**
- **Department**
- **Cost center**
- **Inventory number**
- **Setup and startup**
- **Serial number**
- **[custom attributes]**
- **Unit ID**
- **MAC address**
- **Product**
- **Product ID**
- **Version**
- **Firmware description**
- **IGEL Cloud Gateway**
- **Expiry date of the maintenance subscription**
- **Last contact**
- **Last start time**
- **Network name at last restart**
- **Runtime since last restart**
- **Runtime since setup and startup**
- Battery Level: The battery level is shown on mobile devices. The display can be updated by clicking on . This function is available from IGEL OS 10.03.100. The frequency at which the device sends details of the current battery level to the UMS can be set via the setup; further information can be found under [Battery Level Control](#)⁶⁰.
- **CPU speed (MHz)**
- **CPU type**
- **Size of the flash memory (MB)**
- **Memory (MB)**
- **Network speed**
- **Duplex mode**
- **Graphic chipset 1**
- **Graphics memory 1 (MB)**

⁶⁰ <https://kb.igel.com/pages/viewpage.action?pageId=23501086>



- **Graphic chipset 2**
- **Graphics memory 2 (MB)**
- **Device type**
- **Operating system type**
- **BIOS manufacturer**
- **BIOS version**
- **BIOS date**
- **Boot mode**
- **Serial number of the device**
- **Structure tag**

Template Definition Check Results

- **Type**
- **Profile**
- **Template expression**
- **Description**

Monitor Information

- **Monitor 1**
 - **Vendor**
 - **Model**
 - **Serial Number**
 - **Size**
 - **Native Resolution**
 - **Date of Manufacture**
- **Monitor 2**
 - **Vendor**
 - **Model**
 - **Serial Number**
 - **Size**
 - **Native Resolution**
 - **Date of Manufacture**
- Further monitors, if applicable...

Features

In this area, the features available on the device are listed.

Windows Updates and Hotfixes

In this area, the *Windows* updates and hotfixes installed on the device are listed.



Partial Updates

In this area, the partial updates installed on the device are listed. This information is available from *IGEL Universal Desktop W7 Version 3.12.100* and *IGEL Universal Management Suite Version 5.03.100*.

The following information regarding partial updates is shown.

- **Name**
- **Version**
- **Date**
- **Description**

File Transfer Status

As of UMS version 5.09.100 and device Firmware IGEL OS 10.05.100, the transfer status of assigned files is displayed here, regardless of whether they have been assigned directly or indirectly (via Profiles or FWC).

You will receive the following information:

- **Filename**
- **File ID**
- **Classification**: The classification assigned when the file is uploaded, or the use case of the firmware customization or the description of the profile.
- **Status** - possible values:
 - OK
 - Error
 - unknown
- **Status Message**
- **Assigned via**: For directly assigned files, the file name is displayed here, otherwise the name of the profile or of the firmware customization will be displayed.

User Login History

Specific types of user login can be logged in the UMS.

The user logins are logged if the following options are enabled:

- device or profile: **System > Remote management > Options > Log login and logoff events** checkbox
- **UMS: UMS Administration > Misc Settings > Enable user logon history** checkbox

If logging is enabled, the following information is saved:

- **User name**
- **Login time**
- **Logout time**
- **Login type**

The following login types can be logged in the UMS:

- **Shared Workplace**
- **AD/Kerberos**



- Citrix

3.12.4 Managing Devices

In the IGEL UMS, you can sort devices according to directories via a structure tree. You can use this facility to provide devices forming groups on the basis of their location or structure with the same profiles or to sort the devices in keeping with your company structure.

Actions performed at the directory level apply to all subdirectories and devices contained in this directory.

- [Creating a Directory](#)(see page 387)
- [Copying a Device Directory](#)(see page 388)
- [Importing a Directory](#)(see page 388)
- [Deleting a Directory](#)(see page 389)
- [Moving Devices](#)(see page 389)
- [Assigning Updates](#)(see page 390)
- [Default Directories](#)(see page 391)

See also the video with an overview of how to search for devices, add directories, move devices to a directory and create profiles(see page 331) with settings for devices:



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=sXw9GW95dgw&list=PLwmmael4krnP_0oALne0k107MHvB9da3B&index=4

Creating a Directory

You can create as many directories and sub-directories as you want in order to group the devices together. When you create sub-directories, the devices organized in it form sub-groups of a group.

A device that is unequivocally identified by its MAC address can only be stored in a single directory, i.e. only as a member of a single group.

To create a directory or sub-directory, proceed as follows:

1. Select a directory, e.g. **Devices**.
2. Click **System>New >New Directory** in the main menu bar
or select the option **New Directory** from the context menu of the selected directory.
3. Enter a name for the new directory.
4. Click **OK**.
The new directory will be displayed directly below the selected directory in the structure tree.



You can now move devices to this new directory.

For details on how to create a directory in the [UMS Web App](#)(see page 720), see [Creating a Directory](#)(see page 742).

Copying a Device Directory

Menu path: Structure Tree > **Devices** > [Name of the device directory] > Context Menu > **Copy**

You can copy a device directory and paste it into any directory. Only an empty directory as well as the subdirectories contained in it will be copied; devices cannot be copied.

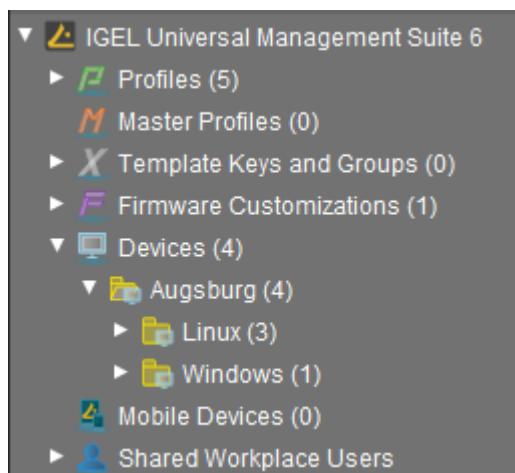
To copy a device directory, proceed as follows:

1. Click on the directory that you want to copy.
 2. Open the context menu for the directory and select **Copy**.
 3. Click on the directory in which you would like to paste the copy of the directory. This can also be the directory in which the original directory is located.
 4. Open the context menu for the directory and select **Paste**.
- A new device directory which has the same name as the original directory will be created. The new directory will contain newly created copies of the subdirectories contained in the original directory.

For details on how to copy a directory in the [UMS Web App](#)(see page 720), see [Copying a Device Directory](#)(see page 743).

Importing a Directory

If you are planning a complex directory structure, you do not need to set it up in a step-by-step manner in the UMS Console. Instead, you can create a `.csv` file (e.g. with a spreadsheet program) in which you determine the directory structure and then import the structure from this list.



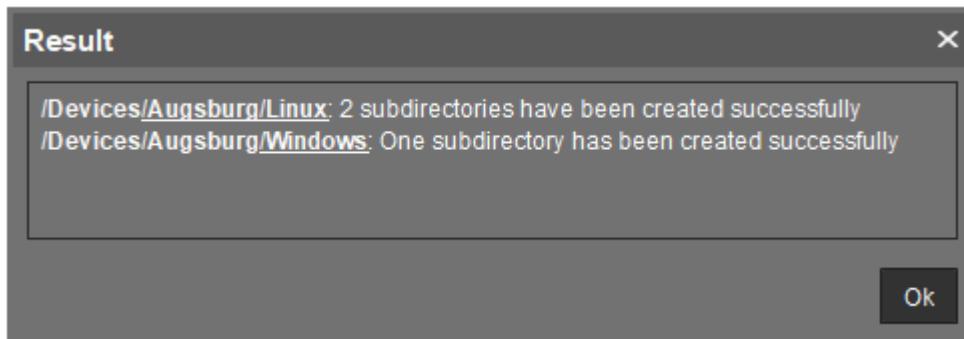
The tree structure shown above is based on the following file:

```
Devices; Augsburg; Linux
Devices; Augsburg; Windows
```

To import a directory structure from a `.csv` file, proceed as follows:



1. Select **System > Import > Import Directories** from the main menu.
The **Import Directories** window will appear.
2. Click **Open File** in order to load a csv file. In the first column, you must specify one of the default master directories. In this way, you can also import directory structures for profiles, tasks, views or files.
3. Click **Import Directories** in order to create the directory structure.
A window showing the result of the import will appear. Any newly created directories will be underlined.



Deleting a Directory

To delete a directory, proceed as follows:

1. Select the directory that is to be deleted.

ⓘ Be sure to delete the directory in the structure tree rather than in the content panel of the console window, otherwise the entire directory path will be deleted at the same time.
2. Click **Delete** in the context menu of the directory
or click **Delete** in the tool bar
or press the [Del] button.

A list of all objects that are to be deleted will appear.

- ⓘ If a directory is deleted, all sub-directories and objects such as devices, profiles or views contained in it will be deleted too.
3. Confirm that you wish to delete the relevant objects by clicking **OK**.

For details about directory deletion in the [UMS Web App](#)(see page 720), see [Deleting a Directory](#)(see page 744).

Moving Devices

Drag-and-drop is the easiest way of moving devices from one directory to another:

1. Press and hold down the [Ctrl] key if you would like to select a number of devices.
2. Use the [Shift] key to select a row of devices.



3. Confirm that you wish to move the relevant objects by clicking on **Yes**.

The **Time Changed** window will appear. If profiles are indirectly assigned to a device or revoked as a result of the device being moved to a different directory, its configuration too will change. The new configuration can take effect either immediately or when the device is next rebooted.

4. Select when you want the changes to take effect and confirm this by clicking on **OK**.

You can disable these confirmation dialogs in the relevant window. You can then undo this change again under **Misc > Settings > General**.

For details on how to move devices in the [UMS Web App](#)(see page 720), see [Moving Devices](#)(see page 745).

Assigning Updates

There are various options for assigning a registered firmware update to a device:

- Directly:
 - using drag & drop
 - using **Assigned Objects** in the device view
- Indirectly:
 - via a directory

i Assigning a firmware update will not trigger the update process. Only the information required for the update will be transferred to the device.

⚠ If you are using a Windows-based device, refer to the chapters [Snapshots](#)⁶¹ and [Partial Update](#)⁶² in the Windows 10 IoT manual.

The update process can be launched in two ways:

- Manually:
 - a. Right-click on the device in the UMS structure tree.
 - b. From the context menu, select **Update & snapshot commands > Update** or **Update when shutting down**.
- As a job:
 - a. Right-click on **Jobs** in the UMS structure tree.
 - b. Select **New Scheduled Job** from the context menu.
 - c. Enter a **Name**.
 - d. As **Command**, select **Update**, or **Update on Boot**, or **Update when shutting down**.
 - e. Complete the setup procedure for the job, see [Details](#)(see page 427) and [Schedule](#)(see page 428).
 - f. Assign the job to devices or directories, see [Assignment](#)(see page 428).

⁶¹ <https://kb.igel.com/display/w10iot404/Snapshots>

⁶² <https://kb.igel.com/display/w10iot404/Partial+Update>



Default Directories

From *UMS version 5.03.100*, the rules for default directories can be found under **UMS Administration > Default Directory Rules**(see page 485). Information is available for *UMS version 5.03.100* and for the previous versions in the associated chapters in the manual.

3.12.5 Configuring Devices

You can configure a device via the UMS in the following ways:

1. Via **Structure tree > [Device Context Menu] > Edit Configuration**: Here, you can edit the device setup as you would if you were working at the device itself.
2. Via a profile: You assign part-configurations to the device via a profile.
3. Via shadowing with VNC: By shadowing the client, you can work in the setup on the device itself.

You can edit the device configuration locally in the client setup or directly for this client in the IGEL UMS:

► Double-click on the device in the structure tree
or select **Edit configuration** from the menu / context menu
or select the corresponding symbol from the symbol bar.

The configuration dialog for a device in the UMS and the profile configuration procedure are structured in the same way as the local setup for a device. Details of this are set out in the relevant manual.

	With a click on this symbol you can reset settings to the default value from UMS version 5.09.100 on.
--	---

- ⓘ From UMS Version 5.05.100, the start page of the configuration dialog contains a link to the page last opened. The symbol for the link is at the very top of the list of links. A link will also be created if the last page opened belongs to another device or to another profile. If the page last opened is not available in the configuration dialog that is currently open, a link to the next page up in the structure tree will be created. Example: In the configuration dialog for device 1, a setting for the RDP session **My RDP Session** was changed (menu path: **Sessions > RDP > RDP Sessions > My RDP Session**). The configuration dialog for device 2 is then opened but device 2 does not have a session with the session name **My RDP Session**. A link to the higher-level page **RDP Sessions** will therefore be shown (menu path: **Sessions > RDP > RDP Sessions**).

To determine when changes to the configuration are to take effect, proceed as follows.

1. Change the configuration.
2. Click on **Save**.
3. Select when the settings are to take effect.
 - **Next Reboot**: The device will automatically retrieve its settings each time it boots.
 - **Now**: The settings will be transferred to the device immediately.

If the device is not switched on, this operation cannot be performed and the device will be given its settings the next time it reboots. In both cases, the settings will initially be saved in the database.



- ⓘ If you have selected **Immediately**, a pop-up dialog will ask the user whether the new settings should take effect immediately. You can change the user message using the following two registry parameters: `userinterface.rmagent.enable_usermessage` and `userinterface.rmagent.message_timeout`.

Copying a Session

You can copy a session in the configuration dialog of a device. This creates a duplicate with all properties of the original session.

To copy a session, proceed as follows:

1. Open the configuration dialog via **Structure tree > Devices > [Directory]** by double-clicking on the device.
2. In the configuration dialog, select **Sessions > [Session Type] > [Sessions of the Session Type]**.
Example: **RDP sessions**
The sessions already set up are shown.
3. Highlight the session that you want to copy.
4. Click A duplicate of the original session will be created and pasted below.

- ⓘ From *UMS Version 5.03.100*, you can also copy a session via the context menu in the structure tree of the device configuration.

3.12.6 Exporting and Importing Data

You can export and import data for devices. The settings and parameters are saved in an XML format.

- [Export Firmwares](#)(see page 392)
- [Import Firmwares](#)(see page 393)
- [Export Device Settings](#)(see page 393)
- [Import Devices as Profiles](#)(see page 394)

Export Firmwares

Menu path: **System > Export > Export Firmwares**

You can export the data for specific firmware versions. The exported data contain all settings parameters which are available in the UMS and in the local setup.

To export firmware data, proceed as follows:



1. Go to **System > Export > Export Firmwares**.
In the **Export firmwares** window, all available firmware data will be shown.
2. In the **Include** column, select the firmware data that you want to export.
3. With **Create archive**, specify how the firmware data are to be saved:
 - The firmware data will be saved as a ZIP archive.
 - Each firmware data set will be saved in a file of its own.
4. Click on **OK** and select a save location.
5. Click on **Save**.
The firmware data will be saved.

Import Firmwares

Menu path: **System > Import > Import Firmwares**

You can import the configuration data for specific firmware versions. The firmware configuration data contain all settings parameters that are available in the UMS and in the local setup of the device. These firmware data are needed to create profiles and when importing devices.

To import firmware data, proceed as follows:

1. Go to **System > Import > Import Firmwares**.
2. Select the file with the firmware data and click on **Open**.
If you have selected an individual file, the firmware data will be imported immediately.
3. If you have selected a ZIP archive, select the firmware data to be imported and click on **OK**.
The imported firmware data will be shown in the **Results** window.

Export Device Settings

Menu path: **System > Export > Export Device Settings**

You can export device settings. All changed settings are saved in the exported file, i.e. all settings which deviate from the default values.

To export device settings, proceed as follows:

1. If you would like to preselect device settings, highlight the desired devices or directories in the navigation tree.
2. Go to **System > Export > Export Device Settings**.
In the **Export Device Settings** window, the previously selected devices or all available devices will be displayed.
3. In the **Include** column, select the devices whose settings you want to export.
4. With **Create archive**, specify how the settings are to be saved:
 - A dedicated XML file will be created for each device. The XML files will be combined in a ZIP archive.
 - The settings for all devices will be saved in a single XML file.
5. Click on **OK** and select a save location.
6. Click on **Save**.



Import Devices as Profiles

Menu path: **System > Import > Import Devices as Profiles**

You can import device settings as profiles. In order for this to be possible, the settings must have been exported with **System > Export > Export Device Settings**; see [Export Device Settings](#)(see page 393).

To import device settings as profiles, proceed as follows:

1. Go to **System > Import > Import Devices as Profiles**.
2. Select the file with the settings and click on **Open**.
The **Import Devices as Profiles** window will open.
3. In the **Import** column, select the settings that are to be imported.
4. In the **Firmware (selectable)** column, select the firmware on which the profile will be based.
(default: the firmware installed on the device when the export takes place)
The profiles are set up in the **Profiles** directory. The name of each profile is identical to the name of the device from which the settings originate.
The profiles created from the import are shown in the **Results** window.

3.12.7 Send Message

Menu path: **Structure tree > Devices > [Directories] > [Name of the device] > Other Commands > Send Message**

You can send a message to any device. The message will be displayed to the user immediately. Messages to devices are enabled and configured under **UMS Administration > Global Configuration > Messages to Devices**; see [Messages to Devices](#)(see page 502).

You can launch the editor via the context menu in the **Device** node or via the main menu: **Devices > Other Commands > Send Message**.

- i** Devices with firmware from IGEL OS 10.03.100 can display these formatted messages. With older firmware versions, the message will be without formatting.

Under **Select Template**, you can choose from various format templates. These include preset templates and those that you created under **UMS Administration > Global Configuration > Messages to Devices**(see page 502):

- {01 template: Info}: For informative texts, with an information symbol
- {02 template: Warning}: For warning texts, with an attention symbol
- {03 template: Error}: For error messages, with an error symbol
- {04 template: Custom Icon}: Freely configurable message with its own symbol (see below)
- {05 template: Alert}: Red alarm message, with an information symbol and a table with a moving bell symbol
- {06 template: Blue}: Blue message window, with an IGEL symbol
- ... own templates ...



Own Icon

In order to distribute your own icon from the UMS, select a PNG file which should not be bigger than 4 kB.

Users who have the right to send messages can view all saved templates and change them for an immediate message. However, these changes will not be saved.

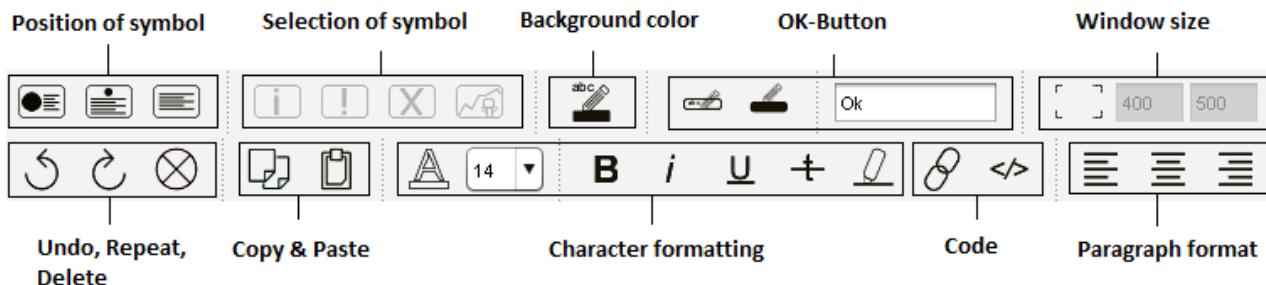
- i In order to save templates, the user will need to write rights on the [Messages to Devices](#)(see page 502) node.

In order to format the text, you can either use the integrated toolbar or you can create HTML snippets using an expert tool and insert them using copy and paste.

- i A message may have up to 7,000 characters including the formatting elements.

Message Editor

Menu path: **Structure tree > Devices > [Directories] > [Name of the device] > Other Commands > Send Message**



3.12.8 View Asset Information

i License Required

For IGEL OS 11 devices:

The Asset Inventory Tracker requires a valid license from the IGEL Enterprise Management Pack (EMP). When the license expires, the feature is no longer available; devices whose licenses have expired will no longer send updated asset information to the UMS. For information on license deployment, see [Setting up Automatic License Deployment](#)⁶³.

For IGEL OS 10 devices:

The Asset Inventory Tracker requires a separate license; when the license has expired, the UMS will no longer update the asset information. For information on license deployment, see [Licensing AIT](#)⁶⁴.

⁶³ <https://kb.igel.com/pages/viewpage.action?pageId=10325058>

⁶⁴ <https://kb.igel.com/display/licensesmorelegacy/Licensing+AIT>



With this function, you find information about peripherals connected to an endpoint device. The peripherals are sorted according to categories. A device can belong to more than one category and, accordingly, may be shown a number of times.

The Asset Inventory Tracker can be activated or deactivated under **UMS Administration > Global Configuration > UMS Features > Enable inventory tracking**.

- ▶ Click on the triangle symbols to expand or collapse hierarchy levels.

/Thin Clients/ITC000BCA050027

ITC000BCA050027

Seriennummer des Geräts	ITC02GVAAAAZ903
Struktur Tag	

▶ **Monitorinformationen**

▼ **Asset Inventory**

- ▼ **Bluetooth**
- ▼ **Bluetooth Dongle (HCI mode)**

Attribut	Wert
Name	Bluetooth Dongle (HCI mode)
Anschlusstyp	usb
Anbieter	Cambridge Silicon Radio, Ltd
Geräte ID	0001
custom_productName	CSR8510_A10
custom_vendorName	0a12
maxPower	100mA
revision	8891
speed	12

- ▶ **Human Interface Device**
- ▶ **Keyboard**
- ▶ **Mouse**
- ▶ **Features**
- ▶ **Windows Updates und Hotfixes**

Read out Asset Data via API

If you have a license for Asset Inventory Tracker (AIT), you can read out asset information as well as the asset history via a REST interface. For details, see [Asset Information⁶⁵](#) in the [IMI API V3 Reference⁶⁶](#).

⁶⁵ <https://kb.igel.com/display/igelimi/Asset+Information>

⁶⁶ <https://kb.igel.com/display/igelimi/IMI+API+V3+Reference>



3.12.9 Secure Terminal (Secure Shell)

You can establish a secure terminal connection to a device.

The device must meet the following requirements:

- The firmware of the devices is IGEL Linux v5.11.100 or higher or IGEL OS 10.01.100 or higher.

- i** You can allow access via the secure terminal for all registered devices. To do this, enable the **UMS Administration > Global Configuration > Remote Access > Enable secure terminal globally**.

For IGEL OS 10.01.100 or newer

1. In IGEL Setup, go to **System > Remote Access > Secure Terminal**.
2. Enable **Secure Terminal**.

For IGEL Linux v5

- In IGEL Setup, enable the following options under **System > Registry**:

- **network > telnetd > enabled > allow telnet access**
- **network > telnetd > secure_mode > secure telnet**

Configuring the Secure Terminal

With the following settings, you can configure and manage access to devices via a secure terminal.

- **Misc > Settings > Remote Access > External terminal client**: Command line for the external terminal client, made up of the path to the executable (e.g. putty.exe) and the appropriate parameters. IGEL recommends **PuTTY**⁶⁷.

For PuTTy under MS Windows, the minimal command line without further configuration is:

[Path and file name for putty.exe] -telnet <hostname> -P <port>

For PuTTy under Linux, the minimal command line without further configuration is:

[Path and file name for the PuTTy executable] -telnet <hostname> -P <port>

- i** <port> and <hostname> are placeholders that are automatically replaced by the port number and the IP address of the device during execution. Background: The actual connection to the device is provided by the UMS and is available to the external terminal client as a tunnel.

Examples:

PuTTy under MS Windows: C:\Program Files\PuTTY\putty.exe -telnet <hostname> -P <port>

⁶⁷ <http://www.chiark.greenend.org.uk/~sgtatham/putty/>



PuTTY under Linux: /bin/putty -telnet <hostname> -P <port>
 If the **External terminal client** field is empty, the internal terminal client of the *UMS* will be used.

- **Misc > Settings > Remote Access > Show end dialog if two or more sessions are open**
 - If two or more sessions are open, a closing dialog will be shown if you attempt to close a window of the external terminal client.
 - No closing dialog will be shown when you close the window of the external terminal client.
- **Misc > Settings > Remote Access > Show warning for sessions that end unexpectedly**
 - A warning will be shown if a session with an external terminal client was terminated without any user input.
 - No warning will be shown.
- **UMS Administration > Global Configuration > Remote Access > Enable secure terminal globally**
 - Access via the secure terminal is enabled for all registered devices. The firmware must be *IGEL Linux version 5.11.100* or higher.
 - Access via the secure terminal is not enabled for all registered devices. However, it can be enabled for individual devices.
- **UMS Administration > Global Configuration > Remote Access > Log user for secure terminals:**
 Specifies whether the user name of the *UMS* user who established the connection to the device is logged. The log is shown under **System > Logging > Remote Access**.
 - The user name is contained in the log.
 - The user name is not contained in the log.
- **System > Logging > Remote Access:** Shows the log of all secure access to devices.
 The following data are logged:
 - **Device Name**
 - **MAC Address**
 - **Unit ID**
 - **Device IP**
 - **User:** The user name of the *UMS* user who established the connection to the device is logged. This is only logged if **Log user name for SSH remote access** is enabled.
 - **VNC Start time:** Point in time at which the connection was established
 - **Duration in seconds**
 - **Comment**
 - **Protocol:** Connection protocol

Using the Secure Terminal

To establish a secure terminal connection to a device, proceed as follows:

1. In the navigation tree, right-click the device that you would like to connect to.
2. Select **Secure Terminal** from the context menu.
 The terminal window opens. The **Security Certificate** dialog shows the device's certificate.
3. Click on **Accept** to accept the device certificate.



4. Log in with user.

The secure terminal connection to the device is established. You can become root by entering su.

3.12.10 Shadowing (VNC)

The IGEL UMS Console allows you to observe the desktop of a device on your local PC via shadowing with VNC. In order to enable shadowing, you must allow remote access in the security options for the device.

Limitations for Special Characters

Some special characters might not be transmitted through the VNC connection. The processing of special characters depends on the following factors:

- Keyboard layout configured on the VNC client and on the VNC server
- VNC viewer in use: An external viewer and the internal viewer behave differently.
- Firmware version of the endpoint device
- UMS user interface: The UMS Console and the UMS Web App have different VNC viewers.

See also the how-to document [Secure Shadowing](#)⁶⁸.

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=dqH6fBUBHXw>

Launching a VNC Session

Limitations for Special Characters

Some special characters might not be transmitted through the VNC connection. The processing of special characters depends on the following factors:

- Keyboard layout configured on the VNC client and on the VNC server
- VNC viewer in use: An external viewer and the internal viewer behave differently.
- Firmware version of the endpoint device
- UMS user interface: The UMS Console and the UMS Web App have different VNC viewers.

To launch a VNC session, proceed as follows:

1. In the context menu, click **Shadowing**.
A connection dialog will appear.
2. Enter the password if you have set one in the security options.

⁶⁸ <https://kb.igel.com/pages/viewpage.action?pageId=24385099>



If you have a user account, you can connect to the *UMS* Server and launch the *IGEL* VNC Viewer separately. The *IGEL* applications folder in the *Windows* Start Menu contains a link to it.

1. Enter a **host name** or the **IP address** manually on the first tab.
2. On the second tab, select a **device** from the structure tree.

IGEL VNC Viewer

If you have launched a VNC session, the shadowed desktop will be shown in the *IGEL* VNC Viewer window. This window has its own menu with the following items:

File	Overview	Shows an overview of all VNC sessions currently connected. Double-click of the displayed desktops for a full-screen view of it.
	Terminate	Terminates all VNC sessions and closes the window.
Tab	New	Opens the connection dialog so that you can launch another VNC session.
	Adjust	With this option, you can adjust the size of the window in which the desktop currently selected is displayed.
	Send Ctrl-Alt-Del	Sends the key combination [Ctrl]+[Alt]+[Del] to the remote host currently displayed.
	Refresh	Refreshes the window content.
	Screenshot	Saves a screenshot of the window contents on the local hard drive.
	Options	Opens a dialog window in which you can specify further options such as coding, color depth, update interval etc.
	Close	Closes the currently selected tab.
Help / Info		Shows the software version of the <i>IGEL</i> VNC Viewer.

You can specify the following parameters as options:

Preferred Coding	The coding used when sending image data from the device to your PC. The coding option Tight is particularly useful in a network with a low bandwidth. It contains two additional parameters: <ul style="list-style-type: none"> • Compression level: The higher the compression, the longer the computing operation takes! • JPEG quality: If you select Off, no JPEG data will be sent.
-------------------------	--



Use Draw Rectangle Method	This option improves performance. However, artifacts may be encountered.
Color Depth	8 or 24 bits per pixel
Update Period	Time period between two updates. A longer time period reduces network traffic, but the update may not be seamless. Please note: An update query will be sent as soon as you move the mouse or enter a key in the VNC Viewer. This event will be passed on to the remote host.
Save Properties as Standard Values	Saves the current settings as standard values for future VNC sessions.

External VNC Viewer

⚠ Limitations for Special Characters

Some special characters might not be transmitted through the VNC connection. The processing of special characters depends on the following factors:

- Keyboard layout configured on the VNC client and on the VNC server
- VNC viewer in use: An external viewer and the internal viewer behave differently.
- Firmware version of the endpoint device
- UMS user interface: The UMS Console and the UMS Web App have different VNC viewers.

You can specify an external VNC Viewer program from another provider in the UMS Console:

- Click on **Misc > Settings > Remote Access**.

To pass on the IP address of the device to an external application, add the parameters and in **External VNC Viewer**.

Examples:

- TightVNC: "C:\Program Files\TightVNC\tvnviewer.exe" <hostname>:<port>
- UltraVNC: "C:\Program Files\uvnc\UltraVNC\vncviewer.exe"
 -connect <hostname>:<port>
- RealVNC: "C:\Program Files\RealVNC\VNC
 Viewer\vncviewer.exe" <hostname>:<port>
- TigerVNC: "C:\Program Files\TigerVNC\vncviewer.exe" <hostname>:<port>

i Place the program path in double quotation marks as shown above to ensure that the call-up works even if there are spaces in the path.

Secure Shadowing (VNC with SSL/TLS)

Menu path: **Setup > System > Shadowing**



⚠ Limitations for Special Characters

Some special characters might not be transmitted through the VNC connection. The processing of special characters depends on the following factors:

- Keyboard layout configured on the VNC client and on the VNC server
- VNC viewer in use: An external viewer and the internal viewer behave differently.
- Firmware version of the endpoint device
- UMS user interface: The UMS Console and the UMS Web App have different VNC viewers.

The **Secure Shadowing** function is only relevant to clients which meet the requirements for secure shadowing and have enabled the corresponding option. Secure shadowing improves security when remote maintaining a client via VNC at a number of locations:

- **Encryption:** The connection between the shadowing computer and the shadowed client is encrypted.
This is independent of the VNC Viewer used.
- **Integrity:** Only clients in the UMS database can be shadowed.
- **Authorization:** Only authorized persons (UMS administrators with adequate permissions) can shadow clients.
Direct shadowing without logging in 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 client by another computer is likewise not permitted.
- **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.

3.13 Shared Workplace Users

IGEL Shared Workplace is an optional, licensed feature of the IGEL OS firmware. It allows user-dependent configuration using profiles created in the IGEL Universal Management Suite and linked to the AD user accounts. In the process, user-specific profile settings are passed on to the device along with the device-dependent parameters.

You will find the complete documentation here: [Shared Workplace](#)(see page 693).

- ❗** If you deactivate **Enable Shared Workplace** under **UMS Administration > Global Configuration > UMS Features**, the structure tree node **Shared Workplace Users** will be hidden and Shared Workplace users will NOT be able to log in!

3.14 Views

Menu path: Structure tree > **Views**

A view is a selection of devices according to definable criteria which are logically linked one after another. You can generate views, edit or delete views and export results of a view in various formats (e.g. XML). This tree structure can also contain sub-directories for arranging views.



You can use a view to define a scheduled job for a specific selection of devices, e.g. a firmware update.

To specify which columns are shown in the view, proceed as follows:

1. Click on the selection button in the top right-hand corner of the window.



The **Choose visible columns** dialog will open.

2. Select the columns that are to be displayed.

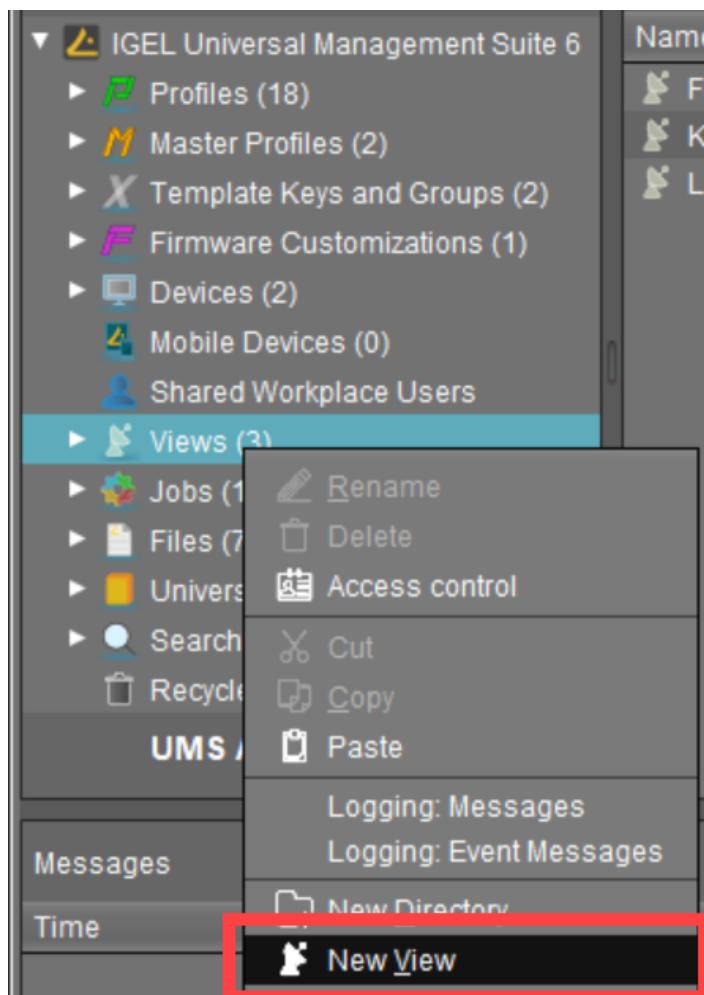
-
- [How to Create a New View in the IGEL UMS\(see page 403\)](#)
 - [Copying a View\(see page 421\)](#)
 - [Copying a View Directory\(see page 422\)](#)
 - [Saving the View Results List\(see page 422\)](#)
 - [Sending a View as Mail\(see page 423\)](#)
 - [Assigning Objects to a View\(see page 424\)](#)

3.14.1 How to Create a New View in the IGEL UMS

Menu path: **Structure Tree > Views > [Context Menu] > New View**

The following article details how to create a view in the IGEL Universal Management Suite (UMS). A view is a selection of devices according to definable criteria which are logically linked one after another, see [Views\(see page 402\)](#). You can create a view using a standard procedure or graphical / text expert mode.

For information on how you can configure the display of view results, see [Views and Searches\(see page 320\)](#).



- ⓘ View editing is possible only in expert mode. In order to change the created view, e.g. for adding further criteria, select **Views > [name of the view] > [context menu] > Edit view.**

How to Create a View: Standard Procedure

Typically, you create a view as follows:

1. In the UMS Console, go to **Views > [context menu] > New View** or **System > New > New View**.
The **Create new view** window will open.
2. Give a **Name** and a **Description**.
3. Click **Next**.
4. In the **Select criterion** window, select a parameter.
You will find a list of all available search parameters under [Possible Search Parameters](#)(see page 414).



Create new view

Select criterion

Basic Information

- Comment
- Department
- DeviceAttributes
- Expiration date of OS 10 maint...
- IGEL Cloud Gateway
- Keystore Alias
- Name
- Site
- Configuration changes pending
- Device License
- Direct Profile Assignment
- Feature
- In-Service Date
- Last Known IP Address
- Online
- Structure Tag
- Cost Center
- Device Serial Number
- Directory
- Has ICG certificate with SHA1 f...
- Indirect Profile Assignment
- MAC address
- Serial Number
- Unit ID

Asset Inventory

- Asset ID
- BIOS Date
- BIOS Vendor

Buttons: Back, Next, Finish, Cancel

5. Click **Next**.

6. In the entry field in the **Text search** window, enter a text with which the parameter value is to be compared and select one or more search options.

Depending on the parameter, the following search options are available:

- **Consider case**

- The case of the parameter value must match the case of the text entered.
- The case of the parameter value can differ from the case of the text entered.

- **Compare whole text**

- The parameter value must match the text entered completely.
- The parameter value does not need to match the text entered completely; it is sufficient if the text entered is contained in the parameter value.

- **Use regular expression**

- The **Consider case** and **Compare whole text** options are grayed out. You can enter a regular expression of your own in the entry field. Example: RDD.* selects all devices whose serial number contains the string RDD.

General information on regular expressions can be found e.g. under [Class Pattern⁶⁹](#) in the Oracle documentation.

- You cannot enter a regular expression in the entry field. However, you can use regular expressions when subsequently editing the view.

- **Not like**

- The parameter value must differ from the pattern entered.
- The parameter value must match the pattern entered.

- **Exact:** The parameter value must match the value entered.

⁶⁹ <https://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html>



- **Above:** The parameter value must be above the value entered.
- **Below:** The parameter value must be below the value entered.
- **Not like:** The parameter value must differ from the value entered.

7. Click **Next**.

8. In the **Finish view creation** window, select one of the following options:

- **Create view:** The view will be generated when you click **Finish**.
- **Narrow search criterion (AND):** You can specify a further selection criterion that must likewise apply. This selection criterion and the previously defined selection criterion are linked with a logical AND.
- **Create additional search criterion (OR):** You can specify a further selection criterion that must apply as an alternative. This selection criterion and the previously defined selection criterion are linked with a logical OR.

9. Depending on the option selected, click **Finish** or **Next**. You can add as many criteria with AND/OR links as you want.

For an example, see [Example: Creating a View\(see page 416\)](#).

How to Create a View: Expert Mode

You can also create a new view using expert mode – either in graphical form or in text mode. It is possible to switch back and forth between graphical and text mode as long as the entered data in either mode is complete and valid.

How to Create a View Using Graphical Mode

To create a view using graphical mode, proceed as follows:

1. In the UMS Console, go to **Views > [context menu] > New View** or **System > New > New View**.
The **Create new view** window will open.
2. Click **Expert mode**.
The **New View** window will open.



3. Select **Graphical mode**.

The screenshot shows the 'New View' dialog box. At the top, there are tabs for 'Graphical mode' (which is selected and highlighted with a red box) and 'Text mode'. Below the tabs, there are fields for 'Name' and 'Description'. The main area is titled 'Rule' and contains a search interface. It includes a dropdown for 'Criterion' (set to 'Device License'), an 'Operator' dropdown (set to 'equal to'), and a 'Value' input field ('WORKSPACE_EDITION'). There are also sections for 'Monitor Serial Number', 'Direct Profile Assignment', 'Monitor Vendor', 'Battery Level', and 'Partial Update (Relative)'. The interface uses logical operators 'AND' and 'OR' to link criteria. Buttons for 'Add column', 'Add row', 'Ok', and 'Cancel' are visible at the bottom.

4. Give a **Name** and a **Description**.

5. Under **Criterion**, select a parameter.

You will find a list of all available search parameters under [Possible Search Parameters](#)(see page 414).

6. Select an **Operator** and define the **Value**. The list of operators can vary depending on the selected criterion.

- **equal to:** The parameter value must match the value entered.
- **like:** The parameter value must match the pattern entered.
- **not like:** The parameter value must differ from the pattern/value entered.
- **less than:** The parameter value must be less than the value entered.
- **greater than:** The parameter value must be greater than the value entered.

7. Click **Add column / Add row** to define further criteria / values.

- Criteria / values in the same row are linked with a logical AND.
- Criteria / values in different rows are linked with a logical OR.

8. Click **OK**.

How to Create a View Using Text Mode

To create a view using text mode, proceed as follows:

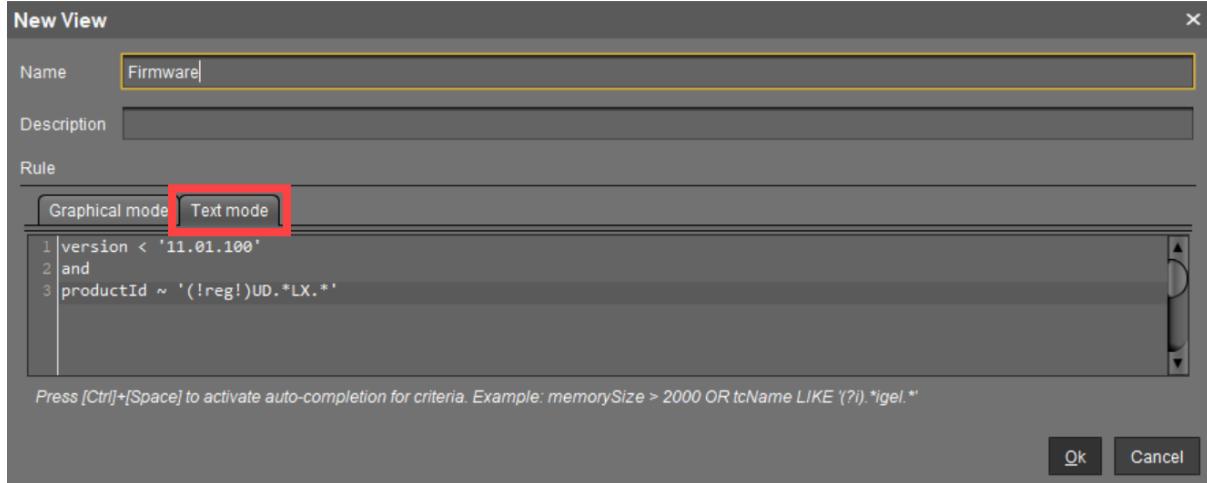
1. In the UMS Console, go to **Views > [context menu] > New View** or **System > New > New View**. The **Create new view** window will open.



2. Click **Expert mode**.

The **New View** window will open.

3. Select **Text mode**.



4. Give a **Name** and a **Description**.

5. Under **Rule**, enter your query.

Text mode allows entering a rule in an SQL-like query, consisting of one or more expressions, see [Queries in Text Mode of Views: Expression Parts](#)(see page 408) below.

You can press [Enter] to type from the new line. Line breaks can be entered at any time for convenience, but they are not preserved as the query is generated dynamically whenever a switch to text mode occurs.

6. Click **OK**.

Queries in Text Mode of Views: Expression Parts

- An expression consists of three parts: CRITERION OPERATOR VALUE

Example: `memorySize > 1000`

This query will find all devices with a system memory greater than 1000 MB.

- Multiple expressions can be combined with logical operators AND and OR. Note that AND takes precedence over OR and binds its surrounding expressions stronger.

Example: `memorySize > 1000 and department = '(?i)sales'` or `tcName ~ 'Dev.*'`

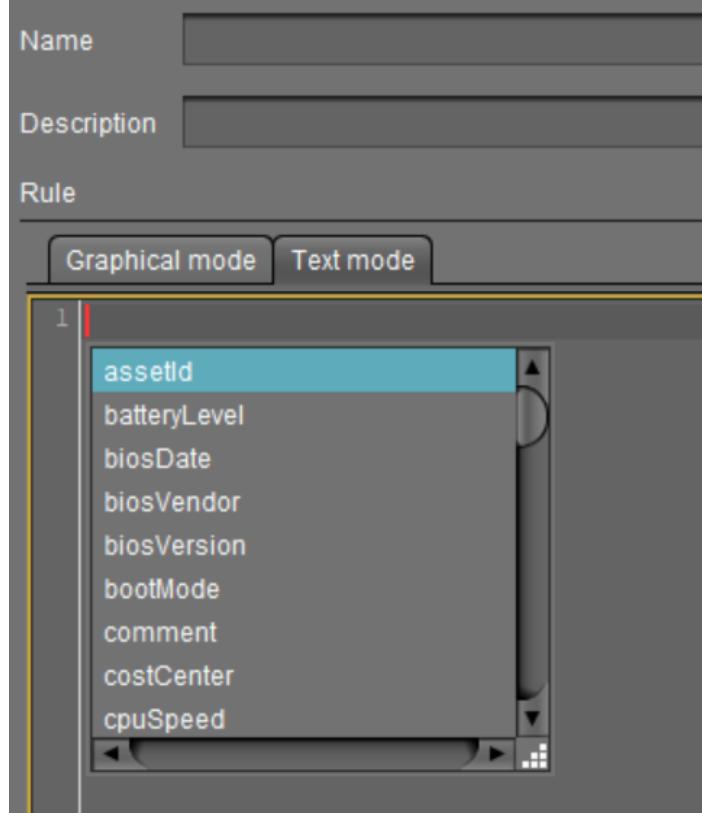
The search result of this query will contain all devices that fulfill the memory and department constraints simultaneously and additionally all devices whose name starts with 'Dev'.

Criterion

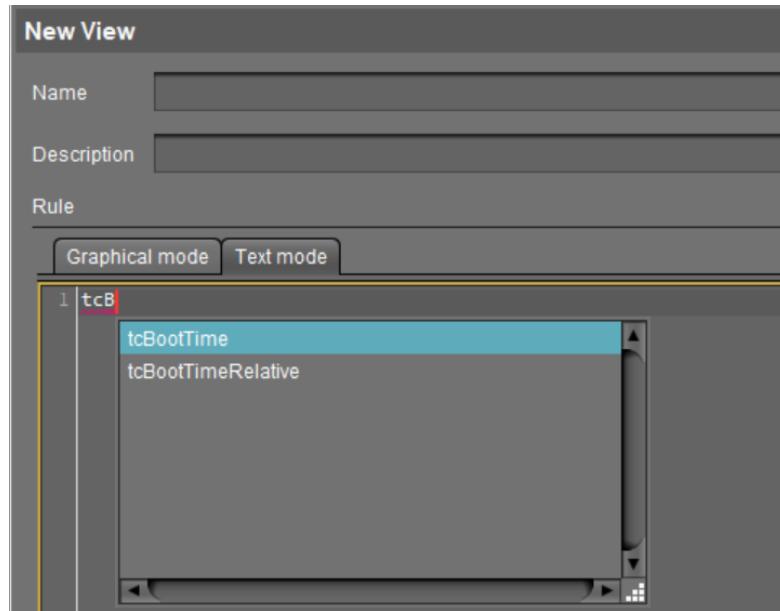
- Possible criteria and their internal identifiers can be found under [Text Mode of Views: Matrix of Possible Criteria and Operators](#)(see page 417).
- [Ctrl] + [Space] for auto-completion:



- At any time when a criterion is expected, you can press [Ctrl] + [Space] to activate auto-completion.
A popup window listing all possible criteria opens. Device attributes are also listed here via their internal identifier if such an identifier has been specified under **UMS Administration > Global Configuration > Device Attributes > UMS internal identifier**, see [Device Attributes](#)(see page 463).

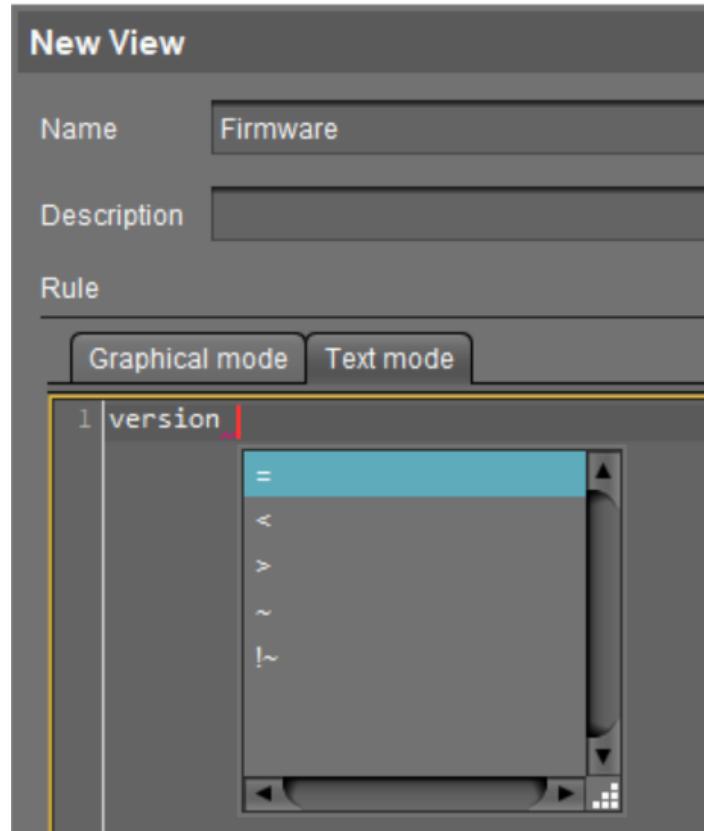


- Auto-completion also works when a criterion is entered only partially. It will then show only criteria matching the already entered fragment. If only one criterion matches the fragment, it will be completed without showing the popup window.

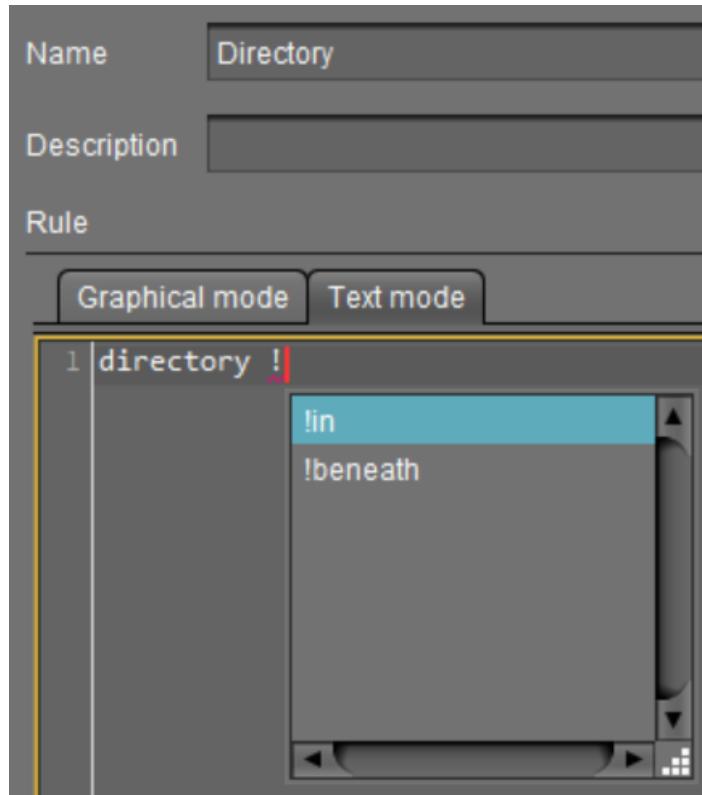


Operator

- For the list of operators possible for the criterion entered, see [Text Mode of Views: Matrix of Possible Criteria and Operators](#)(see page 417).
- [Ctrl] + [Space] for auto-completion:
 - At any time when an operator is expected, i.e. after a criterion and an entered space, you can press [Ctrl] + [Space] to activate auto-completion.
A popup window listing all operators which are possible for the entered criterion opens.



- Auto-completion also works when an operator is entered only partially. It will then show only operators matching the already entered fragment. If only one operator matches the fragment, it will be completed without showing the popup window.



- The available operators are listed in the following table. The "Operator" column shows the operator names as they are provided in the selection lists of graphical mode. Multiple variations of operators are recognized for convenience or readability. Therefore, "LIKE" can also be written, for example, as "~".

Operator	Pattern(s)				
equal to	=				
less than	<				
greater than	>				
like	~	like	Like	LIKE	
not like	!~	!like	!Like	!LIKE	
in	in	In	IN		
not in	!in	!In	!IN		
beneath	beneath	Beneath	BENEATH		
not beneath	!beneath	!Beneath	!BENEATH		
is true	= true				
is false	= false				

Value

- Text- and date-based values have to be enclosed in double ("") or single ('') quotation marks.
- Numeric values (integer, decimal values) do not require quotation marks.



Examples of Queries in the Text Expert Mode of Views

Device's **Name** contains "igel", where (?i) is a flag expression for case-insensitive matching:

```
tcName LIKE '(?i).*igel.*'
```

Consider case:

```
tcName LIKE '.*IGEL.*'
```

Compare whole text:

```
tcName LIKE '(?i)td-IGEL01'
```

Devices with a specific **Monitor Size**:

```
monitorSize = 24.1
```

Devices with a specific **Last Boot Time (Absolute)**:

```
tcBootTime > '2021-05-01' and tcBootTime < '2021-06-25'
```

Devices with device attribute values "KB" or "KM", where `deviceAttributeSubdepartments` is an identifier specified under **Device Attributes > UMS internal identifier**, see [Device Attributes\(see page 463\)](#):

```
deviceAttributeSubdepartments ~ 'KB' or deviceAttributeSubdepartments ~ 'KM'
```

Examples of Regular Expressions in the Text Expert Mode of Views

Regular expressions are introduced by (!reg!). For general information on regular expressions, see e.g. [Class Pattern⁷⁰](#) in the Oracle documentation. Note that not all regular expression constructs described there are supported by the UMS, or their behavior in the UMS may be different.

- Any character zero or more times: .*
- All devices whose product ID contains "UD-LX", e.g. UD3-LX51

```
productId LIKE '(!reg!)UD.*LX.*'
```

⁷⁰ <https://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html>



- Any character one or more times: .+

All devices whose name contains any character one or more times after "igel", e.g. igel1, igel20
3

```
tcName ~ '(!reg!)igel.+'
```

- Any character one time or not at all: .?

All devices whose name contains any character one time or not at all after "igel", e.g. igel and igel1

```
tcName like '(!reg!)igel.?'
```

- A digit [0-9]: \d

All devices whose name contains a digit after "igel", after which any character follows one or more times, e.g. igel20, igel00E0C520986A, igel3DE

```
tcName ~ '(!reg!)igel\d.+'
```

- Range: [a-zA-Z]

All devices whose name contains a hexadecimal number (e.g. for MAC addresses) one or more times after "igel", e.g. igel00E0C520986A

```
tcName ~ '(!reg!)igel[0-9A-F]+'
```

Possible Search Criteria

The following parameters can be used as search parameters for a view:

Basic Information

- **Configuration changes pending**
- **Comment**
- **Cost Center**
- **Department**
- **Device License**
- **Device Serial Number**
- **Direct Profile Assignment**
- **Directory**
- **Expiration date of OS 10 maintenance subscription**
- **Feature**
- **Has ICG certificate with SHA1 fingerprint**
- **IGEL Cloud Gateway**
- **In-Service Date**
- **Indirect Profile Assignment**



- **Keystore Alias**
- **Last Known IP Address**
- **MAC address**
- **Name**
- **Online**
- **Serial Number**
- **Site**
- **Structure Tag**
- **Unit ID**
- **[Name of the Device Attribute]**. For details on device attributes, see [Device Attributes](#)(see page 463).

Asset Inventory

- **Asset ID**
- **BIOS Date**
- **BIOS Vendor**
- **BIOS Version**
- **Battery Level**
- **Boot Mode**
- **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)** (see [Monitoring Device Health and Searching for Lost Devices](#)(see page 177))
- **Last Boot Time (Relative)** (see [Monitoring Device Health and Searching for Lost Devices](#)(see page 177))
- **Last contact time (absolute)**
- **Last contact 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**
- **Monitor Serial Number**
- **Monitor Size**
- **Monitor Vendor**

Monitor Information (legacy)

- **Monitor 1 Date of Production**
- **Monitor 1 Model**
- **Monitor 1 Native Resolution**
- **Monitor 1 Serial Number**
- **Monitor 1 Size**
- **Monitor 1 Vendor**
- **Monitor 2 Date of Production**
- **Monitor 2 Model**
- **Monitor 2 Native Resolution**
- **Monitor 2 Serial Number**
- **Monitor 2 Size**
- **Monitor 2 Vendor**

Example: Creating a View

Menu path: **Structure Tree > Views > Context Menu > New View**

In the following example, a view which covers all devices with IGEL OS whose firmware version is lower than 11.01.100 is created. With this view, you can determine which devices are to receive an upgrade.

1. Click on **Views** in the structure tree.
2. Select **New View** in the context menu.
3. Under **Name**, give a suitable name for the view, e.g. UDLX Update.
4. Click on **Next**.
5. In the **Select criterion** window, select the parameter **Firmware Version**.
6. Click on **Next**.
7. In the **Version search** window, select the **below** option under **Version number** and enter 11.01.100 in the text box.
8. Click on **Next**.
9. In the **Finish view creation** window, select the **Narrow search criterion (AND)** option.
10. Click on **Next**.
11. In the **Select criterion** window, select the parameter **Product ID**.
12. In the **Text search** window, enter the text UD.*LX.* and enable **Use regular expression**.



13. Click on **Next**.

14. Click on **Finish**.

The result is shown in the content panel. See also [Views and Searches](#)(see page 320) to learn about the options for displaying the view results.

Text Mode of Views: Matrix of Possible Criteria and Operators

Criterion name	Internal identifier	equal to	less than	greater than	like	not like	i n	not in	beneath	not beneath	is true	is false
Asset ID	assetId	x	x	x	x	x						
BIOS Date	biosDate	x	x	x								
BIOS Vendor	biosVendor	x	x	x	x	x						
BIOS Version	biosVersion	x	x	x	x	x	x					
Battery Level	batteryLevel		x	x								
Boot Mode	bootMode	x	x	x	x	x	x					
CPU Speed	cpuSpeed		x	x								
CPU Type	cpuType	x	x	x	x	x	x					
Comment	comment	x	x	x	x	x	x					
Configuration changes pending	tcConfigChange									x	x	
Cost Center	costCenter	x	x	x	x	x	x					
Department	department	x	x	x	x	x	x					
Device License	licenseInfo	x										
Device Serial Number	deviceSerialNumber	x	x	x	x	x	x					
Device Type	deviceType	x	x	x	x	x	x					
Direct Profile Assignment	profile2TCA	x				x						
Directory	directory						x x	x	x	x		
Duplex Mode	duplexMode	x										
Expiration date of OS 10 maintenance subscription	subscriptionExpirationDate	x	x									
Feature	tcFeature	x				x						



Criterion name	Internal identifier	equal to	less than	greater than	like	not like	i n	not in	beneath	not beneath	is true	is false
Firmware Description	customFirmwarename	x	x	x	x	x						
Firmware Update (Relative)	tcFwupdateTimeRelative		x	x								
Firmware Version	version	x	x	x	x	x						
Flash Player	parameter					x	x					
Flash Player Version	flashPlayerVersion	x	x	x	x	x						
Flash Size	flashSize		x	x								
Graphics Chipset 1	graphicsChipset1	x	x	x	x	x	x					
Graphics Chipset 2	graphicsChipset2	x	x	x	x	x	x					
Graphics Memory Size 1	graphicsMemorySize1		x	x								
Graphics Memory Size 2	graphicsMemorySize2		x	x								
Has ICG certificate with SHA1 fingerprint	usgCertFingerprint	x				x						
IGEL Cloud Gateway	usg									x	x	
IGEL Cloud Gateway, last boot via ICG	usgLastBoot									x	x	
In-Service Date	inServiceDate	x	x	x	x	x	x					
Indirect Profile Assignment	indProfile2TCAssignment	x				x						
Keystore Alias	keystoreAlias	x	x	x	x	x	x					



Criterion name	Internal identifier	equal to	less than	greater than	like	not like	i n	not in	beneath	not beneath	is true	is false
Last Boot Time (Absolute)	tcBootTime	x	x	x								
Last Boot Time (Relative)	tcBootTime		x	x								
Last Known IP Address	ipAddress	x	x	x	x	x						
Last contact time (absolute)	tcLastContact	x	x	x								
Last contact time (relative)	tcLastContactRelative		x	x								
License Id	licenseInfoLicenseId	x										
License expiration date	licenseInfoExpirationDate	x	x	x								
MAC address	macAddress	x	x	x	x	x						
Memory Size	memorySize	x	x									
Monitor 1 Date of Production	monitor1DateOfProduction	x	x	x	x	x						
Monitor 1 Model	monitor1Model	x	x	x	x	x						
Monitor 1 Native Resolution	monitor1NativeResolution	x	x	x	x	x						
Monitor 1 Serial Number	monitor1SerialNumber	x	x	x	x	x						
Monitor 1 Size	monitor1Size	x	x			x						
Monitor 1 Vendor	monitor1Vendor	x	x	x	x	x						
Monitor 2 Date of Production	monitor2DateOfProduction	x	x	x	x	x						



Criterion name	Internal identifier	equal to	less than	greater than	like	not like	i n	not in	beneath	not beneath	is true	is false
Monitor 2 Model	monitor2Model	x	x	x	x							
Monitor 2 Native Resolution	monitor2NativeResolution	x	x	x	x							
Monitor 2 Serial Number	monitor2SerialNumber	x	x	x	x	x						
Monitor 2 Size	monitor2Size	x	x	x			x					
Monitor 2 Vendor	monitor2Vendor	x	x	x	x	x						
Monitor Date of Production	monitorDateOfProduction	x	x	x	x	x	x	x				
Monitor Model	monitorModel	x	x	x	x	x						
Monitor Native Resolution	monitorNativeResolution	x	x	x	x	x						
Monitor Serial Number	monitorSerialNumber	x	x	x	x	x						
Monitor Size	monitorSize	x	x	x			x					
Monitor Vendor	monitorVendor	x	x	x	x	x	x	x				
Name	tcName	x	x	x	x	x	x	x				
Network Name	tcNetworkName	x	x	x	x	x	x	x				
Network Speed	networkSpeed		x	x								
OS Type	osType	x	x	x	x	x	x	x				
Online	online									x	x	
Partial Update (Name)	partialUpdateName					x	x					
Partial Update (Relative)	partialUpdateTimeRelative		x	x								



Criterion name	Internal identifier	equal to	less than	greater than	like	not like	i n	not in	beneath	not beneath	is true	is false
Partial Update (Version)	partialUpdateVersion	x			x	x						
Product	model	x	x	x	x	x						
Product ID	productId	x	x	x	x	x	x					
Serial Number	serialNumber	x	x	x	x	x	x					
Site	site	x	x	x	x	x	x					
Structure	umsStructure	x	x	x	x	x	x					
Tag	alTag											
Total Operating Time	totalUsageTime		x	x								
Unit ID	unitId	x	x	x	x	x	x					
[Name of the Device Attribute]	Identifier specified under UMS Administration > Global Configuration > Device Attributes > UMS internal identifier (see page 463)	x	x	x	x	x	x					

3.14.2 Copying a View

Menu path: **Structure Tree > Views > [Name of the View] > Context Menu > Copy**

You can copy a view and paste it in any view directory.

To copy a view, proceed as follows:

1. Click on the view that you want to copy.
2. Open the context menu for the view and select **Copy**.
3. Click on the view directory in which you would like to paste the copy of the view. This can also be the directory of the original view.



4. Open the context menu for the directory and select **Paste**.

A new view which has the same name and properties as the original view will be created.

3.14.3 Copying a View Directory

Menu path: **Structure Tree > Views > [Name of the View Directory] > Context Menu > Copy**

You can copy a view directory and paste it in any directory.

To copy a view directory, proceed as follows:

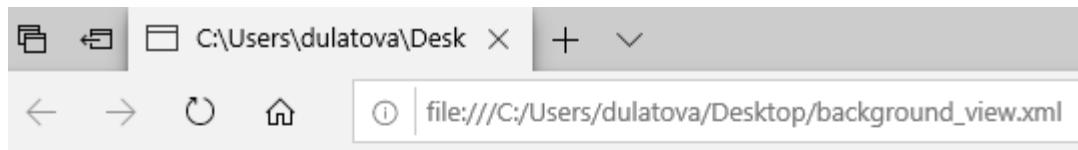
1. Click on the view directory that you want to copy.
2. Open the context menu for the directory and select **Copy**.
3. Click on the directory in which you would like to paste the copy of the view directory. This can also be the directory in which the original view directory is located.
4. Open the context menu for the directory and select **Paste**.

A new view directory which has the same name as the original view directory will be created. The new view directory will contain newly created copies of the view contained in the original directory as well as copies of the sub-directories.

3.14.4 Saving the View Results List

- Select **Save as...** in the context menu of a view in order to save the current view results in file form. Four file formats are available for the export: XML, HTML, XSL-FO, and CSV.

Example of an XML file for a view:



```

<?xml version="1.0" encoding="ISO-8859-1"?>
- <table>
  <creation-date>October 1, 2019</creation-date>
  <caption>background_profile_view</caption>
  <description/>
  <columnheader>Name</columnheader>
  <columnheader>Last Known IP Address</columnheader>
  <columnheader>MAC Address</columnheader>
  <columnheader>Product</columnheader>
  <columnheader>Version</columnheader>
  - <row>
    <cell>ITC00E0C520986A</cell>
    <cell>172.30.91.211</cell>
    <cell>00E0C520986A</cell>
    <cell>IGEL OS 11</cell>
    <cell>11.02.100.rc8</cell>
  </row>
</table>

```

- ⓘ The **Save as...** option is always active in the context menu if **Automatically load amount and items** is selected under **Menu Bar > Misc > Settings > Views and Searches > Page Behavior > When opening a view result...**. If one of the other parameters is chosen, the **Save as...** option will only be active after clicking a button **Load devices** (or **Search for hits > Load devices**) in the content panel of the view. See also [Views and Searches](#)(see page 320).

3.14.5 Sending a View as Mail

- ⓘ Emails can only be sent if you have configured appropriate [mail settings](#)(see page 501) under **UMS Administration > Global Configuration > Mail Settings**.

To send a view as mail, proceed as follows:

1. Right-click on a view.
2. Select **Send view result as mail...** in the context menu.
The **Send view result as mail...** window opens.
3. Enter the recipient address in the **Mail recipient** field. A number of recipient addresses can be entered, separate them with a semicolon ";".
4. Under **Result format**, select the format in which the view is to be sent.



5. Check the **Create archive** box to send the view as a zip file.

The screenshot shows the UMS interface with the following details:

- Left Panel (Server - 172.30.91.216):**
 - IGEL Universal Management Suite
 - Profiles (3)
 - Master Profiles (0)
 - Template Keys and Groups (0)
 - Firmware Customizations (1)
 - test_custom
 - Devices (1)
 - New Directory (1)
 - ITC00E0C520986A
 - Mobile Devices (0)
 - Shared Workplace Users
 - Views (1)
 - firmware (1) **(highlighted in blue)**
 - Jobs (0)
 - Files (0)
 - Universal Firmware Update (1)
 - IGEL OS 11-11.02.150
 - Search History (4)
 - Geräte suchen - 09.10.2019: I
 - Search devices - 09.10.2019: I
- Right Panel (View Details):**
 - Name: firmware
 - Description:
 - Rule: Firmware version is greater than 10.6.100 AND Product ID is like (?reg!)UD.*LX.*
 - Result list was last updated at 03:05. Refresh
- Matching devices (1 device):**

Name	Last known IP address
ITC00E0C520986A	172.30.91.211
- Send View result as Mail ... dialog:**
 - Mail recipient: user@example.com
 - Result format: XML
 - Create archive:

i You can also send views automatically and regularly as an [administrative task](#)(see page 476).

3.14.6 Assigning Objects to a View

Via the context menu of a view, you can assign on a one-off basis objects to devices that you have filtered via the view. If you want to be certain that the object is assigned even to newly recorded devices that fulfill the view criterion, you can do this using an [administrative task](#)(see page 480).

i Using the same principle, you can assign objects to devices that you have filtered via a [search](#)(see page 435).

To assign an object to a view result, proceed as follows:

1. Create a corresponding view.
2. Right-click on the view to open the context menu.
3. Select **Assign objects to the devices of the view...** .



The **Assign objects** window will open.

4. Select the desired object from the left-hand column and move it to **Selected objects** on the right by clicking on .
 5. Click **OK**.
- The **Update time** window will open.
6. Select **Next Reboot** or **Now**.
 7. Click **OK**.

 Via **Detach objects from the devices of the view...**, you can undo the assignment of objects.

 Options **Assign objects to the devices of the view...** and **Detach objects from the devices of the view...** are always active in the context menu if **Automatically load amount and items** is selected under **Menu Bar > Misc > Settings > Views and Searches > Page Behavior > When opening a view result...**. If one of the other parameters is chosen, the above options will only be active after clicking a button **Load devices** (or **Search for hits > Load devices**) in the content panel of the view. See also [Views and Searches\(see page 320\)](#).

3.15 Jobs

Menu path: Structure tree > **Jobs**

You can define jobs for the UMS. A job consists in sending a command for specific devices automatically at a defined time. Jobs can be repeated at intervals or on specific days of the week.

You have the following options in the context menu for a job:

- **Edit Job:** Opens the **Edit Job** dialog with which you can change settings for the job.
- **Rename:** Opens the **Input** dialog in which you can give the job a new name.
- **Delete:** Removes the job.
- **Clear outdated results:** Removes outdated results.
- **Access control:** Opens the **Access control** dialog with which you can change the rights for the job. Further information can be found under [Object-Related Access Rights\(see page 515\)](#).
- **Cut:** Cuts the job from the current directory so that it can be pasted into another directory.
- **Paste:** Pastes the cut job into the current directory.
- **Logging: Messages:** Opens the **Messages** dialog. Further information can be found under [User Logs\(see page 521\)](#).
- **Execute Job:** Executes the job immediately.

-
- [Setting Up a New Job\(see page 426\)](#)
 - [Commands for Jobs\(see page 426\)](#)
 - [Details\(see page 427\)](#)
 - [Schedule\(see page 428\)](#)
 - [Assignment\(see page 428\)](#)



- [Execution Results](#)(see page 429)

3.15.1 Setting Up a New Job

Menu path: Structure tree > **Jobs** > [context menu] > **New Scheduled Job**

► To add a job, select **Jobs** > [context menu] > **New Scheduled Job** or **System** > **New** > **New Scheduled Job**.
The configuration window contains:

- [Details](#)(see page 427)
- [Schedule](#)(see page 428)
- [Assignment](#)(see page 428)

3.15.2 Commands for Jobs

Menu path: Structure tree > **Jobs** > [context menu] > **New Scheduled Job**

You can define one of the following commands for a job:

- **Update**: Executes the firmware update with the existing settings, see also [Universal Firmware Update](#)(see page 493).
- **Shutdown**: Shuts down the device.
- **Reboot**: Restarts the device.
- **Suspend**: Puts the device into suspend mode.
- **Wake up**: Starts the device via the network (Wake-on-LAN).
- **Update on Boot**: Executes the firmware update when the device is booting.
- **Update when shutting down**: Executes the firmware update when the device shuts down.
- **Settings Device->UMS**: Reads the local device settings to the UMS.
- **Settings UMS->Device**: Sends the UMS local settings to the device.
- **Download Flashplayer**: Downloads the Flash Player plugin for Firefox.
- **Remove Flashplayer**: Removes the Flash Player plugin for Firefox.
- **Download Firmware Snapshot**: Executes the firmware update with the existing settings (WES).
- **Send Message**: Sends a selected message template to the devices. You can create templates for messages under **UMS Administration > Global Configuration > Messages to Devices**. For more information on templates, see [Send Message](#)(see page 394).
- **Partial Update**: Executes the partial update with the existing settings (WES). See also [Partial Update](#)⁷¹.
- **Update desktop customization**: Updates the desktop background and the boot logo.
- **Deploy Jabra Xpress package**: Installs a [Jabra Xpress package](#)⁷² (IGEL OS).
- **OS 11 Upgrade**: Upgrades devices from IGEL OS 10 to IGEL OS 11. For details, see [Mass Deployment Using a Scheduled Job](#)⁷³.
- **Start Login Enterprise launcher**: Starts Login Enterprise Launcher if it has been configured, see [Login Enterprise Launcher in IGEL OS](#)⁷⁴.

⁷¹ <https://kb.igel.com/display/w10iot404/Partial+Update>

⁷² <https://kb.igel.com/display/igelos1104/Jabra+Xpress>

⁷³ <https://kb.igel.com/display/igelos1006/Mass+Deployment+Using+a+Scheduled+Job>

⁷⁴ <https://kb.igel.com/display/igelos1104/Login+Enterprise+Launcher+in+IGEL+OS>



3.15.3 Details

Menu path: Structure tree > **Jobs** > [context menu] > **New Scheduled Job**

Name: Name of the job.

Command: Command which is executed for all assigned devices.

Execution time / Start date: Time of the first execution.

Enable

Jobs can be enabled or skipped as necessary.

Comment: Further information regarding the job.

Options

Log results

Loggable results are collected in the database. This is not possible with the Wake-on LAN command.

Retry next boot

Parameter for the update command - devices that are switched off perform the update when they next boot.

Max. threads: Maximum number of processes executed simultaneously, these processes may thus be executed in block fashion.

Delay: The minimum waiting time before the UMS sends the command to the next device.

Timeout: The maximum waiting time before the UMS sends the command to the next device.

- ⓘ The **Max. threads**, **Delay**, and **Timeout** options make sense for all commands which take a long time to execute or cause heavy network traffic, e.g. downloading a firmware update, codec or snapshot. To prevent a large number of devices downloading data from a file server at once, it is advisable to reduce the number of simultaneous threads (e.g. to 10) and to set up a delay (e.g. 1 minute).

Job Info

Job ID: Internal job number which cannot be changed. This field is empty if a job is new.

Next execution: Date and time of the next execution.

User: Name of the UMS user executing the command.

⚠ Administrative Task Notification

If you have not set an administrative task "[Delete Job Execution Data\(see page 470\)](#)", after the start of the UMS Console, the following notification pop-up will be shown:



Notifications					
<input type="checkbox"/> Don't show again	Info Type	Notification Type	Message	Message creation date	
<input type="checkbox"/>	i Information	Admin Tasks	Care: you did not create an automatic backup task	May 22, 2019	
<input type="checkbox"/>	i Information	Admin Tasks	Care: you did not create a cleanup task for Delete job execution data	May 22, 2019	
<input type="checkbox"/>	i Information	Admin Tasks	Care: you did not create a cleanup task for Delete logging data	May 22, 2019	

Only users with read permission for administrative tasks can see this notification. You can set the rights under **Edit > Access control**.

You can manage the display settings under **Misc > Settings > Notifications**.

You can find the notifications under **Help > Notifications**.

3.15.4 Schedule

Menu path: Structure tree > **Jobs** > [context menu] > **New Scheduled Job**

Execution time / Start date: Time of the first execution.

Expiration date / Time: After this point, no further commands will be executed.

Repeat job: A job can be repeated at fixed intervals or on specific days. Public holidays can be excluded separately. You can update the list of public holidays under **Misc > Scheduled Jobs > Manage Public Holidays**.

⚠ If Update, Update when Starting or Update when Shutting Down is selected as the command for the job, **Repeat job** should not be enabled.

Cancel job execution: Defines how long the system is allowed to wait for the completion of the job execution. Possible options:

- "Never": Jobs are never aborted.
- "Time": Point in time in hours and minutes when the job execution will be aborted.

Example: If the **Execution time** and **Cancel job execution** are set to "19:00" and "20:00" respectively, the timeout for the job execution amounts to 1 hour. After 20:00, no further commands for the job execution will be sent to devices.

i If the **Time** configured under **Cancel job execution** precedes the **Execution time**, the job will not be aborted.

- "Max. duration": The maximum waiting time in hours and minutes for the completion of the job execution.

Example: If **Max. duration** is set to "00:05", the timeout for the job execution amounts to 5 minutes. After 5 minutes starting from the **Execution time**, no further commands for the job execution will be sent to devices.

3.15.5 Assignment

By selecting **Add (+)**, you can assign a job to specific devices.



You can also select a devices directory. The job will then be assigned to all devices located in this directory at the point of execution.

The most flexible assignment can be achieved by selecting devices dynamically with the help of a selected view. At the point of execution, the devices will first be ascertained on the basis of the selection conditions for the view. The jobs will then be assigned to them.

- i** Write authorization for the relevant objects is required in order to set up static devices assignment via the MAC address or dynamic assignment via the directory or view. At the point of execution, the user who has set up the job must have write authorization for the relevant devices. This must be taken into account, even if other users have write authorization for a job and especially if the database user has set up a job.

3.15.6 Execution Results

Menu path: Structure tree> **Jobs**

Execution Results appear in the view for a completed job. Here, you are given an overview of the status for the execution of a job. You can choose items from the overview using a selection list. This results view can be deleted and updated using two buttons. The following -**message**- job status reports are issued for the assigned devices:

Being executed	The job is currently being executed.
OK	The job is complete, all assigned devices have been dealt with.
Out of time	The job was aborted before all assigned devices could be dealt with because the abort time or the maximum duration has been reached.
Canceled	The job was stopped for an unknown reason (e.g. server failure).

The job execution status is also displayed for the devices:

Running	The command is currently being executed. The server is waiting for a reply.
Waiting	The job is running, the command will be executed when the next process is available.
Transferred	The command was successfully executed or transferred to the device.
Canceled	Aborted owing to an internal error or an unknown cause.
Failed	The command could not be executed, the reason is shown in the message column.
At next boot	The command will be executed when the device next boots.
Not done	The command was not executed because the time-out for the job was reached.



3.16 Files

Menu path: Structure tree > **Files**

Through a **file transfer**, you can save files in the device's local file system. A file must be registered on a UMS Server before it can be sent to the device. Examples include virus scanner signatures required locally on the device, browser certificates, license information, etc.

- [Registering a File on the UMS Server](#)(see page 430)
- [Transferring a File to a Device](#)(see page 430)
- [Removing a File from a Device](#)(see page 431)
- [Transferring a File to the UMS Server](#)(see page 432)

3.16.1 Registering a File on the UMS Server

A file must be registered on the UMS Server before it can be loaded onto a device.

To register a file on the UMS Server, proceed as follows:

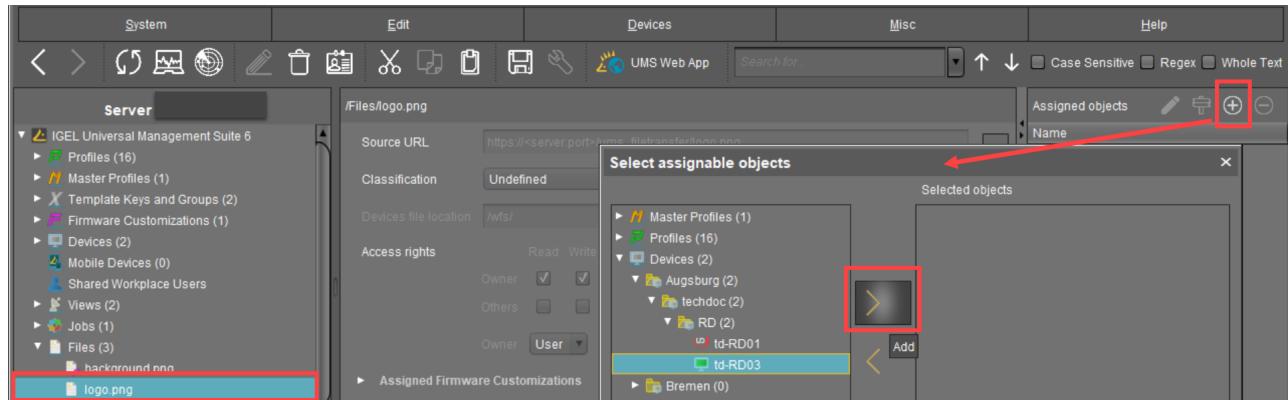
1. In the UMS Console, select **Files** > **[context menu]** > **New file** or **System** > **New** > **New File**.
2. Under **File source**, select a local file or one already on the server.
3. Select the upload location (URL). From UMS 5.01.100, you can only use the directory `ums_filetransfer` or sub-directories created in it.
4. Under **Classification**, select the type of file. This serves to automatically establish suitable storage locations and file authorizations. Choose between:
 - **Undefined**
 - **Web browser certificate**
 - **SSL certificate**
 - **Java certificate**
 - **IBM iAccess certificate**
 - **Common certificate**
5. For the **Undefined** classification, specify the path in the device's local file system under **Device file location**.
6. For the **Undefined** classification, allocate **access rights** and the owner.
These will be attached to the file when it is transferred to the device and will be used on the destination system.
7. Confirm the settings by clicking on **OK**.
The file will now be copied to the web resource and will be registered on the UMS Server.

3.16.2 Transferring a File to a Device

In order to upload a file to a device, it must be assigned to the device either directly or indirectly via a device directory or profile.

- ▶ Via drag and drop, move the file to the device directory or integrate the file on the device itself in the **Assigned objects** window via the symbol as you would when assigning profiles.

Example:



If a file has been assigned to a profile, it will be transferred to the assigned clients along with the profile settings.

When the UMS settings are transferred, a file assigned in this way will be copied to the device, e.g. while the device is booting. As long as the file is assigned to the device, it will be synchronized with the file registered on the UMS Server, for example, if the file `bookmarks.html` is replaced by a new version. The MD5 checksum for the file assigned to the device is compared to the registered file. If the checksums differ from each other, the file will be transferred again.

- i Up until UMS Version 5.02.100, the device must be able to contact the UMS Server with its fully qualified domain name (e.g. `mytcserver.mydomain.tld`). From UMS Version 5.02.100, the IP address of the UMS will be used when transferring the file. This ensures that the transfer works even in the event of DNS problems.

If a file was directly replaced in the file system in the `ums_filetransfer` directory, it must be updated in the UMS Console using the command **Update file version** from the file's context menu. The UMS Server will otherwise not recognize the change in the file version.

- [Transferring a File Without Assignment](#)(see page 431)

Transferring a File Without Assignment

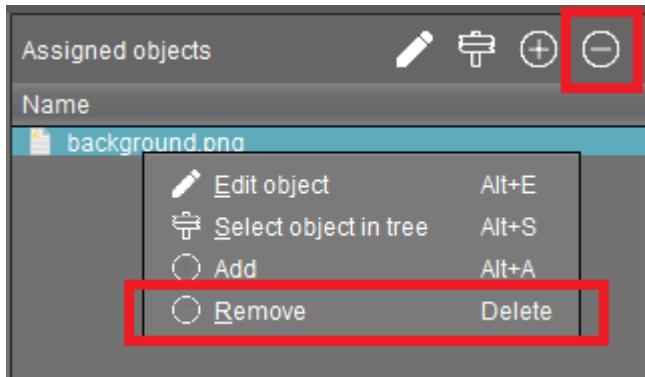
A file registered on the UMS Server can also be transferred to the device without preparation:

- Select **Other commands > File UMS->Device** from the device's context menu or under **Devices** in the menu bar. The file does not need to be assigned to the device.

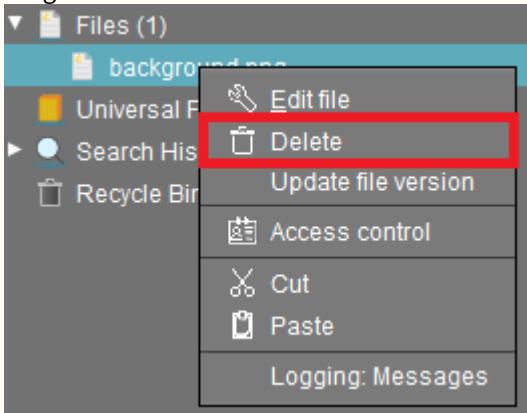
This is a straightforward file copying operation. The file is not updated if the file version on the UMS Server changes.

3.16.3 Removing a File from a Device

- To permanently remove a file from a device, select the device in the structure tree and delete the file assignment in the **Assigned objects**(see page 328) area.



- ⚠** If you delete a file in the structure tree under **Files**, it will be removed from ALL devices to which it was assigned.



3.16.4 Transferring a File to the UMS Server

To download a file on a device to the web resources, proceed as follows:

- ▶ In the context menu of a device, select **Other commands > Device File->UMS**.

The UMS cannot search through the device's local file system. Therefore, you have to know the location and name of the file you would like to download to the web resource.

- ⓘ** A file transferred from a device to WebDAV is not automatically registered on the UMS Server. It can then be found in the UMS' http server area. However, you can register existing files later on via **New File**, see [Registering a File on the UMS Server](#)(see page 430).

Example

The **Device File->UMS** command can be used when you have to read out the current local configuration of the device and, thus, need to copy the two local files `setup.ini` and `group.ini` via the UMS.

1. Select **Other commands > Device File->UMS** from the device's context menu in the UMS Console.



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. Begin the file transfer by selecting **Device File->UMS**.

See also [Exporting the Local Device Configuration](#)⁷⁵.

3.17 Universal Firmware Update

Menu path: **Server - [UMS Server address] > Universal Firmware Update**

In this area, you can search for new firmware updates for IGEL devices and devices converted by OSC, import the configuration data for specific firmware versions, and provide the firmware files for distribution.

The following options are available in the context menu:

- [Check for new firmware updates](#)(see page 433)
- **Snapshot -> Universal Firmware Update**
- **Firmware archive (zip file) -> Universal Firmware Update**
- **Access control**. See [Access Rights](#)(see page 509).

When you select **Snapshot -> Universal Firmware Update** or **Firmware Archive (zip file) -> Universal Firmware Update**, you can choose one of the following options:

- [Import Firmwares](#)(see page 393): Imports the configuration data for specific firmware versions from XML files that have been generated by a UMS instance.
- [Snapshot -> Universal Firmware Update](#)(see page 434): Registers a Windows Embedded Standard snapshot as a Universal Firmware Update.
- [Firmware archive \(zip file\) -> Universal Firmware Update](#)(see page 435): Registers the firmware files for IGEL OS as a Universal Firmware Update.

⚠ Once you have provided the update files, you must assign them to the devices and launch the update process. See [Assigning Updates](#)(see page 390).

ⓘ You can use an FTP server for distributing the firmware updates to the devices, as an alternative to the WebDAV capability of the UMS. An FTP server is required if your devices are connected via ICG. For further information, see [Universal Firmware Update](#)(see page 493). If you have a High Availability environment and use the WebDAV for downloading the firmware updates, see [How to Detect Which Files Are Synchronized Automatically](#)(see page 159).

3.17.1 Check for New Firmware Updates

Menu path: **Server - [UMS Server address] > Universal Firmware Update > [context menu] > Check for new firmware updates**

⁷⁵ <https://kb.igel.com/display/igelos1105/Exporting+the+Local+Device+Configuration>



In this area, you can search the public IGEL server for firmware updates that can be downloaded and provided as Universal Firmware Updates by the UMS.

The icons at the top right of the window have the following meanings:

	Select a WebDAV directory as the target directory
	Specify an FTP target directory
	Undo changes

Universal Firmware Updates

Include

- The relevant firmware will be downloaded.

Model: Name of the firmware.

Version: The version number of the firmware for selection.

Target directory: Directory to which the firmware is downloaded.

This is the `ums_filetransfer` folder or, in the case of an FTP server, the directory specified under **UMS Administration > Global Configuration > Universal Firmware Update**.

Release notes: Show the release notes for the relevant firmware as an HTML page or in text format.

Show only latest firmware versions (hides already downloaded versions)

- Only the latest version of the relevant models is shown. If the latest version has already been downloaded to the UMS, it will no longer be shown.
- All available versions will be shown. (Default)

Download: The update will be added to the UMS structure tree and the current processing status will be shown.

3.17.2 Snapshot -> Universal Firmware Update

Menu path: **Server - [UMS Server address] > Universal Firmware Update > [context menu] > Snapshot -> Universal Firmware Update**

In this area, you can register a snapshot of a Windows Embedded Standard device as a Universal Firmware Update. The snapshot file is stored in a [WebDAV](#) directory.

Snapshot file: Name of the snapshot file.

Select snapshot: Opens a dialog for the selection of the snapshot file. Only snapshot files with an SNP filename extension can be uploaded.

Name: Name of the modified snapshot.



3.17.3 Firmware Archive (Zip File) -> Universal Firmware Update

Menu path: **Server - [UMS Server address] > Universal Firmware Update > [context menu] > Firmware Archive (Zip File) -> Universal Firmware Update**

In this area, you can load firmware updates for IGEL OS from a local source. The firmware file is stored in a WebDAV directory.

- ⓘ An item of firmware from a local source does not have the metainformation stored on the IGEL server.

Firmware file: Path and name of the zip file. Example: c:\Updates\IGEL_LINUX_10.03.100.zip, selectable by selecting a file.

Display name: Names for displaying the updates in the UMS.

WebDAV target directory: Directory in which the update is saved in order to distribute it to the devices.

3.18 Search History

Menu path: **Structure Tree > Search History**

Here, all search queries are saved as individual objects and can be edited further via the context menu.

Possible search types:

- Devices
 - Profiles
 - Views
-
- Context Menu of a Search Query(see page 435)

3.18.1 Context Menu of a Search Query

Menu path: **Structure Tree > Search History**

The following options are available to you in the context menu of a search query:

- **Delete:** Deletes the search result from the list.
- **Edit Search:** Allows you to change the search query. Search editing is possible only in expert mode. For details on expert mode, see [Expert Mode\(see page 406\)](#). Text expert mode is possible for the search type **Devices** only.

The following options are always active if **Automatically load amount and items** is selected under **Menu Bar > Misc > Settings > Views and Searches > Page Behavior > When opening a search result...** . If one of the other parameters is chosen, the options below will only be active after clicking the button **Load device** (or **Load profile / Load view**) in the content panel of the search query.

- **Save as...:** Saves the search result in one of the following formats: XML, XSL-FO, HTML, or CSV.

The following options are only active if you have chosen **Devices** as a search type:



- **Assign objects to the devices from the search...**: Assigns objects to the devices that you searched for.
For details of the procedure, see [Assigning Objects to a View\(see page 424\)](#).
- **Detach objects from the devices from the search...**: Removes the assigned objects.

3.19 Recycle Bin

Menu path: Structure tree > **Recycle Bin**

In the IGEL Universal Management Suite, you can move objects to the **Recycle Bin** instead of permanently deleting them straight away. The **Recycle Bin** is enabled or disabled globally for all UMS users.

- ▶ Enable the recycle bin under **UMS Administration > UMS Features > Enable recycle bin**.

If an object in the structure tree is deleted (**Delete** function in the symbol bar, in the context menu or the [Del] key), it will be moved to the **Recycle Bin** following confirmation.

- (i) If the recycle bin is active, objects can also be deleted directly and permanently by pressing [Shift-Del].

Directories are moved to the **Recycle Bin** along with their sub-folders and all elements and can therefore be restored again as a complete structure. You will find the UMS **Recycle Bin** as the lowest node in the UMS Console structure tree. Elements in the **Recycle Bin** can be permanently deleted there or restored. To do this, bring up the context menu for an element in the **Recycle Bin**.

- (i) If you cannot bring up the context menu for elements in the **Recycle Bin**, the recycle bin is probably inactive. Check the status of the recycle bin as described above.

Virtually all elements from the UMS structure tree can be moved to the **Recycle Bin**: Devices, profiles, views, tasks, files and their directories. Shared Workplace users cannot be deleted, while administrator accounts (in account management) and search history elements can only be deleted permanently (with [Shift-Del]). The highest nodes in the structure tree cannot be deleted either. However, this procedure will affect all deletable elements beneath this node!

- Objects in the **Recycle Bin** cannot be found via the search function or views and cannot be addressed by scheduled tasks.
- Devices in the **Recycle Bin** will not receive any new settings from the UMS but will remain registered in the UMS and can be restored again from the **Recycle Bin** along with all assigned profiles.
- The fact that profiles in the **Recycle Bin** are no longer effective means that the settings for devices may change. Profiles previously assigned to devices will be reactivated if they are restored again.
- Planned tasks, views and search queries in the **Recycle Bin** will not be executed.
- At the same time, assigned profiles, files, views and firmware updates in the **Recycle Bin** are not active.



3.20 UMS Administration

- [UMS Network](#)(see page 437)
- [Global Configuration](#)(see page 442)

3.20.1 UMS Network

Menu path: **UMS Administration > UMS Network**

Here you can view and manage UMS Servers, UMS Load Balancers, and IGEL Cloud Gateways (ICG).

- [Server - View Your IGEL UMS Server Information](#)(see page 437)
- [Load Balancer - View Your IGEL UMS Load Balancer Information](#)(see page 439)
- [IGEL Cloud Gateway](#)(see page 441)

Server - View Your IGEL UMS Server Information

Menu path: **UMS Administration > UMS Network > Server**

In the **Server** node of the IGEL Universal Management Suite (UMS) Console, you can find basic information on all servers that belong to your UMS installation. For an individual server, additional details such as process information, service status, statistical data, etc. are available.

"Server" Node in the IGEL UMS

The **Server** node lists all servers belonging to the UMS installation:

- With a standard installation, only one available server normally appears here.

Host	Device Communication Port	Version	IP address
td-ums-srv2019	30001	6.08.100.rc7	

- In a [High Availability \(HA\) network](#)(see page 657), all installed servers are shown.

Process ID	Process Name	Timestamp	Service status	Mode
9c8ad658-d5e5-42e4-9747-87a45cc5ff3e	qajshasrv02	14.07.2021 12:54	Service is running	Update Mode
2591491b-1144-4357-b00d-48aa056cfcb8	qajshasrv03	14.07.2021 12:54	Service is running	Update Mode
e4eb53f3-703c-479e-87c9-b5039c2b2cc0	qajshasrv01	14.07.2021 12:54	Service is running	Update Mode
dbd51173-6a77-4d06-a34e-a85d204c69f5	qajshawsv03.qa.test	14.07.2021 12:41	Service is running	Normal Mode
39d52c12-5942-4563-a81c-31f7df124f11	qajshawsv02.qa.test	14.07.2021 12:52	Service is running	Update Mode
b912ca44-ed59-455b-96f6-95478a62fe95	qajshawsv01.qa.test	14.07.2021 12:42	Service is running	Update Mode

Normal Mode and Update Mode (for HA Installations Only)



A server is in normal mode whenever it is NOT temporarily connected to the embedded update database created during the UMS HA update, see [Updating HA Installation: Without Downtime of the Servers](#)(see page 676). Thus, **normal mode** means that the server is running with the normal "run configuration", but not with the database in update mode.

Individual Server

For an individual server, the following basic options are available:

Status Displays for the IGEL UMS Server

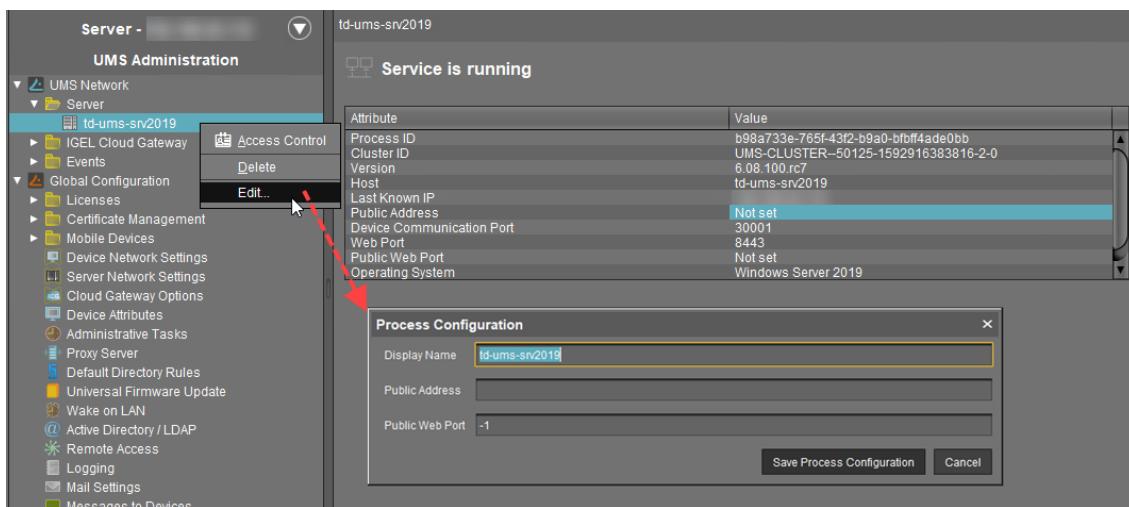
The status of the servers is shown by the following icons:

	The server is online.
	The server is offline.
	The server status is unknown (e.g. when a new server is being propagated in the network).

Process Configuration for the IGEL UMS Server

For each server, you can edit the process configuration, e.g. you can change the **Display Name** for the server. You can also configure here the **Public Address** and **Public Web Port** – they will be used when accessing files created in the UMS Console under **Files** (see [Files](#)(see page 430)) and Universal Firmware Updates (see [Universal Firmware Update](#)(see page 433) and the section "Connection Data Used during the Update" under [How to Detect Which Files Are Synchronized Automatically](#)(see page 159)). If set, the **Public Address** will also be used for the automatically generated web certificates, see [Web](#)(see page 455).

- To edit the process configuration, click **Edit** in the context menu of the required server.



Process Tasks (for HA Installations Only)

In the case of the UMS HA installation, you can also start, stop, or restart the **IGEL RMGUIServer** service:



Attribute	Value
Process ID	41e55af9-3aab-4f87-bfaa-5ff68c16573b
Cluster ID	UMS-CLUSTER--49689-1634546402343-2...
Version	6.09.100.rc2
Host	td-ums-sv2012
Last Known IP	
Public Address	Not set
Device Communication Port	30002
Web Port	8443
Public Web Port	Not set
Operating System	Windows Server 2012 R2

For how you can start or stop services, see also [HA Services and Processes](#)(see page 691).

Statistics for the IGEL UMS Server

An overview of **Requests** and **Failed and Waiting Requests** by devices makes it possible to estimate the server load across the relevant time period.

- ▶ Click on **Show History** to bring up a scalable view. You can use the mouse to zoom in on sections or restore the view by pressing the mouse button and moving the mouse to the left.

Attribute	Value
Process ID	b959733e-765f-43f2-b9a0-bfbff4ade0bb
Cluster ID	UMS-CLUSTER--50125-192916383816-2-0
Version	6.08.100.rc2
Host	td-ums-sv2019
Last Known IP	
Public Address	Not set
Device Communication Port	30001
Web Port	8443
Public Web Port	Not set
Operating System	Windows Server 2019

Load Balancer - View Your IGEL UMS Load Balancer Information

Menu path: **UMS Administration > UMS Network > Load Balancer**

In the **Load Balancer** node of the IGEL Universal Management Suite (UMS) Console, you can find basic information on all load balancers that belong to your UMS installation. For an individual load balancer, additional details such as process information, service status, statistical data, etc. are available.

"Load Balancer" Node in the IGEL UMS

The **Load Balancer** node is visible in the UMS structure tree and active only if you have installed a UMS High Availability network with **UMS Load Balancer** activated. See [High Availability \(HA\)](#)(see page 657).

The **Load Balancer** node lists all load balancers belonging to the UMS installation:



Load Balancer					
Process ID	Process Name	Timestamp	Service status	Mode	
ums-broker-49849-163455...	td-ums-srv2012	Oct 19, 2021 15:55	Service is running	Normal Mode	
ums-broker-49649-123655...	td-ums-srv2016	Oct 19, 2021 15:55	Service is running	Normal Mode	

- i** **Normal Mode** means that the load balancer is running with the normal "run configuration". Note that it does not serve as an indicator of the overall proper functioning of load balancers. If you want to check your HA environment, see [UMS HA Health Check](#)(see page 688).

Individual Load Balancer

Status Displays for the UMS Load Balancer

The status of the load balancers is shown by the following icons:

	The load balancer is online.
	The load balancer is offline.
	The load balancer status is unknown (e.g. when a new load balancer is being propagated in the network).

Process Configuration for the UMS Load Balancer

For each load balancer, you can edit the process configuration, e.g. you can change the **Display Name** for the load balancer.

- To edit the process configuration, click **Edit** in the context menu of the required load balancer.

Process Tasks for the UMS Load Balancer

Under **Process tasks**, you can also start, stop, or restart the IGEL UMS Load Balancer service. For how you can start or stop services, see also [HA Services and Processes](#)(see page 691).



Statistics for the UMS Load Balancer

An overview of **Requests** and **Failed and Waiting Requests** by devices makes it possible to estimate the server load across the relevant time period.

- ▶ Click on **Show History** to bring up a scalable view. You can use the mouse to zoom in on sections or restore the view by pressing the mouse button and moving the mouse to the left.

IGEL Cloud Gateway

Menu path: **UMS Administration > UMS Network > IGEL Cloud Gateway**

You can connect the UMS to one or more IGEL Cloud Gateways (ICG).

	Install a new IGEL Cloud Gateway with the ICG Remote Installer See Installing the IGEL Cloud Gateway ⁷⁶ .
	Uninstall the selected IGEL Cloud Gateway with the ICG Remote Installer. If the IGEL Cloud Gateway has been uninstalled with this function, it can be reinstalled using the ICG Remote Installer.
	Update the selected IGEL Cloud Gateway with the ICG Update Wizard See Updating the ICG ⁷⁷ .
	Update the keystore of the selected IGEL Cloud Gateway with the Update Keystore Wizard For renewing the end certificate, see Renewing a Signed Certificate for the ICG ⁷⁸ . For exchanging the root certificate, see Exchanging the Root Certificate for ICG ⁷⁹ .
	Add an existing IGEL Cloud Gateway to the UMS database. This IGEL Cloud Gateway must be reachable.
	Remove the selected IGEL Cloud Gateway from the UMS database permanently. <div style="border: 2px solid red; padding: 5px; margin-top: 10px;"> ! If you remove an IGEL Cloud Gateway from the UMS database, you can not add it to the UMS database again. In most cases, it is preferable to uninstall the IGEL Cloud Gateway and then reinstall it using the ICG Remote Installer. </div>
	Edit the settings of the selected IGEL Cloud Gateway
	Navigate to the ICG instance view

⁷⁶ <https://kb.igel.com/display/igelicg201/Installing+the+IGEL+Cloud+Gateway>

⁷⁷ <https://kb.igel.com/display/igelicg201/Updating+the+ICG>

⁷⁸ <https://kb.igel.com/display/igelicg202/Renewing+a+Signed+Certificate+for+the+ICG>

⁷⁹ <https://kb.igel.com/display/igelicg202/Exchanging+the+Root+Certificate+for+ICG>



Set a limit for ICG connections (ICG 2.02 or higher required)

Add an IGEL Cloud Gateway to the UMS Database

- **Display name:** Display name of the gateway. The maximal length of the name is restricted to 200 characters.
- **Host:** DNS name or IP address of the gateway
- **Port:** TCP port on which the gateway is listening (default: [8443](#))
- **Host (external):** External DNS name/IP address of the gateway
- **Port (external):** TCP port on which the gateway is listening for external connections
- **Proxy Server Settings:**
 - **No Proxy Server:** Direct connection to ICG
 - **Use Default Proxy Server:** Use the proxy server which is configured as default in [Proxy Server](#)(see page 484)
 - **Use selected Proxy Server:** Select a proxy server from the list

For details of how to set up all components for a connection to ICG, read [Installation and Setup](#)⁸⁰.

IGEL Cloud Gateway (Instance)

Menu path: **UMS Administration > UMS Network > IGEL Cloud Gateway > [Display Name]**

Here, you will find information regarding a configured gateway and can establish or disconnect the connection.

	Connect Cloud Gateway
	Disconnect Cloud Gateway
	Reload information about Cloud Gateway

Statistics

An overview of **Requests** by devices makes it possible to estimate the server load across the relevant time period.

- Click on **Show History** to bring up a scalable view. You can use the mouse to zoom in on sections or restore the view by pressing the mouse button and moving the mouse to the left.

3.20.2 Global Configuration

Menu path: **UMS Administration > Global Configuration**

Under **Global Configuration**, you can regulate administrative tasks(see page 464), integrate user data from the [Active Directory](#)(see page 497), set up [Universal Firmware Updates](#)(see page 493) and manage [licenses](#)(see page 443).

⁸⁰ <https://kb.igel.com/display/igelicg201/Installation+Guide>



-
- [Licenses](#)(see page 443)
 - [Mobile Devices](#)(see page 451)
 - [Certificate Management](#)(see page 453)
 - [Device Network Settings](#)(see page 457)
 - [Server Network Settings](#)(see page 459)
 - [Cloud Gateway Options](#)(see page 460)
 - [Device Attributes](#)(see page 463)
 - [Administrative Tasks](#)(see page 464)
 - [Proxy Server](#)(see page 484)
 - [Default Directory Rules](#)(see page 485)
 - [Universal Firmware Update](#)(see page 493)
 - [Wake-on-LAN](#)(see page 495)
 - [Active Directory / LDAP](#)(see page 497)
 - [Remote Access](#)(see page 498)
 - [Logging](#)(see page 500)
 - [Mail Settings](#)(see page 501)
 - [Messages to Devices](#)(see page 502)
 - [Misc Settings](#)(see page 503)
 - [UMS Features](#)(see page 504)

Licenses

Menu path: **UMS Administration > Global Configuration > Licenses**

In this area, you can manage licenses for the UMS as well as licenses for devices which are managed by the UMS.

- [UMS Licensing ID](#)(see page 444)
- [UMS Licenses](#)(see page 445)
- [Device Licenses](#)(see page 446)
- [Deployment](#)(see page 447)
- [UDC2 Deployment](#)(see page 450)



UMS Licensing ID

Menu path: **UMS Administration > Global Configuration > Licenses > UMS Licensing ID**

The UMS Licensing ID enables the communication between the UMS and the IGEL License Portal (ILP).

The UMS Licensing ID allows for using fully Automatic License Deployment (ALD), that is, Automatic License Deployment without the need to handle an ALD Token with each purchase. For this purpose, the UMS Licensing ID must be registered with the IGEL License Portal. For further information, see [Setting up Automatic License Deployment \(ALD\)](#)⁸¹.

The UMS Licensing ID consists of a public/private key pair. The public key is a certificate and can be exported as a .cert file. The registration of the UMS Licensing ID is done by uploading the certificate file to the IGEL License Portal.

A UMS Licensing ID is not affected or changed when the UMS database is restored from a backup. The UMS Licensing ID does not change if any parameters of the UMS installation are changed, for instance, the host name / IP address. Thus, it can be transferred to any other server. Also, multiple UMS installations can share one UMS Licensing ID, which allows for sharing [Product Packs](#)⁸² between them.

For the backup options of the UMS Licensing ID, see [UMS Licensing ID Backup](#)(see page 534) and [UMS Licensing ID Backup on the Command Line](#)(see page 535).

UMS Licensing ID

- ⓘ The UMS Licensing ID is generated upon each UMS Server installation. Therefore, if you have a [High Availability](#)(see page 657) environment, each of the servers has its own UMS Licensing ID, i.e. **Local UMS Licensing ID**. For the communication of all HA servers with the ILP, a **Main UMS Licensing ID** is used. Therefore, the **Main UMS Licensing ID** must be synchronized between all servers in the HA network, see [UMS Licensing ID status](#)(see page 445) below.

Main UMS Licensing ID: The UMS Licensing ID used for communication with the ILP. The first and last 10 characters are displayed.

Export UMS Licensing ID: Export the UMS Licensing ID as a .cert file.

Main UMS Licensing ID fingerprint: The SHA-256 fingerprint of the UMS Licensing ID.

UMS Licensing ID Status

If you are operating a single server, this area shows the status of the UMS Licensing ID for your server.

If you are operating a UMS HA environment, this area lists the UMS Licensing ID status for each server of the HA network. Each server gets the UMS Licensing ID on startup or restart.

Host name: Name of the host server as shown under **UMS Administration > UMS Network > Server**.

Server status: Status of the server, e.g. "Running"

Possible values:

- 'Running'
- 'Not running'

⁸¹ <https://kb.igel.com/pages/viewpage.action?pageId=10325058>

⁸² <https://kb.igel.com/display/licensesmoreigelos11/Overview>



UMS Licensing ID status: Indicates whether the server has the current main UMS Licensing ID or not. If it has the main UMS Licensing ID, the field reads "Main UMS Licensing ID" or "in sync". If not, the server must be restarted to get synchronized.

Possible values:

- 'Main UMS Licensing ID'
- 'In sync'
- 'Not in sync, please restart server'

i If the restart was unhelpful, the UMS Licensing ID has to be synchronized manually, see [Manual Synchronization of the UMS Licensing ID](#)(see page 164).

UMS Licensing ID: The UMS Licensing ID currently used on the server. The first and last 10 characters are displayed.

UMS Licensing ID fingerprint: The SHA-256 fingerprint of the UMS Licensing ID.

UMS Licenses

Menu path: **UMS Administration > Global Configuration > Licenses > UMS Licenses**

In this area, you are given an overview of the availability and status of all licenses for UMS extensions.

License Summary

- **License Type:** Name of the licensed UMS extension
- **Available Licenses:** Total number of units in the license file
- **Used Licenses:** License units which are currently used by the system
- **License Status:** Validity of the license

Registered Licenses

	Add license file
	Delete license
	Show content of the license file

- **License ID:** Identification number of the license
- **License registered on:** Point in time when the license file was generated on the activation portal
- **Quantity:** Total number of units in the license file
- **Customer:** Customer name (optional)
- **Services:** Licensed service, e.g. IGEL Cloud Gateway
- **Maintenance Subscription:** Authorization to install updates for the licensed extension
- **Activation Key:** Key used to generate the license in the activation portal
- **Test License:** Shows whether a license is a test license
- **Expiration Date:** End of the license period



Device Licenses

Menu path: **UMS Administration > Global Configuration > Licenses > Device Licenses**

IGEL Licenses

Here, you can manage licenses for devices, e.g. for devices converted with UDC3.

	Add license file
	Delete license
	Show content of the license file

Select Filter / Reset Filter

IGEL Licenses (17)

Set filters: Category: Add-on Expiration Date: Between May 1, 2020 and Aug 20, 2020

Select filter Reset filter

Matching licenses (2)

Order Number	Category	Pack ID	Expiration Date
69-4578788	Add-on	90M-CDHOP	Jun 5, 2020
69-3467788	Add-on	TER-WOLRE	Jun 4, 2020

Hardware

00E0C51C5087

To get an overview that is suitable for your needs, you can filter the display of existing licenses. A maximum of 20,000 licenses can be displayed.

You can create a filter by combining several criteria or create a separate filter for each criterion. When you have created several filters, you can remove each one separately.

- ▶ To configure a filter, click **Select filter**.
- ▶ To remove all existing filters, click **Reset filter**.

The following criteria are available:

Category

Possible options:

- "All": No selection of categories is made.
- "Maintenance": Selects maintenance licenses.
- "Subscription": Selects subscription licenses.



- "Add-on": Selects add-on licenses.
- "Evaluation": Selects evaluation licenses.

Order Number: Selects all licenses which belong to the given order number.

Pack ID: Selects all licenses which belong to the Product Pack with the given Product Pack ID.

Expiration Date: Selects the licenses with the given expiration date.

Possible options:

- "All"
- "Date range"
- "Date"
- "Endless"

Unit ID: Selects the licenses that are assigned to the device with the given unit ID. The unit ID can be selected from the structure tree by clicking .

Table Columns

Order Number: Order number under which the license was ordered

Category: Category to which the license belongs; possible categories: "Maintenance", "Subscription", "Add-on" or "Evaluation"

Pack ID: ID of the Product Pack to which the license belongs

Expiration Date: Expiry date of the license

Hardware

Here, you can view device lists or export them for the Igel Licensing Portal (ILP).

Export unit ID list: Opens the export wizard.

Device lists: Opens the end device list with a filter option.

Deployment

Menu path: **UMS Administration > Global Configuration > Licenses > Deployment**

You can enable and configure the automatic deployment of licenses by the UMS. Automatic license deployment includes licenses for UDC3/OSC, UMA and UD Pocket.

 Demo licenses are not supported by Automatic License Deployment. To deploy a demo license, see [Activate Your IGEL OS⁸³](#).

Automatic license deployment requires a connection between the UMS and the IGEL license server as well as the IGEL update server. This connection can be established via a proxy.

For details about the process of automatic license deployment, see [Intervals for Automatic License Deployment⁸⁴](#).

⁸³ <https://kb.igel.com/display/igelos1103/Activate+Your+IGEL+OS>

⁸⁴ <https://kb.igel.com/display/licensesmoreigelos11/Intervals+for+Automatic+License+Deployment>



- i** If a number of Product Packs for which suitable and non-allocated licenses are available, a selection will be made in accordance with the following criteria:
- The Product Pack with the most allocated licenses will be used first.
 - Product Packs with an earlier registration date will be used before Product Packs with a later registration date.

As soon as a license is registered in the UMS, the UMS stores the license and adds a license download link to the device settings. After that, the UMS sends the settings to the devices. When the devices have received their settings, they download the licenses and reboot. After the reboot, all licensed features are available on the devices.

For further information about setting up and using automatic license deployment, see [Setting up Automatic License Deployment \(ALD\)](#)⁸⁵.

- **Enable automatic deployment**
 - Automatic license deployment is enabled.
 - No automatic license deployment will take place.
- **Used proxy server:** Description of the proxy currently used
- **Edit proxy configuration:** Opens a dialog allowing you to select a proxy for communication with the license server. Under **UMS Administration > Global Configuration > Proxy Server**, one or more proxies must be configured; see [Proxy Server](#)⁸⁶.

Possible options:

- **No proxy server:** No proxy server will be used.
- **Use default proxy server:** The default proxy server defined under [Proxy Server](#)⁸⁷ will be used.
- **Use selected Proxy Server:** A server from the **Configured Proxy Servers** list can be selected.
- **Connection test:** Shows the result of the connection test.
- **Test connection:** Tests the connection between UMS or the proxy and the IGEL license server as well as the IGEL update server (<http://fwu.igel.com/>).

Registered packs

This table shows all Product Packs currently registered in the UMS. You can add, delete, enable or disable Product Packs.

Search for:	Search in all columns of the table
	Add Product Pack
	Delete Product Pack

⁸⁵ <https://kb.igel.com/pages/viewpage.action?pageId=10325058>

⁸⁶ <https://kb.igel.com/display/endpointmgmt509/Proxy+server>

⁸⁷ <https://kb.igel.com/display/endpointmgmt509/Proxy+server>



<input checked="" type="checkbox"/>	Enable Product Pack
<input type="checkbox"/>	Disable Product Pack. A disabled Product Pack will not be used for deploying licenses.
<input type="checkbox"/>	Update information regarding all registered Product Pack. The current information will be obtained from the license server
<input type="checkbox"/>	Show Product Pack details: <ul style="list-style-type: none"> • Attribute: Shows the attributes of a Product Pack. • Licensed hardware: Shows all devices licensed with the Product Pack belonging to the entry.

The following information is shown:

- **Pack ID:** ID of the Product Pack
- **Product:** Product pack type
- **Used licenses:** Licenses currently in use
- **Subscription status (expiration date/validity period):** For new Product Packs, the validity period is shown; for activated Product Packs, the expiration date is shown.
- **Status**
Possible statuses:
- "Active"
- "Inactive"
- **Manual Distribution**
Possible statuses:
- "Enabled"
- "Disabled"
- **Automatic Distribution**
Possible statuses:
- "Enabled"
- "Enabled (with conditions)"
- "Disabled"
- **Registration Error:** If the registration of a Product Pack has failed, the error message is shown here.

Executed actions

The actions last performed are shown in this area.

<input type="checkbox"/>	Delete entries older than a specific date
<input type="checkbox"/>	Delete selected entries



	Update display
	Show details regarding the selected action

The following information is shown:

- **Time:** Time at which the action was performed
- **Action:** Description of the action
- **Used Pack ID:** ID of the Product Pack
- **Number of affected devices:** Number of devices for which a license was deployed
- **Result:** Result of the action
Possible results:
- "Successful"
- Error message

UDC2 Deployment

Menu path: **UMS Administration > Global Configuration > Licenses > UDC2 Distribution**

From Version 5.02.100, the UMS offers the option of using an IGEL device as a license server in order to automatically allocate licenses to devices converted using UDC2.

- This method for automatic license deployment only works for UDC2, not for UDC3. From UMS Version 5.08, there is a method for automatic license deployment with UDC3 which uses the license server; see [Distribution⁸⁸](#).

The How-To [Setting up Automatic UDC2 License Deployment⁸⁹](#) describes the complete procedure.

- **Enable automatic UDC deployment:**
 - UDC2 devices newly registered on the UMS will automatically receive a license.
 - Automatic license distribution is disabled.
- **License server:** Select one of the license servers shown.
- **Connection state:** Indicates whether a network connection to the license server exists.
- **License type:** The licenses available on the license server
- **License OS:** Operating system for which licenses are available
- **Number of licenses:** Number of licenses still available
- **Check license server again:** Checks the network connection to the license server again, for example if you have switched on the server in the meantime.
- **Deployed licenses:** List of licenses deployed by the selected license server since it was last restarted.
 - **License deployed at:** Date and time when the license was deployed
 - **Unit ID:** Unique ID of the device

⁸⁸ <https://kb.igel.com/display/endpointmgmt509/Deployment>

⁸⁹ <https://kb.igel.com/display/licensesmorelegacy/Setting+up+Automatic+UDC2+License+Deployment>



Mobile Devices

Menu path: **UMS Administration > Global Configuration > Mobile Devices**

In this area, you can manage mobile devices that are connected to the UMS. Scan the QR code with the IGEL MDM App for iOS to enroll your device. For more information, see [Connecting Mobile Devices to the UMS](#)(see page 716).



QR Code

- **Displayname:** The display name
- **Host:** The host
- **Port:** The port
- **Apns Status:** Status of the connection to the Apple Push Notification service
- **Firmware available:** Shows if the firmware required for MDM is available
- **Enrollment URL:** The enrollment URL

Possible actions related to the QR code:

- **show:** Show the QR code in a separate window
 - **send via email:** Send the QR code via email
 - **save as jpg:** Save the QR code as JPG file
 - **send as png:** Save the QR code
-
- [Apple iOS Devices](#)(see page 451)

Apple iOS Devices

Menu path: **UMS Console > UMS Administration > Global Configuration > Mobile Devices > Apple iOS devices**

In this section, you can set up the required certificate for connecting the UMS to the Apple Push Notification Service. How you set up the certificate to connect the UMS with the Apple Push Notification Service is described in the [MDM Setup Guide](#)(see page 715).

You can perform the following actions:

Icon	Description
	Create a new certificate-signing request and save it as a *.csr file



Icon	Description
	Open the Apple Push Certificate Portal at https://identity.apple.com in the system browser
	Import the Apple MDM Push Certificate (*.pem file)
	Create and save certificate-signing request for renewal
	Show the certificate details of the Apple MDM Push Certificate
	Cut the certificate
	Delete the certificate

Status information:

Icon	Description
	Certificate successfully set up
	Waiting for certificate upload
	Incomplete / certificate error

You may further specify:

- **Enrollment profile displayname:** Displayname for the enrollment profile
- **Enrollment profile description:** Description of the enrollment profile
- **Adjust UMS-internal name with name on device**

For further instructions, see:

- [MDM Manual](#)(see page 706)
- [MDM How-Tos](#)(see page 715)
- [MDM Troubleshooting](#)(see page 718)



Certificate Management

Menu path: **UMS Administration > Global Configuration > Certificate Management**

Here, you can manage certificates for communication with endpoint devices, for communication over the Web Port (default: 8443), and for communication with the IGEL Cloud Gateway (ICG).

- [Device Communication](#)(see page 453)
- [Web](#)(see page 455)
- [Cloud Gateway](#)(see page 456)

Device Communication

Menu path: **UMS Administration > Global Configuration > Certificate Management > Device Communication**

Overview

In this section, you can manage certificates for the communication between the UMS and the devices. The preconfigured certificate, which has the **Keystore alias** "tkey", is used by default if no changes are made.

You can set a different certificate as default; if you do so, all newly registered devices will use this certificate, and already registered devices will replace their previously used certificate with the new default certificate.

- i** At an interval of 5 minutes, the UMS checks whether the certificate on the device and the default certificate are still identical.

If a device does not support the default certificate, the UMS checks for each certificate whether it is supported, starting from the top of the list. The first one that matches the requirements will be used. If no certificate matches, the device is not registered.

If you select a certificate in the area **Device Communication**, all devices which use this certificate are shown in the area **Devices which use the selected certificate (<number>)**.

⚠ High Availability

If you are running the UMS in a High Availability (HA) network, be aware that if you make changes to certificates (import of a key pair, generation of a new key pair, deletion, activation/deactivation of a certificate, changes of a certificate's priority), a new network token is automatically generated and you will have to define a location in which the new network token should be stored. The changes are then automatically synchronized within a HA network, and no restart of the IGEL RMUIServer/igelRMserver services is required.

i Restoring from a Backup

When restoring from a backup, check if certificates included in the backup differ from the certificates that are currently in use. If this is the case, all devices that have been registered before restoring will have to be registered again.



UMS Update

Certificates are not overwritten in the course of an update.

Possible Actions



Import a certificate from a file. The private key must be included in the file. The file path is provided under **Keystore file** and the import password is entered under **Keystore password**. The certificate's signature algorithm is checked. If the signature algorithm is not supported by the UMS, the certificate is not imported.

Supported Signature Algorithms

The following signature algorithms are supported: SHA512withRSA, SHA384withRSA, SHA256withRSA, SHA1withRSA, SHA256withDSA, and SHA1withDSA.

Supported Keystore Types

The following keystore types are supported: JCEKS, JKS, PKCS#12, BKS-V1, BKS, UBER, and BCFKS.

No Support

Certificate chains and expired certificates cannot be imported. Certificates that use the MD5 algorithm are also not supported.



Generate a new certificate.



Delete the selected certificate.

Do not delete a certificate that is being used by a device; otherwise, the UMS will not be able to communicate with this device anymore.



Move the selected certificate up in the list to increase its priority.

If you move the selected certificate to the top of the list, it will become the default certificate. The change of the default certificate is propagated to the devices in a background task of the UMS. This task replaces the certificate on all devices that are compatible with this certificate and runs every 5 minutes.



Move the selected certificate down in the list to decrease its priority.



Activate the selected certificate. When a certificate is activated, it can be used for communication between UMS and devices.



Deactivate the selected certificate. A deactivated certificate will not be used when a new device is registered. If a certificate is deactivated while it is in use, communication between UMS and device is still possible. If only 1 certificate is active, this certificate can not be deactivated.



Export the selected certificate.



Export the key pair of the selected certificate.



Show the content of the selected certificate.

Web

Menu path: **UMS Administration > Global Configuration > Certificate Management > Web**

Overview

Here, you can manage the certificates for communication via the Web Port (default: 8443).

The Web Port is used for the following tasks:

- Provide data for the endpoint devices (WebDAV etc.)
- Provide data for other servers (High Availability; WebDAV etc.)
- Provide data for the UMS Web App
- Provide an entry point for IMI and WebStart

Use

- UMS Web App: Providing the browser with the certificate; see [UMS Web App: The Browser Displays a Security Warning \(Certificate Error\)](#)(see page 187)
- If you need to use an alternative certificate chain instead of the pre-installed one, see [Using Your Own Certificates for Communication over the Web Port \(Default: 8443\)](#)(see page 123)

Possible Actions



Automatic renewal: ON

Used certificates will be renewed automatically.

Open the dialog **Change Automatic Renewal Setting** to toggle automatic certificate renewal.

The private key of the parent certificate (root CA or intermediate CA) must be known. The renewed certificate is assigned to the servers automatically.

Possible options:

- **ACTIVATE automatic renewal:** The end certificates in use will be renewed according to the number specified in **Renew a used end certificate [number] days ahead of its expiration date**.
- **DEACTIVATE automatic renewal:** The end certificates will not be renewed automatically.



Create a root certificate.



Create a signed certificate from the CA certificate (root or intermediate) that is currently selected.



Remove the selected certificate from the UMS. Only certificates that are not currently in use can be removed.



Renew the selected certificate; the dialog **Create signed certificate** is opened.

All settings except the expiry date (**Valid until**) can be left unchanged. The public key of the parent certificate (root CA or intermediate CA) must be known. Also, the expiry date of the parent certificate must be later than the new expiry date for the end certificate.



Show the content of the selected certificate.



Import a root CA certificate.



Import a signed certificate for which the currently selected certificate is a parent certificate (root CA or intermediate CA).



Import the decrypted private key for the selected certificate.



Import a certificate chain from a keystore.



Export the certificate and its child certificates as a certificate chain to a keystore.



Assign the selected certificate to one or more servers. For more information, see [Using Your Own Certificates for Communication over the Web Port \(Default: 8443\)](#)(see page 123).

Cloud Gateway

Menu path: **UMS Administration > Global Configuration > Certificate Management > Cloud Gateway**

Overview

Here, you can manage the certificates for the communication between the IGEL Cloud Gateway (ICG) and the endpoint devices.

Use

- [Renewing a Signed Certificate for the ICG⁹⁰](#)
- [Exchanging the Root Certificate for ICG⁹¹](#)

Possible Actions



Create a root certificate.



Import a root CA certificate.

⁹⁰ <https://kb.igel.com/display/igelicg202/Renewing+a+Signed+Certificate+for+the+ICG>

⁹¹ <https://kb.igel.com/display/igelicg202/Exchanging+the+Root+Certificate+for+ICG>



Create a signed certificate from the CA certificate (root or intermediate) that is currently selected.



Remove the selected certificate from the UMS. Only certificates that are not currently in use can be removed.



Export the selected end certificate and its complete certificate chain to a keystore in the IGEL Cloud Gateway keystore format.



Show the content of the selected certificate.



Navigate to an IGEL Cloud Gateway that is using the selected certificate.

Device Network Settings

Menu path: **UMS Administration > Global Configuration > Device Network Settings**

Configuration of the System Information Update

Update system information on selection of a device

- The system information of the device will be read in again as soon as the **device** is selected. (Default)
- The system information from the last update will be shown.

Advanced Device's Status Updates

Devices send updates

- The devices report changes in their advanced status. (Default)
- The only thing that is displayed is whether a device is online or offline.

Heartbeat Signal

Configure devices to send periodic contact signal

- The devices send a regular heartbeat signal according to the setting of **Heartbeat interval**.

Heartbeat interval: Interval between each heartbeat signal

Possible values: 1 ... 6 hours, 12 hours, 24 hours

For more information, see [Monitoring Device Health and Searching for Lost Devices](#)(see page 177).

Automatic Registration

Enable automatic registration (without MAC address import): This option is provided for the following scenario: The MAC addresses were already imported before the devices were added to the UMS database. As a result, preparations such as creating profiles can be made before the devices are delivered. If the option is enabled, each device will automatically receive the intended settings after it has logged on for the first time.

Further information regarding the importing of devices can be found under [Import Devices](#)(see page 308).



- Each device that contacts the UMS will automatically be registered in the UMS database.
- A device that contacts the UMS will not be automatically registered. (Default)

Device Requests

Maximum number of concurrent threads for device requests: Defines the number of concurrent device requests that are accepted by the UMS. (Default: 50)

- i** If you require higher performance and high availability, you can use [IGEL UMS High Availability \(HA\)](#)(see page 657).

Queue limit:

No limit: Additional request will have to wait until a thread is available. (Default)

Queue size: Defines the queue size. Additional threads that exceed the queue size will be rejected. (Default value: 0)

Adjust Names of Devices

Adjust UMS-internal names if network name has been changed

- If the network name of the device is changed, the UMS-internal name will be set to the new network name.
- The UMS-internal name will not be set to the network name of the device. (Default)

Adjust network name if UMS-internal name has been changed

If the UMS-internal name of the device is changed, the network name of the device will be set to the new UMS-internal name. If this setting is enabled, the maximal length of the device name is restricted to 15 characters.

- i** If you enable **Naming Convention**, the input of non-standard characters for **Prefix** will be limited.

- The network name of the device will not be set to the UMS-internal name. (Default)

Naming Convention

Enable naming convention for new devices

- The UMS-internal names of the devices will be formed from the **prefix** and a consecutive number.
- The names of the devices will not be allocated in accordance with the naming convention. (Default)

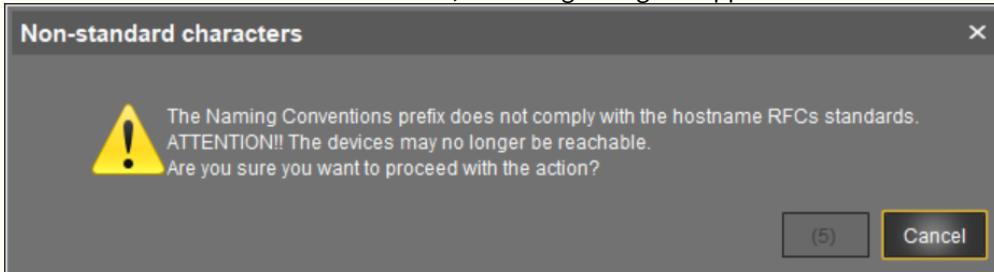
Prefix: Prefix for automatically allocating names. The prefix can be between 1 and 7 characters long; if no prefix is specified, the default prefix "UMS-" will automatically be added.

- ⚠** If **Adjust network name if UMS-internal name has been changed** has been enabled, the input of non-standard characters is limited. Example: "&", "/", "!", etc. will not be accepted.
To comply with the network naming standard, a prefix
 - must contain letters or numbers: "A" to "Z", "a" to "z", or "0" to "9".
 - can start or end with a letter or a number: "A" to "Z", "a" to "z", or "0" to "9".



- can contain a dash "--" but must not start with it.

If **Adjust network name if UMS-internal name has been changed** is enabled after a non-standard character has been entered under **Prefix**, a warning dialog will appear:



Confirm the dialog after the countdown only if you are sure that your devices will be reachable with new network names based on the prefix entered.

Minimum digits: Minimum number of digits for the consecutive number added to the prefix. The digits not allocated will be filled with zeros. Examples: If **2** is selected, the consecutive number of the first device will be **01**, if **3** is selected, the consecutive number will be **001** and so on.

- ⓘ If the number of devices exceeds the value defined here, the numbering will simply continue without an error occurring.

Preview: Displays the current naming convention comprising a prefix and a consecutive number with the number of digits specified under **Minimum digits**.

Rename all devices: All devices registered in the UMS will be renamed in accordance with the naming convention using the existing numeration.

Rename and renumber all devices: All devices will be renamed in accordance with the naming convention, this will result in continuous, end-to-end numbering. All names will be reallocated. If numbers have become free because devices were taken out of service, these numbers will be used for other devices.

Server Network Settings

Menu path: **UMS Administration > Global Configuration > Server Network Settings**

Online Check Parameters

Disable online check

- The online check is disabled.

Timeout (ms): Specifies how long the system will wait for a response to an online status query message. The UMS attempts to contact all devices that are currently visible in the UMS Console. Each device in this area must respond to the status query in the specified time or will otherwise be flagged as "offline". Minimum: 100; maximum: 10000; default: 1000

- ⓘ **Changed Values on Update**

The maximum and minimum value and the new default value have been introduced with UMS 6.04.100. If you update to version 6.04.100 from an older version, the value will be handled as follows:



- If the value was between 100 and 10000, it remains unchanged.
- If the value was lower than 100, it is changed to 100.
- If the value was the old default value of 100, it is changed to the new default value 1000.
- If the value was higher than 10000, it is changed to 10000.

Specify online check port (UDP)

- You specify the port to which the devices respond if the UMS checks their online status.
- The UMS will select any free port.

Scheduled Jobs

Scheduled jobs never expire

- No time limit for scheduled jobs

Expiration time for scheduled jobs: Time in minutes after which a scheduled job will expire. (Default: 40)

Scan Parameters

Timeout (ms): Specifies how long in milliseconds the UMS will wait for a response to scan packages. (Default: 6000)

Broadcast IP: Broadcast address that is used for scan packages. It is only used for scanning the local network. If IP ranges are used, the UDP packets will be sent to each client within the IP range. (Default: 255.255.255.255)

Specify scan reply port (UDP)

- You specify the port to which the devices respond if the UMS scans for devices
- The UMS will select any free port.

Cloud Gateway Options

Menu path: **UMS Administration > Global Configuration > IGEL Cloud Gateway**

Here you can create and manage ICG certificates and first-authentication keys for connecting devices via IGEL Cloud Gateway (ICG).

For details of how to set up all components for a connection to the ICG, read [Installation and Setup⁹²](#).

Certificates

	Generate root certificate
	Import root certificate
	Generate signed certificate

⁹² <https://kb.igel.com/display/igelicg202/Installation+Guide>



	Delete certificate
	Export certificate chain in the IGEL Cloud Gateway Keystore format
	Show content of the certificate
	Navigate to ICG instance view

Generate root certificate

- **Displayname:** Name in the root certificate (common name, CN).
- **Your organization:** Organization, company, government agency.
- **Your city or district:** The location of the organization.
- **Your two-letter country code:** ISO 3166 country code, e.g. DE for Germany.
- **Valid until:** Local date on which the certificate expires. (Default: in 10 years)

Import root certificate

- The file selection window opens, allowing you to select the certificate file which must be in the PEM format.

Generate a signed certificate

- **Name:** Name in the certificate (common name, CN).
- **Your first name and surname:** Name of the certificate holder.
- **Your organization:** Organization, company, government agency.
- **Your city or district:** The location of the organization.

The name in a signed certificate must be different from the one in the root certificate with which it is signed. UMS provides a warning in this case:

Expiring date	Status	Used
Apr 13, 2027 10:38:00 AM	✓	
Apr 13, 2018 10:38:47 AM	✗	
Apr 13, 2018 10:48:27 AM	✓	
Apr 18, 2018 10:12:12 AM		Subject and issuer of certificate are equal. This is not a valid certificate!

- **Your country code (two letters):** ISO 3166 country code, e.g. DE for Germany.
- **Host name and/or IP of the target server for the certificate:** Host name(s) and IP address(es) for which the certificate is valid. Multiple entries should be separated by a semicolon. To generate a wildcard certificate, use the asterisk, e.g. *.example.com.
- **Valid until:** Local date on which the certificate expires. (Default: in a year)
- **Certificate type**
Possible options:
- **CA Certificate:** The certificate can be used to sign other certificates, but it can not be used by the ICG.



- **End Entity:** The certificate can be used by the ICG, but it can not be used to sign other certificates.

Context menu (root certificate)

- **Generate signed certificate:** Collects certificate data and signs them with the selected root certificate.
 - **Import signed certificate:** Imports a certificate in PEM format that was already signed outside the UMS by the imported CA.
 - **Import decrypted private key:** Imports a private key file.
- Info:** If the private key is protected with a passphrase, you must decrypt it on the command line with OpenSSL before importing it: `openssl rsa -in encrypted.key -out decrypted.key`
- **Delete certificate:** Deletes the certificate from the UMS.
 - **Export certificate chain in the IGEL Cloud Gateway Keystore format:** Produces a file for ICG installation program.
 - **Export certificate:** Exports certificate file in the PEM format.
 - **Show content of the certificate:** Shows the content of the certificate in a text window.

First-authentication Keys

	Create new one-time passwords
	Delete logon data
	Disable logon data
	Enable logon data
	Send one-time passwords via mail
	Export one-time passwords (in XML, HTML or CSV format)
	Allows you to copy one-time passwords to the clipboard

- Info:** If you send one-time passwords via mail, anyone who can read the mail can log in to the IGEL Cloud Gateway. It is advisable to combine sending via mail with a link to unit IDs.

Create new first-authentication keys

You have the following options here:



- **Create new one-time keys**
 - **Quantity:** Desired number of passwords to be created
- **Create new one-time passwords associated with a device**
 - **Unit ID**
 - **Add:** Adds unit ID entered in the text field to the list.
 - **Select:** Selects from the devices in the UMS structure tree.
 - **Import:** Reads in a CSV file with unit IDs.
- **Create new mass-deployment key**
 - **Generate random mass-deployment key:**
 - A random multiple-time password will be generated. (Default)
 - You can enter the desired password yourself.

Device Attributes

Menu path: **UMS Administration > Global Configuration > Device Attributes**

In this area, you can set up additional attributes for devices.

- Click on to set up a new device attribute:
- The additional device attributes are used when displaying device system information, in views, and in searches.
- From UMS Version 5.07.100, attributes with set values can be defined, e.g. to avoid typing errors when entering the values. To do this, select the “List” attribute **type** and give the values together with any descriptions under **Values for the Attribute Type "List"**.

Name: Display name of the attribute

UMS internal identifier: This identifier is only required for creating/editing views or editing searches in *text mode*, see [How to Create a New View in the IGEL UMS](#)(see page 407). You can leave this field empty if you do not plan to use the device attribute in text mode of views and searches.

You can either generate the internal identifier automatically by clicking **Generate ID** or specify it manually.

- The **UMS internal identifier** must start with a lower-case letter. Only the following characters are allowed: a-z, A-Z, 0-9.

Type: Data type of the attribute

Possible values:

- **String:** A sequence of letters, numbers, and special characters is expected.
- **List:** A list of values is provided for selection. These values are specified as shown below:
Values for the Attribute Type "List"
 - **Value:** Name of the predefined value
 - **Description:** Optional description of the value
- **Number:** A numerical value is expected.
- **Date:** A date is expected.



Description: Optional description of the attribute

- ▶ Using the up and down arrows, you can change the order of the additional attributes.
- ▶ In the device **System Information**, you can set the values for the attributes.

Attribute	Value
Name	
Site	
Comment	
Department	
Cost Center	
Asset ID	
In-Service Date	
Serial Number	
DeviceAttribute_Subdepartments	KB

Administrative Tasks

Menu path: **UMS Administration > Global Configuration > Administrative Tasks**

You can define administrative tasks for the UMS. A task consists in sending an action automatically at a defined time. Examples of such actions include creating a database backup (for embedded databases only) or removing unused firmware files. Tasks can be repeated at intervals or on specific days of the week.

-
- [Create Administrative Task](#)(see page 464)

Create Administrative Task

Menu path: **UMS Administration > Global Configuration > Administrative Tasks**

To create an administrative task, proceed as follows:

1. Click on
2. In the **Create Administrative Task** dialog, configure the necessary settings. What settings are available depends on the chosen **action**. The settings are spread over a number of pages. You can switch between these by clicking on **Next** and **Back**.

The following actions are available:

- [Create Data Backup](#)(see page 465)
- [Remove Unused Firmwares](#)(see page 467)
- [Delete Logging Data](#)(see page 468)
- [Delete Job Execution Data](#)(see page 470)
- [Delete Administrative Task Execution Data](#)(see page 472)
- [Delete Process Events](#)(see page 474)
- [Delete Devices](#)(see page 475)
- [Export View Result via Mail](#)(see page 476)
- [Save View Results in the File System](#)(see page 478)



- [Assign Objects to the Devices of Views\(see page 480\)](#)
- [Delete Asset Information History\(see page 481\)](#)
- [Send Notification Information via Email\(see page 482\)](#)

3. Click on **Finish**.

The task is defined and will be shown in the content panel.

Create Data Backup

Menu path: **UMS Administration > Administrative Tasks >** Dialog "**Create Administrative Task**" > Action "**Create backup**"

You can define a scheduled backup of the database as an administrative task.

General

Name: Name for the task.

Action: "**Create backup**".

Description: Optional description of the task.

Send result as mail

The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under [Mail Settings\(see page 501\)](#).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

The task will be executed at the set time. (Default)

The task will not be executed.

Configuration

Maximum amount of backups: If the number of backup files defined in **Target directory** of the data backup package is reached, the oldest backup file will be deleted when a new backup is created. The value "0" means that the number of backup files is unlimited.

Target directory for created backup: Local directory path on the UMS Server in which the backup files are saved.

- ⓘ Ensure that the target directory is a valid local directory path on the UMS Server. The UMS Server can be on a different computer, i.e. not on the one where the UMS Console is located.

Backup components: Select at least one of the following components:

- ["Database \(embedded DB only\)"](#)
- ["Configurations"](#)
- ["Transfer files \(embedded DB only\)"](#)



Server Assignment

- i** The **Server Assignment** settings page is displayed only if you deploy **High Availability**(see page 657) environment.

Assignment type

Possible options:

- "One server (random)": The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- "One server (select one)": You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- "All servers": The task will be executed by all servers.

Assigned servers: List of servers that are available for this task.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

- The task will be repeated at the set time interval.
 The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

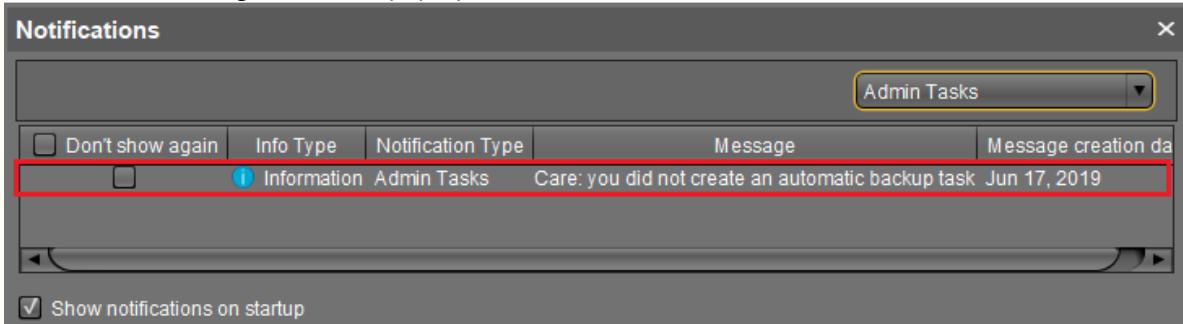
Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via . Further information on the public holiday lists can be found under **Misc**(see page 317).

Expiration: Point in time as of which the task will no longer be repeated.

⚠ Administrative Tasks Notification

If you have not set an administrative task "[Create Data Backup](#)(see page 465)", after the start of the UMS Console, the following notification pop-up will be shown:





Only users with read permission for administrative tasks can see this notification. You can set the rights under **Edit > Access control**.

You can manage the display settings under **Misc > Settings > Notifications**.

You can find the notifications under **Help > Notifications**.

Remove Unused Firmwares

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Remove unused firmwares"**

You can define the removal of unused firmware as an administrative task.

- (i) The first firmware that was registered in your UMS installation can not be removed.

General

Name: Name for the task.

Action: "Remove unused firmwares".

Description: Optional description of the task.

Send result as mail

- The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

- The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under [Mail Settings](#)(see page 501).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

- The task will be executed at the set time. (Default)
- The task will not be executed.

Server Assignment

- (i) The **Server Assignment** settings page is displayed only if you deploy [High Availability](#)(see page 657) environment.

Assignment type

Possible options:

- "One server (random)": The server for this task will be automatically selected from the servers listed under **Assigned servers**.



- "One server (select one)": You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- "All servers": The task will be executed by all servers.

Assigned servers: List of servers that are available for this task.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

- The task will be repeated at the set time interval.
- The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via . Further information on the public holiday lists can be found under [Misc](#)(see page 317).

Expiration: Point in time as of which the task will no longer be repeated.

Delete Logging Data

Menu path: **UMS Administration > Administrative Tasks >** Dialog "**Create Administrative Task**" > Action "**Delete logging data**"

You can define the deletion of UMS message and event logs as an administrative task.

- The logs for [Secure Shadowing](#)(see page 401) as well as [performance logs](#)(see page 501) will not be deleted as a result of this administrative task.

General

Name: Name for the task.

Action: "**Delete logging data**".

Description: Optional description of the task.

Send result as mail

- The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

- The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under [Mail Settings](#)(see page 501).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active



- The task will be executed at the set time. (Default)
- The task will not be executed.

Configuration

Target directory for export files: Local directory path on the UMS Server in which the backup files are saved. If you leave the field empty, the directory \rmguiserver\temp will be used. The file names will be formed as follows: Igel_log_events_.xml, Igel_log_messages_.xml.

- ⓘ Ensure that the target directory is a valid local directory path on the UMS Server. The UMS Server can be on a different computer from the one on which the UMS Console is located. If you do not specify a directory, the data will automatically be exported to the following directory: C:\Program Files\IGEL\RemoteManager\rmguiserver\temp

The following deletion settings specify which data from the **Delete logging data** administrative task are deleted. The deletion settings only take effect if this administrative task is executed.

Log message deletion settings

- **Keep no more than [number] messages:** When this administrative task is executed, the oldest log entries will be deleted so that the number of log entries set here is retained. (Default: 10,000)
Example: In the UMS, 100 log entries are saved. In the administrative task, **Keep no more than 10 messages** is set. When the administrative task is executed, the 90 oldest log entries will be deleted while the 10 newest log entries will be retained.
- **Delete messages older than [number] days:** Message log entries that are older than the number of days specified here will be deleted. (Default: 5)

Log event deletion settings

- **Keep no more than [number] events:** The oldest event log entries will be deleted so that the number of event log entries set here is retained. (Default: 10,000)
Example: In the UMS, 100 event log entries are saved. In the administrative task, **Keep no more than 10 events** is set. When the administrative task is executed, the 90 oldest event log entries will be deleted while the 10 newest event log entries will be retained.
- **Delete events older than [number] days:** Event log entries that are older than the number of days specified here will be deleted. (Default: 5)

Server Assignment

- ⓘ The **Server Assignment** settings page is displayed only if you deploy [High Availability](#)(see page 657) environment.

Assignment type

Possible options:

- "One server (random)": The server for this task will be automatically selected from the servers listed under **Assigned servers**.



- "One server (select one)": You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- "All servers": The task will be executed by all servers.

Assigned servers: List of servers that are available for this task.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

- The task will be repeated at the set time interval.
- The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via . Further information on the public holiday lists can be found under [Misc](#)(see page 317).

Expiration: Point in time as of which the task will no longer be repeated.

Administrative Task Notification

If you have not set an administrative task "[Delete Logging Data](#)(see page 468)", after the start of the UMS Console, the following notification pop-up will be shown:

Notifications				
<input type="checkbox"/> Don't show again	Info Type	Notification Type	Message	Message creation date
<input type="checkbox"/>	Information	Admin Tasks	Care: you did not create an automatic backup task	May 22, 2019
<input type="checkbox"/>	Information	Admin Tasks	Care: you did not create a cleanup task for Delete job execution data	May 22, 2019
<input type="checkbox"/>	Information	Admin Tasks	Care: you did not create a cleanup task for Delete logging data	May 22, 2019

Only users with read permission for administrative tasks can see this notification. You can set the rights under **Edit > Access control**.

You can manage the display settings under **Misc > Settings > Notifications**.

You can find the notifications under **Help > Notifications**.

Delete Job Execution Data

Menu path: **UMS Administration > Administrative Tasks > Dialog "Create Administrative Task" > Action "Delete job execution data"**

You can define the deletion of the results of [Jobs](#)(see page 425) as an administrative task.

General

Name: Name for the task.

Action: "Delete job execution data".

Description: Optional description of the task.



Send result as mail

- The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

- The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under [Mail Settings](#)(see page 501).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

- The task will be executed at the set time. (Default)
- The task will not be executed.

Configuration

Target directory for export files: Directory on the UMS Server in which the logging data are to be backed up before they are deleted from the UMS database. The data will only be deleted from the database if the backup was successful. If you leave the field empty, the directory \rmguiserver\temp will be used. The file name for the logging data is structured as follows: Igel_deleted_job_exec_.csv.

Deletion settings: You can specify here the criteria according to which task protocols are deleted.

- **Keep no more than [number] executions per job:** Each job has executions. Each execution can have thousands of results. This task deletes all executions and their results except for the specified number of the newest executions. (Default: 10)
- **Delete events older than [number] days:** Protocols that are older than the number of days specified here will be deleted. (Default: 5)

Server Assignment

- ⓘ The **Server Assignment** settings page is displayed only if you deploy [High Availability](#)(see page 657) environment.

Assignment type

Possible options:

- "One server (random)Assigned servers.
- "One server (select one)": You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- "All servers": The task will be executed by all servers.

Assigned servers: List of servers that are available for this task.

Schedule

Start: Point in time at which the task is executed.



Task starts every [number of time units]

- The task will be repeated at the set time interval.
- The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via  . Further information on the public holiday lists can be found under [Misc\(see page 317\)](#).

Expiration: Point in time as of which the task will no longer be repeated.

Administrative Task Notification

If you have not set an administrative task "[Delete Job Execution Data\(see page 470\)](#)", after the start of the UMS Console, the following notification pop-up will be shown:

Notifications					
	Don't show again	Info Type	Notification Type	Message	Message creation date
<input type="checkbox"/>	<input type="checkbox"/>	Information	Admin Tasks	Care: you did not create an automatic backup task	May 22, 2019
<input type="checkbox"/>	<input type="checkbox"/>	Information	Admin Tasks	Care: you did not create a cleanup task for Delete job execution data	May 22, 2019
<input type="checkbox"/>	<input type="checkbox"/>	Information	Admin Tasks	Care: you did not create a cleanup task for Delete logging data	May 22, 2019

Only users with read permission for administrative tasks can see this notification. You can set the rights under **Edit > Access control**.

You can manage the display settings under **Misc > Settings > Notifications**.

You can find the notifications under **Help > Notifications**.

Delete Administrative Task Execution Data

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Delete administrative task execution data"**

You can define the deletion of the results of [Administrative Tasks\(see page 464\)](#) as an administrative task.

General

Name: Name for the task.

Action: "**Delete administrative task execution data**".

Description: Optional description of the task.

Send result as mail

- The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

- The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under [Mail Settings\(see page 501\)](#).



Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

- The task will be executed at the set time. (Default)
- The task will not be executed.

Configuration

Directory for export files: Directory on the UMS Server in which the logging data are to be backed up. The data will only be deleted from the database if the backup was successful. If you leave the field empty, the directory \rmguiserver\temp will be used. The file name for the logging data is structured as follows:

Igel_deleted_job_exec_.csv.

Keep no more than [number] executions per administrative task: Each administrative task has executions. Each execution can have thousands of results. This task deletes all executions and their results except for the specified number of the newest executions. (Default: 10)

Delete events older than [number] days: Event log entries that are older than the number of days specified here will be deleted. (Default: 5)

Server Assignment

- (i) The **Server Assignment** settings page is displayed only if you deploy [High Availability](#)(see page 657) environment.

Assignment type

Possible options:

- "One server (random)": The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- "One server (select one)": You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- "All servers": The task will be executed by all servers.

Assigned servers: List of servers that are available for this task.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

- The task will be repeated at the set time interval.
- The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via . Further information on the public holiday lists can be found under [Misc](#)(see page 317).



Expiration: Point in time as of which the task will no longer be repeated.

Delete Process Events

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Delete process events"**

You can define the deletion of process events as an administrative task.

General

Name: Name for the task.

Action: "Delete process events".

Description: Optional description of the task.

Send result as mail

- The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

- The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under [Mail Settings](#)(see page 501).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

- The task will be executed at the set time. (Default)
- The task will not be executed.

Configuration

Directory for exported files: Directory on the UMS Server in which the logging data are to be backed up before they are deleted from the UMS database. The data will only be deleted from the database if the backup was successful. If you leave the field empty, the directory \rmguiserver\temp will be used. The file name for the logging data is structured as follows: Igel_deleted_job_exec_.csv.

Keep no more than [number] process events: When this administrative task is executed, the oldest log entries will be deleted so that the number of log entries set here is retained. (Default: 1,000)

Example: In the UMS, 100 log entries are saved. In the administrative task, **Keep no more than 10 process events** is set. When the administrative task is executed, the 90 oldest log entries will be deleted while the 10 newest log entries will be retained.

Delete events older than [number] days: Event log entries that are older than the number of days specified here will be deleted. (Default: 5)

Server Assignment

- i** The **Server Assignment** settings page is displayed only if you deploy [High Availability](#)(see page 657) environment.



Assignment type

Possible options:

- "One server (random)": The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- "One server (select one)Assigned servers.
- "All servers

Assigned servers: List of servers that are available for this task.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

- The task will be repeated at the set time interval.
 The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via . Further information on the public holiday lists can be found under [Misc\(see page 317\)](#).

Expiration: Point in time as of which the task will no longer be repeated.

Delete Devices

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Delete devices"**

You can define an administrative task as a result of which specific devices will be deleted from the UMS database. Which devices are to be deleted is defined through the criteria of a view. Example: All devices that have not been booted for more than a year.

General

Name: Name for the task.

Action: "**Delete devices**".

Description: Optional description of the task.

Send result as mail

- The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

- The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under [Mail Settings\(see page 501\)](#).



Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

- The task will be executed at the set time. (Default)
- The task will not be executed.

Configuration

Attach to view: View which specifies the criteria for deleting devices. The view is selected via the  button.

View ID: ID of the selected view.

Server Assignment

- (i) The **Server Assignment** settings page is displayed only if you deploy [High Availability](#)(see page 657) environment.

Assignment type

Possible options:

- "[One server \(random\)Assigned servers.](#)
- "One server (select one)": You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- "All servers": The task will be executed by all servers.

Assigned servers: List of servers that are available for this task.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

- The task will be repeated at the set time interval.
- The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via  . Further information on the public holiday lists can be found under [Misc](#)(see page 317).

Expiration: Point in time as of which the task will no longer be repeated.

Export View Result via Mail

Menu path: **UMS Administration > Administrative Tasks >** Dialog **Create Administrative Task > Action "Export view result via mail"**



You can define an administrative task as a result of which the results of a view will be exported as a mail attachment.

- (i) In order for emails to be sent, the UMS mail settings must be correct. Further information can be found under [Mail Settings](#)(see page 501).

General

Name: Name for the task.

Action: "Export view result via mail".

Description: Optional description of the task.

Send result as mail

- The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

- The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under [Mail Settings](#)(see page 501).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

- The task will be executed at the set time. (Default)
- The task will not be executed.

Configuration

View ID: ID of the selected view. The view is selected via the button.

Visible columns configuration: Data fields which the email will contain.

View export name: Custom name for the export file (optional). Date and time will be added automatically, separated by an underscore. Example: CUSTOMNAME_2021-05-02_10-34.xml

Mail recipients: Email addresses of the recipients. If you enter a number of addresses, you must separate them using a semicolon ";".

Result format: Data format in which the results are sent as a mail attachment.

Possible options:

- "XML"
- "HTML"
- "CSV"

Create archive

- The mail attachment will be compressed as a ZIP archive.
- The mail attachment will retain its data format (XML, HTML, or CSV). (Default)



Server Assignment

- i** The **Server Assignment** settings page is displayed only if you deploy **High Availability**(see page 657) environment.

Assignment type

Possible options:

- "One server (random)Assigned servers.
- "One server (select one)": You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- "All servers": The task will be executed by all servers.

Assigned servers: List of servers that are available for this task.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

- The task will be repeated at the set time interval.
 The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via . Further information on the public holiday lists can be found under **Misc**(see page 317).

Expiration: Point in time as of which the task will no longer be repeated.

Save View Results in the File System

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Save view results in the file system"**

You can define an administrative task as a result of which the results of a view will be saved in the file system of the UMS Server.

General

Name: Name for the task.

Action: "**Save view results in the file system**".

Description: Optional description of the task.

Send result as mail

- The result of the task will be sent to the specified recipients via email.



The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under [Mail Settings](#)(see page 501).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

- The task will be executed at the set time. (Default)
- The task will not be executed.

Configuration

View ID: ID of the selected view. The view is selected via the button.

Visible columns configuration: Data fields which the email will contain. The data fields are selected via the button. With the checkbox next to **Column name**, you can select all data fields at once.

View export name: Custom name for the export file (optional). Date and time will be added automatically, separated by an underscore. Example: CUSTOMNAME_2021-05-02_10-34.xml

Target directory for export files: Directory on the UMS Server in which the view results are saved. If no directory is specified, the default directory will be used. The target directory is shown under the entry field.

Result format: Data format in which the results are saved:

Possible options:

- "XML"
- "HTML"
- "CSV"

Create archive

- The file is compressed as a ZIP archive.
- The file retains its data format (XML, HTML, or CSV). (Default)

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

- The task will be repeated at the set time interval.
- The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via . Further information on the public holiday lists can be found under [Misc](#)(see page 317).

Expiration: Point in time as of which the task will no longer be repeated.



Assign Objects to the Devices of Views

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Assign objects to the devices of views"**

You can assign objects to devices that you have filtered via a view or search and update this assignment regularly using a schedule.

See also the instructions in [Assigning Objects to a View](#)(see page 424).

General

Name: Name for the task.

Action: "Assign objects to the devices of views".

Description: Optional description of the task.

Send result as mail

- The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

- The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under [Mail Settings](#)(see page 501).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

- The task will be executed at the set time. (Default)
- The task will not be executed.

Select Views / Device Searches

- ▶ Click on  to select views or device searches that will be assigned to one or more objects.

Select Objects

- ▶ Click on  to select one or more objects to which you would like to assign the views or device searches.

Objects can be

- profiles
- firmware customizations
- files
- firmware updates.

Server Assignment

 The **Server Assignment** settings page is displayed only if you deploy [High Availability](#)(see page 657) environment.



Assignment type

Possible options:

- "One server (random)": The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- "One server (select one)Assigned servers.
- "All servers

Assigned servers: List of servers that are available for this task.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

- The task will be repeated at the set time interval.
 The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via . Further information on the public holiday lists can be found under [Misc\(see page 317\)](#).

Expiration: Point in time as of which the task will no longer be repeated.

Delete Asset Information History

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Delete asset information history"**

You can define the deletion of the history of [asset information\(see page 699\)](#) as an administrative task.

General

Name: Name for the task.

Action: "**Delete asset information history**".

Description: Optional description of the task.

Send result as mail

- The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under [Mail Settings\(see page 501\)](#).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".



Active

- The task will be executed at the set time. (Default)
- The task will not be executed.

Configuration

Target directory for export files: Directory on the UMS Server in which the asset data are to be backed up. If you leave the field empty, the directory C:/Program Files/IGEL/RemoteManager/rmguiserver/temp will be used.

History deletion settings

Delete asset info history older than: Indication in days how old the information to be deleted should be. (Default: 5)

Delete only unused assets:

- Only unused assets are deleted in the specified time period. (Default)
- All assets are deleted in the specified time period.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

- The task will be repeated at the set time interval.
- The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via . Further information on the public holiday lists can be found under [Misc\(see page 317\)](#).

Expiration: Point in time as of which the task will no longer be repeated.

Send Notification Information via Email

Menu path: **UMS Administration > Global Configuration > Administrative Tasks > Dialog Create Administrative Task > Action "Send notification information via email"**

You can send a [notification\(see page 229\)](#) information via email scheduled with an administrative task.

General

Name: Name for the task.

Action: "Send notification information via email".

Description: Optional description of the task.

Send result as mail

- The result of the task will be sent to the specified recipients via email.



The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

- The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under [Mail Settings](#)(see page 501).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

- The task will be executed at the set time. (Default)
- The task will not be executed.

Configuration

Mail recipients: Email address(es) of the recipients.

Result format: Data format in which the results of the task are sent as a mail attachment.

Possible options:

- "XML" (Default)
- "HTML"
- "CSV"

Create archive

- An archive is created.
- No archive is created. (Default)

Export: Defines whether all notifications or only new ones have to be exported.

Possible options:

- **All notifications** (Default)
- **Only new notifications**

Export notifications about: Defines the [type of notifications](#)(see page 322) that will be exported.

Possible options:

- **Universal Firmware Updates**
- **Universal Management Licenses**
- **Device Licenses**
- **Disk Usage**
- **Global Notifications**

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

- The task will be repeated at the set time interval.
- The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.



Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via ■■■. Further information on the public holiday lists can be found under **Misc**(see page 317).

Expiration: Point in time as of which the task will no longer be repeated.

Proxy Server

Menu path: **UMS Administration > Global Configuration > Proxy Server**

In this area, you can add and configure proxy servers in order to use them in the following scenarios:

- [IGEL Cloud Gateway⁹³](#)
- [Automatic license distribution⁹⁴](#)
- [Universal Firmware Update⁹⁵](#)
- [UMS update check⁹⁶](#)

ⓘ After an update to UMS Version 5.08.100, the proxy server that was previously used for the Universal Firmware Update will be adopted as the default proxy server.

The automatic license distribution, Universal Firmware Update and UMS update check scenarios are automatically linked to the default proxy server.

ⓘ The settings for the IGEL Cloud Gateway are not changed; the proxy server must be added manually here.

Proxy Server

All configured proxy servers are shown in this list.

- **Show passwords**
 - Passwords are made visible in the list.
 - Passwords are not shown. (Default)

	Add proxy server
	Delete proxy server
	Edit proxy server

⁹³ <https://kb.igel.com/display/endpointmgmt509/Cloud+Gateway+Configuration>

⁹⁴ <https://kb.igel.com/display/endpointmgmt509/Deployment>

⁹⁵ <https://kb.igel.com/display/endpointmgmt509/Universal+Firmware+Update+Administration>

⁹⁶ <https://kb.igel.com/display/endpointmgmt509/Help>



<input checked="" type="checkbox"/>	Define selected proxy server as default server
-------------------------------------	--

- i** Only servers that are not used can be deleted. The proxy server added first will automatically be the default proxy server.

Proxy Server Uses

All uses for the selected proxy servers are shown in this list.

The entries in this list appear automatically as soon as an application was linked to a selected proxy server.

Default Directory Rules

Menu path: **UMS Administration > Global Configuration > Default Directory Rules**

Rules for default directories are used to automatically classify devices into specific directories during registration. These directories can be linked to profiles which are then assigned to the devices contained. As a result, you can automatically configure the devices during registration (zero touch deployment).

See also the following how-tos for further information:

- [Creating a Default Directory Rule](#)(see page 487)
- [Using Structure Tags](#)(see page 97)

► Go to **UMS Administration > Global Configuration > Default Directory Rules**.

The user interface looks like this:

Default Directory Rule Configuration		Find:			↑ ↓	← →	☰	⊕ ⊖	✖	✖	✖	✖	✖
Rule	Directory		Overriding	Apply on boot									
▼ Default Directory Rules													
▼ Product name is like (?i).*LX.*	/Thin Clients/Linux/												Double-click to edit item
▼ OS type is like (?i).*Windows.*													
Product ID is like (?i).*64bit.*	/Thin Clients/Windows/64bit/	✓	✓										
Product ID is like (?i).*W7*	/Thin Clients/Windows/32bit/	✓	✓										

- i** When you open a UMS database from an older version with UMS Version 5.03.100 or newer for the first time, the default directory rules will automatically be converted into the new structure. Rules for the IP range will be split into two rules (IP greater than and IP less than).



Symbol Bar

Menu path: **UMS Administration > Global Configuration > Default Directory Rules**

In the symbol bar for default directory rules, you will find buttons for frequently used commands:



The symbols are as follows (in the correct order):

	Find (in all columns)
	Expand all rules
	Collapse all rules
	Move rule a level up
	Move rule a level down
	Move rule up in the sequence
	Move rule down in the sequence
	Add rule (as last child of the currently selected rule)
	Delete rule (including subordinate rules)
	Cut objects
	Copy objects
	Paste objects
	Edit



Creating a Default Directory Rule

Menu path: **UMS Administration > Global Configuration > Default Directory Rules**

1. Click on the symbol.
2. The **Create Default Directory Rule** dialog will open.
3. Select a **criterion**. To help you, a search field narrows down the selection to matching parameter names while you type.

The screenshot shows the 'Create default directory rule' dialog with the title 'Select criterion'. A search bar at the top contains the text 'ver'. Below it, a section titled 'Asset Inventory' is expanded, showing three radio button options: 'BIOS Version' (selected), 'Firmware Version', and 'Flash Player Version'. At the bottom are navigation buttons: '< Back' (disabled), 'Next >', 'Finish', and 'Cancel'.

4. Specify the comparative value and comparative operator for the criterion.



Create default directory rule

Version search

Version number exact above below Not like

Use regular expression

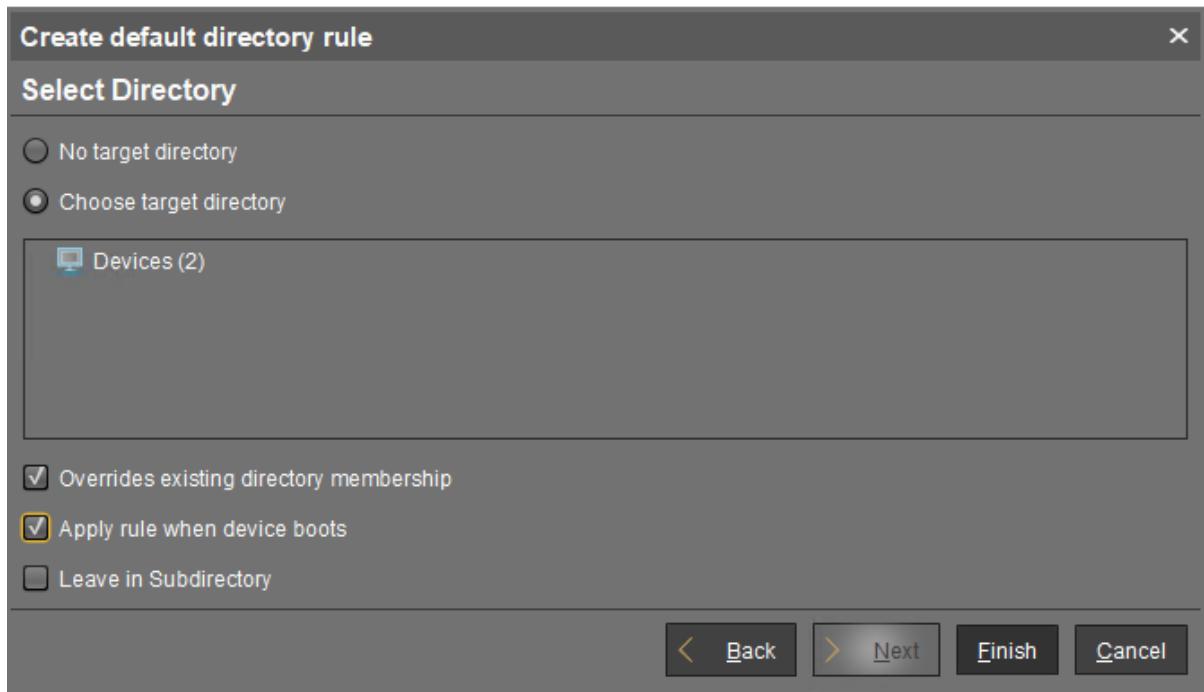
Back Next Finish Cancel

- i** If you create a rule which contains a range (from - to), this will automatically be converted into a pair of rules linked with AND (from AND to). This applies for example to date or IP ranges.

5. Select a target directory (must already exist) or select the **No target directory** option.

With the **Choose target directory** option, you have the following further options:

- **Overrides existing directory membership**
 A previously registered device is re-registered in the target directory.
- **Apply rule when device is booting**
 The rule is applied not only when registering but also each time the devices boot.
- **Leave in Subdirectory**
 A device will not be moved if it is already in a subdirectory of the target directory.



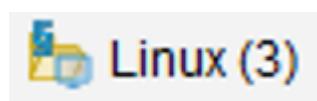
6. Finish creating the rule by clicking on **Finish**.

- i** The order of the rules is important. Generally speaking, the default directory rules tree is worked through from top to bottom for each device. If the criterion of a rule applies and it has a target directory, its children rules will be scrutinized. If none of the children rules apply, the device will be moved to the target directory of the rule above. If however one of the children rules applies and it has a target directory, this child rule will be taken as a new starting rule and the search will begin again. If an applicable rule does not have a target directory, its children rules will be scrutinized.

Finding Default Directory Rules

From UMS Version 5.03.100 only:

In the structure tree, you can see which directories are the target of a default directory rule. The folder symbol then has a small § symbol.



- i** A directory which is the target of a default directory rule cannot be deleted. In order to delete it, you must change or delete the directory rule first.

To jump from the directory straight to linked rules, proceed as follows:



1. Right-click on the folder symbol.
2. Select **Find default directory rules** in the context menu.
The view will switch to the overview of the default directory rules. The first linked rule is highlighted.
3. Press the enter key to jump to further found rules.

Applying Rules

The rules can be applied regardless of new clients being imported or existing clients booting:

From UMS Version 5.03.100:

1. Right-click on **Default Directory Rules** under **UMS Administration > Global Configuration**.
2. Select **Apply rules now...**
A dialog with further options will open.
3. Select from the following options:
 - **Overrides all existing directory memberships**
 A previously registered device is re-registered in the target directory.
 - **Default directory for devices:**
 - Leave in current directory
 - Device root directory
 - Other directory (select)
4. Click **Apply** to apply the rules.

Prior to UMS Version 5.03.100:

1. Click on the **Apply rules now...** button in the overview of directory rules.
A dialog with further options will open.
2. Select from the following options:
 - **Overwrite all existing directory allocations**
 A previously registered device is re-registered in the target directory.
 - **Default directory for devices:**
 - Leave in current directory
 - Basic directory for devices
 - Other directory (select)
3. Click **Apply** to apply the rules.

Editing a Rule

From UMS Version 5.03.100:

- In the rule overview, double-click on a row...
- in the **Rule** column in order to edit the **Criterion, Operator** and **Value**.
 - in the **Directory** column in order to change or remove the target directory.



- in the **Overriding**, **Apply on boot** or **Leave in subdirectory** column in order to change [these options](#)⁹⁷.

Rule	Directory	Overriding	Apply on boot
Default Directory Rules			
Product name is like (?i).*LX.*	/Thin Clients/Linux/		
OS type is like (?i).*Windows.*			
Double-click to edit item	/Thin Clients/Windows/64bit/	✓	✓
Product ID is like (?i).*W7*	/Thin Clients/Windows/32bit/	✓	✓

Prior to UMS Version 5.03.100:

- Highlight the desired rule in the overview by clicking on it once.
 - Click the symbol
 - The **Modify Default Directory Rule** window will open.
 - Change the **Directory**, **Criterion**, **Operator**, **Value** and options as required.
- You can also add further conditions with AND or OR links here, see [Combining conditions](#)⁹⁸.

Combining Conditions

In the *UMS*, you can combine the conditions of directory rules using AND and OR links.

From UMS Version 5.03.100:

- Indent a rule using in order to create an AND link with the condition of the superordinate rule:

Rule	Directory	Overriding
Default Directory Rules		
Product name is like (?i).*LX.*	/Thin Clients/Linux/	
OS type is like (?i).*Windows.*		
AND Product ID is like (?i).*64bit.*	/Thin Clients/Windows/64bit/	✓
Product ID is like (?i).*W7*	/Thin Clients/Windows/32bit/	✓

Example: In the illustration, devices whose **product ID** contains Windows AND 64bit are moved to the /devices/Windows/64bit/ directory.

⁹⁷ <https://kb.igel.com/display/endpointmgmt601/Creating+a+Default+Directory+Rule>

⁹⁸ <https://kb.igel.com/display/endpointmgmt601/Combining+Conditions>



- i** You can use rules which do not have a target directory (linking rules) to combine conditions.

- Leave rules equally indented and assign to them the same target directory in order to create an OR link for the conditions.

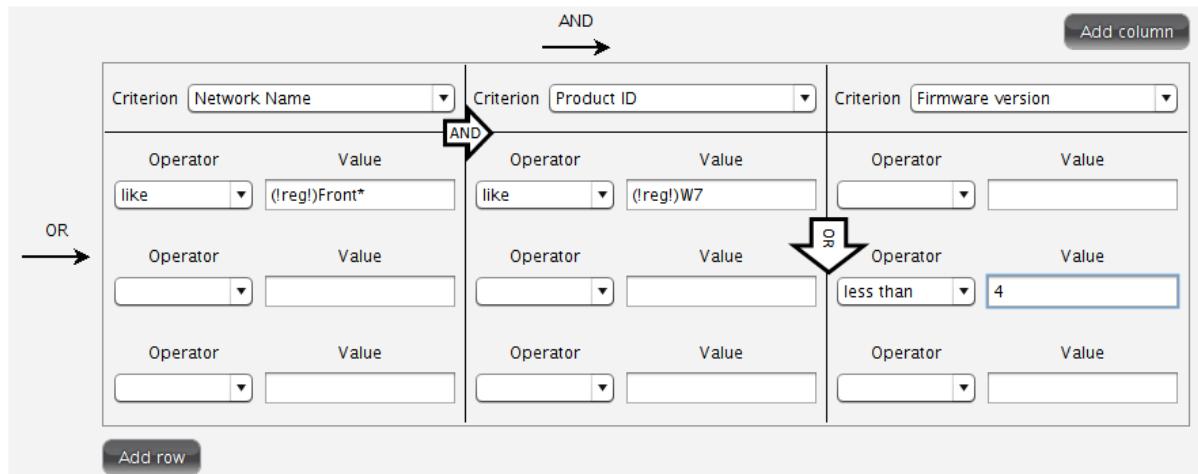
Rule	Directory	Overriding
Default Directory Rules		
Product name is like (?i).*LX.*	/Thin Clients/Linux/	
OS type is like (?i).*Windows.*		
Product ID is like (?i).*64bit.*	/Thin Clients/Windows/64bit/	✓
Product ID is like (?i).*W10*	/Thin Clients/Windows/64bit/	✓
Product ID is like (?i).*W7*	/Thin Clients/Windows/32bit/	✓

Example: In the illustration, devices whose **product ID** contains 64bit OR W10 are moved to the /devices/Windows/64bit/ directory.

- i** You can move rules and groups of rules using drag and drop or by copying and pasting with the help of the symbol bar.

Prior to UMS Version 5.03.100:

- When adding a new rule:
 - Select **Narrow search criterion** in the wizard to add an AND-linked condition.
 - Select **Create additional search criterion** to add an OR-linked condition.
- When editing an existing rule:
 - Add a further condition on the right-hand side to create an AND link.
 - Add a further condition below to create an OR link.



Using the Netmask

When creating a directory rule, select the criterion **Net mask**. The thin clients will then be sorted into automatically created directories according to IP address ranges. The name of the folder is determined through this bitwise operation:

Folder = IP address of the thin client AND net mask

Examples:

IP address	Net mask	Resulting directory
130.094.122.195	255.255.255.224	130.094.122.192
172.16.232.15	255.255.0.0	172.16.0.0
192.168.1.1	255.255.255.0	192.168.1.0

As the **target directory**, select the device directory under which the subfolders for the IP address ranges are to be created.

Because this rule always applies, it is not a good idea to define a further rule. If the net mask rule sorts all devices into directories, no further rule is active.

Universal Firmware Update

Menu path: **UMS Administration > Global Configuration > Universal Firmware Update**

Here, you can configure the connection to the IGEL firmware server and the connection to an FTP server.

You can use an FTP server for distributing firmware updates to devices, as an alternative to the WebDAV capability of the UMS. If your devices are connected via ICG, an FTP server is required.

Edit....: Changes the Universal Firmware Update settings and the FTP server settings.

Proxy server: Optional proxy server to access the IGEL firmware server.



The FTP server settings where the files are downloaded to (optional): Changes the settings of the FTP server which is used by the devices for the firmware downloads.

Protocol: Protocol and mode to be used.

Possible options:

FTP: FTP in active mode (Default)

FTP passive: FTP in passive mode

FTPS: FTPS in active mode

FTPS passive: FTPS in passive mode

SFTP: SFTP

Host: Hostname of the server

Port: Port number. (Default: 21 for FTP and FTPS, 22 for SFTP)

User name: Name of the user

Password: User password

Directory: Path of the FTP server

- ⓘ For the SFTP protocol, the path must be defined as an absolute path on the SFTP server. For FTP and FTPS, relative paths are also valid.

Edit proxy configuration:

Possible options:

- **No proxy server:** Direct connection to the configured server.
- **Use default proxy server:** Use the proxy server which is configured as default in [Proxy Server](#).(see [page 484](#))
- **Use selected proxy server:** Select a proxy server from the list.

Test server connection: Tests communication between the IGEL server and your FTP server.

Synchronize downloaded Universal Firmware Updates within UMS WebDAV directories

- Downloaded Universal Firmware Updates are automatically synchronized between the servers in a High Availability (HA) network. This applies only if a WebDAV directory is configured as the target path for the download. See [How to Detect Which Files Are Synchronized Automatically](#)(see [page 159](#)).
- The Universal Firmware Updates are not synchronized between the HA servers.



The screenshot shows the UMS Administration interface under the 'Server' tab. The left sidebar lists various administration categories, with 'Universal Firmware Update' selected and highlighted in blue. The main right panel displays the 'Universal Firmware Update' configuration settings. At the top, there are three buttons: 'Edit...', 'Edit proxy configuration', and 'Test server connection'. Below these are sections for 'Universal update settings' and 'The FTP server settings where the files are downloaded to (optional)'. In the 'Universal update settings' section, a checkbox is checked for 'Synchronize downloaded Universal Firmware Updates within UMS WebDAV directories'. In the 'FTP server settings' section, the protocol is set to 'FTP', host is '<ftpServername>', port is '21', user name is '<ftpUser>', password is masked, and directory is '<ftpServerpath>'.

Further information regarding the Universal Firmware Update can be found under [Universal Firmware Update](#)(see page 433).

Wake-on-LAN

Menu path: **UMS Administration > Global Configuration > Wake On LAN Configuration**

Devices can be wakened via the network using *magic packets*. A *magic packet* contains the MAC addresses of the devices that are to be wakened. In order for a device to be wakened, it must be in either S3 (suspend to RAM – STR), S4 (suspend-to-disk – STD) or S5 (soft-off) mode. In the *UMS* administration, you can specify the network addresses to which the *magic packets* are sent.

For scenarios where the *UMS* is outside the devices' network and broadcast packets from the WAN are not allowed, you can define one or more Linux devices as a Wake-On-LAN proxy.

- i The Wake-On-LAN proxy function is supported by Linux devices from *Version 5.09.100*.

- **Broadcast address**
 - The *magic packet* will be sent to the broadcast address of the network.
- **Last known IP address of the Device**
 - The *magic packet* will be sent to the last known IP address of the device.
- **Automatic Wake On LAN Proxy Detection**
 - If any other client in the subnet is online, this client is automatically used as WoL proxy.
- **All defined subnets**
 - The *magic packet* will be sent to the network addresses of all subnets that are defined for the *UMS*.



To add a subnet, proceed as follows:

- a. Click on in the area below **All defined subnets**.
The **Define subnets** dialog will open.
- b. In the **Subnet** field, enter the network address of the subnet.
- c. Under **CIDR** (Classless Inter-Domain Routing), select the suitable suffix for the network mask.

i Values between 8 and 28 are appropriate. Example 1: The network address 10.43.8.0 with the suffix 24 corresponds to the CIDR notation 10.43.8.0/24 with the network mask 255.255.255.0. This network corresponds to a Class C network. The addresses that can be used by hosts lie between 10.43.8.1 and 10.43.8.254. Example 2: The network address 10.43.8.64 with the suffix 28 corresponds to the CIDR notation 10.43.8.64/28 with the network mask 255.255.255.240. The addresses that can be used by hosts lie between 10.43.8.65 and 10.43.8.78.

- a. If you wish, add a **Comment**.
- b. Click on **OK**.

- **Network address of the last known IP address**

The *magic packet* is sent to the network address of the network in which the last known IP address of the device is located. In order for this network address to be determined, you will need to specify a network mask for each of the possible networks.

To add a network mask, proceed as follows:

- a. Click on in the area below **Network address of the last known IP address**.
The **Define network mask** dialog will open.
- b. Enter the **Network Mask**.
- c. If you wish, add a **Comment**.
- d. Click on **OK**.

- **Wake On LAN Proxies**

The *magic packet* will be sent to the devices defined as Wake-On-LAN proxies. Each Wake-On-LAN proxy will send the *magic packets* as a broadcast within the network in which it is located.

i The **Broadcast address**, **Last known IP address of the device**, **All defined subnets** and **Network address of the last known IP** settings have no effect on the Wake-on-LAN proxy.

The *magic packet* will not be sent to the devices defined as Wake-On-LAN proxies.

i Devices configured as a Wake-on-LAN proxy will retain their role, even if **Wake-On-LAN proxies** is disabled.

To define one or more devices as a Wake-On-LAN proxy, proceed as follows:

- a. Click on in the area below **Wake On LAN Proxies**.
The **Edit Wake On LAN Proxies** dialog will open.
- b. Highlight the desired device in the left-hand column.



- c. Click on to select the device.
 - d. Click on **OK**.
- The device will now function as a Wake-On-LAN proxy.

i A device that is configured as a Wake-On-LAN proxy can no longer be put on standby or shut down. This restriction applies as soon as the device receives the settings from the UMS.

To undo the configuration as a Wake-On-LAN proxy, proceed as follows:

- a. Click on in the area below **Wake On LAN Proxies**.
The **Edit Wake On LAN proxies** dialog will open.
- b. Highlight the desired device in the right-hand column.
- c. Click on to deselect the device.
- d. Click on **OK**.
The device will no longer be configured as a Wake-On-LAN proxy as soon as the setting is sent to the device.

Active Directory / LDAP

Menu path: **UMS Administration > Global Configuration > Active Directory / LDAP**

It can make sense to link the UMS Server to an existing Active Directory for two reasons:

- You would like to import users from the AD as UMS administrator accounts.
- You would like to use user profiles via IGEL Shared Workplace.

For both purposes, you first need to link the relevant Active Directories in the **UMS Administration** area under **Global Configuration > Active Directory / LDAP**. See also the how-to [Configuring an AD Connection](#)(see page 209).

1. If you have user and group dependencies between different configured domains/subdomains, you might want to activate **Include all configured AD domains for search and import of AD users / groups**. This option activates the group search for a user within all configured domains. On activation, a confirmation dialog is shown.

i If this option is activated, a user may gain additional permissions. This will be the case if

- the user is in a group that has been discovered due to this option,
- this group has been imported under **System > Administrator accounts**,
- and permissions have been assigned to this group i.e. permissions the user would not have otherwise.

Please note that, due to the additional lookups, this option might have an impact on the performance in the following areas:

- UMS login
- Permission dialogs
- Shared Workplace (SWP)

2. Add a new entry to the list of linked Active Directories by selecting **Add (+)**.
3. Specify the **Domain Name**.



4. Enter the **Domain Controller(s)**.

- i If the option **Use LDAPS connection** (see below) is activated, a fully qualified name of the domain controller must be entered, e.g. dc01.your.domain
- i To separate several domain controllers, a semicolon must be used.

5. Specify the **Page Size**.

The page size limits the number of hits (i.e. objects) in the Active Directory on the server side. The default value is "1000". Change this value according to your server configuration.

6. Activate **Use LDAPS connection** to secure the connection with the provided certificate.

The **Port** changes automatically to the default value "636".

7. Click **Import SSL Certificate** to configure the certificate and to verify the **Certificate DN**.

- ! The **Domain Controller** name and the certificate must correspond, otherwise the connection to the LDAP server will fail. See [Problems When Configuring an Active Directory with LDAP over SSL\(see page 218\)](#).
- i If more than one domain controller is used, the root certificate of the domain must be configured.
- i The supported certificate formats are .cer, .pem and .der

8. Enter valid user data under **User name** and **Password**.

- i For the user, the read permission is sufficient since no changes will be made to the AD data.

9. Specify aliases under **UPN Suffix** if they have been configured (semicolon separated list). Example: domain.local;test.local

10. Click **Test connection** to check the connection.

- i Several Active Directories can be linked. Therefore, you should ensure that you provide the correct domain when logging in (e.g. to the UMS Console).
- i In this document, the terms "Active Directory" and "LDAP" are, to an extent, used interchangeably:
 - Administrative users / UMS administrators can be imported both from an AD and from LDAP.
 - Shared Workplace users can only authenticate against an Active Directory. An LDAP service cannot be used for this purpose.

11. Click **Ok** to save the changes.

Remote Access

Menu path: **UMS Administration > Global Configuration > Remote Access**

You can enable a secure terminal session and a secure VNC connection globally.



Secure terminal

- **Enable secure terminal globally:**
 - Access via the secure terminal is enabled for all registered devices. The firmware must be *IGEL Linux Version 5.11.100* or higher.
 - Access via the secure terminal cannot be enabled for all registered devices. However, it can be enabled for individual devices.
- **Log user for secure terminal:** Specifies whether the user name of the UMS user who established the connection to the device is logged. The log is shown under **System > Logging > Log secure access**.
 - The user name is contained in the log.
 - The user name is not contained in the log.

Secure VNC

- **Enable secure VNC globally:**
 - Access via secure VNC is enabled for all registered devices.
 - Access via secure VNC is not enabled for all registered devices. However, it can be enabled for individual devices.
- **Log user for secure VNC:** Specifies whether the user name of the UMS user who established the connection to the device is logged. The log is shown under **System > Logging > Remote Access**.
 - The user name is contained in the log.
 - The user name is not contained in the log.
- **Preferred encoding**
Possible options:
 - Tight
 - Raw
 - RRE
 - Hextile
 - Zlib
- **Color depth**
Possible values:
 - 24 bit
 - 8 bit
- **Refresh Period:** Time in milliseconds within which the display in the VNC Viewer is refreshed.
- **Compression Level:** Specifies the extent to which the transferred data are compressed.
- **JPEG Quality:** Specifies the image quality.
- **Use "Draw Rectangle" mode**
 - The "draw rectangle" mode will be used.

Override VNC viewer settings:

- The settings for the VNC Viewer will be overwritten by the settings here.
- The VNC Viewer can overwrite the settings here.



Logging

Menu path: **UMS Administration > Global Configuration > Logging**

In this area, you can specify the logging behavior of the UMS for messages and events as well as activate performance logging.

UMS Web App

Log messages for actions done in the UMS Web App are currently displayed only in the UMS Web App. For details on logging in the UMS Web App, see [Logging\(see page 754\)](#).

Log Message Settings

Enable logging

- UMS user actions will be logged.
- UMS user actions will not be logged.

Logs can be viewed via:

- 1) Menu Bar > **System > Logging > Log Messages**
- 2) Context menu of an object in the structure tree > **(Logging) > Logging: Messages**

The following options are available if **Enable logging** is activated:

Log administrator data

- The name of the administrator who started the action will be logged.
- The name will not be logged.

Log level

- Message body and details: The log tells you what action was performed on which object. Further information regarding the object is also saved.
- Message body only: The log tells you what action was performed on which object.

Log level configuration: Enables or disables logging for individual start commands. Examples: **Create profile**, **Delete view**.

Log Event Settings

Activate event logging

- Actions initiated by a device will be logged.
- Actions initiated by a device will not be logged.



- ⓘ Logs can be viewed via:
 - 1) Menu Bar > **System > Logging > Event Messages**
 - 2) Context menu of an object in the structure tree > (**Logging**) > **Logging: Event Messages**

The following option is available if **Activate event logging** is enabled:

Log level configuration: Enables or disables logging for individual start commands. Examples: **Authenticate user**, **Shut down device**.

⚠ Administrative Task Notification

If you have not set an administrative task "[Delete Logging Data](#)(see page 468)", after the start of the UMS Console, the following notification pop-up will be shown:

Notifications				
<input type="checkbox"/> Don't show again	Info Type	Notification Type	Message	Message creation date
<input type="checkbox"/>	Information	Admin Tasks	Care: you did not create an automatic backup task	May 22, 2019
<input type="checkbox"/>	Information	Admin Tasks	Care: you did not create a cleanup task for Delete job execution data	May 22, 2019
<input type="checkbox"/>	Information	Admin Tasks	Care: you did not create a cleanup task for Delete logging data	May 22, 2019

Only users with read permission for administrative tasks can see this notification. You can set the rights under **Edit > Access control**.

You can manage the display settings under **Misc > Settings > Notifications**.

You can find the notifications under **Help > Notifications**.

Performance Log Settings

Activate performance logging

- The monitoring of the UMS Server and, if available, the UMS Load Balancer is started. The monitoring provides statistical data and information on the methods called internally and their parameters, e.g. number of calls, total time execution, etc. The collected data are to be analyzed by IGEL Support.

For the proper data collection: wait for 3 minutes after enabling the performance logging and then you can either perform normal operations or start the actions you want to monitor. After stopping the monitoring, wait for 5 minutes to allow the system to collect all data.

⚠ Always consult IGEL Support before activating performance logging. The collected data can be sent to IGEL Support via UMS Console > [Help > Save support information](#)(see page 525).

- The monitoring is disabled. (Default)

In the case of [High Availability](#)(see page 657) installation: when you deactivate performance logging, check that a semaphore file [Installation directory] /umsbroker/etc/conf/statistics.lck, which is created by the UMS Load Balancer upon monitoring startup, is deleted.

Mail Settings

Menu path: **UMS Administration > Global Configuration > Mail Settings**

The mail settings described here are required for the following functions:



- [Sending a View as Mail](#)(see page 423)
- [Export view result as mail](#)(see page 476)
- Export results of the following administrative tasks as mail:
 - [Database backup \(only for embedded DB\)](#)(see page 465)
 - [Remove unused firmwares](#)(see page 467)
 - [Delete logging data](#)(see page 468)
 - [Delete job execution data](#)(see page 470)
 - [Delete Devices](#)(see page 475)
 - [Assigning Objects to a View](#)(see page 424)
- Mailing of one-off passwords for IGEL Cloud Gateway (ICG)
If you would like to use Gmail for sending mails, see [E-Mail Settings for Gmail Accounts](#)(see page 235).

Mail Settings

- **SMTP host:** Host name or IP address of the SMTP server (outbox)
- **Sender address:** Sender address which is to appear in UMS mails.
- **Activate SMTP authentication**
 - The UMS will log on to the SMTP server in order to send mails. The login data must be defined under **SMTP user name** and **SMTP password**.
- **SMTP user name:** User name when logging on to the SMTP server
- **SMTP password:** Password when logging on to the SMTP server
- **SMTP port:** Port for the connection between the UMS and the SMTP server. For unencrypted SMTP, port 25 is used by default. For SMTP-SSL, the default port is 465; for STARTTLS, it is port 587.
- **Activate SMTP-SSL**
 - The mails will be sent with SMTPS encryption.
- **Activate SMTP-STARTTLS**
 - TLS encryption for transporting mails will be enabled in accordance with the STARTTLS procedure.
- **TLS Protocols Available:** Defines the protocols used for communication with the SMTP server.

i If no protocol is selected, TLS 1.0 is used. At least one protocol has to be selected. If more than one version is selected, the best choice selected (starting from left) which is accepted by the SMTP server is used.
- **Send Test Mail:** If you click on this button, the UMS will send a test mail. You have two options:
 - Test mail will be sent to the sender address (no sender address configured). (Default)
 - Send test mail to the following address
- **Result:** Indicates whether the test mail was sent successfully. If the mail was sent successfully, the text will be highlighted in green. If not, it will be highlighted in red.
- **Mail recipients:** Mail addresses to which the result mails for administrative tasks and the service mails are sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Messages to Devices

Menu path: **UMS Administration > Global Configuration > Messages to Devices**

Here you can create, change or remove templates for messages to the devices.



To write a message, go to **Devices > Other Device Commands > Send Messages** either in the context menu of a device or in the main menu under **Devices**. For further information, see [Send Message](#)(see page 394).

Allowed Format for Messages to Device

Possible options:

- "Rich messages": The message text can be formatted. Templates can be used. Common formats like font styles and sizes, bullet lists, icons and many more are available.
- "Plain text messages only": The message text is written in plain text. A template can be selected, but the message is converted to plain text.
- "No message allowed": The sending of messages is disabled.

Misc Settings

Menu path: **UMS Administration > Global Configuration > Misc Settings**

The following global parameters can be found here:

User Login History

Enable user login history

- Recording of the user login activity is enabled. (Default)

Add last device users to quick search

- The user who logged in last will be added.

Add only still logged-in users

- Only users who are currently logged in will be added. (Default)

i In the event of configuration changes, the page will need to be reloaded by clicking on in order for the settings to be applied.

i In order to view the user login history for a device, click on the relevant device in the structure tree under **Devices**. All information regarding the device will now be shown in the content panel. Scroll right to the bottom to open **User Login History**. The following information is recorded here:

- **User name:** Name of the user who logged in to the device
- **Login time:** Time at which the user logged in
- **Logoff time:** Time at which the user logged off
- **Logon type:** At the moment, this can be Shared Workplace or Kerberos/Active Directory.

Notifications

Enable notifications

- Notifications are enabled and will be shown on each connection to the UMS Console, see also [Notifications](#)(see page 322). (Default)



- The notification function is disabled for all users.

For each license, certificate, or Product Pack, a new notification will be created [...] day(s) before expiration: Sets a time limit for a notification to remind you about the expiration of your license, certificate, or Product Pack.

A notification will be created when the free disk space is below [...] GB: When the free disk space is below this value, a warning will be created.

For each license or Product Pack, a new notification will be created when the amount of used licenses is above [...] %: If the number of used licenses in a Product Pack is higher than this limit (integer percentage), a notification is created.

UMS Features

Recycle Bin

Enable recycle bin

- The recycle bin is enabled. If an object is deleted in the structure tree, it will be moved to the recycle bin. (Default)

i If the recycle bin is disabled, the objects are removed permanently straight away.

See also [Deleting Objects in UMS / Recycle Bin](#)(see page 330).

Template Profiles

Enable template profiles

- [Template profiles](#)(see page 361) are enabled.

Master Profiles

Enable master profiles

- [Master profiles](#)(see page 359) are enabled.

Shared Workplace

Enable Shared Workplace

- [IGEL Shared Workplace \(SWP\)](#)(see page 402) is enabled. (Default)

i **Licensed Feature**

This feature requires a valid license from the [IGEL Enterprise Management Pack \(EMP\)](#)⁹⁹.

⁹⁹ <https://kb.igel.com/display/licensesmoreigelos11/Enterprise+Management+Pack>



! If you deactivate **Enable Shared Workplace**, the structure tree node **Shared Workplace Users** will be hidden and Shared Workplace users will NOT be able to log in!

Asset Inventory Tracker

Enable inventory tracking

[Inventory tracking](#)(see page 395) is enabled. (Default)

3.21 Importing Active Directory Users

Users can be imported from the Active Directory to the UMS console in three steps:

- Logging in to the Active Directory
- Selecting the users to be imported and starting the import
- Logging the import process

To import users from the Active Directory to the UMS console, proceed as follows:

1. Launch the UMS console's import dialog via **System > Administrator Accounts > Import**.
2. Log in to the AD/LDAP service.
The connection process is described under [Linking Active Directory / LDAP](#)(see page 497). When importing user accounts, only connected ADs are available for selection.
3. Click on **Continue**.
The Active Directory browser will open.
4. Select individual users or groups from the navigation tree of your AD.
The highlighted users/groups can be added to or removed from the selection to be imported via the context menu or using drag and drop. The users/groups found in the **Found AD Accounts** hit list can be transferred to the **Selected Accounts** list using the symbols.
Multiple users and groups can be selected.



Import Users from AD / LDAP Directory

Search User / Group in the AD / LDAP Directory

Search Result	
Display name	Account name

▼ ● Users

- Administrator
- Allowed RODC Password
- Cert Publishers
- Denied RODC Password
- DnsAdmins
- DnsUpdateProxy
- Domain Admins
- Domain Computers
- Domain Controllers
- Domain Guests
- Domain Users**
- elch
- Enterprise Admins
- Enterprise Read-only Dom
- Gottschalk2

Search | Details

Account name Starts w... ▾

Object type Undefined ▾

Userdefined Filter ne=*)(givenName=*)(sn=*))

Start searching from dc=UMS,dc=TEST

Default Search

Selected entries

Display name	Account name
elch	elch@ums.test
Domain Users	

Back Next Finish Cancel

As an alternative to navigating in the navigation tree, you can also highlight and add users or groups to the selection via the **Search** function.

- Click on **Continue** to start the import.

A confirmation window will appear.

Once a user has been successfully imported, this action cannot be undone. A UMS administrator set up by mistake must be deleted manually via the administrator account management system. The **IGEL UMS** uses the **account** as the name of the AD user imported.

3.21.1 Searching in the Active Directory

The options in the AD navigation tree have the following meanings:

Account name: Allows you to search on the basis of account names of parts thereof

Object type: Allows you to restrict a search to users or groups

User-defined filter: Filter criteria in accordance with the RFC-2254 standard

Start searching from	Element within the tree where the search begins
Default	Resets all search options to the standard values



Search	Starts the specified search
---------------	-----------------------------

The context menu allows the following actions to be performed on items in the list of hits:

- **Add user**
- **Add group**
- **Start searching from**
- **Details...**

Under **Details**, you can once again bring up the properties of the objects selected for import and remove objects prior to the import if necessary.

3.21.2 Import Results List

Once the import is complete, a results window will appear.

This shows how many accounts were ignored during the import and which ones were imported successfully. If a user account already exists in the UMS, this AD account will be skipped during the import.

Import Users from AD / LDAP Directory X

Result of the AD / LDAP Service trustee import

Ignored user	0
Imported user	elch@ums.test CN=Domain Users,CN=Users,DC=ums,DC=test
Existing user	

Back **Next** **Finish** **Cancel**



3.22 Create Administrator Accounts

Menu path: Menu bar > **System > Administrator accounts**

For the purpose of logging in to the [UMS Console / UMS Web App](#)(see page 257), you can either import UMS administrator accounts from a linked Active Directory or create, organize, and remove accounts manually.

Access rights to objects or actions within the IGEL UMS are attached to these administrator accounts and groups. The rights of the UMS superuser that was created during the installation (see [IGEL UMS Installation under Linux](#)(see page 261) or [IGEL UMS Installation under Windows](#)(see page 283)) cannot be restricted. The UMS superuser always has full access rights in the UMS.

 **UMS Web App**

The [UMS Web App](#)(see page 720) supports the same permissions as the UMS Console. To get access to devices in a directory, read permissions on this directory are required; permissions to devices only are not sufficient.

- [Administrators and Groups](#)(see page 508)
- [Access Rights](#)(see page 509)

3.22.1 Administrators and Groups

Menu path: Menu bar > **System > Administrator accounts**

- In the menu bar, click **System > Administrator accounts** to manage the IGEL UMS administrator accounts.



This screenshot shows a modal dialog box titled "Administrator accounts". It has two main columns: "Administrators" on the left and "Groups" on the right.
 - In the "Administrators" column, there is a list of four users: "helpdesk", "igel1", "igel2", and "igel3".
 - In the "Groups" column, there are two groups: "Administrators" and "Helpdesk".
 - To the right of each column is a vertical stack of buttons:
 - For the "Administrators" column: "New", "Import", "Edit", "Effective Rights", "Member of", "Change Password", and "Remove".
 - For the "Groups" column: "New", "Edit", "Members", and "Remove".
 - At the bottom right of the dialog is a "Close" button.

All available accounts are listed in the left-hand column, while the available groups are listed in the right-hand column. To the right of each column, you will find the associated buttons such as **New**, **Edit**, and **Remove**. For administrator accounts, you can also change the password (**Change Password**) and show group memberships (**Member of**). The **Members** button provides details on the members who make up a selected group. The **Effective Rights** button provides an insight into the rights that were directly or indirectly granted to users or taken away from them.

3.22.2 Access Rights

Access rights in the IGEL UMS include:

- General rights which can be granted to an administrator or denied either directly via the account or indirectly on the basis of the group membership
- Access rights to objects in the structure tree
- Access rights to the nodes within the UMS Administration area of the UMS Console

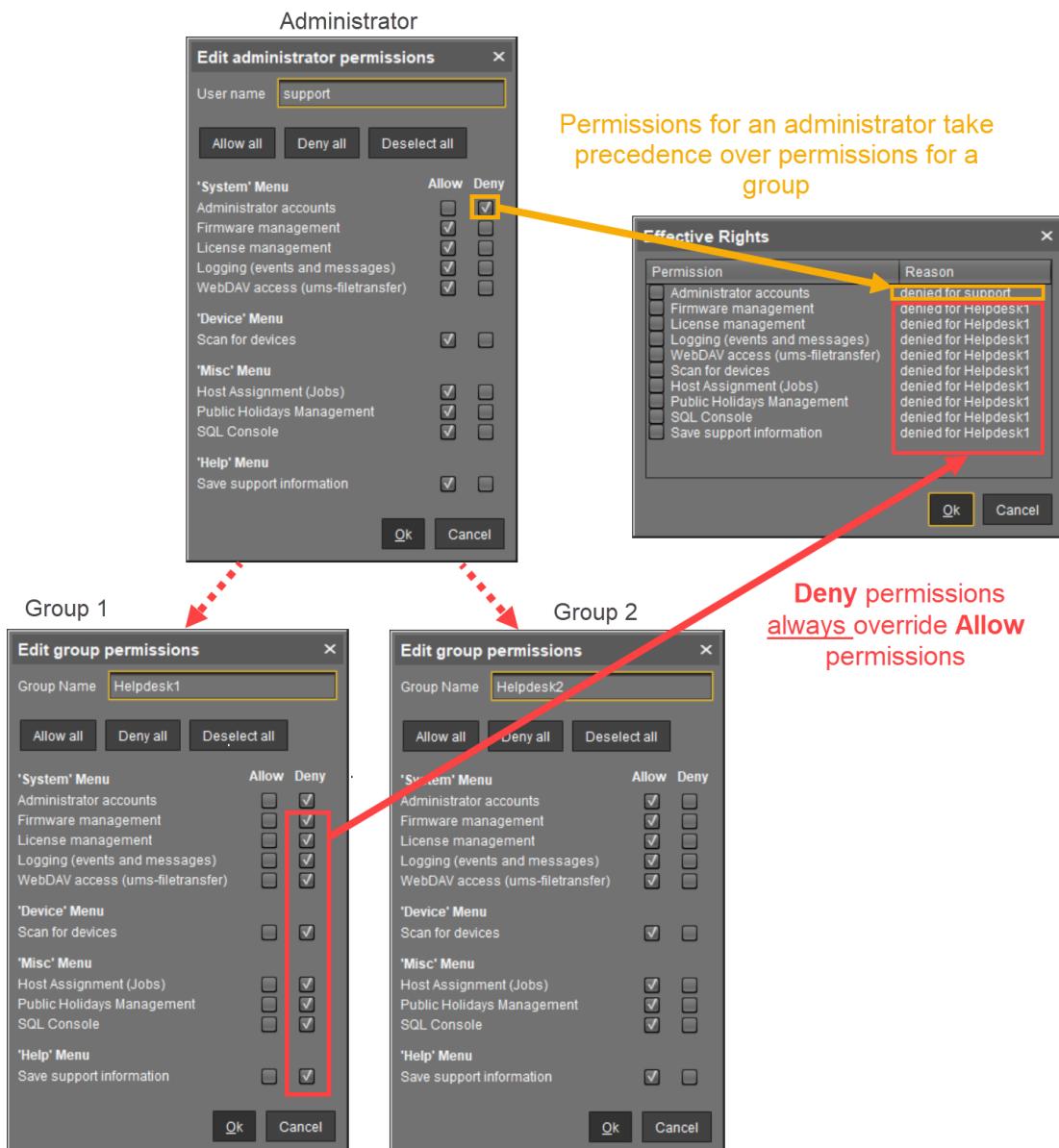
The indirect rights given to an administrator on the basis of their group membership can be changed further for each administrator in the group.

⚠ Take notice:

1. Permissions that were granted directly have precedence over those granted indirectly.
2. Nevertheless, the withdrawal of permissions ALWAYS overrides the granting of permissions.

The precedence of the **Deny** permission over the **Allow** permission means:

- If an administrator is a member of several groups with permissions contradicting each other, the **Deny** permission will overrule the **Allow** permissions from other groups. Also, if the permission is granted to an administrator directly, it will be nevertheless denied via a group.



Administrator

Edit administrator permissions

	Allow	Deny
Administrator accounts	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Firmware management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
License management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Logging (events and messages)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
WebDAV access (ums-filetransfer)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Scan for devices	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Host Assignment (Jobs)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Public Holidays Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SQL Console	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Save support information	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Group 1

Edit group permissions

	Allow	Deny
Administrator accounts	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Firmware management	<input type="checkbox"/>	<input checked="" type="checkbox"/>
License management	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Logging (events and messages)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
WebDAV access (ums-filetransfer)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Scan for devices	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Host Assignment (Jobs)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Public Holidays Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SQL Console	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Save support information	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Group 2

Edit group permissions

	Allow	Deny
Administrator accounts	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Firmware management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
License management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Logging (events and messages)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
WebDAV access (ums-filetransfer)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Scan for devices	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Host Assignment (Jobs)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Public Holidays Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SQL Console	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Save support information	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Effective Rights

Permission	Reason
Administrator accounts	denied for support
Firmware management	denied for Helpdesk1
License management	denied for Helpdesk1
Logging (events and messages)	denied for Helpdesk1
WebDAV access (ums-filetransfer)	denied for Helpdesk1
Scan for devices	denied for Helpdesk1
Host Assignment (Jobs)	denied for Helpdesk1
Public Holidays Management	denied for Helpdesk1
SQL Console	denied for Helpdesk1
Save support information	denied for Helpdesk1

Permissions for an administrator take precedence over permissions for a group

Deny permissions always override Allow permissions

- If a prohibition is issued for an object in the structure tree or a node in the UMS Administration area, it will apply for all subobjects/subnodes and cannot be withdrawn directly for these



subobjects/subnodes.

The screenshot shows two UMS Access Control dialog boxes. The top dialog is for the directory '/Devices' and the bottom one is for '/Devices/Augsburg'. Both dialogs show a list of permissions (Browse, Read, Move, Edit Configuration, Write) and their 'Allow' and 'Deny' status. A red box highlights the 'Edit Configuration' row in both tables. Red arrows point from the 'Edit Configuration' row in the top dialog to the corresponding row in the bottom dialog, indicating that the permission settings are inherited from the parent directory. The word 'Inactive' is written vertically in red between the two arrows.

Permission	Allow	Deny	Effective Rights
Browse	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for group Helpdesk allowed for group Helpdesk
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for group Helpdesk
Move	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Helpdesk
Edit Configuration	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Helpdesk
Write	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Helpdesk

Permission	Allow	Deny	Effective Rights
Browse	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for group Helpdesk (inherited from /ROOT/Devices/)
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for group Helpdesk (inherited from /ROOT/Devices/)
Move	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Helpdesk (inherited from /ROOT/Devices/)
Edit Configuration	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Helpdesk (inherited from /ROOT/Devices/)
Write	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Helpdesk (inherited from /ROOT/Devices/)

Generally speaking, the same permission settings are used for groups and administrators. The following description of individual configuration options therefore applies equally to administrators and groups.

- [Basic Access Rights](#)(see page 511)
- [General Administrator Rights](#)(see page 512)
- [Object-Related Access Rights](#)(see page 515)
- [Access Rights in the Administration Area](#)(see page 520)

Basic Access Rights

The following table lists the basic access rights needed to set up, edit, or delete objects. An object can be a directory, an element in a tree structure (devices, profiles...) or nodes in the administration area of the UMS Console, e.g. administrative tasks or the AD connection.



Action	Objects affected	Browse	Read	Move	Edit Configuration	Write	Access control
<u>General</u>							
View Object	Tree Element (Profile, TC...)		X				
	Directory	X					
Create Object	Target Directory				X		
Delete Object	Object				X		
	Source Directory				X		
Edit Object	Object				X		
Rename Object	Object				X		
Show Configuration	Thin Client, Profile		X				
Edit Configuration	Thin Client				X		
	Profile				X		
Show Effective Rights	Object		X				
	Directory	X					
Edit Object Permissions	Object, Directory					X	
Import	Target Directory					X	

General Administrator Rights

Menu path: Menu bar > **System** > **Administrator accounts**

Permissions are managed via **System** > **Administrator accounts**. An administrator can grant himself and others rights, take away those rights, and set up new accounts.

The following options are available here, split according to administrators or groups:

New: A new administrator or a new group will be created.

Import: A user will be imported from the AD/LDAP directory.

- ⓘ This procedure requires an AD/LDAP connection. For further details, see [Importing Active Directory users](#)(see page 505).

- **Domain:** Domain in which the AD/LDAP service runs
- **User:** Name of the user
- **Password:** Password of the user

Edit: Existing administrator or group settings can be edited.

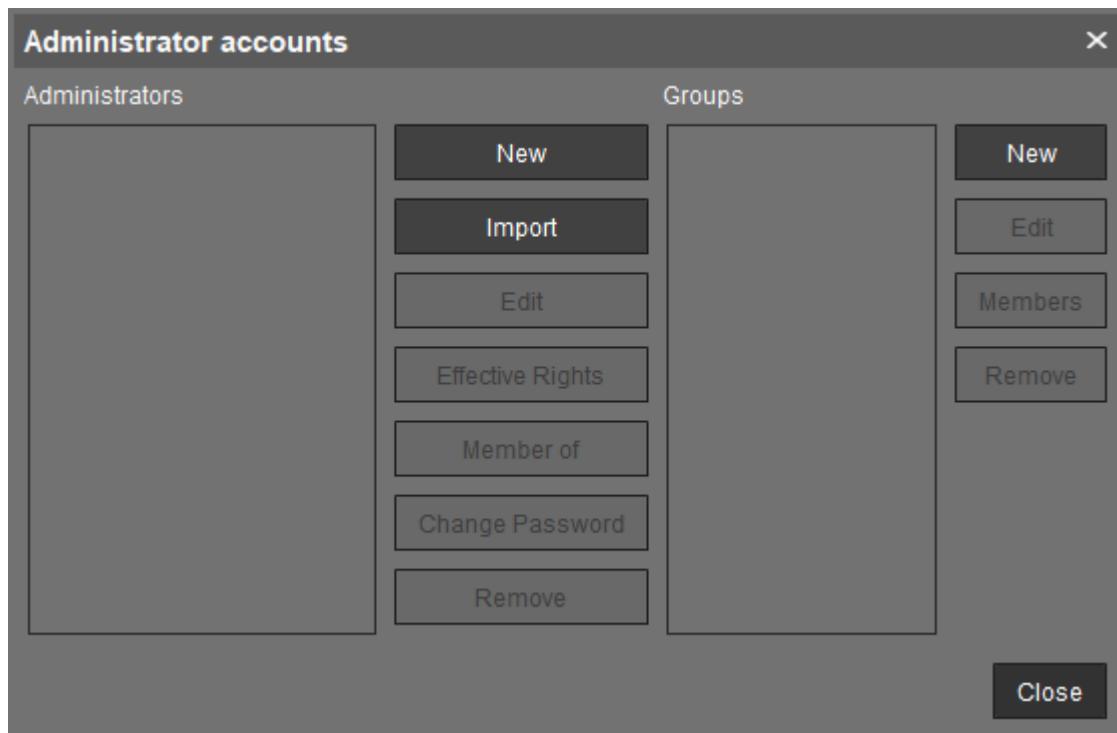
Effective Rights: A list of all assigned rights for a specific administrator is shown.



Member of / Members: The assignment of memberships and groups is shown.

Change Password: Changes an administrator password.

Remove: Removes a highlighted administrator or a group.



Below, you will find a list of permissions that can be given to individual administrators or groups under **System > Administrator accounts > New** or **Edit**. Each permission has three possible states: not set, **Allow** or **Deny**.



New Administrator

User name	<input type="text"/>																																																																			
Password	<input type="password"/>																																																																			
Confirm Password	<input type="password"/>																																																																			
<input type="button" value="Allow all"/> <input type="button" value="Deny all"/> <input type="button" value="Deselect all"/>																																																																				
<table border="1"> <thead> <tr> <th>'System' Menu</th> <th>Allow</th> <th>Deny</th> </tr> </thead> <tbody> <tr> <td>Administrator accounts</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Firmware management</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>License management</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Logging (events and messages)</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>WebDAV access (ums-filetransfer)</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td colspan="3"> </td> </tr> <tr> <td colspan="3">'Device' Menu</td> </tr> <tr> <td>Scan for devices</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td colspan="3"> </td> </tr> <tr> <td colspan="3">'Misc' Menu</td> </tr> <tr> <td>Host Assignment (Jobs)</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Public Holidays Management</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>SQL Console</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td colspan="3"> </td> </tr> <tr> <td colspan="3">'Help' Menu</td> </tr> <tr> <td>HA Health Check</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Save support information</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td colspan="3"> </td> </tr> <tr> <td colspan="3">General - WebApp</td> </tr> <tr> <td>Delete Log Messages</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Device Bulk Action</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>			'System' Menu	Allow	Deny	Administrator accounts	<input type="checkbox"/>	<input type="checkbox"/>	Firmware management	<input type="checkbox"/>	<input type="checkbox"/>	License management	<input type="checkbox"/>	<input type="checkbox"/>	Logging (events and messages)	<input type="checkbox"/>	<input type="checkbox"/>	WebDAV access (ums-filetransfer)	<input type="checkbox"/>	<input type="checkbox"/>	 			'Device' Menu			Scan for devices	<input type="checkbox"/>	<input checked="" type="checkbox"/>	 			'Misc' Menu			Host Assignment (Jobs)	<input type="checkbox"/>	<input type="checkbox"/>	Public Holidays Management	<input type="checkbox"/>	<input type="checkbox"/>	SQL Console	<input type="checkbox"/>	<input type="checkbox"/>	 			'Help' Menu			HA Health Check	<input type="checkbox"/>	<input type="checkbox"/>	Save support information	<input type="checkbox"/>	<input type="checkbox"/>	 			General - WebApp			Delete Log Messages	<input type="checkbox"/>	<input type="checkbox"/>	Device Bulk Action	<input type="checkbox"/>	<input type="checkbox"/>
'System' Menu	Allow	Deny																																																																		
Administrator accounts	<input type="checkbox"/>	<input type="checkbox"/>																																																																		
Firmware management	<input type="checkbox"/>	<input type="checkbox"/>																																																																		
License management	<input type="checkbox"/>	<input type="checkbox"/>																																																																		
Logging (events and messages)	<input type="checkbox"/>	<input type="checkbox"/>																																																																		
WebDAV access (ums-filetransfer)	<input type="checkbox"/>	<input type="checkbox"/>																																																																		
'Device' Menu																																																																				
Scan for devices	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																																																		
'Misc' Menu																																																																				
Host Assignment (Jobs)	<input type="checkbox"/>	<input type="checkbox"/>																																																																		
Public Holidays Management	<input type="checkbox"/>	<input type="checkbox"/>																																																																		
SQL Console	<input type="checkbox"/>	<input type="checkbox"/>																																																																		
'Help' Menu																																																																				
HA Health Check	<input type="checkbox"/>	<input type="checkbox"/>																																																																		
Save support information	<input type="checkbox"/>	<input type="checkbox"/>																																																																		
General - WebApp																																																																				
Delete Log Messages	<input type="checkbox"/>	<input type="checkbox"/>																																																																		
Device Bulk Action	<input type="checkbox"/>	<input type="checkbox"/>																																																																		
<input type="button" value="Ok"/> <input type="button" value="Cancel"/>																																																																				

'System' Menu

Administrator accounts

- The management of permissions can be performed: administrators and groups, as well as their rights, can be added and edited.

⚠️ Administrator accounts permission should only be granted to users who are to have full access to all objects and actions in the UMS!

Firmware management

- Firmware versions can be imported, exported, and removed from the database.

License management

- IGEL firmware licenses can be allocated to devices.

Logging (events and messages)

- The event and message log may be viewed if **Logging** is enabled.



WebDAV access (ums-filetransfer)

- The user is authorized to add, modify, and delete files in the directory /ums_filetransfer/.

'Devices' Menu

Scan for devices

- The network can be scanned for devices, for example, if they are to be registered on the UMS Server.

'Misc' Menu

Host Assignment (Jobs)

- Scheduled jobs can be assigned to various hosts.

Public Holidays Management

- Public holidays can be defined to plan jobs.

SQL Console

- The SQL Console may be run. **Warning:** The SQL Console can cause considerable damage to the database.

'Help' Menu

HA Health Check

- The [UMS HA Health Check](#)(see page 688) feature for an overall check of the High Availability environment can be used.

Save support information

- Database and server log files can be exported for support purposes.

General - WebApp

Delete Log Messages

- Log messages can be deleted with the UMS Web App.

Device Bulk Action

- Actions can be performed for any number of devices with the UMS Web App, e.g. by using directories.
- With the UMS Web App, actions can only be performed for one device at a time.

⚠ This only applies to the UMS Web App; bulk actions can still be performed from the UMS Console.

Object-Related Access Rights

Administrators and administrator groups can be granted specific rights with regard to objects in the structure tree. These permissions are inherited "downwards", e.g. from a folder to the devices within this folder.



You can change the permission settings after selecting an object in the following ways:

- via **Access control** in the context menu of the object
- via the **Access control** symbol  in the symbol bar
- via the menu item **Edit > Access control**

Permission	Allow	Deny	Effective Rights
Browse	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for group Helpdesk
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for group Helpdesk
Move	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Helpdesk
Edit Configuration	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Helpdesk
Write	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Helpdesk
Edit System Information	<input type="checkbox"/>	<input type="checkbox"/>	not set
Access Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign	<input type="checkbox"/>	<input type="checkbox"/>	not set
Power Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Firmware Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Settings Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Remote access	<input type="checkbox"/>	<input type="checkbox"/>	not set
Send Message	<input type="checkbox"/>	<input type="checkbox"/>	not set

The above list contains all object-related permissions available in the UMS structure tree. Only one selection is available for each selected object. For example, a view cannot be assigned updates and cannot be shut down.

Associated permissions are automatically set together but can be changed manually later on. Enabled permissions or denials relating to nodes affect all objects within the node.

⚠ The withdrawal of permissions, i.e. **Deny**, always overrides the granting of permissions, i.e. **Allow**.

The overview shows selected administrator rights to an object. Details can be found under **Effective Rights**. The rules for determining rights are also shown here, e.g. whether the permission was granted directly or whether it is granted via a group or an inheritance within the tree structure.



The screenshot shows the IGEL Universal Management Suite (UMS) interface. On the left, there is a navigation tree with categories like Profiles, Master Profiles, Template Keys and Groups, Firmware Customizations, Devices, and Views. A specific device node 'techdocRD1' is selected. In the center, the 'Access Control' dialog is open for this device. It lists 'Administrators' and 'Helpdesk' under 'Groups'. The 'Helpdesk' group is highlighted with a yellow border. Below this, there is a table of permissions with columns for 'Permission', 'Allow', 'Deny', and 'Effective Rights'. The 'Effective Rights' column contains detailed inheritance information. Red arrows point from the 'Helpdesk' group selection in the 'Access Control' dialog to the 'Helpdesk' entry in the 'Effective Rights' table, and from the 'Helpdesk' entry in the 'Effective Rights' table to the 'Helpdesk' entry in the 'Access Control' dialog. At the bottom of the 'Access Control' dialog are buttons for 'OK', 'Cancel', and 'Apply'. A separate window titled 'Effective Rights' shows a list of permissions and their reasons, also with a 'Helpdesk' entry highlighted.

Available Rights

General	Browse	Visibility of the object in the structure tree (path as far as the object must also be allowed!)
	Read	Read permission in respect of folder contents and object attributes
	Move	Devices can be moved without write permission.
	Edit configuration	Write permission for the configuration of a device (TC Setup)
	Write	Write permission in respect of folders and object attributes (not TC Setup)



	Access Control	The permission settings for the object can be changed.
	Shadowing	VNC access to the device
	Send message	The device's message function
Assignment	Assign profile	A profile may be assigned to the object.
	Assign file	A file may be assigned to the object.
	Assign update	A firmware update may be assigned to the object.
Energy	Reboot	Rebooting the device.
	Idle state	Putting the device into the idle state.
	Shut down	Shutting down the device
	Wake up	Waking up the device using wake-on-LAN.
Firmware	Update	The firmware update may be carried out.
	Reset	Resetting the firmware to the factory defaults.
	Media Player	Downloading Media Player codec licenses.
	Flash Player	Downloading an Adobe Flash Player license.
	File transfer	An assigned file may be transferred to the device.

Assignment of Objects

The assignment of objects requires the following permissions:

- **Browse**
- **Read**
- **Assign** on both sides

ⓘ Write permission is not required directly for the assignment of objects.

Example 1: Assigning a File to a Profile

A user can only assign a file to a profile or delete this assignment. He cannot make any changes to the file or profile, i.e. he cannot edit, rename, or delete them.

Permissions on the Profile



Permission	Allow	Deny	Effective Rights
Browse	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike (inherited from /ROOT/Profiles/)
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike (inherited from /ROOT/Profiles/)
Write	<input type="checkbox"/>	<input type="checkbox"/>	not set
Access Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
▼ Assign	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign File	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike
Assign device	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign Shared Workplace ...	<input type="checkbox"/>	<input type="checkbox"/>	not set

Permissions on the File

Permission	Allow	Deny	Effective Rights
Browse	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike (inherited from /ROOT/Files/)
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike (inherited from /ROOT/Files/)
Write	<input type="checkbox"/>	<input type="checkbox"/>	not set
Access Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
▼ Assign	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign Profile	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike
Assign Master Profile	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign FWC	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign device	<input type="checkbox"/>	<input type="checkbox"/>	not set

Example 2: Assigning a Device to a Profile

A user can only assign a device to a profile or delete this assignment. He cannot make any changes to the device or profile, i.e. he cannot rename, delete the device or profile, or edit their configuration.

Permissions on the Profile

Permission	Allow	Deny	Effective Rights
Browse	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike (inherited from /ROOT/Profiles/)
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike (inherited from /ROOT/Profiles/)
Write	<input type="checkbox"/>	<input type="checkbox"/>	not set
Access Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
▼ Assign	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign File	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign device	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike
Assign Shared Workplace U...	<input type="checkbox"/>	<input type="checkbox"/>	not set

Permissions on the Device



Permission	Allow	Deny	Effective Rights
Browse	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike (inherited from /ROOT/Devices/)
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike (inherited from /ROOT/Devices/)
Move	<input type="checkbox"/>	<input type="checkbox"/>	not set
Edit Configuration	<input type="checkbox"/>	<input type="checkbox"/>	not set
Write	<input type="checkbox"/>	<input type="checkbox"/>	not set
Edit System Information	<input type="checkbox"/>	<input type="checkbox"/>	not set
Access Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign Profile	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike
Assign Master Profile	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign File	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign Firmware Up...	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign FWC	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign Template Val...	<input type="checkbox"/>	<input type="checkbox"/>	not set
Power Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Firmware Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Settings Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike
UMS -> Device	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike
Device -> UMS	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike
Remote access	<input type="checkbox"/>	<input type="checkbox"/>	not set
Send Message	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike

Access Rights in the Administration Area

In the **UMS Administration** area of the UMS Console, you can grant or deny general rights **Browse**, **Read**, and **Write**, as well as **Access Control** for administrator accounts. Permissions should only be granted to users who will actually perform administrative tasks on the UMS.

You can change the permission settings after selecting a tree node in the following ways:

- via **Access control** in the context menu



- via the **Access control** symbol in the symbol bar
- via the menu item **Edit > Access control**

Permission	Allow	Deny	Effective Rights
Browse	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user Administrator 1
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user Administrator 1
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user Administrator 1
Access Control	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for user Administrator 1



3.23 User Logs

The logging system is used by the UMS and the registered devices in order to record all changes to the database. Only successful actions are logged. You will not find details of any errors in the log file of the UMS GUI Server.

The logging system is subdivided into two areas:

Messages:	Actions initiated by a user
Events:	Actions initiated by a device

3.23.1 Administration

The administration settings for the logging procedure are configured in the IGEL UMS Console under **UMS Administration > Global Configuration > Logging**, see [Logging](#)(see page 500).

- **Messages** can be logged either with or without details.
There are no details for **events**.
- With the **Log Level Configuration** buttons, you can enable logging for selected commands.
Logging for all possible commands is selected as standard.
- The deletion and export of log messages are configured under **UMS Administration > Global Configuration > Administrative Tasks**.

3.23.2 Displaying Logs

Information regarding **messages** and **events** can be displayed in the UMS Console in the following ways:

- via the **System > Logging** menu
 - via **Logging** in the context menu of the directories and objects in the tree structure
-
- [Logging Dialog Window: Setting a Filter](#)(see page 522)



3.23.3 Logging Dialog Window: Setting a Filter

To set a filter, proceed as follows:

1. In the **Filter** window area, specify criteria in order to load a specific selection of messages from the database.
All filter fields are combined with the operator **AND**.
These values can be connected with the operator **OR** only if a filter field allows multiple selections, e.g. if several devices can be selected.
2. Click on **Apply Filter** to enable the new settings.

The log messages or events will be reloaded from the database on the basis of the filter settings.

Messages/events can be exported to HTML, XML, and CSV files by selecting **Export**.

Log Messages

Messages					
Timezone	Europe/Berlin (CET)				
Export ...					
Time	Command	Category	Object Type	User	Message
3/10/21 5:33 PM	Sending device command.	OBJECTS	THINCLIENT	admin	sending command <Write runtime info>
3/10/21 5:19 PM	Sending device command..	OBJECTS	THINCLIENT	admin	sending command <Write runtime info>
3/10/21 4:51 PM	Sending device command..	OBJECTS	THINCLIENT	admin	sending command <Write runtime info>
3/10/21 4:51 PM	Sending device command..	OBJECTS	THINCLIENT	admin	sending command <Write runtime info>
3/10/21 3:40 PM	Sending device command..	OBJECTS	THINCLIENT	admin	sending command <Write runtime info>
3/10/21 3:16 PM	Sending device command..	OBJECTS	THINCLIENT	admin	sending command <Write runtime info>
3/10/21 12:21 PM	Sending device command..	OBJECTS	THINCLIENT	admin	sending command <Write runtime info>

- [Setting a Filter for Events\(see page 522\)](#)
- [Filter for Messages\(see page 523\)](#)
- [Setting a Filter for Categories\(see page 524\)](#)
- [Notes\(see page 524\)](#)

Setting a Filter for Events

To set a filter for events, proceed as follows:

1. Specify the **Command** if you know which one you need.



2. Specify the **Unit ID** of the device for which you wish to display the events.

A screenshot of the "Event Messages" filter interface. On the left, there's a "Filter" section with "Start" and "End" date pickers set to "2020-09-16" and "2020-09-23" respectively, and a "Command" dropdown. Below that is a "Unit ID" section containing a text input field with the value "00E0C520986A". Underneath the Unit ID input are two buttons: "Select Unit ID..." (which is highlighted with a red box) and "Clear Unit ID List". At the bottom of the filter panel is an "Apply Filter" button. To the right of the filter panel is a large empty table area with columns labeled "Time", "Command", and "IP address". Below the table is a checked checkbox labeled "Select objects in tree". At the bottom of the right panel is a "Message objects" section with three items: "Master Profiles (1)", "Profiles (11)", and "Template Keys and Groups (0)".

Filter for Messages

User	Select the name of the UMS administrator who is responsible for the message.
Object type	Specify an object for which you would like to display the messages.
Category	Each command belongs to a category, e.g. security, settings and objects.
Command	If a command is known, you can specify it yourself.
Time zone	You can specify the time zone with which the logging time for messages is shown.



Log Messages

Filter

Start	2021-03-04
End	2021-03-11
User	
Object type	Device

Selected Objects

- td-RD03

Category

Command

Details

Select objects in tree

- Master Profiles (1)
- Profiles (13)
- Template Keys and Groups (2)
- Firmware Customizations (1)
- Devices (2)
 - Mobile Devices (0)
- Views (2)
- Jobs (1)
- Files (2)
- Universal Firmware Update (1)

Messages

Timezone: Europe/Berlin (CET) Export ...

Time	Command	Category	Object Type	User	Message
3/10/21 5:33 PM	Sending device command...	OBJECTS	THINCLIENT	admin	sending command <Write runtime infor
3/10/21 5:19 PM	Sending device command...	OBJECTS	THINCLIENT	admin	sending command <Write runtime infor
3/10/21 4:51 PM	Sending device command...	OBJECTS	THINCLIENT	admin	sending command <Write runtime infor
3/10/21 4:51 PM	Sending device command...	OBJECTS	THINCLIENT	admin	sending command <Write runtime infor
3/10/21 3:45 PM	Sending device command...	OBJECTS	THINCLIENT	admin	sending command <Write runtime infor
3/10/21 3:18 PM	Sending device command...	OBJECTS	THINCLIENT	admin	sending command <Write runtime infor
3/10/21 12:01 PM	Sending device command...	OBJECTS	THINCLIENT	admin	sending command <Write runtime infor

Setting a Filter for Categories

► To adjust the filter, select the option **Category** if you would like to select all messages for a specific category (e.g. those relating to firmware updates).

All commands within this category such as **Delete firmware update** or **Assign firmware update** will then be evaluated in order to identify the messages or events.

Notes

The quick filter does not apply to the export action.

One of the most important commands is the command **GET_SETTINGS_ON_REBOOT**. The time stamp for this command provides details of the time when the device last booted. This can be used to define a new **BOOT TIME** view criterion. With the help of this criterion, you can easily determine which devices have not been booted after a certain date.

- i** The administration settings for the number of messages and – more importantly – for the events should be handled with great care. The higher these values are, the more space will be required for the tablespace in the database. If you enable logging, you should monitor your database closely until you are sure that sufficient space is available for the messages and/or events.



3.24 Save Support Information / Send Log Files to Support

If you have problems with the UMS and contact your service provider, you can send various UMS log files to Support. The [Support Wizard in the IGEL UMS](#)(see page 525) will help you here.

If you have any questions regarding an IGEL product and are already an IGEL customer, please contact your dedicated sales partner first.

If you are currently testing IGEL products or your sales partner is unable to provide the help you need, please fill in the support form after logging on to the [IGEL Customer Portal](#)¹⁰⁰.

We will then contact you as soon as possible. It will make things easier for our support staff if you provide us with all the information that is available. Please see our notes regarding [support and service information](#)¹⁰¹ too.

3.24.1 Support Wizard in the IGEL UMS

Menu path: **Menu Bar > Help > Save support information**

With the Support Wizard in the IGEL Universal Management Suite (UMS), you can collect the log files which are important for your support case and send them via e-mail to IGEL Support.

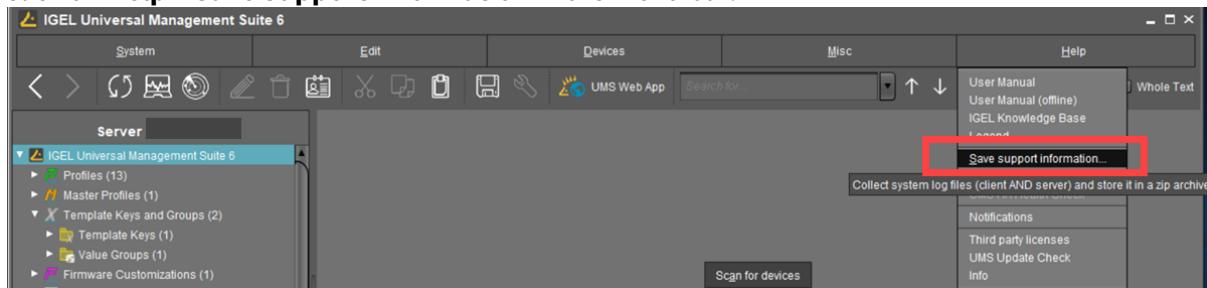
The Support Wizard saves log files from the UMS Server and UMS Console as well as profiles and associated firmware information for the selected devices in a ZIP file. If IGEL Cloud Gateway (ICG) is in use, log files from the connected ICGs and the basic information of the used ICG certificates will also be saved. If the IGEL Management Interface (IMI) extension is used, its API log file will be saved too. In the case of performance logging (to be activated only upon recommendation of IGEL Support; see [Logging\(see page 501\)](#)), monitoring data for the UMS Server and UMS Load Balancer will be collected too.

- ⓘ In order to send log files using the Support Wizard, the mail settings must be correct; further information can be found under [Mail settings\(see page 501\)](#). The support ID must also be valid.

How to Send Log Files via Support Wizard in the IGEL UMS

To send log files using the Support Wizard, proceed as follows:

1. Click on **Help > Save Support Information** in the menu bar.



¹⁰⁰ <https://support.igel.com>

¹⁰¹ <https://www.igel.com/wp-content/uploads/2019/11/F-501-EN.pdf>



2. Optionally, enter the **support ID** for your support case.

Support Wizard

Introduction

This wizard collects common information about the UniversalManagementSuite necessary for support requests.
(e.g. LOG files of server and console application).
If devices are involved in an issue, information about these devices are added to the support information.

If you have got a support ID for the issue, please enter the ID here. Otherwise select "Next".

Support ID

Next steps:

- Selected devices involved in this case (optional)
- Choose folder to store support information in
- Send mail with support information via internal mail client (optional)
(only possible if the mail settings are configured and you enter the support ID for this issue)

Cancel **Finish** **> Next** **< Back**

3. Click on **Next**.
4. If the support case concerns devices (otherwise, click on **Next**): Highlight the devices where the problem has occurred.
5. If the support case concerns devices (otherwise click on **Next**): Click on to select the highlighted devices.
6. Click on **Next**.
7. Under **Number of days back**, specify the maximum age in days of the log entries to be sent.
8. Click on **Next**.
9. Using **Look In**, select the directory in your file system in which the zipped log files are to be saved.
10. Click on **Next**.

If the zipped log files have already been saved, you will be asked whether the existing ZIP file should be overwritten.

If the mail settings are configured, entry fields for the mail will be shown.
If the mail settings are not configured, a message about saved files will be shown.



11. If applicable, give the following information for the mail:
 - **Cc:** Mail address to which a copy is to be sent. If you enter a number of addresses, you must separate them using a semicolon ";".
 - **Reply address:** Mail address to which the reply from Support is to be sent. If you leave the field empty, the reply will be sent to the **mail sender address** defined under **UMS Administration > Mail Settings**.
 - **Subject:** Subject of the mail. When the mail is sent, the **support ID** will be shown before this text.
 - Text entry field: Mail text.
12. Check the information in the mail and click on **Send**.
13. Click on **Finish**.

Related Topics

[IGEL Support Registration¹⁰²](#)

[Sending Device Log Files to IGEL Support¹⁰³](#)

[Save Device Files for Support](#)(see page 527)

[Exporting the Local Device Configuration¹⁰⁴](#)

3.25 Save Device Files for Support

Menu path: **Menu bar > Help > Save device files for support**

You can use the UMS for collecting log files from a device. These log files will be zipped, so you can easily send them to the IGEL support team. The exact behavior is dependent on the device's firmware version.

3.25.1 Saving the Log Files of a Device

1. Go to **Help > Save device files for support**.
A wizard appears. In the screen **Select Devices**, the devices section of the structure tree is shown.
2. Select the device whose log files you want to save and click **Next**.
The screen **Select a target directory for the zipped files** is shown.
3. Select a target directory and click **Next**.
The log files are collected from the device and zipped. The file path is shown.
4. Click **Finish**.

For the detailed instruction with screenshots, see [Sending Device Log Files to IGEL Support¹⁰⁵](#).

¹⁰² <https://kb.igel.com/display/gettingstarted/IGEL+Support+Registration>

¹⁰³ <https://kb.igel.com/display/igelos1106/Sending+Device+Log+Files+to+IGEL+Support>

¹⁰⁴ <https://kb.igel.com/display/igelos1106/Exporting+the+Local+Device+Configuration>

¹⁰⁵ <https://kb.igel.com/display/igelos1105/Sending+Device+Log+Files+to+IGEL+Support>



3.25.2 Log Files Collected with IGEL OS 10.04 or Higher

The UMS asks the device to send log files. The selection of log files is configurable on the device. The following log files are collected by default:

- /config/Xserver/card0
- /config/Xserver/monitor-info
- /config/Xserver/xorg.conf-0
- /config/sound/card0
- /config/sound/default_card_name
- /var/log/Xorg.0.log
- /wfs/group.ini
- /wfs/setup.ini
- dhclient lease files

You can add more log files via the IGEL Setup under **Accessories > System Log Viewer > Options**. For further information, see [Options¹⁰⁶](#).

3.25.3 Log Files Collected with Other IGEL OS Versions

The UMS requests the following log files:

- setup.ini
- group.ini
- messages
- Xorg.0.log
- xorg.conf-0
- Xorg.0.log.old
- wpa_debug.all
- tcsetup.log
- tcsetup.log.1

3.25.4 Log Files Collected with Windows IoT 4.03 or Higher

The UMS asks the device to send log files. The selection of log files is configurable on the device. The following log files are collected by default:

- D:\data\setup.ini
- D:\data\group.ini
- D:\data\sysinfo.ini
- D:\data\uptime.ini
- D:\data\ftreg\ftreg.ini
- C:\Program Files (x86)\IGEL\upd\tcsetup.log
- C:\Program Files (x86)\IGEL\upd\xplog.txt
- C:\Program Files (x86)\IGEL\z_ramdrive

¹⁰⁶ <https://kb.igel.com/pages/viewpage.action?pageId=42011209>

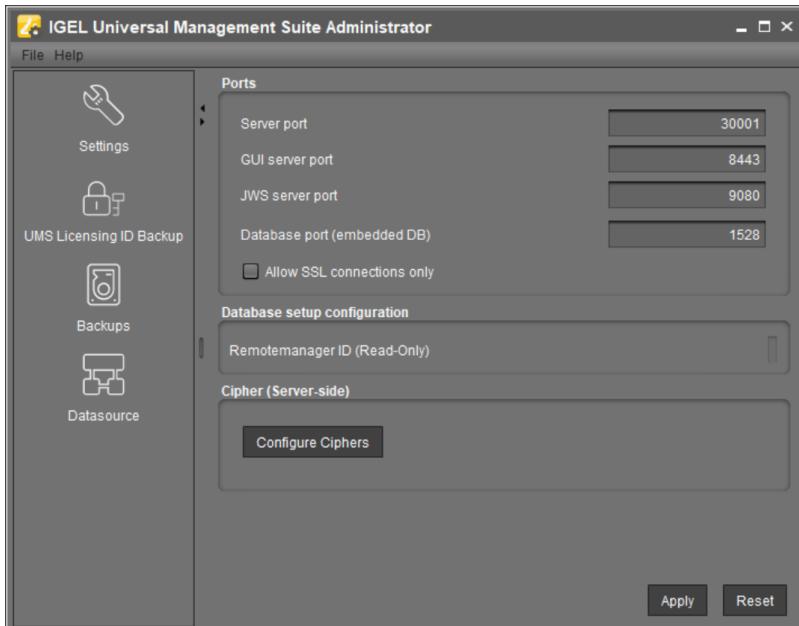


- C:\Program Files (x86)\IGEL\log
- C:\ProgramData\IGEL\DualbootQT_Inst_Log.txt
- C:\ProgramData\IGEL\DualbootQT_UnInst_Log.txt
- C:\ProgramData\IGEL\LogMisc.txt
- C:\Windows\System32\winevt\Logs\Application.evtx
- C:\Windows\System32\winevt\Logs\System.evtx
- C:\Windows\System32\Sysrep\Panther\setuperr.log

You can add more log files via the IGEL Setup under **System > Registry > System > support_files%** > **Add Instance** (Registry key: system.support_files% resp. system.support_files<number>).

3.26 The IGEL UMS Administrator

The IGEL UMS Administrator application is only available on a UMS Server as it enables you to change the communication between the services directly. You can edit basic settings such as the ports to be used or the data sources to be connected. These functions are not available in the administration area of the UMS Console.



- i** If the UMS Administrator cannot be launched under Linux via a menu or desktop link, you can launch the application on the command line with the following command: /[IGEL installation directory]/RMAdmin.sh (when the default installation directory is used: /opt/IGEL/RemoteManager/RMAdmin.sh)
It is NOT recommended to execute RMAdmin.sh with sudo. On Red Hat Enterprise Linux 8, RMAdmin.sh can be executed only without sudo.

- i** The default path to the UMS Administrator under Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe

You can change the language of the Administrator tool under **File > Settings > Language**.



- ⓘ The rights for changing the settings depend on whether the user is authorized to change IGEL UMS files on the server system. When using the IGEL UMS Administrator, you should therefore use the same user account as you did when you installed the UMS.

- [Settings for IGEL UMS Administrator](#)(see page 530)
- [UMS Licensing ID Backup](#)(see page 534)
- [UMS Licensing ID Backup on the Command Line](#)(see page 535)
- [Backups](#)(see page 536)
- [Data Source](#)(see page 543)
- [IGEL UMS Administrator Command-Line Interface](#)(see page 547)

3.26.1 Settings for IGEL UMS Administrator

Menu path: **UMS Administrator > Settings**

Using the IGEL Universal Management Suite (UMS) Administrator, you can change various server settings. The IGEL UMS Administrator application is only available on a UMS Server as it enables you to change the communication between the services directly. You can edit basic settings such as the ports to be used or the data sources to be connected.

- ⓘ Default path to the UMS Administrator:
Linux: /opt/IGEL/RemoteManager/RMAdmin.sh
Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe



IGEL Universal Management Suite (UMS) Administrator Settings:

Ports

Device Communication Port	30001
Web server port	8443
JWS server port	9080
Database port (embedded DB)	1528

Allow SSL connections only

Database setup configuration

Remotemanager ID (Read-Only)

Cipher (Server-side)

Configure Ciphers

SSL Certificates

Reset web certificates (Only for disaster recovery)

Apply Reset

Ports

Device Communication Port: The devices connect to this port. (Default: 30001)

- ⓘ Changes to this port can only be made if you ensure that devices will establish a connection to the new port. For more information on ports, see [UMS Communication Ports](#)(see page 48).

Web server port: Establishes the connection to the server. This port must be entered in the login window for the IGEL UMS Console or in the [URL for the UMS Web App](#)(see page 732). (Default: 8443)



- ⓘ If the port is changed, the service IGEL RMGUIServer/igelRMserver must be restarted.

JWS server port: This port allows the [UMS Console to be started with Java Web Start](#)(see page 222) via a non-encrypted connection. For this to be possible, this port must be specified in the connection URL, e.g. `http://hostname:9080/start_rm.html`. (Default: 9080)

Database port (embedded DB): Port for communication with the embedded DB. (Default: 1528)
For external databases, the port is defined under **Data Sources**.

Allow SSL connections only

- A connection will only be allowed via SSL.

- ❗ Do not use the **Allow connection via SSL only** option if you use Windows Embedded 7 in Version 3.08.100 or older and would also like to use the Universal Firmware Update feature. These older Windows firmware versions do not support firmware updates via HTTPS.

Database Setup Configuration

Remote manager ID (read-only): Unique key for the UMS instance. This is read out automatically.

Cipher (Server-Side)

- ❗ The cipher configuration is server-specific and excluded from database backups.

- ⓘ If you are using UMS High Availability (HA), the ciphers have to be configured for each server separately.

Configure Ciphers: Use this button to open the **Cipher Selection** dialog, where you can define which ciphers can be used by the UMS Server.

In the **Cipher Selection** dialog, you can perform the following actions:

- **Set active:** Add the cipher selected in the **Inactive Ciphers** list to the list of active ciphers.
- **Set inactive:** Remove the cipher selected in the **Active Ciphers** list from the list of active ciphers.
- **Use defaults:** Restore the default cipher settings.

The List of Default Cipher Suites

```

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

```



TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256

- **Ok:** Save the changes.
- **Cancel:** Discard all changes.

- i** On new UMS installations, only the [default ciphers](#)(see page 532) are activated. By updating the existing UMS installations, the already configured ciphers are kept.

If your server has ciphers from previous installations, there is a possibility that some ciphers are not considered trustworthy any longer.

The levels of security are represented by colors:

- Normal display color (black or white, depending on the theme): The cipher is considered trustworthy and is used by Tomcat.
- **Red color:** The cipher is not considered trustworthy and is not used by Tomcat. This cipher cannot be used.
- **Orange color:** The cipher is used by Tomcat but is not considered trustworthy by IGEL or Tomcat or another institution. It is recommended not to use this cipher.

The following example includes ciphers with all 3 levels of security:

Inactive Ciphers	Active Ciphers
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256	TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	SSL_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	RC4_MD5_EXPORT
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	RC4_MD5_US
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	RC4_SHA_US
TLS_RSA_WITH_AES_256_CBC_SHA	SSL_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	ECDHE_ECDSA_3DES_EDE_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	ECDHE_RSA_3DES_EDE_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS_ECDH_ECDSA_WITH_RC4_128_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256	TLS_ECDH_RSA_WITH_RC4_128_SHA
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	

Buttons:
 Set active
 Set inactive
 use defaults
 OK
 Cancel



SSL Certificates

Reset web certificates (Only for disaster recovery): Use this only if you cannot access the UMS Server from the UMS Console or the UMS Web App. This function deactivates the certificate chain that was previously used for communication over the Web Port (i.e. the port used for HTTPS; default: 8443; for more information, see [UMS Communication Ports](#)(see page 48)). Also, it creates a new certificate chain which is then used for HTTPS.

- ⓘ If you want to use your own certificate or certificate chain after the reset, see [Using Your Own Certificates for Communication over the Web Port \(Default: 8443\)](#)(see page 123).

3.26.2 UMS Licensing ID Backup

Menu path: **UMS Administrator > UMS Licensing ID Backup**

- ⓘ Default path to the UMS Administrator:
Linux: /opt/IGEL/RemoteManager/RMAdmin.sh
Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe
- ⓘ The UMS Licensing ID is generated upon each UMS Server installation. Therefore, if you have a [High Availability](#)(see page 657) environment, each of the servers has its own UMS Licensing ID, i.e. **Local UMS Licensing ID**. For the communication of all HA servers with the ILP, a **Main UMS Licensing ID** is used. Further information about the UMS Licensing ID can be found under [UMS Licensing ID](#)(see page 444).

Main UMS Licensing ID: The first and last 10 characters of the main UMS Licensing ID are displayed here.

Main UMS Licensing ID fingerprint: The SHA-256 fingerprint of the main UMS Licensing ID.

Local UMS Licensing ID: The first and last 10 characters of the local UMS Licensing ID are displayed here.

- ⚠ In an HA environment, the local UMS Licensing ID can differ from the main UMS Licensing ID. If this is the case, restart the server to get it synchronized. See also [Manual Synchronization of the UMS Licensing ID](#)(see page 164).

Local UMS Licensing ID fingerprint: The SHA-256 fingerprint of the local UMS Licensing ID.

Create new Main UMS Licensing ID: If the installation does not have a UMS Licensing ID, then this was not created during the installation and the creation must be triggered manually.

UMS Licensing ID Backup

Directory: Path where to store the backup.

UMS Licensing ID backup name: The name of the backup which you have defined during the creation.

Date: Date of the backup.



Creating a Backup

UMS Licensing ID backup name: Define the name of the backup.

Set UMS Licensing ID password: The backup of the UMS Licensing ID can only be restored if you enter the password specified here.

3.26.3 UMS Licensing ID Backup on the Command Line

You can create and restore backups of the [UMS Licensing ID](#)(see page 444) using the command line program `ksbackup.exe`. It can be found in the `rmadmin` sub-directory in the UMS installation directory.

Example:

```
Administrator: C:\Windows\system32\cmd.exe
C:\Program Files (<x86>)\IGEL\RemoteManager\rmadmin> ksbackup.exe -b C:\Users\Documents idPassword -s_
```

Program Launch Options

<code>-b path/file_name password</code>	Creates a backup of the specified file secured by a given password.
<code>-r path/file_name password</code>	Restores the specified backup file with a given password.
<code>-s</code>	During processing, all program outputs (except error messages) will be suppressed.



- The part of the path after the last / or \ is always used as the file name. If a backup is created and the file path ends with a / or \, the backup will be saved as `umsLicensingIDBackup.ksbak`.
- If a new backup is given a file name of a backup which already exists in this directory, the existing backup will automatically be overwritten.
- If you are using an [HA environment](#)(see page 657), please note the following:
It is always the UMS Licensing ID of the local server that is backed up. If this server is part of an HA environment, it is not guaranteed that this local UMS Licensing ID is the same as the main UMS Licensing ID. This has to be manually checked beforehand. If the local UMS Licensing ID does differ from the main UMS Licensing ID, restart the server to get it synchronized. See also [Manual Synchronization of the UMS Licensing ID](#)(see page 164).



3.26.4 Backups

Menu path: **UMS Administrator > Backups**

- ⓘ Default path to the UMS Administrator:

Linux: /opt/IGEL/RemoteManager/RMAdmin.sh

Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe

The internal Embedded DB of the UMS Server can be backed up directly via the UMS Administrator. Backups created previously can also be loaded up again.

- [Creating a Backup](#)(see page 536)
- [Restoring a Backup](#)(see page 540)
- [Deleting a Backup](#)(see page 541)
- [Backup on the Command Line](#)(see page 542)
- [Planned Backup](#)(see page 543)

- ⚠ For external database systems, please use the backup and recovery procedures recommended by the DBMS manufacturer. For more information, see [Creating a Backup](#)(see page 536).

Creating a Backup

Menu path: **UMS Administrator > Backups**

- ⓘ Default path to the UMS Administrator:

Linux: /opt/IGEL/RemoteManager/RMAdmin.sh

Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe

Embedded Database

To create a backup of the UMS installation with the embedded database, proceed as follows:

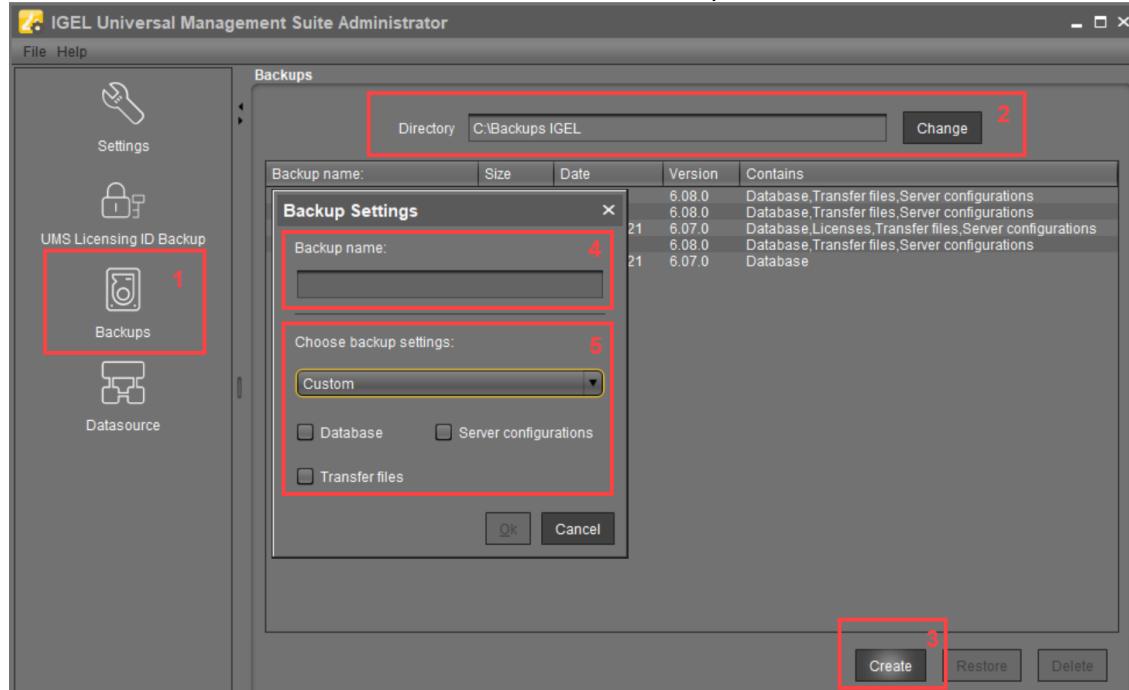
1. In the left-hand column, select **Backups**.
2. Click on **Change** to change the storage location for your backups.
3. Click on **Create**.
4. Under **Backup name**, enter a name for the backup.
5. Select the backup settings under **Choose backup settings**:

The following can be selected:

- **Select all:** Database, [server configurations](#)(see page 537), and transfer files (normally, you'll use this option to ensure that no components are missing from the backup)
 - **Embedded Database:** Database
 - **All files:** Transfer files (e.g. images, session certificates, etc.)
- Note that files which have not been registered in the UMS, but are only stored in the system web resources (e.g. were manually placed in the folder ums_filetransfer) are NOT backed up by the UMS Administrator.



- **Custom:** You can select the data which are to be backed up.



- As of UMS version 5.09, all certificates are included in the database backup.
- As of UMS version 6.08, all device licenses are included in the database backup. Backups of licenses made with the previous UMS versions are supported: Restore the backup, and the license files stored in the backup will eventually be saved in the database; see [Restoring a Backup](#)(see page 540).



Universal Firmware Updates

The files of firmware updates are not part of the UMS embedded DB backup. They are not included in the **Transfer files** backup, and, therefore, have to be copied manually from `[IGEL installation directory]/rmguiserver/webapps/ums_filetransfer`.



- The backup of **Server configurations** includes most configurations of the [Settings for IGEL UMS Administrator](#)(see page 530) area in the UMS Administrator application. Exceptions: **Web server port**, **JWS server port**, and **ciphers** – they are host-specific, i.e. stored separately on each server and cannot be part of any backup. Therefore, you should note the values of these settings if they differ from the defaults and, in the case of recovery/migration procedure, they must be changed on each server manually.

6. Confirm your selection by clicking on **OK**.

The data will be saved in the directory you have selected.



Remember to back up also the UMS Licensing ID, see [UMS Licensing ID Backup\(see page 534\)](#) or [UMS Licensing ID Backup on the Command Line\(see page 535\)](#).

External Database

The full range of backup options in the UMS Administrator is only available if you use the embedded database for your UMS Server installation.

If you use an [external database\(see page 289\)](#), proceed as follows to make a complete backup of your system:

1. For the database itself, use the backup and recovery procedures recommended by the DBMS manufacturer.

Certificates

As of UMS version 5.09, all certificates are included in the database backup.

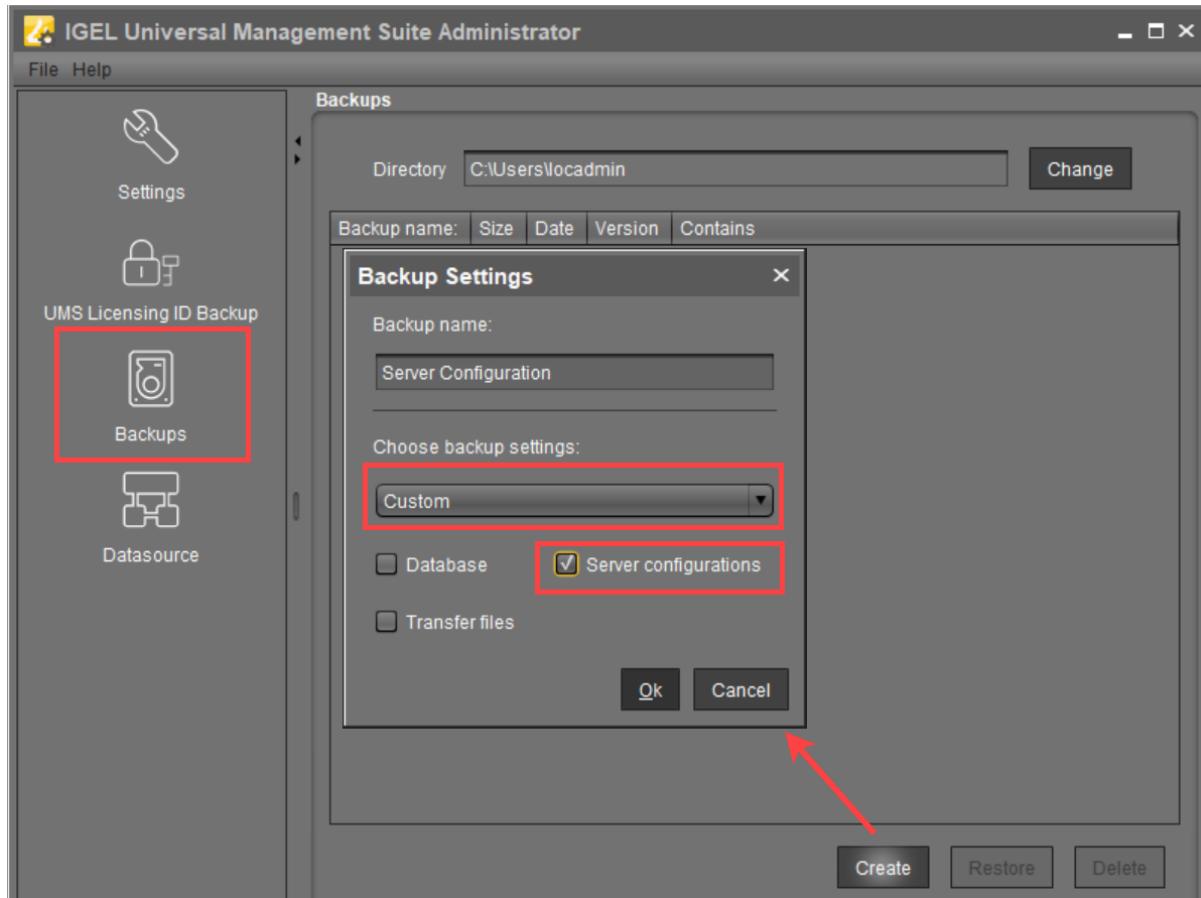
If you need to back up the certificates manually, you can find them here:

- [IGEL installation directory]/rmtcserver/*
It includes the tc.keystore file, which is necessary for the communication with the endpoint devices. The certificate of this keystore can also be exported via the UMS Console under **UMS Administration > Global Configuration > Certificate Management > Device Communication > Export key pair** .
- [IGEL installation directory]/rmclient/cacerts
- [IGEL installation directory]/rmguiserver/
[https_cert_chain.keystore](https://cert_chain.keystore)

Licenses

As of UMS version 6.08, all device licenses are included in the database backup. Previously, they were stored in [IGEL installation directory]/rmguiserver/webapps/e08ce61-d6df-4d2b-b44a-14c1ec722c44 and had to be backed up separately, i.e. manually copied to a secure storage medium.

2. Back up server configurations with the **UMS Administrator > Backups > Create > Custom > Server configurations**. Note separately host-specific configurations that differ from the defaults, see above [Server configurations\(see page 537\)](#):



3. Files and firmware updates must be backed up separately, i.e. manually copied to a secure storage medium. You can find them here: [IGEL installation directory]/rmguiserver/webapps/ums_filetransfer
4. Back up also the UMS Licensing ID, see [UMS Licensing ID Backup](#)(see page 534) or [UMS Licensing ID Backup on the Command Line](#)(see page 535).

i If you are using an HA environment, note the following:
It is always the UMS Licensing ID of the local server that is backed up. Therefore, make sure at first that the **local UMS Licensing ID** is the same as the **main UMS Licensing ID**. If not, restart the UMS Server to synchronize the local UMS Licensing ID with the main UMS Licensing ID and then proceed with creating the backup. See also [Manual Synchronization of the UMS Licensing ID](#)¹⁰⁷.

5. For [HA installations](#)(see page 657) only: Save the current IGEL network token (allows the integration of new servers into the same HA network). This is usually a token created during the installation, see [Installing the First Server in an HA Network](#)(see page 662). If a new IGEL network token has been generated in the meantime, e.g. if changes to certificates were made (see "High Availability" under [Device Communication](#)(see page 453)), this is the token to be backed up.

¹⁰⁷ <https://kb.igel.com/display/ENLITEUMS/.Manual+Synchronization+of+the+UMS+Licensing+ID+v6.01>



Restoring a Backup

Menu path: **UMS Administrator > Backups**

- ① Default path to the UMS Administrator:
Linux: /opt/IGEL/RemoteManager/RMAdmin.sh
Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe

- ① When a backup is restored, your current database status will be overwritten. It is strongly recommended that you create a backup of the current data before another backup is restored, see [Creating a Backup](#)(see page 536).

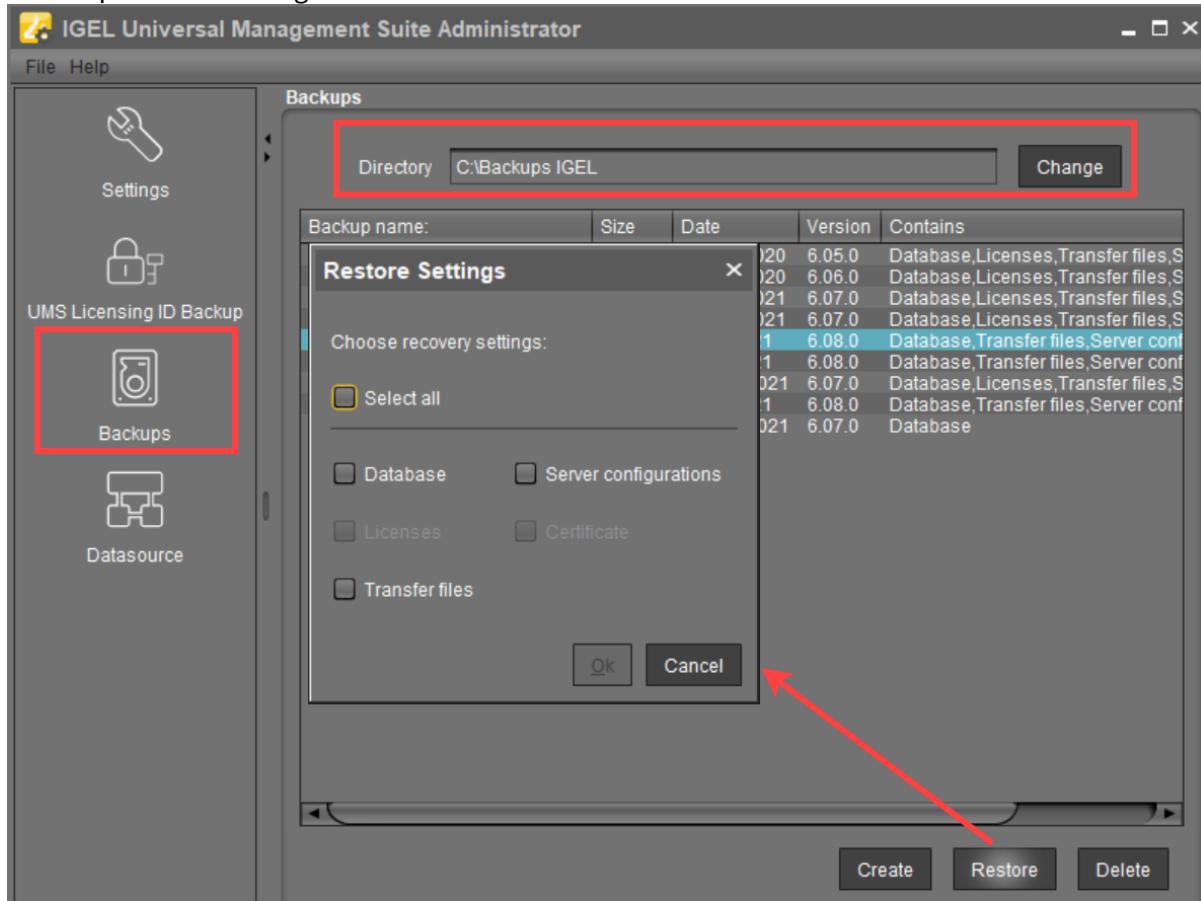
- ① If you restore a database backup of an embedded database of a UMS version prior to 6.05, the superuser credentials are identical to the credentials of the database user. It is recommended to reset the superuser password.
For database backups of UMS versions 6.05 and higher, the superuser credentials have already been stored in the database backup and are taken from there.

To restore a saved backup, proceed as follows:

1. Check under **UMS Administrator > Backups** if the **Directory** is the one that contains your backup; if not, click **Change** to change to the right directory.
2. Select the desired backup from the backup list.
3. Click on **Restore**.
4. Select the components to be restored.
In UMS installations with an external database, you can use the UMS Administrator only to restore



a backup of server configurations.



- i The **Certificate** and **Licenses** options are greyed out since they are included in the database backup as of UMS version 5.09 and 6.08 respectively.

Once your data have been restored, the login data for the database will be displayed.

Tip

To avoid problems with backup restoring and with UMS performance generally, it is highly recommended to use administrative tasks to automatically clean up logs – logging data, job execution data, execution data of administrative tasks, process events, asset information history; see [Create Administrative Task](#)(see page 464). See also [Performance Optimizations](#)(see page 251).

Deleting a Backup

Menu path: **UMS Administrator > Backups**

- i Default path to the UMS Administrator:



Linux: /opt/IGEL/RemoteManager/RMAdmin.sh

Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe

To delete a saved backup, proceed as follows:

1. Select the desired backup from the backup list.
2. Click **Delete** to remove backups that you no longer need.

i Both the entry in the UMS Administrator and the backup file on the hard disk will be deleted!

Backup on the Command Line

A command line program for creating a backup with batch file scripts is also available. With the embackup.exe command line program, you can create backups with the help of batch scripts. You will find embackup.exe in the rmadmin sub-directory in the UMS installation directory.

Example:

```
C:\Program Files (x86)\IGEL\RemoteManager\rmadmin> embackup -b C:\Users\Documents -f -s
```

Program Launch Options

-b path/file name	Creates a backup of the database.
-b path/file name -f	Creates a backup with all three components.
-r path/file name	The backup file with the specified path will be restored in the database.
-s	During processing, all program outputs (except error messages) will be suppressed.



- The part of the path after the last / or \ is always used as the file name. If for example when calling up -b the path of a directory is specified, a backup with the name of the directory will be created and saved in the higher-level directory.
- If a new backup is given a file name of a backup which already exists in this directory, the existing backup will automatically be overwritten.
- When a backup is created, the UMS server does not shut down.



- When a backup is restored, the UMS server briefly shuts down and automatically restarts afterwards.

Planned Backup

You can define a scheduled backup under **UMS Administration > Administrative Tasks**, see [Create Data Backup](#)(see page 465).

3.26.5 Data Source

Menu path: **UMS Administrator > Datasource**

The connection to a database system is provided via data sources which you can manage in the UMS Administrator.

- ⓘ Default path to the UMS Administrator:
Linux: /opt/IGEL/RemoteManager/RMAdmin.sh
Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe

If you have chosen the standard installation, the embedded DB is already set up as the data source and enabled.

See also [Connecting External Database Systems](#)(see page 289).

- [How to Set Up a Data Source in the IGEL UMS Administrator](#)(see page 543)
- [Activating a Data Source](#)(see page 546)
- [Copying a Data Source](#)(see page 546)
- [Optimizing the Active Embedded DB](#)(see page 546)
- [Changing the UMS Superuser](#)(see page 547)

How to Set Up a Data Source in the IGEL UMS Administrator

Menu path: **UMS Administrator > Datasource**

The following article details how to configure the IGEL Universal Management Suite (UMS) data source.

The IGEL UMS supports the following data source types:

- Embedded DB (installed via the IGEL UMS)
- Microsoft SQL Server
- Oracle
- PostgreSQL
- Apache Derby

- ⓘ For details on the supported database systems, see the "Supported Environment" section of the [release notes](#)(see page 565). Details of the requirements when installing and operating the database can be found in the documentation for the particular DBMS.

For information on the external database systems, see also [Connecting External Database Systems](#)(see page 289).

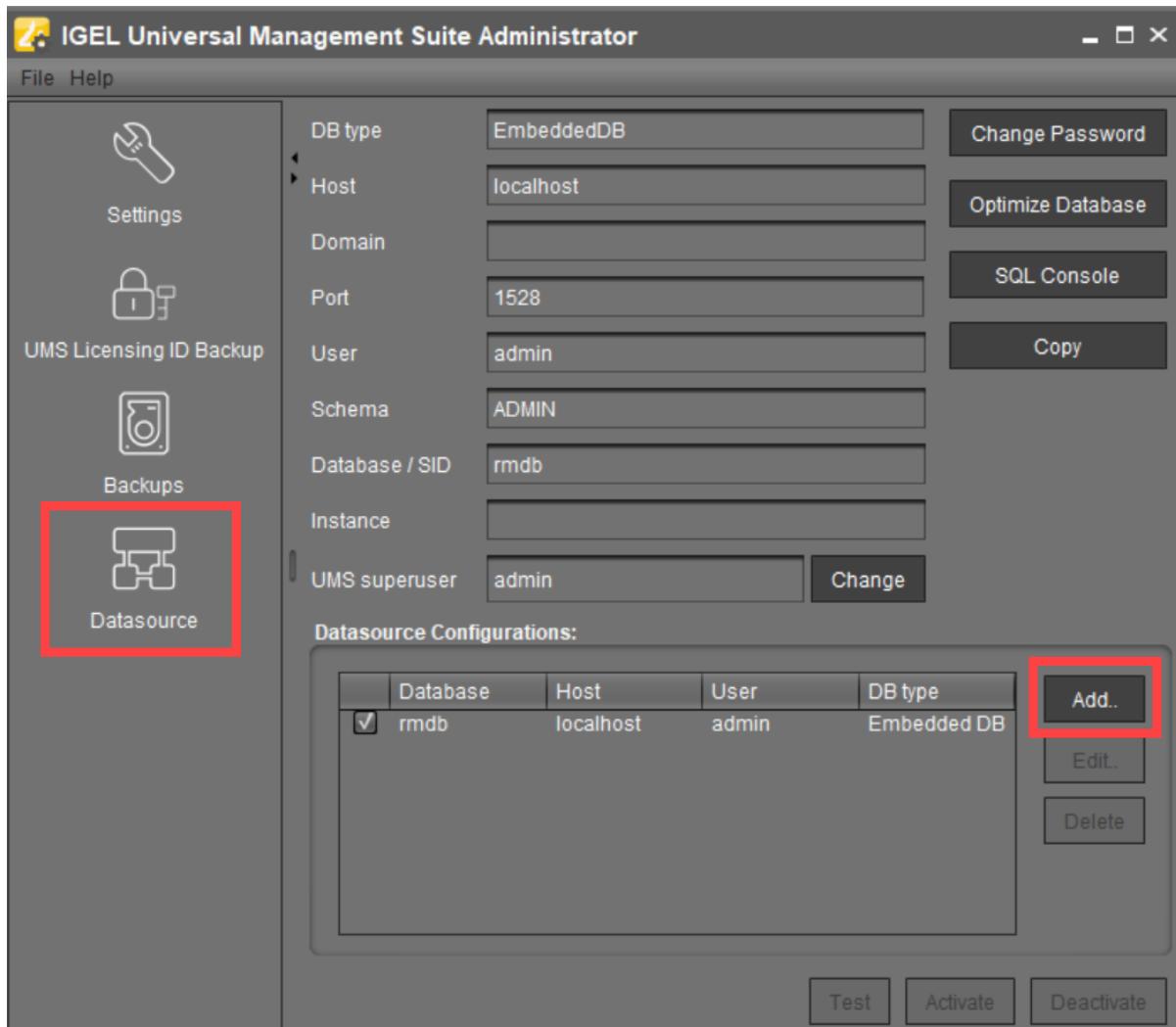


- ⓘ Default path to the UMS Administrator:
Linux: /opt/IGEL/RemoteManager/RMAdmin.sh
Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe

How to Add the Database Connection in the IGEL UMS Administrator

To set up a data source, proceed as follows:

1. Go to **UMS Administrator > Datasource** and click **Add** to add a first data source or an additional one.



A dialog window **New Datasource** will open.



New Datasource

DB type: Oracle

Host: localhost

Domain:

Port: 1521

User:

Schema:

Database / SID: orcl

Instance:

Ok Cancel

2. Select the **DB type**, and enter the **Host**, and the **Port**, as well as the **User** that is set up on the DBMS. For SQL Server Cluster and Oracle RAC, specify the **Instance**.

- i Provided that a data source has not been enabled, these settings can still be changed by selecting **Edit**. The active data source is protected against changes to its configuration. By selecting **Change Password**, you can set a new password for the database user. This is also possible when a data source is active.

- i If you deploy MS SQL Server Always On Availability Groups, use **SQL Server** as a **DB type** and specify under **Host** the domain name of the Always On Availability Group listener.

3. Click on **Test** to test the connection to the database.
This is also possible when a data source is inactive.
4. If required, **activate** the data source. See [Activating a Data Source\(see page 546\)](#).



Activating a Data Source

Menu path: **UMS Administrator > Datasource**

- ⓘ Default path to the UMS Administrator:

Linux: /opt/IGEL/RemoteManager/RMAdmin.sh

Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe

You can set up a number of data sources. However, only one can be actively used by the server.

To activate this data source, proceed as follows:

1. Select a data source from the list of sources that have been set up.
2. Click **Activate**.
3. Enter the password for the data source that you have selected.
While the data source is being activated, the application checks whether a valid database schema can be found. If no schema is found, a new schema will be created. An out-of-date schema will be updated, and, if the schema contains unfamiliar data, these will be overwritten.
4. Confirm each of these actions.

 Overwriting existing data means that the entire database schema will be deleted and not just the out-of-date tables used by the IGEL UMS.

Copying a Data Source

Menu path: **UMS Administrator > Datasource**

- ⓘ Default path to the UMS Administrator:

Linux: /opt/IGEL/RemoteManager/RMAdmin.sh

Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe

To switch from the standard installation with an Embedded DB to an external database system, e.g. an Oracle RAC cluster, proceed as follows:

1. Prepare the new database in accordance with the installation instructions for the UMS.
2. Set up a suitable new data source for this DBMS.
3. Select the Embedded DB data source which is still active.
4. Click **Copy**.
5. Select the destination data source.
6. Start the process after entering the destination login data.
7. Activate the new data source.

Optimizing the Active Embedded DB

Menu path: **UMS Administrator > Datasource**



- ⓘ Default path to the UMS Administrator:
 Linux: /opt/IGEL/RemoteManager/RMAdmin.sh
 Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe

► Click **Optimize Database** to optimize an active embedded database.
 The contents of the database will be restructured.
 The database index will be renewed in order to speed up database operations.
 A message window will appear once the procedure has been successfully completed.

Changing the UMS Superuser

Menu path: **UMS Administrator > Datasource**

The UMS superuser is created initially during the installation process. This user is needed for the first login to the UMS Console and for further configuration tasks, in particular, the definition of additional administrator accounts with restricted rights. The UMS superuser user always has full access rights.

You can change the UMS superuser, which does not affect the user for database connections.

- ⚠ In an HA environment, changing the UMS superuser during operation can lead to issues when the servers are exchanging files. However, these issues are temporary.

► Click **Change** beside the **UMS superuser** field to change the **User name** and **Password** for the UMS superuser.

3.26.6 IGEL UMS Administrator Command-Line Interface

The Universal Management Suite (UMS) Administrator command-line interface allows you to control the IGEL UMS Administrator via a terminal and to automate UMS Administrator actions via scripting. Among these actions are creating and editing database connections for the UMS Server, backing up and restoring the embedded database, configuring communication ports and security, managing the UMS Licensing ID, configuring the superuser, and restarting the UMS Server.

As this feature allows complete control without any graphical desktop environment, it is possible to run the CLI application on headless Linux systems.

Basic Usage

Like the graphical UMS Administrator application, the CLI requires elevated privileges.

- Windows: Open a command prompt (cmd.exe) as Administrator.
- Linux: Become root or use sudo

You can run the main command `umsadmin-cli` from any directory, as the command is made available on the PATH.



- To see the global options and the primary subcommands, enter `umsadmin-cli`

```
root@td-:~/Downloads# umsadmin-cli -h
Usage: umsadmin-cli [-hv] [--machine-readable] [--no-header] [--quiet]
                     [--separator=<cliSeparator>] [COMMAND]
Configures UMS installation
-h, --help           Show this help message and exit.
--machine-readable   Prints output machine-readable with ';' as default
                     separator.
--no-header          Do not print a header line.
--quiet              Suppress all output to stdout/stderr.
--separator=<cliSeparator>
                     Define custom column separator for CLI output.
-V, --version         Print version information and exit.
Commands:
db                  Provides commands for database operations
ports               Configuration of ports
cipher              Manage cipher configuration.
license             View and change licensing ID data
token               Install network token vor UMS server or broker.
su                 Configuration of superuser
restart-server      Restart the server
help                Displays help information about the specified command
```

- To get all possible options for a specific subcommand, enter `umsadmin-cli` followed by the subcommand, e.g. `umsadmin-cli db create`

```
root@td-:~/Downloads# umsadmin-cli db create
Missing required options: '--type=TYPE', '--user=USER'
Usage: umsadmin-cli db create [-d=DOMAIN] [-H=HOST] [-I=INSTANCE] [-n=NAME]
                             [-p=PORT] [-S=SCHEMA] -t=TYPE -u=USER (-A |
                             --password:file=<passwordFile> | --password:in))
Create a new database connection
-A, --no-activate      Skip activation of database (no password required)
-d, --domain=DOMAIN    The database domain
-H, --host=HOST         The database host
-I, --instance=INSTANCE The database instance
-n, --name=NAME         The database name
-p, --port=PORT         The database port
--password:file=<passwordFile>
                       Path to a file containing the password.
--password:in           Shows an interactive prompt to enter the password.
-S, --schema=SCHEMA     The database schema
-t, --type=TYPE          The database type. Valid values:
                        embedded    -> Embedded DB
                        oracle      -> Oracle
                        oracle-rac -> Oracle RAC
                        mssql       -> SQL Server
```

- To get the complete online help with all commands, enter `umsadmin-cli fullhelp`



```
root@...:/home/ike# umsadmin-cli fullhelp
Usage: umsadmin-cli [-hv] [--machine-readable] [--no-header] [--quiet]
                     [--separator=<cliSeparator>] [COMMAND]
Configures UMS installation
-h, --help           Show this help message and exit.
--machine-readable   Prints output machine-readable with ';' as default
                     separator.
--no-header          Do not print a header line.
--quiet              Suppress all output to stdout/stderr.
--separator=<cliSeparator>
                     Define custom column separator for CLI output.
-V, --version         Print version information and exit.
Commands:
db                  Provides commands for database operations
help                Displays help information about the specified command
activate             Activate a database connection
-i     --id            The database identifier
--password:file      Path to a file containing the password.
--password:in         Shows an interactive prompt to enter the password.
```

- i** Certain subcommands have no options and run immediately. Please refer to the [Command Reference](#)(see [page 550](#)).

Global Options

If you intend to use the UMS Administrator CLI in a script, you may want to configure its output to stdout/stderr according to your needs. This makes it easy to further process the output of `umsadmin-cli` and extract any relevant data.

Please see the available options below.

`--machine-readable`

Prints output machine-readable with a semi-colon (;) as default separator.

Example:

```
root@machine:/home/locadmin# umsadmin-cli --machine-readable db list
ACTIVE;DATABASE;HOST;USER;DB-TYPE;ID
true;rmdb;localhost;root;Embedded DB;1
```

`--no-header`

No header line is printed. (Not all commands print a header.)



Example:

```
root@machine:/home/locadmin# umsadmin-cli --machine-readable --no-header db list
true;rmdb;localhost;root;Embedded DB;1
```

--quiet

All output to stdout/stderr is suppressed for some commands which might take a long time to execute. These are, for instance, db backup, db restore, db copy, and server-restart.

Example:

```
root@machine:/home/locadmin# umsadmin-cli --quiet db backup -o /tmp/mybackup02.pbak --
full
root@machine:/home/locadmin#
```

It is still possible to redirect all output to a null device using operating system functions. For example, to redirect standard output and error output to the null device on Linux, use:

```
command ... >/dev/null 2>&1
```

--separator

Defines a custom column separator for output to stdout/stderr.

Example:

```
root@machine:/home/locadmin# umsadmin-cli --machine-readable --no-header --separator "||"
db list
true||rmdb||localhost||root||Embedded DB||1
```

- i Some separator characters, such as the pipe symbol (||), require quotes because they have special functions in terminals.

Exit Codes

Exit Code	Meaning
0	Successful execution
1	Internal error. An error number is outputted to stderr; for details, see Error Numbers (see page 563).
2	Wrong usage of the CLI or invalid arguments

Command Reference

- i **General Usage of Password Options**



Some commands require a password. Entering the password in plain text on the command line is not secure and therefore not possible. Therefore, one of the following password options must be used:

--password:in for interactively entering the password (possibly with confirmation)

--password:file <FILE> for providing a file containing the password

A password file must have the password as the first line and the passwords must not be pure whitespace. Additional lines with content are allowed but will not be evaluated.

UMS Server Restart Required

Most of the commands in the sections "Ports", "Cipher", "Reset Certificates", and "Superuser" change the UMS configuration and a restart of the UMS server is required to make the new settings take effect. This can be done in two ways:

- Use the appropriate function of the OS (e.g. systemctl on Linux)
- Use the command `umsadmin-cli restart-server`

Database



Action	Primary Sub-command	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
List all configured data sources	db	list					<p>Shows the ID of the data source, which is required by other commands.</p> <p>The lowest ID is 1.</p> <p>IDs may change upon the creation and deletion of data sources.</p> <p>It is strongly recommended to always extract the ID before using it in other commands with --id</p> <p>The ID is calculated like this: highest existing ID + 1</p>



Action	Primary Sub-command	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
Create a new database connection	db	create	-t	--type	string	The database type. For a list of the possible values, type umsadmin-cli db create	Type, user, and port are required. Other options may or may not be required depending on the DB type db create will activate the database by default; this can be prevented by using -A or --no-activate. A password option cannot be used then. If activation fails, the data source entry will still be present and is not active (same behavior as in the graphical UMS Administrator). 'rmdb' is a reserved name for the embedded database



Action	Primary Sub-command	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
							type and cannot be used for other types.
			-H	--host	string	The database host	
			-d	--domain	string	The database domain	
			-p	--port	integer	The database port	
			-u	--user	string	The database username	
			-S	--schema	string	The database schema	
			-n	--name	string	The database name. Free text, except 'rmdb'; this name is reserved for the embedded database.	
			-I	--instance	string	The name of the database instance	
			-A	--no-activate		The database will not be activated.	
				--password:file	string	The password is read from a file (plain text) whose path is provided after this option.	
				--password:in	string	The password is read from stdin; an interactive prompt is shown.	



Action	Primary Sub-command	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
Edit a data source	db	edit	-t	--type	string	The database type. For a list of the possible values, type umsadmin-cli db create	Embedded databases cannot be edited (as in the graphical UMS Administrator). All options are optional, except --id
				--host	string	The database host	
				--id	string	The identifier of the database to be edited	
			-i	--instance	string	The name of the database instance	
			-n	--name	string	The database name. Free text, except 'rmdb'; this name is reserved for the embedded database.	
			-p	--port	integer	The database port	
				--schema	string	The database schema	
			-u	--user	string	The database username	



Action	Primary Sub-command	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
Activate a database connection	db	activate		--password:file	string	The password is read from a file (plain text) whose path is provided after this option. Example: umsadmin-cli db activate --password:file /home/ike/password.txt	
				--password:in	string	The password is read from stdin; an interactive prompt is shown.	
				-i	--id	The identifier of the database to be activated	
Deactivate the active database connection	db	deactivate	-i	--id	string	The identifier of the database to be deactivated	
Test the active database connection	db	test		--password:file	string	The password is read from a file (plain text) whose path is provided after this option. Example: umsadmin-cli db test --	



Action	Primary Sub-command	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
						password:file /home/ike/password.txt	
				--password:in	string	The password is read from stdin; an interactive prompt is shown.	
Optimize the active database	db	optimize					This command can only be applied to an embedded database or a Derby database.
Create a copy of the current database	db	copy	-t	--target	integer	The ID of the target database To get the database ID, enter umsadmin-cli db list	
				--password:file	string	The password is read from a file (plain text) whose path is provided after this option.	
				--password:in	string	The password is read from stdin; an interactive prompt is shown.	



Action	Primary Sub-command	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
Delete a database connection	db	delete	-i	--id	integer	The ID of the database connection that is to be deleted	
Create a backup of the current embedded database	db	backup	-o	--outfile		Path to the target file. The file suffix .pbak is automatically added. Existing backup files are not overwritten.	
			-f	--full		Full backup. Database, server configurations, and transfer files are included.	
			-p	--parent		All directories for the specified path will be created if they are not already existing.	
Restore a backup into the embedded database	db	restore	-f	--file		Path to the backup file	



Ports

Action	Primary Sub-command	Secondary Sub-command	Short Option	Long Option	Value	Option Description
List all ports and SSL flag	ports	list				
Set new port numbers or SSL-only flag	ports	set	-d	--dev-comm	integer	Device communication port. For details, see Devices Contacting UMS (see page 64).
			-j	--java-webstart	integer	Java Web Start port
			-w	--web-server	integer	UMS server port. For details, see UMS with Internal Database (see page 59) and UMS with External Database (see page 60).
			-e	--embedded	integer	Embedded database port
				--ssl-only	boolean	Allow SSL connections only

Cipher

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description
List all ciphers, optionally filtered	cipher	list			List all ciphers
			-e	--enabled	List only enabled ciphers
			-d	--disabled	List only disabled ciphers



Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description
Enable ciphers	cipher	enable			Enable ciphers. The ciphers are separated by whitespaces. Example: umsadmin-cli cipher enable CIPHER1 CIPHER2 CIPHER3
				--all	Apply for all; individual cipher names are ignored.
Disable ciphers	cipher	disable			Disable ciphers. The ciphers are separated by whitespaces. Example: umsadmin-cli cipher disable CIPHER1 CIPHER2 CIPHER3
				--all	Apply for all; individual cipher names are ignored.

Reset Web Certificates

Action	Primary Subcommand	Short Option	Long Option	Option Description
Reset web certificates	reset-certs	-y	--yes	Only if provided as confirmation, the reset will run.

Superuser

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value	Option Description
Show UMS superuser	su	list				



Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value	Option Description
Change UMS superuser	su	change	-u	--user	string	New superuser
			-p	--password:file	string	The password is read from a file (plain text) whose path is provided after this option.
				--password:in	string	The password is read from stdin; an interactive prompt is shown.

Licensing ID

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value	Option Description
Show the current Licensing IDs	licensing	list				
Create a new Licensing ID	licensing	create				
Backup the Licensing ID	licensing	backup	-o	--outfile	string	Path to the target file (file suffix: .ksbak)
			-p	--parent		All directories for the specified path will be created if they are not already existing.
				--password:file	string	The password is read from a file (plain text) whose path is provided after this option.
				--password:in	string	The password is read from stdin; an interactive prompt is shown.
Restore a Licensing ID from a backup	licensing	restore	-f	--file	string	Path to the backup file



Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value	Option Description
				--password:file	string	The password is read from a file (plain text) whose path is provided after this option.
				--password:in	string	The password is read from stdin; an interactive prompt is shown.

Network Token

Action	Primary Subcommand	Short Option	Long Option	Value	Option Description	Remarks
Install a network token for the UMS Server or a broker (UMS HA)	token	-f	--token-file	string	Path to token file	This command is also available as a standalone command named <code>umstokeninstall-cli</code> in broker-only installations. It is equivalent to <code>umsadmin-cli token</code> .
			--server	boolean	Install token for UMS Server	
			--broker	boolean	Install token for broker	

Server Restart

Action	Primary Subcommand
Restart the UMS Server	restart-server



Error Numbers

The error numbers are printed in the following format:

<E-NNNN> : <HUMAN READABLE MESSAGE>

Some error descriptions in the following table contain the phrase „[param]“. These will be replaced during runtime with details for the relevant error, e.g. the problematic path for E-1030.

Error number	Error description
1000	Unable to connect to database. UMS server may be down.
1001	Cannot get database configurations.
1002	Cannot create database.
1003	Cannot activate database. [param]
1004	Internal error while activating database.
1005	Database already exists in this configuration.
1006	Database type is unknown.
1007	Database is already activated.
1008	Cannot edit database configurations.
1009	Internal error while optimize database.
1010	The active data source type is not Embedded or Derby and does not support optimization.
1014	No database is active or the active database is not of type 'Embedded' or 'Derby'.
1051	Authentication error or internal error when an attempt was made to copy the database
1052	Error Accessing credentials of source database
1020	Database could not be deleted.
1011	Test of the active data source failed.
1012	No database is activated.
1013	Cannot deactivate database.
1030	The specified directory for the backup does not exist: [param]
1031	Internal error while attempting database backup.
1040	The specified backup file was not found.
1041	The specified backup file has an invalid file type.
1042	Unable to read the specified backup file.
1043	Internal error while activate data source after restore.
1044	Internal error while attempting to restore database.
1045	The active data source is not embedded or there is no active data source.
1090	A name is required for non-embedded database types.
1100	The name 'rmdb' is reserved for the Embedded database.
1091	Activation failed, incorrect password provided.



Error number	Error description
1092	Backup failed, the specified file already exists.
1093	Port number is required for non-Embedded database.
1094	A data source of the Embedded type cannot be edited.
2000	Internal error while reading port configuration.
2001	Internal error while setting port configuration.
2002	Internal error while restarting UMS server.
2003	Invalid port number provided.
2004	Port number [param] already configured.
3000	Internal error while reading cipher data.
3001	Internal error while changing cipher configuration.
3002	Invalid ciphers provided: [param]
4000	Resetting web certificates requires '--yes' option for confirmation.
4001	Internal error while resetting web certificates.
5000	Internal error while reading super user credentials.
5001	Internal error while writing super user credentials.
5002	No username was provided for new credentials.
5003	Unable to set superuser credentials. There is no active data source.
6000	Unable to create new licensing ID.
6001	The specified file for the license key backup already exists.
6002	No internal license keystore found.
6003	Internal error while creating license key backup.
6004	Internal error while restoring license key backup.
6005	The specified file for the license key backup does not exist.
6006	The specified password for the license key backup is incorrect.
6007	The specified path for the license key backup does not exist: [param]
7000	Token file was not found.
7001	Setup type not defined, token not installed.
8000	Internal error while restarting UMS server.
9000	An error with the password file occurred: [param]
9001	The provided passwords did not match. Aborted.
9002	The provided password exceeds the maximum character limit ([param]) or contains only whitespace.



4 UMS Release Notes

- [Notes for Release 6.09.100\(see page 565\)](#)
- [Notes for Release 6.08.120\(see page 569\)](#)
- [Notes for Release 6.08.110\(see page 571\)](#)
- [Notes for Release 6.08.100\(see page 573\)](#)
- [Notes for Release 6.07.100\(see page 578\)](#)
- [Notes for Release 6.06.110\(see page 583\)](#)
- [Notes for Release 6.06.100\(see page 585\)](#)
- [Notes for Release 6.05.110\(see page 591\)](#)
- [Notes for Release 6.05.100\(see page 594\)](#)
- [Notes for Release 6.04.120\(see page 600\)](#)
- [Notes for Release 6.04.110\(see page 602\)](#)
- [Notes for Release 6.04.100\(see page 605\)](#)
- [Notes for Release 6.03.130\(see page 611\)](#)
- [Notes for Release 6.03.110\(see page 613\)](#)
- [Notes for Release 6.03.100\(see page 615\)](#)
- [Notes for Release 6.02.110\(see page 620\)](#)
- [Notes for Release 6.02.100\(see page 623\)](#)
- [Notes for Release 6.01.100\(see page 629\)](#)
- [Notes for Release 5.09.100\(see page 633\)](#)
- [Notes for Release 5.08.120\(see page 641\)](#)
- [Notes for Release 5.08.110\(see page 643\)](#)
- [Notes for Release 5.08.100\(see page 646\)](#)
- [Notes for Release 5.07.110\(see page 650\)](#)
- [Notes for Release 5.07.100\(see page 651\)](#)

4.1 Notes for Release 6.09.100

Software:	Version 6.09.100
Release Date:	2021-11-15
Release Notes:	RN-609100-1
Last update:	2021-11-15

-
- [Supported Environment 6.09.100\(see page 565\)](#)
 - [New Features 6.09.100\(see page 567\)](#)
 - [Resolved Issues 6.09.100\(see page 568\)](#)

4.1.1 Supported Environment 6.09.100

- **UMS Server:**



Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Microsoft Windows Server 2022	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows 11	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Microsoft Windows Server 2022	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**



Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 12c	(with Cluster Support)
PostgreSQL	9.6 and 10 - 13
Apache Derby	10.9 - 10.14

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#) (see page 47).

4.1.2 New Features 6.09.100

UMS common

- Added: Support for **Microsoft Windows Server 2022**. See <https://docs.microsoft.com/en-us/windows/release-health/windows-server-release-info>.
- Added: **Monitoring** endpoint for **requesting the status of UMS Server / ICG**.
- Updated: **Apache Tomcat** from version 8.5.66 to **8.5.72**
- Updated: **Azul Zulu JRE** from version 8u282 to **8u302**

Console, common

- Added: **Microsoft Windows 11** to the supported environment for **UMS Client**.
- Added: **Basic information of used ICG certificates** is now part of the support information (**Help > Save support information...**).

IGEL Cloud Gateway (ICG)

- Added: It is now possible to **add existing ICGs to newly installed UMS** when the messaging is not working.

Administrator application

- Added: **Command-line interface for UMS Administrator** with full feature set (except SQL console)
- Note:** The **functionality** of the command line tools '**embackup**', '**installNetworkToken**', and '**ksbackup**' is **completely included in** the new tool '**umsadmin-cli**'. Therefore, these tools will no longer be available in future UMS releases.

UMS Web App

Security

- Added: **Login brute-force protection**.
 - A1. **Multiple failed login attempts** will lead to a **temporary ban for the user account**.
 - A2. This **includes accounts that do not exist** to prevent probing.



B1. Inserted **dynamic login delay** (milliseconds) to prevent probing.
(Response-time could otherwise be an indicator for the (non-)existence of an account.)

4.1.3 Resolved Issues 6.09.100

UMS, common

- Fixed: **No message templates** available for **Postgres** installations.
- Fixed: **Heavy WebDav access** may cause **poor AD login performance** due to authentication checks.
- Fixed: In some circumstances, the **directory's information for Firmware Customizations and Files** in the UMS-Cache could be out of date.
- Changed: Improved **performance of online check**.

Console, common

- Fixed: **Log Message dialog** did not show any results if the '**Selected Objects**' option was left empty (**System > Logging > Log Messages**).

Console, web start

- Fixed: **UMS Console** couldn't be started **via Java Web Start**.

Views

- Changed: Improved **execution of views** with the condition '**device (NOT) IN directory**'.

Console, administration section

- Fixed: **License file registration failed** when UMS Server and UMS Console are not installed on the same machine (**UMS Administration > Global Configuration > Licenses > Device Licenses**).

Permissions

- Changed: **Passwords saved in the database are hashed with SHA-512** for optimal security.

IGEL Cloud Gateway (ICG)

- Fixed: **ICG with display name with more than 200 characters** can no longer be installed.

Server, common

- Fixed: Devices were **displayed offline after** the used **network adapter** had been **changed**.
- Fixed: Internal issue that resulted in **redundant error log-entries of inability to parse asset inventory events**.

High Availability Feature

- Fixed: **Load balancer** on Linux does not show the full OS version.
- Fixed: **Assigned files** of imported Firmware Customizations **weren't synchronized** within the HA network.

Installer (Linux)

- Fixed: **Upgrade from non-HA to HA** installation on Linux servers.



UMS Web App

Configuration

- Changed: **Folders in the configuration tree** now show the **amount of contained profiles**.
- Fixed: Wrong **naming for number of contained profiles** for a profile directory.
- Fixed: Wrong **German translation** for 'Site'.
- Fixed: Device **icon not aligned** in filter.

Devices

- Changed: **German translations** for detaching objects.
- Changed: The **order of assigned objects** is improved.
- Fixed: **Color** and **text of attachment cards** are incorrect during a drag operation.

Misc

- Changed: **Assign Object icon** now persistent throughout the Web App.
- Changed: **Values** are now **checked before the creation of a new directory**.
- Fixed: **Gaps in the header**.
- Fixed: **Header alignment**.
- Fixed: **Missing icons** in various dropdown components.

4.2 Notes for Release 6.08.120

Software:	Version 6.08.120
Release Date:	2021-09-27
Release Notes:	RN-608120-1
Last update:	2021-09-24

-
- Supported Environment 6.08.120(see page 569)
 - Resolved Issues 6.08.120(see page 571)

4.2.1 Supported Environment 6.08.120

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	



Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 12c	(with Cluster Support)
PostgreSQL	9.6 and 10 - 13
Apache Derby	10.9 - 10.14

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹⁰⁸.

¹⁰⁸ <https://kb.igel.com/display/endpointmgmt608/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>



4.2.2 Resolved Issues 6.08.120

Security

- Fixed: CRITICAL SECURITY ISSUE

UMS Web App can be made to **reveal critical information**, including the UMS Superuser password.

The critical security vulnerability in UMS Web App affects the following IGEL products:

- **UMS 6.8.x** with UMS Web App installed
- **UMS 6.7.x** with UMS Web App installed
- **UMS 6.6.x** with UMS Web App installed
- **UMS 6.5.x** with UMS Web App installed

IGEL strongly recommends that all affected users (UMS Web App installed) **update/upgrade to UMS 6.08.120**.

If you have reasons not to do that, you can do the following:

1. Make a UMS data backup.
2. Re-run your current installer and re-install the UMS without the UMS Web App.

4.3 Notes for Release 6.08.110

Software:	Version 6.08.110
Release Date:	2021-09-13
Release Notes:	RN-608110-1
Last update:	2021-09-13

-
- Supported Environment 6.08.110(see page 571)
 - New Features 6.08.110(see page 573)
 - Resolved Issues 6.08.110(see page 573)

4.3.1 Supported Environment 6.08.110

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	



Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 12c	(with Cluster Support)
PostgreSQL	9.6 and 10 - 13
Apache Derby	10.9 - 10.14

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹⁰⁹.

¹⁰⁹ <https://kb.igel.com/display/endpointmgmt608/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>



4.3.2 New Features 6.08.110

Views

- Added: The text mode in the enhanced expert mode can now **auto-complete** supported operators and recognize unsupported operators as **syntax errors**.

4.3.3 Resolved Issues 6.08.110

Views

- Fixed: **Views that contain a 'is true' or 'is false' constraint** could not be edited in the expert mode.

Console, administration section

- Fixed: It was not possible to edit a **device attribute** without also **changing the internal identifier**.
- Fixed: License file registration failed when UMS Server and UMS Console were not installed on the same machine (**UMS Administration > Global Configuration > Licenses > Device Licenses**).

High Availability Feature

- Fixed: Assigned files of **imported Firmware Customizations** were not synchronized within the HA network.

4.4 Notes for Release 6.08.100

Software:	Version 6.08.100
Release Date:	2021-07-15
Release Notes:	RN-608100-1
Last update:	2021-07-15

-
- Supported Environment 6.08.100(see page 573)
 - Known Issues 6.08.100(see page 575)
 - New Features 6.08.100(see page 575)
 - Resolved Issues 6.08.100(see page 576)

4.4.1 Supported Environment 6.08.100

- UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
-------------------------------	----------	--



Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 12c	(with Cluster Support)
PostgreSQL	9.6 and 10 - 13



Apache Derby

10.9 - 10.14

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹¹⁰.

4.4.2 Known Issues 6.08.100

UMS common

- **CAUTION:** For **Oracle** database installations, **verify the 'open_cursors' setting prior to an upgrade.** The **recommended** setting is **3000**. For more information, see [Oracle](#)(see page 290).

License Deployment

- **Manual registration** of license files fails if UMS Console and server are **not installed on the same machine**. The following error message is displayed to the user: “Unable to register the license file. The license is invalid.”

Workaround: Start the UMS Console from the same server where the UMS is installed.

4.4.3 New Features 6.08.100

Views

- Added: **Enhanced expert mode** to create and adjust complex views using a comfortable text input field.

Admin tasks

- Added: It is possible to specify a **custom view export name for the administrative tasks** "Export view result via mail" and "Save view results in the file system" (**UMS Administration > Global Configuration > Administrative Tasks**).

UMS common

- Updated: **Apache Tomcat** from version 8.5.61 to **8.5.66**

UMS Web App

Master Profiles

- Added: Master profile tree
- Added: Master profile list
- Added: Master profile details

Quick Jump

- Added: Quick Jump **from profile** and **master profile to devices**
- Added: Quick Jump **from device to the assigned profiles**

Configuration

- Added: **Profile directory details** in the **Configuration** app

¹¹⁰ <https://kb.igel.com/display/endpointmgmt608/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>



- Added: **Filtering of activated settings** is now possible.

Devices

- Added: **Last Contact** (last time an endpoint successfully communicated with the UMS) is now displayed **in the device properties section**.

Misc

- Changed: **New icon set** has been implemented to improve accessibility.

4.4.4 Resolved Issues 6.08.100

UMS common

- Fixed: **Restore of embedded database** sometimes fails with **database timeout**.
- Fixed: **Delete actions in UMS Console fail** if the used **MS SQL Server** database is set up **in 'contained' mode**.
- Fixed: **Heavy WebDav** access may cause **poor AD login performance** due to authentication checks.

Console, common

- Fixed: **Only the UMS superuser was allowed to make changes to Access Control** of certain tree nodes.

Devices

- Fixed: Added missing **check for write permission** for certain device actions

Views

- Changed: Small text changes of view/search criterium '**Configuration Changes pending**'

Jobs

- Fixed: **Some jobs were not executed** when the "**retry next boot**" option was selected.

Automatic License Deployment (ALD)

- Changed: **Created device licenses are now containing only one Unit ID** and the **license files are stored in the database** instead of the file system. From now on, **it is no longer possible to create a separate license file backup** since the license files are part of the database.

Console, administration section

- Fixed: **Refresh was needed after adding/removing device attributes** in order to see the correct list of attributes.

AD / LDAP integration

- Fixed: Improved **AD logon performance** when the option '**Include all configured AD domains for search and import of AD users / groups**' (**UMS Administration > Global Configuration > Active Directory/LDAP**) is active.
- Fixed: In the dialog '**Administrator accounts**', the action "**Members**" now **search users for the selected group in all configured ADs** when the option '**Include all configured AD domains for**



search and import of AD users / groups' (UMS Administration > Global Configuration > Active Directory/LDAP) is active.

WebDAV

- Fixed: WebDAV was **no longer accessible after the Web server port** had been **changed**.

IGEL Cloud Gateway (ICG)

- Fixed: **Login to Shared Workplace** failed if the **password** contained **certain special characters or umlauts**.

IMI, server

- Fixed: **Device network name** was **not updated** when the device name was **changed via IMI** and option '**Adjust network name if UMS-internal name has been changed**' (**UMS Administration > Global Configuration > Device Network Settings > Adjust Names of Devices**) was active.

Server, common

- Changed: **Administrative tasks are suspended during database backup task** in order to prevent deadlocks.
- Fixed: **Some UMS features and services** e.g. download of Universal Firmware Updates **didn't work properly after an update** installation for UMS 6.05.120 (or prior) to UMS 6.06.100 or higher was performed or after restoring a backup with schema 6.5 or lower for UMS 6.06.100 or higher.
- Changed: Because of security reasons, the **UMS version information** has been **removed from the '.../info' page**.
- Fixed: The **hostname** was **not editable** in case of Web certificate renewal (**UMS Administration > Global Configuration > Certificate Management > Web**)

High Availability Feature

- Fixed: **Internal version number of UMS Load Balancer** was shown **in the health check**.
- Fixed: **Adding a new process to a HA network** failed if a **network token created with UMS 6.05.120 or lower** was used for the installation.

UMS Web App

Configuration

- Added: **Detach assigned objects** is enabled in the **Configuration** app.
- Added: **Quick Assign** is now **available also on 'Enter'** after selecting an assignable object with a keyboard.
- Changed: **Activated Settings Values overwritten by template keys** are now represented as template key icons.

Devices

- Added: If **online check** is activated, GLOBAL_ONLINE_CHECK_INTERVAL is used for device online status update.
- Added: If **online check** is disabled, more components are aware of that setting. Server load is reduced.
- Added: For **Activated Settings** that are **marked as using a template key**, but no template key was set, a warning icon is shown.



- Changed: If **no changes** occurred in "Edit Custom Properties" dialog, then the **Save** button is **disabled**. (No more empty change requests)
- Changed: It is now possible to **filter Template Key Relations**.
- Changed: **Template key icons** in **Activated Settings Values** are now **clickable**.
- Changed: "**Editable Properties**" are renamed to "**Custom Properties**".
- Fixed: The session parameters inside the **Template Key Relation** tab (Profile) will now show the **correct session instance number**.
- Fixed: **Permissions for move and copy device directory** now follow the UMS.
- Fixed: Improved **styling** of **Template Key Relation** table (alternating rows).

Misc

- Changed: **Performance updates** on various sub-systems.
- Changed: Redesigned "**About**" **dialog**
- Changed: **Quotation marks** for device and directory names and configurations **in logs**.
- Changed: **Quotation marks** for object names **in confirmation dialogs and logging entries**.
- Fixed: Items in **Quick Assign** list were not restricted for **profile rights Assign Device and Assign File**.
- Fixed: Removed **redundant and not translated values** inside the **Logging** app.
- Fixed: **Unused actions and categories** were shown in the **Logging** app.

4.5 Notes for Release 6.07.100

Software:	Version 6.07.100
Release Date:	2021-03-29
Release Notes:	RN-607100-1
Last update:	2021-03-29

-
- Supported Environment 6.07.100(see page 578)
 - Removed Support 6.07.100(see page 580)
 - Added Support 6.07.100(see page 580)
 - Known Issues 6.07.100(see page 580)
 - New Features 6.07.100(see page 580)
 - Resolved Issues 6.07.100(see page 581)

4.5.1 Supported Environment 6.07.100

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355



Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 12c	(with Cluster Support)
PostgreSQL	9.6 and 10 - 13



Apache Derby	10.9 - 10.14
--------------	--------------

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹¹¹.

4.5.2 Removed Support 6.07.100

- PostgreSQL 9.5
- Oracle 11g R2

4.5.3 Added Support 6.07.100

- PostgreSQL 11 - 13

4.5.4 Known Issues 6.07.100

UMS common

- **CAUTION:** For **Oracle** database installations, **verify the 'open_cursors' setting prior to an upgrade.** The **recommended** setting is **3000**. For more information, see [Oracle](#)(see page 290).

4.5.5 New Features 6.07.100

UMS common

- Added: New feature to enable **devices** to **send heartbeat signals** in regular intervals. See [Monitoring Device Health and Searching for Lost Devices](#)¹¹².
- Added: Better integration for **Azure & AWS**. See [Installing a UMS Network on Microsoft Azure](#)¹¹³.
- Updated: Apache **Tomcat** from version 8.5.58 to **8.5.61**
- Updated: **Zulu JRE** from version 8u265 to **8u282**

Asset Inventory Tracker (AIT)

- Added: A (global) **switch to enable or disable** the Asset Inventory Tracker (**UMS Administration > Global Configuration > UMS Features**)

AD / LDAP integration

- Added: **Extended** the Active Directory / LDAP-Service **connection test** to give better feedback (**UMS Console > Administration Tree > Global Configuration > Active Directory/LDAP**)
- Added: Option to **resolve AD user group dependency** within multiple domains (**UMS Administration > Global Configuration > Active Directory/LDAP**)

Server, common

- Added: **Active Directory database users for SQL Server Cluster** database type
- Changed: The **Elasticsearch log files** are now also regarded when collecting the log files

¹¹¹ <https://kb.igel.com/display/endpointmgmt607/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>

¹¹² <https://kb.igel.com/display/endpointmgmt607/Monitoring+Device+Health+and+Searching+for+Lost+Devices>

¹¹³ <https://kb.igel.com/display/endpointmgmt607/Installing+a+UMS+Network+on+Azure>



High Availability Feature

- Added: Much faster upgrade installation sequence for HA installation. See [Updating the Installation of an HA Network](#)¹¹⁴.

Views

- Added: New view/search criterion: **Configuration changes pending**. It's now possible to filter for devices which did not get the newest configuration changes.

UMS Web App

- Added: Introduced a **new global permission "Device Bulk Action"**. This permission **only affects the UMS Web App**. Users without this permission cannot perform actions on multiple devices at once.
- Added: **New section** introduced: **Configuration Management**. See [Configuration](#)¹¹⁵.
 - Added: **Profile tree**
 - Added: Base information for **profiles: settings**
 - Added: Base information for **profiles: template key relations**
 - Added: Base information for **profiles: contained files**
 - Added: Base information for **profiles: assigned devices**
 - Added: **QuickAssignment** via profile section
 - Added: Editing of **profile properties** (not settings!)

4.5.6 Resolved Issues 6.07.100

UMS, common

- Fixed: The **size limit of log files** on some **Windows** installation **did not affect the log files**.
- Fixed: **Deadlock** occurred when runtime information of devices was updated **during copying database to Embedded DB**.
- Fixed: **Some log files** did get **very big** and were **not truncated**.
- Fixed: **Upload of Universal Firmware Updates via FTPS** was not possible because of a certificate error.

UMS Web App

- Fixed: The **search** does no longer **crash handling a massive number of devices**.
- Fixed: A **bug** inside the **License Check Service** (UMS Web App) for **Windows10 devices** resulted in **an error that stopped the index service**.
- Fixed: The **renaming of Windows 10 devices** caused an error inside the Web Application.
- Fixed: **Logging** section inside the UMS Web App was **hidden from AD Group Users and Superusers**.
- Fixed: **New log messages** could sometimes **not be deleted** if the **days-value was set to zero**.

Console, common

- Fixed: In rare scenarios, the **last tree selection** in UMS Console **could not be restored**, and as a result the **UMS Console could not start**.

¹¹⁴ <https://kb.igel.com/display/endpointmgmt607/Updating+the+Installation+of+an+HA+Network>

¹¹⁵ <https://kb.igel.com/display/endpointmgmt607/Configuration+UMS+Web+App>



Jobs

- Fixed: **Start date field** is sometimes not filled when a new scheduled job is created.

Automatic License Deployment (ALD)

- Fixed: Configuration changes for Automatic License Deployment were not synchronized within HA network.

Configuration Dialog

- Fixed: The UMS Console configuration dialog didn't show correct settings for parameters configured parallel by FWCs and indirectly assigned master profiles. The settings of Shared Workplace users were also affected.

Admin Tasks

- Changed: "Delete administrative execution data" admin task: deleted executions are now saved to multiple CSV files for large execution numbers.

AD / LDAP integration

- Fixed: In an HA environment, LDAPS certificates are now loaded automatically to all HA servers.
- Fixed: Change Password for Shared Workplace users with more than one domain controller didn't work.

IGEL Cloud Gateway (ICG)

- Fixed: It is now forbidden to import end-certificates without a subject alternative name (UMS Administration > UMS Network > IGEL Cloud Gateway > Install new IGEL Cloud Gateway and Update Keystore)
- Fixed: Wildcard certificate host name validation in ICG update keystore dialog (UMS Administration > UMS Network > IGEL Cloud Gateway)
- Fixed: Feature 'Send ICG Configuration' (Device > [context menu] > ICG Configuration > Send ICG Configuration) always sends the internal ICG Hostname and Port.

Server, common

- Fixed: Some global configuration settings changes were not synchronized within the HA network.
- Fixed: Automatic License Deployment mechanism was improved in order to prevent deadlocks.
- Fixed: Registering device in UMS from the device itself required the user to have 'Move' permission instead of the correct 'Scan' permission.

High Availability Feature

- Fixed: Files of a WebDAV subdirectory were not synchronized within a HA environment.

Views

- Fixed: Devices where "Boot Time" and "Last contact" are empty are now also considered in views and searches if the criterion is relative and the filter is "Date more than X days ago".

Notifications

- Changed: Improved notification messages for expiring licenses, packs, and certificates



Administrator application

- Fixed: **DB update** failed in case of a **specific certificate configuration**
- Fixed: After **changing the password of the database user**, the application had to be restarted to change the settings of the UMS superuser.

Installer (Windows)

- Fixed: **RMClient.exe** and **RMAadmin.exe** did not have a digital signature.
- Fixed: **Changed ports** (in **UMS Administrator > Settings**) are now **reflected in the firewall exclusions**.

4.6 Notes for Release 6.06.110

Software:	Version 6.06.110
Release Date:	2021-01-25
Release Notes:	RN-606110-1
Last update:	2021-01-25

-
- [Supported Environment 6.06.110](#)(see page 583)
 - [Resolved Issues 6.06.110](#)(see page 584)

4.6.1 Supported Environment 6.06.110

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**



Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.5 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹¹⁶.

4.6.2 Resolved Issues 6.06.110

UMS Web App

- Fixed: The **search** does no longer **crash handling a massive number of devices**.
- Fixed: A bug inside the **Licence Check Service (UMS Web App) for Windows 10 devices** resulted in an error that **stopped the index service**.
- Fixed: The **renaming of Windows 10 devices** threw an error inside the Web Application.

¹¹⁶ <https://kb.igel.com/display/endpointmgmt606/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>



- Fixed: **Logging section** inside the UMS WebApp was **hidden from AD Group users and superusers**.
- Fixed: The **device online check** was incorrect if the user had **insufficient permissions for the corresponding Cloud Gateway**.
- Fixed: New **log messages** could sometimes **not be deleted** if the **days value was set to zero**.

Views

- Fixed: Possible errors in **views with license criterion** combination.

UMS common

- Fixed: The **size limit of log files** on some Windows installation did not affect the log files.
- Fixed: **Deadlock** occurred when runtime information of devices was updated during **copying database to Embedded DB**.
- Fixed: Some log files get **very big** and are **not truncated**.

Universal Firmware Update

- Fixed: Universal Firmware Updates are **no longer deleted from UMS WebDAV** if the protocol is **changed from HTTP(S) (UMS WebDAV) to another protocol**.

AD / LDAP integration

- Fixed: **Shared workplace login** was **not possible** if the user had **no settings assigned**.
- Added: Extended the **Active Directory / LDAP service connection test** to give **better feedback**. (**UMS Console -> Administration Tree -> Global Configuration -> Active Directory/LDAP**)

IGEL Cloud Gateway (ICG)

- Fixed: **Wildcard certificates** were **not selectable in the ICG Update KeyStore** dialog.

Server, common

- Fixed: **Automatic license deployment** mechanism was **improved to prevent deadlocks**.

High Availability Feature

- Added: **Upgrade installation sequence** for HA installations with **big databases**.

Default Directory Rules

- Fixed: **Default Directory Rules with an IGEL Cloud Gateway criterion** could, if applied while registering the device, provide wrong results.

4.7 Notes for Release 6.06.100

Software:	Version 6.06.100
Release Date:	2020-11-16
Release Notes:	RN-606100-1
Last update:	2020-11-16



- Supported Environment 6.06.100(see page 586)
- New Features 6.06.100(see page 587)
- Resolved Issues 6.06.100(see page 589)
- Known Issues 6.06.100(see page 591)

4.7.1 Supported Environment 6.06.100

• **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

• **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		



- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.5 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹¹⁷.

4.7.2 New Features 6.06.100

UMS, common

- Added: Management for the **Web Certificate**. This certificate is used for transferring files to the devices, all WebDAV actions, inter-server communication, the IMI, and the UMS Web App. **Own certificates** can be created and managed, as well as **third-party certificates**, including those from **public CAs**. For details, see [Web](#)¹¹⁸.
- Added: Ability to **exchange the IGEL Cloud Gateway root certificate** (IGEL Cloud Gateway version 2.02.100 or later) via the '**Update Keystore**' dialog (**UMS Administration > UMS Network > IGEL Cloud Gateway**). The dialog now contains an **extra page** to give the **possibility to create and automatically navigate to views** showing the affected devices.

Warning

For all UMS installations with a legacy ICG certificate: After updating devices to IGEL OS 11.04.100 and higher, the devices will no longer be manageable because the new firmware does not accept the legacy ICG certificate anymore. See [Device Does Not Connect to ICG after Update to IGEL OS 11.04 or Higher](#)¹¹⁹.

- Added: **New device commands** were added to **define the device ICG configuration remotely** from the UMS (devices with IGEL OS version 11.04.240 and 11.05.100 or higher). For details, see [Moving an Endpoint Device to an ICG](#)¹²⁰.
- Added: New column "**Send-by**" in events view with filter option (**UMS Console > UMS Administration > UMS Network > Events > e.g. Today**)

¹¹⁷ <https://kb.igel.com/display/endpointmgmt606/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>

¹¹⁸ <https://kb.igel.com/display/endpointmgmt606/Web>

¹¹⁹ <https://kb.igel.com/display/igelos1104/Device+Does+Not+Connect+to+ICG+after+Update+to+IGEL+OS+11.04+or+Higher>

¹²⁰ <https://kb.igel.com/display/igelicg202/Moving+an+Endpoint+Device+to+an+ICG>



- Added: The **permission** to use the **UMS HA Health Check** feature can be set under **System > Administrator accounts**.
- Updated: **Apache Tomcat** from version 8.5.56 to **8.5.58**
- Updated: **Bundled Zulu JRE** from version 8u252 to **8u265**

UMS Web App

- Changed: **UMS Web App login** is filled with the current **UMS Console user** when **opening** it via the **toolbar link**.
- Added: Support for several **new commands** (Send settings to device, Receive settings from device, Reset to factory defaults, Update, Update on shutdown, Refresh system information, Refresh license information)
- Added: **Device commands** can be executed **on directory level**.
- Added: **Support** of custom **device attributes**
- Added: **Presentation of all assigned objects** (profiles, master profiles, files, firmware customizations, template keys, value groups, and Universal Firmware Updates) of a device or a device directory
- Added: **Possibility to assign or detach objects** to or from a device or a device directory
- Added: **Responsive design** (min. supported width: **768 px**)

Unified Logging

- Added: New application to **log all user events in the UMS Web App** (only if feature is activated in **UMS Console > UMS Administration > Global Configuration > Logging**)
- Added: New page in the **UMS Web App** to **search and filter all log events**

Template Keys and Groups

- Added: **Template key option for Citrix StoreFront setup parameter**: server location settings, application autostart, quick start and display filter settings

Views

- Added: New **operators "not beneath"** and **"not in"** for the directory criterion
- Added: New **criterion "Indirect Profile Assignment"** and **renamed** existing **"Profile Assignment"** criterion to **"Direct Profile Assignment"**
- Added: New **criterion "Feature"**
- Added: New **criterion "Has ICG Certificate with SHA1 fingerprint"**

Universal Firmware Update

- Added: Option to **synchronize** downloaded **Universal Firmware Updates** in all UMS **WebDAV directories in HA networks** (**UMS Administration > Global Configuration > Universal Firmware Update**)

Asset Inventory Tracker (AIT)

- Added: **Devices with a 'Starter License'** are **licensed for the Asset Inventory Tracker** feature in the UMS.

Installer (Windows)

- Added: **Firewall ports preselection** depending on installation type

Default Directory Rules



- Added: New **operators "not beneath"** and **"not in"** for the directory criterion
- Added: New **criterion "Indirect Profile Assignment"** and **renamed** existing "**Profile Assignment**" criterion to "**Direct Profile Assignment**"
- Added: New **criterion "Feature"**

4.7.3 Resolved Issues 6.06.100

UMS, common

- Changed: Improved **third party license information dialog** (**UMS Console > Help > Third party licenses**)
- Changed: Improved **device communication check** for manipulated commands
- Fixed: **Config change flag** was not set for **file** and **firmware update assignments**.
- Fixed: **Config change flag** was often not set on object in the **device's assigned/indirect assigned objects** table.
- Fixed: Sometimes, **template values** were **missing** in template groups if both were **restored from the recycle bin** at the same time.
- Fixed: In rare cases, it could happen that some **administrator accounts**, except the UMS superuser, were **not editable**.

UMS Web App

- Fixed: **Devices** were **not displayed** on a screen with **1200 px** resolution
- Fixed: '**Runtime since last Boot**' and '**Total Operating Time**' are presented in a human-readable format (Device > System information).
- Fixed: The **Elastic Search service stopped** due to an error on certain machines

Console, common

- Fixed: "**Check template definition**" can flood the server if activated in parallel
- Changed: **SQL Console output as HTML file** now always with white background and black text color
- Fixed: Issues with the **filename extension** of the saved result files from SQL Console (**UMS Console > Misc > SQL Console > Save Result**)

Template Keys and Groups

- Fixed: Template keys and groups **could not be changed** under certain conditions (**Oracle database only**)

Universal Firmware Update

- Fixed: In rare instances, the **firmware update server** was **overwritten by old settings**.

Configuration Dialog

- Fixed: After editing the page permission pages in a configuration dialog/profile, all **other profiles/TC configurations showed not their own but the previous configuration**.
- Fixed: Sometimes, it was not possible to **remove all page permissions in a configuration dialog or profile**.

Console, administration section



- Changed: **Events views** are now **refreshed automatically** (**UMS Administration > UMS Network > Events**)
- Fixed: The '**Generate a new key pair**' dialog inside the **Device Communication** section could be **finished successfully only by the UMS superuser** (**UMS Administration > Global Configuration > Certificate Management > Device Communication**).
- Fixed: Added missing **ICG certificate permission check** for **Remote ICG install** and **ICG Update Keystore** dialog (**UMS Administration > UMS Network > IGEL Cloud Gateway**)

Admin Tasks

- Fixed: **Renamed views** were shown with **old name** in admin task configuration (delete devices)
- Fixed: **Deleted views / views moved to the bin** are no longer present in admin task configuration (delete devices)

AD / LDAP integration

- Fixed: **In HA environments** and for **multiple domains**, AD certificates were **not loaded** sometimes.

Firmware

- Changed: Improved the **GUI workflow** of firmware import / registration (**UMS Console > System > Import > Import Firmwares**)

WebDAV

- Removed: **Tomcat version** in directory listing
- Changed: Improved **security for WebDAV communication** between UMS components

SSH

- Fixed: Reconnecting a failed **secure terminal session over ICG** failed

High Availability Feature

- Fixed: Upgraded **HA messaging** to the **newest version of ActiveMQ** to resolve security issues

Installer (Windows)

- Fixed: "**install.log**" file was **not created** if only UMS Console was installed.
- Fixed: **Silent installation** with "**Console only**" selection always installed the UMS Web App.
- Fixed: Installer **offered** automatic **embedded database backup** after the previous uninstallation.
- Fixed: **Deselecting** the **UMS Web App** in the Windows installer **also deselected "Standard UMS" server**, including subcomponents.
- Fixed: The **UMS Web App** will **no longer** be **preselected** on "**Console only**" update installation (Windows installer).
- Fixed: **Previous selection of the UMS Web App** was not taken into account during the **update installation**.
- Fixed: The **UMS Web App** was **re-selected** upon selection of standard or HA server component.

Installer (Linux)

- Fixed: "**install.log**" file was **not created** if only UMS Console was installed.
- Changed: **Replaced SysVinit** scripts with **systemd** unit files for UMS Server, Load Balancer, and Watchdog during Update to 6.06.100 (Linux only)



- Fixed: **Database passwords with special characters** were misformatted during database setup, leading to password mismatch when used in UMS Console login (Linux only)
- Changed: **Improved support for special characters** (e.g. umlauts) in all input dialogs in Linux installer
- Fixed: The **UMS Web App did not start on Ubuntu 20.04** due to a missing library in Tomcat configuration

Notifications

- Fixed: When **all licenses of a pack are used up**, a warning notification is shown, not an error notification.
- Changed: Improved **notification classification and management**
- Changed: Improved **notification messages for expiring licenses, packs, and certificates**

UI / Look&Feel

- Changed: **Button order for Access Control** dialog is now: **Apply, OK, Cancel**.

Default Directory Rules

- Fixed: **Rules with a "Device License" criterion** did not generate the correct results.

4.7.4 Known Issues 6.06.100

UMS Web App

- **UMS superuser** does not have the permission to access the **Logging** application.

4.8 Notes for Release 6.05.110

Software:	Version 6.05.110
Release Date:	2020-10-08
Release Notes:	RN-605110-1
Last update:	2020-10-07

-
- [Supported Environment 6.05.110](#)(see page 591)
 - [Resolved Issues 6.05.110](#)(see page 593)

4.8.1 Supported Environment 6.05.110

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355



Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.5 - 9.6 and 10.1



Apache Derby

10.9 - 10.14

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹²¹.

4.8.2 Resolved Issues 6.05.110

UMS, common

- Fixed: **Plain messages** (sent to the device) are **not visible**. (**UMS Console > Global Configuration > Messages to Devices**)

UMS Web App

- Fixed: **Shadowing** not working with **Internet Explorer**. (**UMS Web App > Device > Shadowing**)

Devices

- Fixed: Under rare circumstances, **manual license deployment** did not work **via Java Web Start**. (**Device context menu > License manually...**)

AD / LDAP integration

- Fixed: If **multiple Active Directories with LDAP Service** configuration were used, only one of the domains was working correctly. (**UMS Console > Global Configuration > Active Directory / LDAP**)

Server, common

- Fixed: Having **multiple device certificates** could result in a **5 seconds delay for all commands**. (**UMS Console > Global Configuration > Certificate Management**)

Administrator application

- Fixed: **Database ports** for **SQL Server AD** connections are not editable. (**UMS Administrator > Datasource**)

Notifications

- Fixed: When **all licenses of a pack are in use**, a **warning notification** will be shown instead of an error notification. (**UMS Console > Help > Notifications**)
- Changed: Improved notification messages for **expiring licenses, packs, and certificates**. (**UMS Console > Help > Notifications**)
- Changed: **Notification classification and management** were improved. (**UMS Console > Help > Notifications**)

¹²¹ <https://kb.igel.com/display/endpointmgmt605/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>



4.9 Notes for Release 6.05.100

Software:	Version 6.05.100
Release Date:	2020-07-15
Release Notes:	RN-605100-1
Last update:	2020-07-15

- [Supported Environment 6.05.100](#)(see page 594)
- [Removed Support 6.05.100](#)(see page 595)
- [Added Support 6.05.100](#)(see page 596)
- [Known Issues 6.05.100](#)(see page 596)
- [New Features 6.05.100](#)(see page 596)
- [Resolved Issues 6.05.100](#)(see page 597)

4.9.1 Supported Environment 6.05.100

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	



Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.5 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹²².

4.9.2 Removed Support 6.05.100

UMS Server

- Microsoft Windows Server 2008 (64 bit and with SP2) -> EOL 14.01.2020
- Microsoft Windows Server 2008 R2 (64 bit and with SP1) -> EOL 14.01.2020

UMS Client

- Microsoft Windows Server 2008 (64 bit and with SP2) -> EOL 14.01.2020

¹²² <https://kb.igel.com/display/endpointmgmt605/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>



- Microsoft Windows Server 2008 R2 (64 bit and with SP1) -> EOL 14.01.2020
- Microsoft Windows 7 (64 bit and with SP1) -> EOL 14.01.2020

Backend database (DBMS)

- PostgreSQL 9.4 -> EOL Feb 2020

4.9.3 Added Support 6.05.100

UMS Server

- Amazon Linux 2
- Ubuntu 20.04 (64 bit)

UMS Client

- Amazon Linux 2
- Ubuntu 20.04 (64 bit)

4.9.4 Known Issues 6.05.100

UMS Web App

- **Shadowing** is not working with **Internet Explorer**.

4.9.5 New Features 6.05.100

UMS, common

- Added: Support of **Active Directory authentication for MS SQL Server** database.
- Added: New UMS superuser for initial UMS setup. This '**UMS superuser**' is automatically **created during installation** and receives **the same username and password as the database user**.
- **DB user has no longer the rights for** accessing **UMS, UMS Web App, IMI**; UMS superuser has to be used instead. The **UMS superuser** can be **configured with IGEL UMS Administrator** (Settings).
- Updated: **Apache Tomcat** from version 8.5.50 to **8.5.56**.
- Updated: **Java** from version 8u242 to **8u252**.

UMS Web App

- Added: **Web-based user interface** for managing IGEL OS endpoints (**early feature set**)
 - Managing device tree
 - See device details (System information, License information, User login history)
 - Sending power control commands (Reboot, Shutdown, Suspend, Wakeup)
 - Shadow devices
 - Powerful search
 - Network and server overview

See <https://kb.igel.com/ums/webapp/en> for more details.

Console, common



- Added: **Toolbar** in the UMS Console provides the link for the UMS Web App.

Console, administration section

- Changed: The '-' sign is now optional and editable in the prefix of the network name (**UMS Administration > Global Configuration > Device Network Settings > Naming Convention**). Prefixes that generate a non-standard network name are not allowed if **Adjust Names of Devices > Adjust network name if UMS-internal name has been changed** is selected.

IGEL Cloud Gateway (ICG)

- Added: It is now possible to run **ICG on port 443** (ICG 2.02.100 and higher).
- Added: A **limit for possible device connections** can be defined for an ICG; ICG with version 2.02.100 or higher is required (**UMS Administration > UMS Network > IGEL Cloud Gateway > Edit Connection Limit**)

High Availability Feature

- Added: Tool to check the status of an HA environment (**Help > UMS HA Health Check**)

Installer (Windows)

- Added: New Setup Page to configure **Firewall port exclusions** (only **incoming connections**)
- Added: New **option to select the UMS Web App** component for installation
- Changed: Installer shows information and a weblink for the UMS Web App if it is selected for installation.

4.9.6 Resolved Issues 6.05.100

UMS, common

- Removed: **Command Devices > Other commands > Delete file from device**.
- Changed: Import of keystore files **supports** also **JKS keystores** (**UMS Administration > Global Configuration > Certificate Management**).
- Changed: **Certificate chains** could be imported although they are not supported. An import is now prevented (**UMS Administration > Global Configuration > Certificate Management**).
- Fixed: The **user manual** couldn't be opened with the **UMS internal PDF viewer** (**Help > User Manual (offline)**)
- Added: Option for **choosing the PDF viewer** used for the offline manual (**Misc > Settings > General**)

Console, common

- Fixed: **Universal Firmware Update** assignments of devices were not visible in some cases.
- Fixed: Some **scrollbars**, mostly horizontal ones, were extremely slow.
- Fixed: Missing **German translations** in request chart dialog of a selected IGEL Cloud Gateway (**Show History**)
- Fixed: **Rich Message Editor** had wrong background color in **Information/Help tab**



- Fixed: **Save device files for support** (Help menu) and **Export Device Settings** (System > Export...) dialogs opened very slowly when no device was selected and therefore all devices were loaded.
- Fixed: In rare circumstances, the **device specific command** list was not complete.
- Changed: **Online check interval** (Misc > Settings > Online check) has a valid range between 100 ms and 1 hour. For existing installations, values outside this range will be adjusted to the closest valid value.
- Changed: Modified **permissions**. A 'Deny' can't be overwritten by an 'Allow', see <https://kb.igel.com/ums/no-permissions-after-ums-update>

Devices

- Fixed: **License model information** was not updated on up-/downgrade, affecting legacy licenses for ICG, HA, and AIT. Information is **now updated on each boot**.
- Changed: **ICG administrated devices without valid IGEL Enterprise Management Pack license** are now shown with the 'device isn't licensed' icon.

Firmware Customization

- Fixed: Some **exported firmware customizations** could not be imported if they were created with **Oracle Database**.

Profiles

- Fixed: Error occurred when executing '**Take over settings from...**' for devices.

Views

- Fixed: **Update time of views and searches** was not displayed in a localized format.
- Fixed: Error occurred when a **view with a relative date criterion** was created and a **value of 0 days** was specified.
- Changed: '**Device license**' criterion now contains the **possibility to search for all license types**.
- Changed: **Special characters** in **MAC** address search are **ignored**.

Jobs

- Fixed: A **missing library** could lead to failing jobs on **headless installations**.
- Fixed: Jobs **could not be edited/selected** (The error message was '**Error Unable to load details for the tree nodes. Original error message: null**').

Automatic License Deployment (ALD)

- Fixed: Devices **don't receive a renewal license automatically** if the renewed subscription pack is assigned to the UMS Licensing ID and the pack has no ALD Token.

Universal Firmware Update



- Fixed: The **check for** available **firmware updates** does no longer fail if some of the **firmware properties files** are invalid.
- Fixed: **User name could be edited** in the settings of Universal Firmware Updates for special system users.

Searches

- Fixed: User was not told to do a **necessary restart of the UMS Console** if certain configurations changed.
- Fixed: **Search History** used **lifetime settings of views** instead of its own lifetime settings.

Admin tasks

- Changed: Exported **views are split into multiple files** if the file size exceeds 25 MB. This **affects** the administrative tasks '**Save view results in the file system**' and '**Export view result via mail**' (**UMS Administration > Global Configuration > Administrative Tasks**) and the context menu action '**Send view result as mail**' of views.
- Added: **Context menu** action '**Save as...**' offers now the option to **save views or searches as ZIP file**.

VNC

- Fixed: **No confirmation dialog** was displayed if **multiple VNC session tabs** were about to be closed.

IGEL Cloud Gateway (ICG)

- Fixed: **Shadowing over ICG** failed if a **proxy** server was configured.
- Fixed: Selection of a configured IGEL Cloud Gateway took very long when it was not reachable (**UMS Administration > UMS Network > IGEL Cloud Gateway**)
- Fixed: **Shadowing/Secure terminal over ICG** didn't regard **proxy** configuration.
- Fixed: ICG was **displayed online** when it was running, but the **websocket** connection **wasn't established** yet.
- Fixed: **Job** option '**Retry next boot**' was **ignored** if the device is connected via ICG (requires firmware LX 11.03.500 or newer).
- Fixed: Not all **HA Servers** were connected to a newly registered ICG.
- Changed: **Hostname/IP** text field is now **disabled** if '**CA Certificate**' is selected as a certificate type (**UMS Administration > Global Configuration > Cloud Gateway Options > Create signed certificate**).
- Changed: Information about the **last contact** of an IGEL Cloud Gateway is shown in **UMS Administration > UMS Network > IGEL Cloud Gateway > Gateway details**.

Asset Inventory Tracker (AIT)

- Changed: Improved the **loading** of Asset Information.

Administrator application



- Changed: Reduced the list of **available cipher suites** for **GUI server port** (default: 8443) (**UMS Administrator > Settings > Cipher (Server-side) > Configure Ciphers**).
- Fixed: **Shortcut** for IGEL **UMS Administrator** didn't work after the update of UMS installation.

Database schema

- Fixed: **No upgrade** possible if the **MS SQL Server** database has a **schema name** with **dashes**.

High Availability Feature

- Fixed: **Special characters '.' and '-' in database user name** caused problems during HA update.
- Fixed: In some cases, **database configuration** was **not synchronized within the HA network** depending on the available UMS Servers.
- Fixed: **Deletions of files in WebDAV folder** were not synchronized in the UMS HA network.
- Changed: **Changes** referring to the **configured certificates** are now **automatically synchronized** within the HA network and **no longer require a restart** of the **IGEL RMGUIServer** (**UMS Administration > Global Configuration > Certificate Management**).

Installer (Linux)

- Fixed: On some dialogs, the **installation couldn't** be **aborted** with **[ESC]** key.

Notifications

- Added: When the available **amount of licenses of a License Pack** is **below the limit** or when it **exceeds the total amount**, a notification is shown.

4.10 Notes for Release 6.04.120

Software:	Version 6.04.120
Release Date:	2020-05-06
Release Notes:	RN-604120-1
Last update:	2020-05-06

-
- Supported Environment 6.04.120(see page 600)
 - Removed Support 6.04.120(see page 602)
 - New Features 6.04.120(see page 602)
 - Resolved Issues 6.04.120(see page 602)

4.10.1 Supported Environment 6.04.120

- **UMS Server:**



Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	



PostgreSQL	9.5 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹²³.

4.10.2 Removed Support 6.04.120

UMS Server

- Microsoft Windows Server 2008 (64 bit and with SP2) -> EOL 14.01.2020
- Microsoft Windows Server 2008 R2 (64 bit and with SP1) -> EOL 14.01.2020

UMS Client

- Microsoft Windows Server 2008 (64 bit and with SP2) -> EOL 14.01.2020
- Microsoft Windows Server 2008 R2 (64 bit and with SP1) -> EOL 14.01.2020
- Microsoft Windows 7 (64 bit and with SP1) -> EOL 14.01.2020

Backend database (DBMS)

- PostgreSQL 9.4 -> EOL Feb 2020

4.10.3 New Features 6.04.120

- Support of **OSCW** (IGEL OS Creator for Windows)

4.10.4 Resolved Issues 6.04.120

Console, common

- Fixed: **Universal Firmware Update assignments** of devices were **not visible** in some cases.
- Fixed: In rare circumstances, the **device-specific command list** was **not complete**.

IGEL Cloud Gateway (ICG)

- Fixed: **Shadowing/SecureTerminal via ICG** always **used the internal ICG address and port** instead of the external address and port (if available).

4.11 Notes for Release 6.04.110

Software:	Version 6.04.110
Release Date:	2020-03-12
Release Notes:	RN-604110-1
Last update:	2020-03-12

¹²³ <https://kb.igel.com/display/endpointmgmt604/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>



- [Supported Environment 6.04.110\(see page 603\)](#)
- [Resolved Issues 6.04.110\(see page 604\)](#)

4.11.1 Supported Environment 6.04.110

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	with SP1
Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	



Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Backend Database (DBMS):		
Microsoft SQL Server 2012		
Microsoft SQL Server 2014	(with Cluster Support)	
Microsoft SQL Server 2016	(with Cluster Support)	
Microsoft SQL Server 2017	(with Cluster Support)	
Microsoft SQL Server 2019	(with Cluster Support)	
Oracle 11g R2		
Oracle 12c		
PostgreSQL	9.4 - 9.6 and 10.1	
Apache Derby	10.9 - 10.14	

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹²⁴.

4.11.2 Resolved Issues 6.04.110

Jobs

- Fixed: **Jobs could not be edited/selected.** (Error Message was "Error Unable to load details for the tree nodes. Original error message: null")
- Fixed: A **missing library** could lead to **failing jobs on headless installations.**

Automatic License Deployment (ALD)

- Fixed: **Devices did not receive a renewal license** automatically if the renewed subscription pack was assigned to the UMS Licensing ID and the pack had no ALD Token.

Universal Firmware Update

- Fixed: The check for available firmware updates failed with a null pointer message if one of the downloaded firmware properties was invalid.

Searches

- Fixed: **Search History used lifetime settings of views** instead of its own lifetime settings.

Database schema

- Fixed: The **UMS could not be updated** if the used **schema name** contained **dashes**. (Only for Microsoft SQL Server databases)

¹²⁴ <https://kb.igel.com/display/endpointmgmt604/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>



4.12 Notes for Release 6.04.100

Software:	Version 6.04.100
Release Date:	2020-02-17
Release Notes:	RN-604100-1
Last update:	2020-02-17

- [Supported Environment 6.04.100](#)(see page 605)
- [New Features 6.04.100](#)(see page 606)
- [Resolved Issues 6.04.100](#)(see page 608)

4.12.1 Supported Environment 6.04.100

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	with SP1
Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1



Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹²⁵.

4.12.2 New Features 6.04.100

UMS, common

- Added: **Shared Workspace** can be deactivated.
- Added: Support for **Secure Terminal via IGEL Cloud Gateway** (ICG 2.01.100 or higher and IGEL OS 11.02.100 or higher are required).
- Added: **Installer** and **UMS Administrator** perform **database version check** when a database is selected.
- Changed: It is possible to **log in to the UMS Server** via the UMS Console if the **UMS Server is in HA update mode**.

¹²⁵ <https://kb.igel.com/display/endpointmgmt604/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>



- Added: 'Manual Licenses Dialog' – Table with licensable devices shows the **list of licensing pack IDs** in the comment if the information is available in the UMS.
- Updated: Apache **Tomcat** from version 8.5.45 to **8.5.50**.
- Updated: **Java** from version 8u222 to **8u242**.

Universal Customization Builder (UCB)

- Added: **Universal Customization Builder** (for Windows) is now **available for free** (No license required).
- Removed: Obsolete **Linux part of Customization Builder**.

Jobs

- Added: **New Job** command '**Send Message**' added.

Universal Firmware Update

- Added: The UMS Server supports **FTP passive mode for Universal Firmware Upload**.
- Added: **Check for free disk space** on the file system **before downloading firmware updates**.

Console, administration section

- Added: Show **UMS Licensing ID fingerprint** in the **UMS Console (UMS Administration > Global Configuration > Licenses > UMS Licensing ID)**.
- Changed: Option to enable **Master Profiles**, **Template Profiles** and **Recycle Bin** moved to new node **UMS Features (UMS Administration > Global Configuration > UMS Features)**.
- Changed: It is now possible to choose **a specific port for the online check (UMS Administration > Server Network Settings > Online Check Parameters > Specify online check port (UDP))**.

Administrator application

- Added: Show **UMS Licensing ID fingerprint** in the **UMS Administrator** (Administrator application > **UMS Licensing ID Backup**).
- Added: **Multiselect option for cipher selection** (UMS Administrator > **Settings > Cipher > Configure Ciphers**).
- Added: **Confirmation dialog** after the database password change.

Notifications

- Added: Notifications for **expiring** and **expired certificates (Help > Notifications)**.
- Added: Notifications for **expiring** and **expired packs (Help > Notifications)**.
- Added: Option to **show archived notifications (Help > Notification)**.
- Added: Option to **restore archived notifications**.
- Changed: Replaced the "**Do not show again**" **checkbox** for multiple notification selection with a **dropdown action selector** in the Notification dialog (**Help > Notifications**).
- Changed: **Notifications are automatically restored from the archive** when the Info Type is updated to a higher level (from warning to error).



Devices

- Added: **Device file location can now be edited** before sending a file to a device (Device context menu > Other commands > 'File UMS > Device')

Views

- Added: If '**Send view result as mail**' ('View' context menu) fails, **an error message is displayed in the 'Messages' area**.
- Added: It is now **possible to send view results as mail even if the result is not loaded** in the detail view.

VNC

- Added: **Secure Terminal confirmation dialog** shows whether the terminal feature enabled status for each device.

IGEL Cloud Gateway (ICG)

- Added: The **Events table in the UMS Administration** view is always visible in the management tree. **ICG events will be logged in the table (UMS Administration > UMS Network > Events)**

Installer (Windows)

- Updated: **Bundled Microsoft Visual C++ 2017 Redistributable** from version 14.15 to **14.16**.

4.12.3 Resolved Issues 6.04.100

UMS, common

- Changed: **Activation/Deactivation of template profiles/master profiles has to be confirmed now** when at least one key value/master profile exists.
- Fixed: Several **file choosers did not remember the last selected directory**.

Console, common

- Fixed: '**Messages**' area sometimes **forgot its previous size**.
- Fixed: Various **windows did not remember their last size, position** or had an unfavorable default size.
- Fixed: **Save support information** could sometimes not be generated due to the unnecessary size check.
- Added: **Cross-check of a user and group name** when adding a new administrator account.

Server, common

- Fixed: Removed misleading **logging information on updating network name for Linux** clients (network.interfaces.ethernet.use_igel_setup)



Devices

- Fixed: '**Runtime since last Boot**', '**Total Operating Time**', and '**Battery Level**' were **not always refreshed** on Refresh/F5.
- Fixed: **Changes to a device or a profile were lost** when switching to UMS Administrator in UMS Console.
- Fixed: **Update on network name (DNS) was not triggered** if name was changed via system information.

Firmware Customization

- Fixed: **Files or folders with spaces in the name** could not be used in **Firmware Customizations** or **file upload**.

Jobs

- Fixed: **Log messages for jobs** were not displayed.

Universal Firmware Update

- Changed: Snapshot upload in '**Universal Firmware Update**' **only allows** files with **.snp filename extension**.

Searches

- Fixed: **Changes to the Search result** page behavior (**Misc > Settings > Views and Searches > Page Behavior**) were **not applied immediately** after saving the settings and selecting a search result.

Configuration Dialog

- Fixed: "**Always apply settings on reboot...**" checkbox was **missing in Update time dialog** when saving Device/Profile configuration.

Console, administration section

- Fixed: The **split position of the panels** in the detail view of a server (**UMS Administration > UMS Network > Server**) was not persistent.
- Fixed: **Connect/Disconnect operation of ICGs to UMS HA** had inconsistent behavior.
- Changed: **Online Check Response Timeout input** restricted to **100 ms up to 10.000 ms** (**UMS Administration > Global Configuration > Server Network Settings**).

AD / LDAP integration

- Changed: For an administrator account import of users from an AD/LDAP directory (**System > Administrator account > Import**), the **selection for 'Add user/group' was improved**.



- Fixed: **Inherited permissions of an imported AD user were not displayed correctly** in the 'Effective Rights' section of the 'Administrator accounts' window (**System > Administrator accounts > Effective Rights**)

Console, web start

- Fixed: An issue introduced in UMS 6.03.120 prevented the **execution of the UMS Console via Java Web Start**.

VNC

- Fixed: **VNC Viewer always started on the primary screen** instead of the last screen (multidisplay environment).
- Fixed: The **VNC Certificate Dialog could be off-screen** and so blocked the user from interactions.

IGEL Cloud Gateway (ICG)

- Removed: Misleading **log message during ICG installation**.

Mobile Device Management (MDM)

- Fixed: **Synchronization with ICG** failed if the MDM push certificate had expired.

Administrator application

- Fixed: **Backup sizes smaller than 1 KB** were not displayed correctly.
- Added: **Additional check for the existing database schema** before activating a database connection.
- Added: **Check for supported database versions**.

High Availability Feature

- Fixed: **Misc settings** configurations (**UMS Administration > Global Configuration > Misc Settings**) were **not synchronized with all HA servers**.
- Fixed: **WebDAV subfolders** were **not synchronized with other HA servers**.
- Fixed: **Adding an HA server after adding an ICG server** to the environment **caused ICG connection problems**.
- Fixed: The created **support file**, from triggering 'Save support information' (**Help > Save support information**), **did not** always **contain the information of remote components**.

UI / Look&Feel

- Fixed: **Visibility** of various (disabled) **menu icons**.
- Removed: Deprecated **bevel bar from legacy themes**.

Notifications



- Fixed: **Notification dialog** did sometimes not show notifications **when global notifications were enabled**.

4.13 Notes for Release 6.03.130

Software:	Version 6.03.130
Release Date:	2019-12-10
Release Notes:	RN-603130-1
Last update:	2019-12-10

-
- Supported Environment 6.03.130(see page 611)
 - New Features 6.03.130(see page 612)
 - Resolved Issues 6.03.130(see page 613)

4.13.1 Supported Environment 6.03.130

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	with SP1
Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	



Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹²⁶.

4.13.2 New Features 6.03.130

◆ UMS Common

- Changed: **All IGEL services** and resources like the **firmware update server** (which was fwu.igel.com and is now fwus.igel.com) and the **IGEL Knowledge Base** (kb.igel.com¹²⁷) are now contacted via **HTTPS. It is now important to allow the https port (default 443) and the new address (fwus.igel.com) in the firewall rules and the proxy rules.**

¹²⁶ <https://kb.igel.com/display/endpointmgmt603/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>

¹²⁷ <http://kb.igel.com>



4.13.3 Resolved Issues 6.03.130

IGEL Cloud Gateway (ICG)

- Fixed: **ICG root certificates** created with UMS version 6.01.130 or with an older version **can be used again for creating a signed certificate**.

Console, common

- Fixed: **The file transfer status** of firmware customizations without read permission was not displayed in the device detail window.

Firmwares

- Fixed: **Generic commands** could not be triggered by the UMS Console.

4.14 Notes for Release 6.03.110

Software:	Version 6.03.110
Release Date:	2019-10-30
Release Notes:	RN-603110-1
Last update:	2019-10-30

-
- [Supported Environment 6.03.110](#)(see page 613)
 - [Resolved Issues 6.03.110](#)(see page 615)

4.14.1 Supported Environment 6.03.110

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	



Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
-----------------------------------	----------	--

- **UMS Client:**

Microsoft Windows 7	(64 bit)	with SP1
Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹²⁸.

¹²⁸ <https://kb.igel.com/display/endpointmgmt603/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>



4.14.2 Resolved Issues 6.03.110

UMS, common

- Fixed: Files are now applied correctly when assigned to multi-level device folders.

Console, common

- Fixed: Removed unnecessary log entries which occurred if the user had no permission set.
- Fixed: Issue where the 'configuration changed' indicator (blue exclamation mark) was not updated correctly if shared workplace assignments existed.

Views

- Fixed: Amount of hidden devices did not get refreshed if devices were added by another console.

4.15 Notes for Release 6.03.100

Software:	Version 6.03.100
Release Date:	2019-10-15
Release Notes:	RN-603100-1
Last update:	2019-10-15

- [Supported Environment 6.03.100](#)(see page 615)
- [Known Issues 6.03.100](#)(see page 617)
- [New Features 6.03.100](#)(see page 617)
- [Resolved Issues 6.03.100](#)(see page 618)

4.15.1 Supported Environment 6.03.100

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	



Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	with SP1
Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10.9 - 10.14



See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹²⁹.

4.15.2 Known Issues 6.03.100

- **Updating IGEL Windows 10 devices via UMS webdav folder** can result in **an endless update loop** of the devices. Please contact IGEL Support in this case.
To avoid this problem, we recommend distributing the Windows 10 firmware updates via an external FTP or HTTPS server.

4.15.3 New Features 6.03.100

UMS, common

- Added: New display of **legend of UMS icons** (UMS Console > **Help > Legend**).
- Added: Support of **MS SQL Server Always On Availability Groups**.
- Added: Allow **TLS protocol version 1.1 or 1.2 selection for SMTP server** communication in UMS.
- Changed: UMS with **external Derby database** supports only **Derby versions 10.9 up to 10.14**.
- Changed: Increased the **maximum memory usage of UMS Console** (1024mb -> 3072mb), **UMS Server** (2048mb -> 4096mb) and **RMAAdmin** (512mb -> 1024mb).
- Changed: Redesign of the UMS cache. The **cache is now always switched on**. The corresponding configuration dialogs were removed.
- Updated: **Apache Tomcat** from version 8.5.43 to **8.5.45**.
- Updated: **Azul Zulu JRE** from version 1.8.0_212 to **1.8.0_222**.

Console, common

- Added: **Configuration dialog for Views and Searches** (**Misc > Settings > Views and Searches**).
- Added: **Digit grouping** to improve the readability of large numbers (e.g. devices in a folder).
- Added: When creating a new administrator account, the **user name or group name is checked for duplicate names** prior to saving (**System > Administrator accounts > New**).

Devices

- Added: Option to **copy device information** to clipboard **in ASCII format** (**Device > Detail View > Bottom > Copy to Clipboard (ASCII)**).
- Changed: **Import Devices** uses the **Unit ID** instead of the MAC address as the client descriptor **for the long and short import formats**.
- Changed: **States of Device information lists** ("open" or "close") are now saved.

Views

- Added: **Option to cache View results** for more convenience.

Universal Firmware Update

- Changed: **Windows Firmware Updates** are now provided **with https**.

¹²⁹ <https://kb.igel.com/display/endpointmgmt603/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>



- Added: **Universal Firmware Update** supports **FTPS** and **SFTP** (**UMS Administration > Global Configuration > Universal Firmware Update**).

Searches

- Added: **New View/Search criterion** 'Structure Tag'.
- Added: Option to **save Searches** as **CSV, XML, HTML**, and **XSL**.
- Added: **Option to cache Search results** for more convenience.

Console, administration section

- Added: **Choice** between **rich** and **plain text messages** to a device (**UMS Administration > Global Configuration > Messages to Devices**).
- Changed: Available **filter criteria** for registered device licenses (**UMS Administration > Global Configuration > Licenses > Device's Licenses**).
- Changed: It is now possible to **create/import certificates** in the **remote ICG installer/updater**. (**UMS Console > UMS Administration > UMS Network > IGEL Cloud Gateway**).

High Availability Feature

- Added: '**Stop Service**' option in process detail view (**UMS Administration > UMS Network > Server/Load Balancer**).

Installer (Linux)

- Added: **UMS** can be installed **on Red Hat Enterprise Linux 8**.
- Added: Installer will now also **check for a running instance of UMS Administrator** during an update installation.
- Added: **New wizard page** after component selection, **displaying the memory (RAM) requirements** for the selected components.

Installer (Windows)

- Added: **New wizard page** after component selection, **displaying the memory (RAM) requirements** for the selected components.

4.15.4 Resolved Issues 6.03.100

UMS, common

- Fixed: **Deleting a firmware update snapshot** also **deleted the ums_filetransfer folder**. (Only occurred if the firmware update has been stored directly in the UMS webdav folder without parent folder).

Console, common

- Fixed: **Indicator that the device settings have changed** (blue exclamation mark) **did not always appear** when an assigned profile was changed or indirectly assigned to a device.



- Fixed: When using an Oracle database, after moving files/views to a subfolder **the file/view count display of the subfolder was not updated.**
- Fixed: The "**Show Message**" button (UMS Console > Bottom right hand corner) **in "smart contrast"** behaves now analogously to the other themes.
- Fixed: The **UMS firmware statistics** overview (**Misc > Firmware Statistics**) could display **a wrong number of devices** when UD Pocket devices were managed in the UMS.
- Fixed: When a firmware customization has been assigned to a device, this device and all other already assigned devices got a **notification that the settings have changed**. Now only the new device will get the notification.
- Fixed: **Overwriting an existing zip file** when exporting firmware, firmware customizations, template keys / groups and device settings **created an unusable file** (**System > Export...**).

Devices

- Changed: The value of '**Last IP**' in '**System Information**' of a device **is no longer editable** and has been moved from the editable section to the non-editable section.
- Fixed: Possible problems with the **File Transfer Status** if the device is **connected via ICG**.
- Changed: **Renamed** the field 'Expiration Date of Maintenance Subscription' **to 'Expiration Date of OS10-Maintenance Subscription'** in the device detail view to avoid confusion (**Device > Detail View > Advanced System Information**).

Profiles

- Fixed: '**New Profile**' dialog did not resize if expert mode was closed (UMS Console > **Profiles** > context menu > **New Profile**).

Views

- Fixed: **Creating a view with criterion 'Monitor size'** caused an **error with the SQL Server database**.

Configuration Dialog

- Fixed: In the configuration dialog of a device on the **Security > Password** page, the "**Change Password**" buttons are now **properly enabled/disabled** to match the enable states of the corresponding parameters.
- Fixed: In profile configuration dialog (**Devices > Storage Hotplug**), the "Storage Hotplug" selection was not saved.

Console, administration section

- Fixed: Display of **wrong status** after renaming a server (**UMS Administration > UMS Network > Server**).
- Added: **Syntactic check of email address** before sending email in Cloud Gateway Options (**UMS Administration > Global Configuration > Cloud gateway options > First authentications keys > Send first Email authentications keys by Email**).



Firmware Customization

- Fixed: **Importing a firmware customization** without assigned files resulted in a "permission denied" warning.

Mobile Device Management (MDM)

- Fixed: **MDM** is working again **with LDAP users**.

Server, common

- Changed: Server details (**UMS Administration > Server**) will now show the **actual name of the Linux operating system** if it provides the file /etc/os-release.

High Availability Feature

- Fixed: **Support information for HA feature** no longer generates error-entry on other servers.
- Fixed: Issue with data directory in HA update. **HA update changed the data directory** (ums_filetransfer) to c:\programData\igel **without notice**. All files were automatically moved to the new directory. On Linux systems, the issue could lead to loss of files in ums_filetransfer folder.

UI / Look&Feel

- Fixed: **Console used wrong tooltip color** after sending RichMessages.

Installer (Linux)

- Fixed: After an **upgrade installation of the UMS Load Balancer**, it did not talk to the UMS Server anymore.

4.16 Notes for Release 6.02.110

Software:	Version 6.02.110
Release Date:	2019-08-14
Release Notes:	RN-602110-1
Last update:	2019-08-14

-
- [Supported Environment 6.02.110](#)(see page 621)
 - [New Features 6.02.110](#)(see page 622)
 - [Resolved Issues 6.02.110](#)(see page 622)



4.16.1 Supported Environment 6.02.110

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	New: only with SP2
Microsoft Windows Server 2008 R2	(64 bit)	New: only with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	New: only with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	New: only with SP1
Microsoft Windows 8.1	(64 bit)	New: only with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	New: only with SP2
Microsoft Windows Server 2008 R2	(64 bit)	New: only with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	New: only with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

- **Backend Database (DBMS):**

Oracle 11g R2	
Oracle 12c	



Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹³⁰.

4.16.2 New Features 6.02.110

Server, common

- Updated **Apache Tomcat** from version 8.5.40 to **8.5.43**

IGEL Cloud Gateway (ICG)

- Added: Support for **Shadowing via IGEL Cloud Gateway** (ICG 2.01.100 or higher and IGEL OS 11.02.100 or higher are required)

4.16.3 Resolved Issues 6.02.110

AD / LDAP integration

- Fixed: **AD authentication** was not possible in a mixed domain/subdomain environment.

Thin clients

- Fixed: **Firmware update settings** of a device shown in UMS differed from the settings the device received when a **Universal Firmware Update** and a **profile with configured firmware update settings** were assigned to the device.

Views

- Added: The **timeout for the online check of devices** that is set in **UMS Administration > Global Configuration > Server Network Settings > Online Check Parameters** will be used for the **Online criterion** in **Views**.

IGEL Cloud Gateway (ICG)

- Changed: Due to structural changes between ICG 1.04 and ICG 2.01 **a downgrade is not possible**. It is also disabled in the ICG remote installer.
- Fixed: **Changing the name** of an ICG or a UMS Server does no longer result in an error message.

DB command line tools

- Fixed: The **embackup command line tool didn't find the backup file in restore mode** although it existed.

¹³⁰ <https://kb.igel.com/display/endpointmgmt602/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>



Server, common

- Fixed: Downloading global notifications (by UMS itself or via the **Send notification information via mail** administrative task) failed with Microsoft databases.

Installer (windows)

- Fixed: **Updating a UMS installation (4.09.x or older) directly to versions between 5.09.100 and 6.02.100 (inclusive) did not work completely.** In these cases, the installer asked for the data directory (which already existed) and even if the user entered the same path as the UMS used before, the folder was completely overwritten. Additionally, if the UMS used an embedded database before the update, a manual reactivation was sometimes required after the update.

4.17 Notes for Release 6.02.100

Software:	Version 6.02.100
Release Date:	2019-06-14
Release Notes:	RN-602100-1
Last update:	2019-06-14

- Supported Environment 6.02.100(see page 623)
- New Features 6.02.100(see page 624)
- Security Fixes 6.02.100(see page 625)
- Resolved Issues 6.02.100(see page 625)

4.17.1 Supported Environment 6.02.100

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	New: only with SP2
Microsoft Windows Server 2008 R2	(64 bit)	New: only with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	New: only with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

- **UMS Client:**



Microsoft Windows 7	(64 bit)	New: only with SP1
Microsoft Windows 8.1	(64 bit)	New: only with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	New: only with SP2
Microsoft Windows Server 2008 R2	(64 bit)	New: only with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	New: only with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

- **Backend Database (DBMS):**

Oracle 11g R2	
Oracle 12c	
Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹³¹.

4.17.2 New Features 6.02.100

UMS (common)

- Added: **Disk Usage** notification type for the UMS notification system. ([Help > Notifications](#))
- Added: **Global notification** type for the UMS notification system to inform the user of important news like maintenance times, bugfixes, etc. ([Help > Notifications](#))

¹³¹ <https://kb.igel.com/display/endpointmgmt602/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>



- Changed: When a device is renamed, the setting **Adjust network name if UMS-internal name has been changed** is automatically set to enabled (**UMS Administration > Global Configuration > Device Network Settings > Adjust Names of Devices**).
- Changed: The administrative task **Assign objects to the devices of views** now provides the possibility to **assign firmware customizations, files and firmware updates** to the devices of views.

Console (common)

- Added: **Administrative tasks** notification type for the UMS notification system. (**Help > Notifications**)
- Added: The UMS now **displays all connected monitors** of a device. It previously displayed only two.

Console (administration section)

- Added: Option to create **ICG wildcard certificates**. (**UMS Administration > Cloud Gateway Options > Create signed certificate**)

Server (common)

- Changed: Suppress **server identity** in tomcat headers and by disabling default error pages.

AD / LDAP integration

- Added: **LDAPS** support **for AD** configuration.

Mobile Device Management (MDM)

- Added: **Public port** and **address** are now part of the MDM enrollment codes.

4.17.3 Security Fixes 6.02.100

High Availability Feature

- Fixed: HA installation unnecessarily **opened a debug port** (**ISN 2019-05**).

4.17.4 Resolved Issues 6.02.100

UMS (common)

- Fixed: **Resetting** a device **to factory defaults** could lead to various errors. (**UMS > Device > [Device's context menu] > Other commands > Reset to Factory Defaults**)
- Fixed: Missing **configuration state change flag** for template value and value group assignments.
- Fixed: Text **color of warning hints** when some/none of the selected devices have **Secure Terminal** enabled.
- Removed: Unused icons.



- Changed: **Tomcat access log files** are now also collected as a part of the support information. (**UMS > Help > Save support information**)
- Changed: The bundled Oracle JRE was replaced with **Azul Zulu JRE 8 Update 212**.
- Updated: **Apache Tomcat** from version 8.5.37 to **8.5.40**.
- Updated: UMS-bundled Java version from **Java 8** Update 202 to **Update 212**.

Console (common)

- Fixed: Already existing **archive of a profiles export** could not be overridden.
- Fixed: **UMS console login dialog** was not properly focused.
- Fixed: **Notifications** cannot be deactivated for **users of an imported AD group**.
- Fixed: Some texts could not be read because the text and the background had the same color.
- Added: Functionality to **assign objects** (profiles, FWCs, etc.) to more than one device at once.
- Fixed: Error message when **exporting result in SQL** console. (**Misc > SQL Console > Save Result**)
- Changed: In the UMS **Scan for devices** dialog, when the **Rescan** action is executed, the current filter is maintained and applied again to the new scan results. (**UMS > Scan for devices > Scan > Rescan**)
- Fixed: Double click on **Indirect assigned objects** redirects you to the Object and on right-click a pop-up window opens.
- Fixed: Selecting '**Don't show again**' on a notification in the **Notification** dialog had no effect. (**Help > Notifications**)
- Fixed: Wrong color in **Move to recycle bin** confirmation dialog.
- Fixed: Issue when devices were erroneously shown as unlicensed.
- Fixed: Issue when the **Close** button was sometimes invisible in the **Update Check** dialog. (**Help > UMS Update Check**)
- Changed: **Notification pop-up** on start-up is hidden if there are no notifications.

Devices

- Changed: **Save device files for support** dialog was redesigned and completed with the possibility to save files of multiple devices and devices of views. (**Help > Save device files for support**)
- Changed: **Wake up** commands are not sent to devices when they are registered in the UMS through an ICG.

Profiles

- Fixed: Re-added a missing **file picker** for the field **File name** on page **System > Update > Snapshots > Download**. File picker is now properly enabled after resetting the file name parameter with enabled template keys checkbox.
- Fixed: Changes of the **screen rotation**, i.e. rotating a screen with the left/right arrow buttons on the **User Interface > Display** page, could not be saved in profiles.
- Fixed: Re-added a missing **FTP password** field in W7 profile configuration dialog. (**System > Snapshots > Upload/Download**)
- Changed: Simplified dialog to create a new profile.

Template Keys and Groups



- Fixed: **Variable expressions** in template keys are now supported for **devices registered into directories**.

Firmware Customization

- Fixed: The **FWC import** did not upload the provided files.
- Changed: The **Firmware Customization import file** is validated and the import process is aborted if the imported parameters are not supported by the current UMS version.

Views

- Fixed: **CSV-exports** did not include the **column headers** of custom device attributes. (Admin task: Export view as...)
- Fixed: **Special characters from Eastern Europe** are shown incorrectly within **view exports**. (**View context menu > Save as...**)
- Fixed: Reduced processing time of assignment/detachment of profiles to/from the devices of a view.
- Added: A new **View** criterion for **device licenses**.

Jobs

- Changed: By **deleting a server** in **UMS Administration > UMS Network > Server**, the assigned devices are assigned to another available server and the **Job** execution data is deleted.

Automatic License Deployment (ALD)

- Fixed: An **empty error message** is shown if the configuration of **UDC2 Deployment** is changed and the configuration page is left without saving the changes.
- Fixed: A **Product Pack** is occasionally shown twice in the **Registered packs** section. (**UMS Administration > Global Configuration > Licenses > Deployment**)
- Changed: The **default automatic distribution method of new packs** (except for Workspace Edition packs) altered from 'Enabled' to 'Enabled (with conditions)'.

Universal Firmware Update

- Fixed: A **device directory** cannot be assigned to a **Universal Firmware Update** if the directory has already such an assignment.
- Changed: The **progress bar** shows the **download process** of Universal Firmware Update with **a better accuracy**.

Configuration Dialog

- Fixed: Configuration dialog combobox **Multimonitor full-screen mode** was missing in UMS 6 for **clients with firmware 10.4.100. (Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Window)**

Console (administration section)



- Changed: A test mail configured under **UMS Administration > Mail Settings > Send Test Mail** can now be sent to different recipients.
- Fixed: The **Certificate Management Node** was only visible to the **DB administrator**. (**UMS Administration > Global Configuration > Certificate Management**)
- Fixed: Issue when multiple **ICGs** were shown in the wrong order. (**UMS Administration > UMS Network > Igel Cloud Gateway**)
- Updated: **DSA** export graphic. (**UMS Administration > Global Configuration > Licenses > Device's Licenses > Export Unit ID list**)
- Fixed: In the device's **Rich Message Editor**, the **Reject changes** message does not appear anymore if you switch the template and the previous template had no changes. (**UMS > Device > [Device's context menu] > Other commands > Send Message**)
- Fixed: **UMS Licenses** with more than one corresponding notification could not be deleted. (**UMS Administration > Global Configuration > Licenses > UMS Licenses**)
- Added: **Wait dialog during ICG certificate creation** to indicate progress. (**Global Configuration > Cloud Gateway Options**)
- Added: **Server** and **broker icons** now show status.
- Changed: Renamed 'Remove' buttons in the **ICG configuration dialog** to avoid misunderstanding. (**UMS Administration > UMS Network > Igel Cloud Gateway**)
- Added: **Dialog to Naming Convention** feature to guide the user. (**Global Configuration > Device Network Settings > Naming Convention**)
- Fixed **display** of correct **operating system name** for Windows Server 2016/2019 in administration section.

Console (web start)

- Fixed: Webstart sometimes showed **outdated splash screen**.
- Added: **Expressive error and log messages** when uploading files to UMS server fail due to **invalid server hostname**.

WebDAV

- Fixed: **WebDAV credentials** were not recognized under certain circumstances.

IGEL Cloud Gateway (ICG)

- Fixed: **UMS lost ICG connection** if a lot of devices were ICG administrated (device count> 500).
- Changed: When a device is registered on ICG, **ICG credentials** are **cached** before the device is removed from the **Recycle Bin** and then stored again. It only applies for devices that are in the Recycle Bin at the moment of ICG registration.
- Added: **New safeguard** to the ICG certificate dialog to prevent inexperienced users from making mistakes. (**UMS Administration > Global Configuration > Cloud Gateway Options**)
- Added: Option for the **certificate creation dialog** whether a new certificate should be **CA** or **End Entity**.
- Added: Check to prevent users from signing a certificate with a non-CA certificate.
- Added: **X.509 extensions** to show certificate dialog.

Server (common)



- Updated: **Microsoft SQL Driver** to support **TLS 1.2** in Microsoft SQL database connection.
- Fixed: Issue with an **incorrect identification** of the operating system of **Windows Server 2016/2019**. (**UMS Administration > UMS Network > Server > [UMS Server] > Attribute 'Operating System'**)
- Fixed: A **valid Workspace Edition license / Enterprise Management license** was not recognized because of not properly formatted timestamps.
- Fixed: Bug in the device authentication.
- Changed: All tables of the database schema are optimized. (Optimize Database)
- Updated: **EULA** text.

High Availability Feature

- Fixed: HA installation unnecessarily **opened a debug port**. (**ISN 2019-05**)
- Fixed: Communication issues within a HA network.
- Fixed: **Update installation wizard** contained misleading user prompt.
- Fixed: Commands for servers, load balancers and ICGs could create an **unreadable balloon tip**.
- Changed: Now support files also contain **watchdog log files** in **Save support information** function. (**UMS > Help > Save Support Information**)

Installer (Linux)

- Fixed: **Uninstaller on Linux** can be executed from now on only with **root privileges** and shows the correct UMS version.
- Fixed: **Splash screen** was shown as "**win0**" on panel in GNOME desktop on **RHEL 7** and **Oracle Linux 7**.
- Added **check for running UMS** Console in Linux installer.
- Fixed: **UMS binaries** (e.g. RemoteManager.bin) do not start on **RHEL 7.x** or **Oracle Linux 7** due to ABI compatibility issue.

UI / Look&Feel

- Fixed: **Rich Message Templates** could spill their colors into the UMS.

4.18 Notes for Release 6.01.100

Software:	Version 6.01.100
Release Date:	2019-02-15
Release Notes:	RN-601100-1
Last update:	2019-02-15

-
- [Supported Environment 6.01.100](#)(see page 630)
 - [New Features 6.01.100](#)(see page 631)
 - [Resolved Issues 6.01.100](#)(see page 631)



4.18.1 Supported Environment 6.01.100

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	New: only with SP2
Microsoft Windows Server 2008 R2	(64 bit)	New: only with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	New: only with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	New: only with SP1
Microsoft Windows 8.1	(64 bit)	New: only with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	New: only with SP2
Microsoft Windows Server 2008 R2	(64 bit)	New: only with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	New: only with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

- **Backend database (DBMS):**



Oracle 11g R2	
Oracle 12c	
Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹³².

4.18.2 New Features 6.01.100

Automatic License Deployment (ALD)

- Added: Support of new **IGEL OS 11 licensing mechanism** and new license distribution method **Automatic with Condition**. With this option, the device will get a license automatically only when the device accords to one or more of the selected conditions. The conditions can be folder memberships or views.
- Added: New **UMS Licensing ID** for easier license deployment. (**UMS Administrator > UMS Licensing ID** and **UMS Console > UMS Administration > Global configuration > Licenses > UMS Licensing ID**)

UMS (common)

- Updated: **Apache Tomcat** from **version 8.5.32 to 8.5.37**.
- Updated: UMS-bundled Java version from **Java 8 Update 181 to Update 202**.
- Added: Support for **Windows Server 2019**.
- Added: It is now possible to **license devices via context menu (License manually ...** in context menu of **Devices, Device Directories** and **Views**).
- Added: **Device-specific commands** that can be executed in the device's context menu (**UMS > Structure Tree > Devices**) and in the **device's menu bar**. The list of the available commands depends on the current selection. Therefore, a command is only listed when it is possible to execute by at least one of the devices in the current selection. The specific commands can be also selected in **Jobs**. (**UMS Console > Management Tree > Jobs**)

4.18.3 Resolved Issues 6.01.100

UI / Look&Feel

- Changed: **New bootsplash and theme** for UMS 6.01.100

¹³² <https://kb.igel.com/display/endpointmgmt601/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>



IGEL Cloud Gateway (ICG)

- Changed: **Stabilized ICG connections** in UMS High-Availability Environments (UMS HA)
- Fixed: **Sub-Certificates (ICG) were not visible** right after creation. A refresh was necessary.
- Fixed: A **used mass deployment key** was not exportable. (**UMS Console > Global Configuration > Cloud Gateway Options**)
- Fixed: The **usage count of first-authentication keys** did not change. (Affected: Only the GUI representation in **UMS Console > Global Configuration > Cloud Gateway Options**)

UMS (common)

- Fixed: All **certificate management actions**, which generate a new network token, failed to save the network token. (Only in HA environment)
- Changed: **Thin Clients** have been renamed "**Devices**".

Console (common)

- Fixed: The download link in **UMS Update Check** could not be opened on some operating systems. (**UMS Console > Help > UMS Update Check**)

Devices

- Fixed: The function **Take over settings from...** did not work, when the UMS was connected to a PostgreSQL database. (**UMS Console > device > context menu**)
- Fixed: Sometimes an **empty error dialog** occurred by selecting a device (happened only if an assigned file has been deleted before).

Firmware Customization

- Fixed: The **manual import of firmware customizations** from older UMS versions was not possible. (**UMS Console > System > Import > Import Firmware Customizations**)

Automatic License Deployment (ALD)

- Fixed: **Changing the default proxy in the GUI did not change the default proxy in the backend** sometimes. (Only a server restart fixed the bug)
- Changed: Improved the **token validation dialog** to be more user friendly. (**UMS Console > Global Configuration > Licenses > Deployment > Register Pack**)

Console (administration section)

- Changed: Improved **certificate validation mechanism** (**UMS Console > Global Configuration > Certificate Management**)
- Fixed: The '**host**' entry in ICG remote installer dialog is now editable for **wildcard certificates** (e.g.: *.xyz.com¹³³). (**UMS Console > Administration Tree > UMS Network > Igel Cloud Gateway > Install new ICG Cloud Gateway**)

¹³³ <http://xyz.com>



Administrative tasks

- Fixed: The administrative task **Create backup** failed for external databases when the task was configured to **include licenses and files**, which is only possible for the **embedded database**. (**UMS Console > Administration Tree > Global Configuration > Administrative Tasks**)
- Fixed: An issue where the **next execution time of admin tasks** was not properly calculated. (**UMS Console > Administration Tree > Global Configuration > Administrative Tasks**)

Server (common)

- Fixed: The **certificate key pair import fails**, if the UMS data directory differs from the default. (**UMS Console > Administration Tree > Global Configuration > Certificate Management**)

Administrator application

- Fixed: It was not possible to **delete created database backups** even after a restart of the UMS Administrator.

Installer (Linux)

- Fixed: The **update installation** on Linux OS will no longer ask for the **installation directory**.

4.19 Notes for Release 5.09.100

Software:	Version	5.09.100
Release Date:	2018-10-08	
Release Notes:	Version	RN-509100-1
Last update:	2018-10-08	

The following formatting is used in the document:

format type	example	use
bold and underlined	<u>enable/disable</u>	the default setting of a value
bold and arrow	menu > path	menu path in the IGEL setup
bold	GUI [keyboard]	elements of the graphical user interface or commands that are entered using the keyboard
within brackets	[session name]	variable values



-
- [Supported Environment 5.09.100](#)(see page 634)
 - [Warnings 5.09.100](#)(see page 635)
 - [New Features 5.09.100](#)(see page 636)
 - [Resolved Issues 5.09.100](#)(see page 637)

4.19.1 Supported Environment 5.09.100

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 16.04	(64 bit)
Ubuntu 18.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **UMS Client:**

Microsoft Windows 7	(64 bit)
Microsoft Windows 8	(64 bit)
Microsoft Windows 10	(64 bit)
Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 16.04	(64 bit)
Ubuntu 18.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)



- **Backend database (DBMS):**

Oracle 11g R2	
Oracle 12c	
Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹³⁴.

4.19.2 Warnings 5.09.100

- Following 32-bit environment is no longer supported:
(Support removed because of software change to 64 bit)

UMS Server:

Ubuntu 14.04 (32 bit)
Ubuntu 16.04 (32 bit)
Red Hat Enterprise Linux (RHEL) 6 (32 bit)

UMS Client:

Microsoft Windows 7 (32 bit)
Microsoft Windows 8 (32 bit)
Microsoft Windows 10 (32 bit)
Ubuntu 14.04 (32 bit)
Ubuntu 16.04 (32 bit)
Red Hat Enterprise Linux (RHEL) 6 (32 bit)

- Microsoft SQL Server 2008 / 2008 R2 support removed because of incompatible SSL certificates (not supported by Java)
- Ubuntu 14.04 (64 bit) support removed because of incompatible libraries (too old for the new UMS installation files)
- Increased maximal memory usage:

UMS Server: 1024 MB to 2048 MB
UMS Client: 768 MB to 1024 MB
UMS Administrator: 384 MB to 512 MB

¹³⁴ <https://kb.igel.com/display/endpointmgmt509/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>



- Removed function to create a thin client license with smartcard. (**UMS Administration -> Global Configuration -> Licenses -> Thin Client Licenses -> Hardware**)

(i) Care:

Licenses can still be created via Thin Client Smartcard License Server. (**UMS Administration -> Global Configuration -> Licenses -> UDC2 Deployment**)

4.19.3 New Features 5.09.100

UMS Common

- New EULA:** This UMS version is licensed under a new end user license agreement (EULA). Please read it carefully.
- Added: **Notifications.** Now the UMS Console shows a notification pop-up (default: on each console connect) which informs about the latest firmware updates and expiration of UMS or client licences. Notifications can be deactivated (for all users) in **UMS Console -> Administration Tree -> Global Configuration -> Misc**, and the relevant notification types can be set in **UMS Console -> Misc -> Settings -> Notifications** (user specific). Notifications can also be sent via Mail. (**UMS Console -> Administration Tree -> Global Configuration -> Administrative Tasks**)
- Added: It is now possible to **configure the used cipher suites for the UMS SSL port**. This setting is server specific and not part of the database backup. For UMS HA: Cipher suite selection has to be made on each node separately. (**UMS Administrator -> Settings -> Configure Ciphers**)
- Added: New feature **Certificate Management:** It is now possible to replace the certificate, which is mainly used for thin client to UMS communication. Changing the default certificate triggers a mechanism which consistently tries to store the new certificate on each thin client. This can only be done for online thin clients.

⚠ Warning

Incautious usage can lead to loss of the management connection to thin clients. The management functionality can only be restored by deleting the UMS certificate manually (local access) from each affected thin client. Certificate management can be found in **UMS Console -> UMS Administration -> Global Configuration -> Certificate Management**. (Only visible for the database administration user)

- Updated: The UMS is now bundled with a 64 bit JRE. The new JAVA version is 1.8.0_181.

Thin Clients

- Added: **Automatic Wake On LAN Proxy Detection.** The UMS will try to find a thin client that is able to relay the wake up call automatically to the target thin client without configuring thin clients as Wake On Lan Proxy. A thin client can automatically relay the wake up call, if the thin client is online, has a firmware version of LX 5.09.100 or newer and can 'see' the target thin client (same network, subnet ...). This feature can be activated in **UMS Console -> UMS Administration -> Global Configuration -> Wake on LAN -> Automatic Wake On LAN Proxy Detection** (default: off).
- Added: The thin client panel now contains a section **File Transfer Status** which gives status information about the assigned files.



- Added: New field **boot mode** in thin clients system information section.

Profiles

- Added: **Changes in UMS profiles can now be seen in their registry.** (Same colors as in the configuration tree).

Template Keys and Groups

- Added: **Static template keys:** For these template keys it is no longer necessary to configure and assign a template value since the thin client provides the values at runtime. The following three keys are available: MACADDRESS, HOSTNAME and UNITID. (Visible in each **Choose Template Key** dialog)

Firmware Customization

- Added: It is now possible to **assign wallpapers and boot splashes to W10 thin clients** (version 4.02.100 and higher) via firmware customizations.

Configuration Dialog

- Added: Additional **setup admin** user and permission layer on page **Accessories -> Setup -> User Page Permission**
- Added: Each parameter has got a new **reset button** which resets the value to factory defaults. The button is disabled when the parameter already has its default value.

Mobile Device Management (MDM)

- Added: **Mobile Device Management Preview.** Now it is possible to manage up to 5 mobile iOS devices with iOS version 10.3 or newer in the UMS.

UI / Look & Feel

- Added: If a tree node (folder, profile, master profile, firmware customization, view, ...) gets copied, and the target folder already contains an object with this name, the new displayed name will be marked with a **modifier ("COPY")**.

4.19.4 Resolved Issues 5.09.100

UMS, Common

- Removed: **It is no longer possible to create UDC 2 licenses manually from smartcard** (Smartcard was directly connected to the UMS Console). It is still possible to configure and use a thin client as UDC 2 smartcard license server. (Automatic Licensing)
- Removed: **Support for SQL Server 2008 and SQL Server 2008 R2 databases.** (Incompatible SSL certificates)



- Fixed: Bug in **Automatic License Deployment** which occurred with **UD Pocket** devices. If the amount of registered unlicensed UD Pocket devices was higher than the amount of available licenses of one token, no license could be deployed.
- Fixed: **Automatic UDC2 license deployment created several identical licenses for the same thin client.**
- Fixed: **Offline user manual in UMS Console did not open on Linux OS.**
- Fixed: **install.log file** could not be added to the support information.
- Changed **default signature algorithm** for certificates to SHA512withRSA.
- Changed: The knowledge base links point now to kb.igel.com¹³⁵ instead of edocs.igel.com¹³⁶
- Changed: **Apache Tomcat** from version 8.0.47 to version 8.5.32.

Console, Common

- Removed: Unused graphical effects parameters for configuration dialog. (**UMS Console -> Misc -> Settings -> Configuration Dialog**)
- Fixed: **UMS Console window did not request focus anymore** while a firmware update is downloaded.
- Fixed: **Splash screen and accept certificate dialog can be hidden** behind other windows on Linux.
- Fixed: **Clearing the recycle bin** took much too long.
- Fixed: The **ID of non-displayable tree objects** is no longer shown with a thousands separator.
- Fixed: The **cache management dialog** in UMS Console did not open on Linux OS.
- Fixed: A **custom thin client attribute** which is linked to a default directory rule **could falsely be deleted**.
- Changed: **Users without the WebDav Access permission now get a more detailed hint** (message or tooltip) why they can't perform some actions (e.g. creating a UMS file).
- Added: **All file choosers in the UMS Console can now remember their last used directory** (Except the WebDAV file choosers). This can be disabled in **UMS Console -> Misc -> Settings**.

Thin Clients

- Fixed: **User login history** had no entries for UD Pocket devices. (**UMS Console -> Management Tree -> Thin Clients -> Thin Client Content Panel**)
- Fixed: The actions **rename** and **delete** were selectable on the thin client root node. (**UMS Console -> Management Tree**)
- Fixed: After resetting a thin client to factory defaults, the **UMS Console still showed the thin client in the assigned objects**.
- Fixed: **After scanning several thin clients at once** (with specified target directory) **some of the scanned thin clients were not visible in the tree** until a refresh was done.
- Fixed: The thin **client settings cache** was not updated by assignment changes coming from administrative task **Assign profiles to the thin clients of views**.
- Fixed: Although the flag **Adjust network name if UMS-internal name has been changed** had been set, the thin client rename function ignored the maximum name length of 15 characters. (Rename via content panel)

¹³⁵ <http://kb.igel.com>

¹³⁶ <http://edocs.igel.com>



- Fixed: The **Lock screen** icon (Advanced Thin Client Health Status) was permanently set if the thin client was remotely suspended.
- Changed: **Improved usability** of thin client import dialog. (**UMS Console -> System -> Import -> Thin clients**)
- Changed: **Order of entries** in thin client context menu **Update & Snapshot Commands**.
- Changed: The **default thin client name** is now TC-MAC instead of IGEL-MAC to be fully DNS capable.

Profiles

- Fixed: Re-added missing file picker for field **file name** on page **System -> Update -> Snapshots -> Download**
- Fixed: Bug in **display configuration** where the second screen could not be saved on the left of screen one. (Only if both screen resolutions were set to **Autodetect**)

Template keys and groups

- Fixed: The **template check showed a missing value alert** (because no template value had been assigned to the thin client) although the setting in question had been overwritten by a correct profile/master profile and therefore did not affect the thin client.

Firmware Customization

- Fixed: **The config change flag in the thin client assignment panel was not displayed** if firmware customization was changed without sending the changes directly to the assigned thin clients.
- Fixed: In firmware Customizations, **the cancel button of the select file dialog did the same as the OK button**. When clicking the cancel button, changes will now be discarded instead of accepted.

Jobs

- Changed: Improved user interaction for **creating/editing a job where the execution time is in the past**.

Files

- Fixed: File **directories** could be renamed, but **after a refresh received the old name again**. (**UMS Console -> Management Tree -> Files**)

Configuration Dialog

- Fixed: The windows profile setting **Use IGEL Setup for configuration display settings** could be disabled, but after saving and reopening the configuration dialog, the **flag was still enabled**. (**Setup -> Configuration -> User Interface -> Display**)
- Fixed: **Huge memory consumption** in the configuration dialog of display page with high monitor resolutions.

Console, Administration Section



- Fixed: **Windows Server 2016 was not recognized as such.** OS name was displayed as "Windows NT (unknown)". (Visible in **UMS Console -> Administration Tree -> UMS Network -> Server -> Server Content Panel**)
- Fixed: Changes in the **Active Directory / LDAP** configuration didn't affect the management tree node **Shared Workplace Users** until the next connect.
- Fixed: **The thin client license node showed an access denied error on selection**, if the user had the permission to access the thin client license node, but not the UMS license node.
- Added: **Checkbox** to show only the last 20 executions in administrative task execution history to performance-friendly. (**UMS Console -> UMS Administration Tree -> Global Configuration -> Administrative Tasks**)
- Changed: **Configuration of concurrent thin client request threads** is now more user-friendly. (**UMS Console -> Administration Tree -> Global Configuration -> Thin Client Network Settings**)

Administrative Tasks

- Fixed: **Performance problem** which occurred if a newly created administration task with action **Delete logging data** had an incorrect export path set.
- Fixed: The two administrative tasks **Delete job execution data** and **Delete administrative job execution data** had wrong default values (Keep no more than x executions per job).
- Fixed: The administrative task **Delete job execution data** was not able to handle a very large amount of database entries (several millions).
- Fixed: A few 'old' administrative tasks could not be opened/reconfigured anymore.

IGEL Cloud Gateway (ICG)

- Fixed: The **usage date of mass-deployment keys** was not set. (**UMS Console -> Administration Tree -> Global Configuration -> Cloud Gateway Options**)
- Added: **Remote installer** for IGEL Cloud Gateway

Asset Inventory Tracker (AIT)

- Fixed: Asset names in **Asset Inventory Tracker** weren't appropriately truncated
- Added: **New administration task** to delete outdated asset history data. (**UMS Console -> Administration Tree -> Global Configuration -> Administrative Tasks**)

Server, Common

- Fixed: Bug which led to **high CPU-load of the UMS Server**, if the **Advanced Health Check** was enabled (**UMS Console -> Misc -> Settings -> Appearance**).

Administrator Application

- Fixed: The action **restore from backup** failed and the user got an error message. After the user acknowledged it, a wrong message **Database successfully restored** was displayed.
- Fixed: **Error while copying data into an oracle database.** (Only if **Asset Inventory Tracker** was used)



- Fixed: The **UMS Administrator database copy action aborted in some cases** (depending on the values in the database) with the following error: 'An attempt was made to get a data value of type 'BINARY' from a data value of type 'BLOB' '.
- Changed: **It is no longer possible to create a separate certificate backup in UMS Administrator.** The certificates are now contained in the database backup. The certificates (UMS to thin client communication) can be imported/exported in the new tree node **Certificate Management. (UMS Console -> Administration Tree -> Global Configuration)**

Installer (Linux)

- Added: Support for **Ubuntu 18.04**

UI / Look & Feel

- Fixed: **Broken row-sorter** in the license section
- Changed: **New Splash Screen** for UMS Console and UMS Administrator
- Changed: The UMS Console and UMS Administrator received **new task bar icons** and **application icons**.

4.20 Notes for Release 5.08.120

Software:	Version	5.08.120
Release Date:	2018-06-22	
Release Notes:	Version	RN-508120-1
Last update:	2018-06-22	

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	menu > path	menu path in the IGEL setup
bold	GUI [keyboard]	elements of the graphical user interface or commands that are entered using the keyboard
within brackets	[session name]	variable values

- [Supported Environment 5.08.120](#)(see page 642)
- [Resolved Issues 5.08.120](#)(see page 643)



4.20.1 Supported Environment 5.08.120

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 14.04	(32 bit) (64 bit)
Ubuntu 16.04	(32 bit) (64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 6	(32 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **UMS Client:**

Microsoft Windows 7	(32 bit) (64 bit)
Microsoft Windows 8	(64 bit)
Microsoft Windows 10	(64 bit)
Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 14.04	(32 bit) (64 bit)
Ubuntu 16.04	(32 bit) (64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 6	(32 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **Backend database (DBMS):**

Oracle 11g R2	(with RAC support)
Oracle 12c	(with RAC support)



Microsoft SQL Server 2008	
Microsoft SQL Server 2008 R2	
Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
PostgreSQL 9.3 - 9.6 and 10.1	
Apache Derby 10	

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹³⁷.

4.20.2 Resolved Issues 5.08.120

UMS (common)

- Fixed: Automatic UDC2 deployment creates unnecessarily several identical licenses for the same thin client. (Did not influence the smartcard license amount)

4.21 Notes for Release 5.08.110

Software:	Version	5.08.110
Release Date:	2018-05-11	
Release Notes:	Version	RN-508110-1
Last update:	2018-05-11	

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	menu > path	menu path in the IGEL setup

¹³⁷ <https://kb.igel.com/display/endpointmgmt/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>



bold	GUI [keyboard]	elements of the graphical user interface or commands that are entered using the keyboard
within brackets	[session name]	variable values

- [Supported Environment 5.08.110](#)(see page 644)
- [New Features 5.08.110](#)(see page 645)
- [Resolved Issues 5.08.110](#)(see page 645)

4.21.1 Supported Environment 5.08.110

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 14.04	(32 bit) (64 bit)
Ubuntu 16.04	(32 bit) (64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 6	(32 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **UMS Client:**

Microsoft Windows 7	(32 bit) (64 bit)
Microsoft Windows 8	(32 bit) (64 bit)
Microsoft Windows 10	(32 bit) (64 bit)
Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 14.04	(32 bit) (64 bit)



Ubuntu 16.04	(32 bit) (64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 6	(32 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **Backend database (DBMS):**

Oracle 11g R2	(with RAC support)
Oracle 12c	(with RAC support)
Microsoft SQL Server 2008	
Microsoft SQL Server 2008 R2	
Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
PostgreSQL 9.3 - 9.6 and 10.1	
Apache Derby 10	

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹³⁸.

4.21.2 New Features 5.08.110

UMS (common)

- Added: This UMS version is licensed under a **new end user license agreement (EULA)**. Please read it carefully!

4.21.3 Resolved Issues 5.08.110

UMS (common)

- Fixed: A **custom thin client attribute** which is linked to a default directory rule could falsely be deleted.
- Fixed: Bug in **Automatic License Deployment** which occurred with UD Pocket devices. If the number of registered unlicensed UD Pocket devices was higher than the number of available licenses of one token, no license could be deployed.

¹³⁸ <https://kb.igel.com/display/endpointmgmt/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>



- Fixed: The **thin client settings cache** has not been updated by assignment changes coming from the administration task **Assign profiles to the thin clients of views**.

Console (common)

- Fixed: **UMS Console window doesn't request focus** anymore while a firmware update is downloaded.
- Fixed: Although the flag **Adjust network name if UMS-internal name has been changed** has been set, the **thin client rename function** ignored the maximum name length of 15 characters. (Rename via content panel)
- Fixed: **Cache management dialog in UMS Console** did not open on Linux.
- Fixed: **Offline user manual** in UMS Console did not open on Linux.

Console (administration section)

- Fixed: A few 'old' **administrative tasks** could not be opened/ reconfigured anymore.

Profiles

- Fixed: Bug in the **display configuration** where the second screen could not be saved on the left of screen one. (Only if both screen resolutions are set to 'Autodetect').

Configuration Dialog

- Fixed: The Windows profile setting **Use IGEL Setup for configuration display settings** could be disabled, but after saving and reopening the configuration dialog, the flag was still enabled. (**Setup > Configuration > User Interface > Display**).

4.22 Notes for Release 5.08.100

Software:	Version	5.08.100
Release Date:	2018-01-29	
Release Notes:	Version	RN-508100-1
Last update:	2018-01-29	

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	menu > path	menu path in the IGEL setup



bold	GUI [keyboard]	elements of the graphical user interface or commands that are entered using the keyboard
within brackets	[session name]	variable values

- [Supported Environment 5.08.100](#)(see page 647)
- [New Features 5.08.100](#)(see page 648)
- [Resolved Issues 5.08.100](#)(see page 649)

4.22.1 Supported Environment 5.08.100

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 14.04	(32 bit) (64 bit)
Ubuntu 16.04	(32 bit) (64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 6	(32 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **UMS Client:**

Microsoft Windows 7	(32 bit) (64 bit)
Microsoft Windows 8	(64 bit)
Microsoft Windows 10	(64 bit)
Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 14.04	(32 bit) (64 bit)



Ubuntu 16.04	(32 bit) (64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 6	(32 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **Backend database (DBMS):**

Oracle 11g R2	(with RAC support)
Oracle 12c	(with RAC support)
Microsoft SQL Server 2008	
Microsoft SQL Server 2008 R2	
Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
PostgreSQL 9.3 - 9.6 and 10.1	
Apache Derby 10	

See also [Devices Supported by IGEL Universal Management Suite \(UMS\)](#)¹³⁹.

4.22.2 New Features 5.08.100

Console (administration section)

- Added: **Automatic license deployment** for UDC3, UMA and UD Pocket. (**UMS Administration > Global Configuration > Licenses > Deployment**)

i If the feature is enabled (disabled by default) and appropriate tokens have been registered in the UMS, licenses for unlicensed UDC3 devices, UMA devices and UD Pockets are deployed automatically.

- Added: New tree node **Proxy Server** (**UMS Console > UMS Administration > Global Configuration**), to administrate several proxies in an easy way.
As yet, a proxy could be configured for firmware updates only. A proxy now can be used for ICG's and the new **Automatic License Deployment** feature too.

Thin Clients

- Added: **Snapshot upload/download support** for UMA devices with version 3.01.100 or higher.

¹³⁹ <https://kb.igel.com/display/endpointmgmt/Devices+supported+by+IGEL+Universal+Management+Suite+UMS>



Server (common)

- Changed: Because of security reasons, the **https connector of the UMS Server** does now provide **TLSv1.2** only.

UMS (common)

- Updated: **Apache Tomcat** version from 8.0.42 to **8.0.47**.
- Updated: **Java Version** from 1.8.0_121 to **1.8.0_152**.

4.22.3 Resolved Issues 5.08.100

Console (common)

- Fixed: The **UMS Update Check** is now able to use a proxy. When a firmware update proxy is defined, the **Update Check** uses this proxy to verify whether there is a new UMS version available.
- Fixed: **Plenty wrong server log entries**. Occurred when the UMS user had no permission to see the license tree node in the **UMS Administration** tree and the **Advanced thin client health check** was active.
- Changed: Renamed the global permission **Snapshot** into **WebDAV access** (UMS file transfer).
- Changed: Users without the **WebDav Access** permission get now **a more detailed hint** (message or tooltip) why they cannot perform some actions (e.g. creating a UMS file).

Server (common)

- Fixed: Bug which led to high CPU load of the UMS server when the **Advanced Health Check (UMS Console > Misc > Settings > Appearance)** was enabled.
- Updated: PostgreSQL database driver to support **PostgreSQL v9.3 - v9.6 and v10**.

Firmware Customization

- Fixed: With **certain permission combinations**, users were not allowed **to assign files** to newly created firmware customizations.
- Fixed: **FileUpload via FWC-Wizard could lead to errors** when the user had insufficient permissions.
- Fixed: In **Firmware Customizations**, the **Cancel** button of the 'select file' dialog did the same as the **OK** button. By clicking the **Cancel** button, changes will now be discarded instead of accepted.

Universal Firmware Update

- Fixed: The **firmware update text viewer** remembers now its size, and the text font has been changed to a monospaced font to support text formation.

IGEL Cloud Gateway

- Fixed: **Root certificates** are now marked as a **certificate authority**.



- Fixed: After a connection to an **Igel Cloud Gateway** failed with a certificate error, some threads could not be closed.

Administrative Tasks

- Fixed: The **execution time of administration tasks** was reported to be in the past, although it was in the future.

ⓘ This issue occurred only for new or changed administrative tasks with execution time after 12:00 p.m. and before 12:00 a.m.
- Fixed: **Performance problem occurred** when a created administrative task with action **Delete logging data** got an incorrect export path set.

Console (administration section)

- Changed: Stored all license tree nodes into a new **Licenses** folder (**UMS > UMS Administration > Global Configuration**) and updated their icons.

4.23 Notes for Release 5.07.110

Software:	Version	5.07.110
Release Date:	2017-10-19	
Release Notes:	Version	RN-507110-1
Last update:	2017-10-19	

- ⓘ The Linux installation was tested on the following distributions:

 - Ubuntu 16.04 64-bit
 - RedHat Enterprise 7.3
 - Oracle Linux Server 7.3

The following formatting is used in this document:

format type	example	use
bold and underlined	enable/disable	the default setting of a value
bold and arrow	menu > path	menu path in the IGEL setup



bold	GUI keyboard	elements of the graphical user interface or commands that are entered using the keyboard
within brackets	[session name]	variable values

- Resolved Issues 5.07.110(see page 651)

4.23.1 Resolved Issues 5.07.110

Console (common)

- Fixed: **Plenty server log entries** if the UMS user had no permission to see the license tree node in the UMS Administration and if the '**Advanced thin client health check**' was active.
- Fixed: **Firmware customizations could be manipulated** by a user without write permission.
- Changed: Renamed the global permission '**Snapshot**' into **WebDAV access (ums-filetransfer)**.

Firmware Customization

- Fixed: With certain permission combinations, users were not allowed to **assign files to newly created FWCs**.
- Fixed: **FileUpload via FWC-Wizard** could lead to errors if the user had insufficient permissions.

Administrative tasks

- Fixed: The **execution time of administration tasks** was reported to be in the past although it was in the future. This issue occurred only for new or changed administrative tasks with execution time after 12:00 p.m. and before 12:00 a.m.

AD / LDAP integration

- Fixed **AD login issue**: Login to UMS console failed with an AD user that had been indirectly imported to UMS via AD group. This issue occurred only if there was no browse user set in the AD configuration.

4.24 Notes for Release 5.07.100

Software:	Version	5.07.100
Release Date:	2017-08-30	
Release Notes:	Version	RN-507100-1



Last update:	2017-08-30	
--------------	------------	--

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	menu > path	menu path in the IGEL setup
bold	GUI [keyboard]	elements of the graphical user interface or commands that are entered using the keyboard
within brackets	[session name]	variable values

- [New Features 5.07.100](#)(see page 652)
- [Resolved Issues 5.07.100](#)(see page 654)

4.24.1 New Features 5.07.100

UMS (common)

- Added: New Feature **Asset Inventory Tracker**.
With a valid Asset Inventory license, it enables the user to collect Asset Inventory data from thin clients with Linux firmware 10.03.100 and higher.
The data is displayed as part of the thin client details panel.

Console (common)

- Added: Function to **check for new UMS updates**. (**UMS > Help > UMS Update Check**)
- Added: **Export and import actions** for template keys, value groups, and firmware customizations.

Server (common)

- Updated: **Apache Tomcat** from version 8.0.41 to **8.0.44**.

Thin Clients

- Added: New thin client attribute **Battery Level**.
- Added: **Advanced thin client state icons**.
The feature is activated by default and can be disabled via **Misc > Settings > Appearance > Use Advanced Health Status Icons**.
In addition to the existing states (online and offline) four new states have been added: **Never communicated with UMS**, **License violated**, **In Lockscreen**, and **In Firmware Update**.
The states **In Lockscreen** and **In Firmware Update** are only visible if the thin client firmware supports it and if the following option is set in the UMS (activated by default): **UMS Administration > Global Configuration > Thin Client Network > Thin Clients send updates**. This feature requires Linux firmware 10.03.100 or newer.



- Added: **Advanced message functionality.**
The **Send Message** action in the thin client context menu opens a new editor to send customized messages and templates.
Several default templates have been added and can be seen/changed in **UMS > UMS Administration > Global Configuration > TC Rich Message Templates**.
Thin clients which do not support the feature are showing the plain message like before.
- Added: **Clear value button** for thin client attributes with type "DATE".

Universal Firmware Update

- Added: Filter option to show only the latest available firmware version in firmware update dialog.
(UMS Console > Universal Firmware Update Tree Node > Context Menu > Check for new firmware updates)

Console (UMS Administration)

- Added: Possibility to use a list of **predefined thin client attribute values**. (**UMS Console > UMS Administration Tree > Global Configuration > Thin Client Attribute**)
- Changed: The **order of the tree nodes** in **UMS Console > UMS Administration > Global Configuration**.

Administrative Tasks

- Added: Administrative tasks can now be **executed monthly**.
- Added: New administration task to **save a UMS view on the file system**.

Firmwares

- Changed: Unused firmware can now be removed separately. (**UMS Console > Misc > Remove Unused Firmwares**)

IGEL Cloud Gateway (ICG)

- Changed: The **file and user synchronization process** after connecting an Igel Cloud Gateway is now executed in the **background**.

IGEL Management Interface (IMI)

- Added: IMI V3 supports now **Asset Inventory Information**.
- Added: IMI V3 supports now **Reset to factory defaults** for thin clients.
- Added: The thin client details do now contain the field **Battery Level** in IMI V3.

Installer (Linux)

- Added: Enhanced functionality for UMS installations on Linux. **Required libraries can now be installed automatically during UMS installation.**



4.24.2 Resolved Issues 5.07.100

UMS (common)

- Fixed: **Licenses can't be registered at the UMS** if the licenses are located on a network drive.
- Fixed: **UMS installations with more than three domain controllers** were not able to update to UMS version 5.05.100. After the update, each UMS login failed with a "truncation error" message.
- Fixed: The **Confirm deletion** dialog showed nested objects twice.
- Fixed: The **Restore backup** action failed for renamed .pbak backup files.
- Changed: If the internal thin client name is set to **overwrite the network name of the thin client**, there is now a check to make sure that the name is **DNS capable**.

Console (common)

- Changed: All **export actions** in the main menu are now always **enabled**, irrespective of the selected tree-object.
- Fixed: Bug in **UMS Linux installations** where hyperlinks could not be opened. (e.g. **UMS > UMS Administration > Misc Settings**)
- Added: The **thin client** content panel shows **icon corresponding to the current status** (online/offline/advanced health status)

Profiles

- Fixed: **Exporting profiles** (as archive) on a mapped network drive resulted in an unreadable file.
- Fixed: **Inconsistent results in profile comparison** when comparing two profiles in different directions (e.g. A-B vs B-A).

Template Keys and Groups

- Fixed: An error occurs if a template key or value group with **empty description** is edited and the **UMS database is an Oracle DB**.

Firmware Customization

- Fixed: **Display error in thin client directory assignments**. After a reload, the FWC assignments were not visible.
- Added: **FWC directories can now be copied** (including descendants).

Universal Firmware Update

- Fixed: Bug which was responsible for a **very low FTP firmware download rate**.

Configuration Dialog

- Fixed: After assigning two profiles (each with a default printer) to a thin client, the **thin client has now only one default printer set** (coming from a profile with higher priority).



- Fixed: **Coloring** for following changed and saved setup parameter:
User Interface > Desktop
Security > Logon > Active Directory / Kerberos
Security > Smartcard > Middleware

Console (UMS Administrator)

- Fixed: After a change in **UMS Console > UMS Administration > Global Configuration > Server Network Settings > Broadcast IP** the user is not asked to save the change.
- Fixed: The **Igel Cloud Gateway configuration node** depended on permissions of Igel Cloud Gateway server node.
- Fixed: The dialog **Export all Unit IDs from a view** showed duplicated thin client entries in the result list. (**UMS Console > UMS Administration > Global Configuration > Thin Client Licenses > Export Unit ID list**)

Administrative Tasks

- Fixed: **Maximum amount of backups** has been ignored by database backup task.
- Fixed: The **reporting of a database backup job** showed a failed task even if the task was completed successfully.
- Changed: Handling of **immediate execution time** for administrative tasks.

AD / LDAP Integration

- Fixed: **Active Directory login error** for domain names without a separating dot.

IGEL Cloud Gateway (ICG)

- Fixed: **Reregistration of an ICG managed thin client** (before rebooting the ICG) leads to a connection error between the thin client and the ICG.
- Fixed: **UMS lost ICG connection** randomly.
- Fixed: **Thin Client license files could not be downloaded** via IGEL Cloud Gateway.
- Fixed: **File transfer via ICG fails** if a custom UMS file transfer folder location is used.
- Fixed: The **Igel Cloud Gateway configuration node** depended on permissions of Igel Cloud Gateway server node.
- Fixed: After an ICG administrated thin client got changed settings, **the configuration flag has not been cleared** for assigned objects (e.g. profiles).
- Fixed: The thin client **license upload fails** if the ICG license is expired.

Administrator Application

- Fixed: The **backups** section in the UMS Administrator was only active for embedded databases. Now the **backups** section is always enabled to give the possibility to create and restore certificates and server configurations with all databases.

Installer (Windows)



- Changed: To avoid incorrect input, **the backup file path in Windows installer can now only be set by the file chooser dialog.**

Installer (Linux)

- Fixed: Removed **irritating log4j warnings** during database backup process in Linux installer.
- Fixed: Removed **irritating jsvc_server.pid error** message in Linux installer summary.

UI / Look & Feel

- Added: **New splash screen** for UMS Console and UMS Administrator.

5 UMS Extensions

- High Availability (HA)(see page 657)
- Shared Workplace (SWP)(see page 693)
- Asset Inventory Tracker (AIT)(see page 699)
- IGEL Management Interface (IMI)(see page 699)
- Universal Customization Builder (UCB)(see page 699)
- Mobile Device Management Essentials (MDM)(see page 704)

5.1 High Availability (HA)



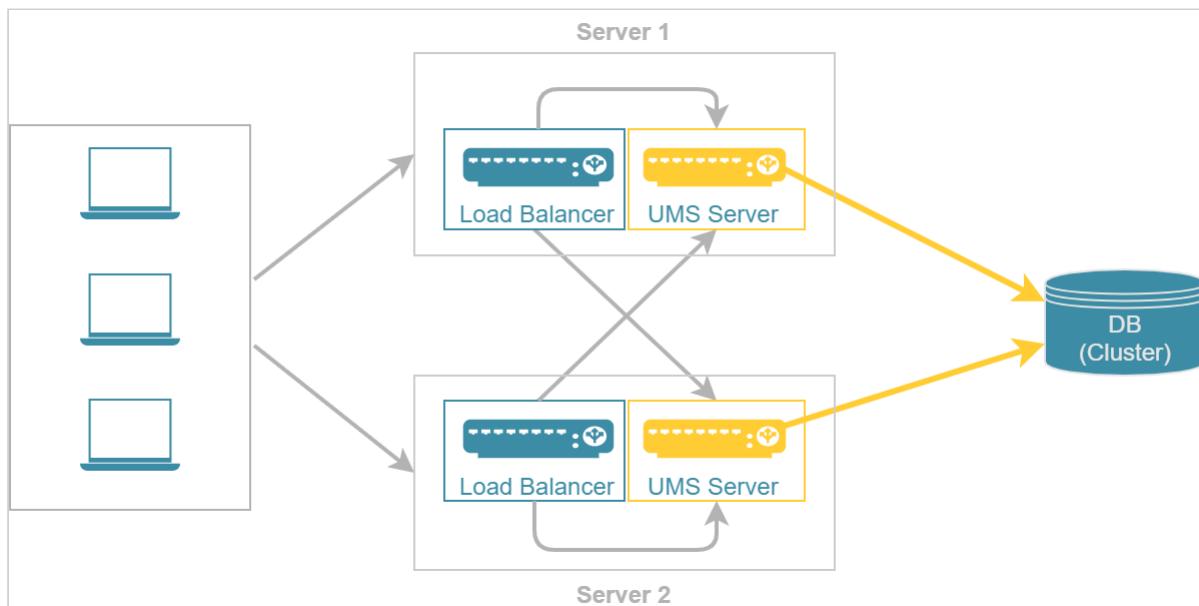
HA

The icon consists of the letters "HA" in a large, blue, sans-serif font, enclosed within a light blue rounded rectangular frame.

The optional High Availability extension is part of the IGEL UMS. It is designed to address the needs of large environments in which new settings need to be rolled out at once, or in which the fail-safe rollout of new settings is mission-critical for the organization concerned. The technical implementation is based on a network of several UMS Servers.

An upstream UMS Load Balancer takes over the load distribution and thus ensures that each device can receive new settings at any time – even at the start of a working day when a large number of devices log in to the UMS Server simultaneously and request new configuration profiles or firmware updates. To ensure maximum process reliability and high availability, IGEL also recommends that the UMS Load Balancer and the database have a redundant design.

Example:





See also [Configuration Options](#)(see page 658).

5.1.1 Licensing with the IGEL OS 11 Licensing Model

The High Availability extension is included in the Workspace Edition, so that IGEL OS 11 devices can use a UMS High Availability network without an additional license.

- [Configuration Options](#)(see page 658)
- [HA Installation](#)(see page 660)
- [Updating the Installation of an HA Network](#)(see page 671)
- [Switching from a Standard UMS Installation to an HA Installation](#)(see page 680)
- [Licensing the High Availability Extension](#)(see page 687)
- [UMS HA Health Check](#)(see page 688)
- [HA Services and Processes](#)(see page 691)

See also the collection of articles [High Availability](#)(see page 157).

5.1.2 Configuration Options

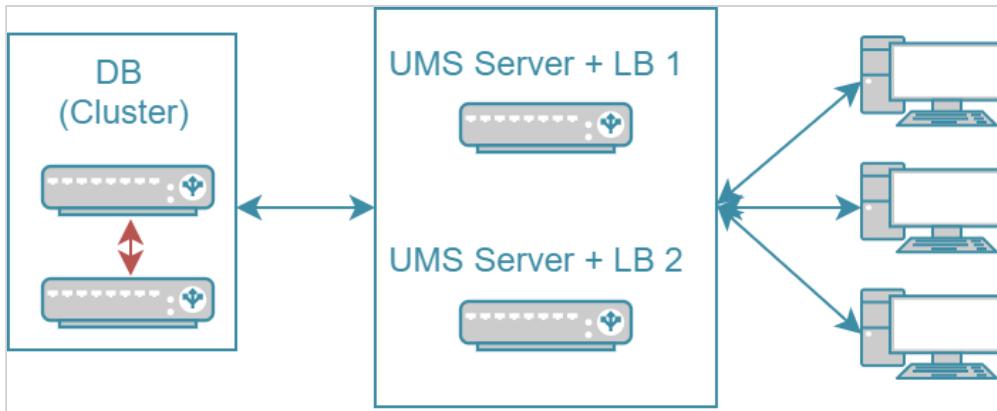
When planning the configuration of your High Availability (HA) network, you have to decide whether you want to install the UMS Server and UMS Load Balancer on the same host or on separate hosts. At the same time, there is a question how many UMS Servers and UMS Load Balancers are required. The following article describes the most common use cases and provides only general sizing recommendations. Your individual configuration may differ.

- i** When deciding how many UMS Servers and UMS Load Balancers you need, simply counting your endpoint devices is not enough. Most importantly, you have to analyze the entire network environment as well as the other circumstances within your workplace. See [Installation and Sizing Guidelines for IGEL UMS](#)(see page 242) as well as [Installation Types & Diagrams](#)(see page 243) and contact your IGEL reseller to get counsel.

UMS Server & UMS Load Balancer Are Installed on the Same Host Machine

The most common scenario when deploying UMS High Availability is to install the UMS Server and UMS Load Balancer on the same host machine. Both the UMS Server and the UMS Load Balancer offer redundancy and are installed on two servers. The database is ideally designed as a cluster.

Typical Use Cases	#UMS Server + UMS Load Balancer
The installation on the same host machine is suitable if <ul style="list-style-type: none"> • the number of devices < 50,000 • you use the Shared Workplace(see page 693) feature 	2 UMS Servers 2 UMS Load Balancers

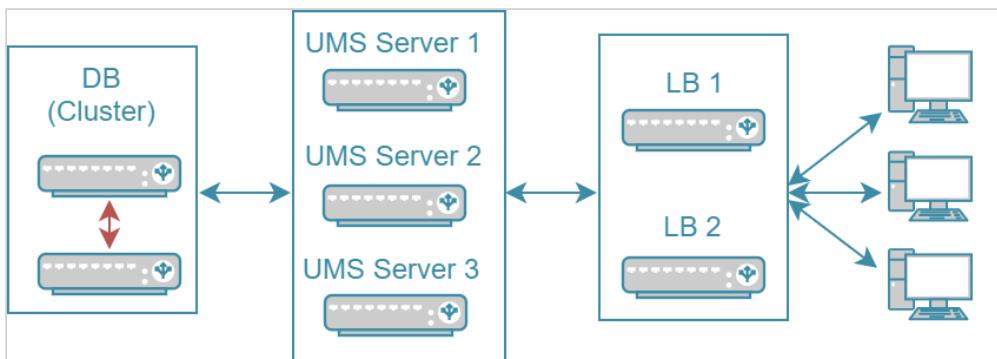


In this configuration, each of the two servers can also perform the tasks as a UMS Server alone. If both servers are active at the same time, this has a load-distributing effect. Note, however, that the load balancer generates extra load along with the actual UMS Server.

UMS Server & UMS Load Balancer are Installed on Separate Host Machines

If you need to manage a very large number of devices and/or do not want the server resources to be shared between the load balancer and the UMS Server, the installation on separate hosts should be considered.

Typical Use Cases	#UMS Server Standalone & Load Balancer Standalone
<p>The installation of the load balancer on a separate host machine is</p> <ul style="list-style-type: none"> • required if the number of devices > 50,000 • recommended if you do not want the load balancer to consume resources on the UMS Server host 	<p>Smallest typical configuration:</p> <p>2-3 UMS Servers 2 UMS Load Balancers</p> <p>General sizing recommendations:</p> <ul style="list-style-type: none"> • up to 6 UMS Servers • up to 3 UMS Load Balancers • 1 UMS Server per max. 50,000 devices • 1 LB per max. 3 UMS Servers



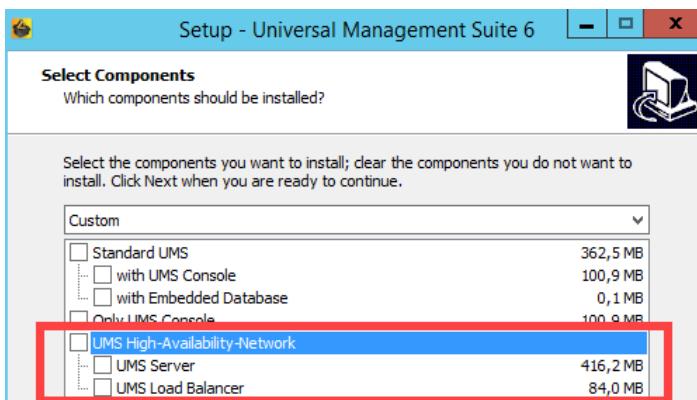


In the smallest typical configuration, queries from the devices are passed on to the UMS Servers by both load balancers. If one of the load balancers should fail, the other remains available and assumes responsibility for communications alone. A great number of UMS Servers could overload a single load balancer, which would then become itself a bottleneck. Therefore, there are provisions for no more than three UMS Servers in this configuration. For very large installations with more than three UMS Servers, the number of load balancers should be increased accordingly.

- ⚠** All UMS Servers and UMS Load Balancers must reside on the same VLAN. Network traffic must be allowed over UDP broadcast port 6155, and TCP traffic and UDP broadcast traffic over port 61616. For more information on UMS ports, see [UMS Communication Ports](#)(see page 48).
 Note: IGEL UMS Server HA is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks.

5.1.3 HA Installation

To use the High Availability Extension, you have to select the option for installing the HA network components in the UMS installer.



When installing the High Availability Extension, it is important to differentiate between the installation of the first HA server and further HA servers.

During the installation of the first HA server (UMS Server obligatory), an IGEL network token is created. This network token allows the integration of new servers into the same HA network and, thus, must be used when installing all subsequent HA servers.

Follow these instructions to install the High Availability Extension:

- [HA: Installation Requirements](#)(see page 660)
- [Installing the First Server in an HA Network](#)(see page 662)
- [Adding Further Servers to the HA Network](#)(see page 667)

For information on how to update the HA installation, see [Updating the Installation of an HA Network](#)(see page 671).

HA: Installation Requirements

In order to install an IGEL UMS High Availability network, your hardware and software must meet the following minimum requirements.



- i** The installation requirements can vary depending on how large your HA environment is. For more information, see [Installation and Sizing Guidelines for IGEL UMS](#)(see page 242).

UMS High Availability Network: Minimum Requirements

UMS Server (includes UMS Server, UMS Administrator, and UMS Console)	UMS Load Balancer	UMS Web App	File System
<p>UMS Server:</p> <ul style="list-style-type: none"> • At least 4 GB of RAM • At least 2 GB of free HDD space <p>UMS Console:</p> <ul style="list-style-type: none"> • At least 3 GB of RAM • At least 1 GB of free HDD space <p>UMS Administrator:</p> <ul style="list-style-type: none"> • At least 1 GB of RAM 	<ul style="list-style-type: none"> • At least 1 GB of RAM • At least 1 GB of free HDD space 	<ul style="list-style-type: none"> • 1 GB of RAM • 1 GB of free HDD space 	<ul style="list-style-type: none"> • 1 GB for the program files • Approx. 10 GB for each firmware update to be downloaded

For the supported operating systems, see the [Supported Environment](#)(see page 586) section of the release notes.¹⁴⁰

- !**
- The UMS Server must not be installed on a domain controller system!
 - Manually modifying the Java Runtime Environment on the UMS Server is not recommended.
 - Running additional Apache Tomcat web servers together with the UMS Server is not recommended either.

! All UMS Servers and UMS Load Balancers must reside on the same VLAN. Network traffic must be allowed over UDP broadcast port 6155, and TCP traffic and UDP broadcast traffic over port 61616. For more information on UMS ports, see [UMS Communication Ports](#)(see page 48).

Note: IGEL UMS Server HA is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks.

¹⁴⁰ <http://www.igel.com/igel-ums-universal-management-suite/>



Database Systems (DBMS)

- ⓘ For details on the supported database systems, see the "Supported Environment" section of the [release notes](#)(see page 565). Details of the requirements when installing and operating the database can be found in the documentation for the particular DBMS.
- ⓘ The embedded database **cannot** be used for an HA network. You can use the embedded database only for a dedicated test installation with only a single server for the UMS Server and UMS Load Balancer.
- ⓘ The database system must be accessible to all UMS Servers.

Installing the First Server in an HA Network

Prerequisites

- A set of servers with the operating system supported by the UMS; see the "Supported Environment" section of the [release notes](#)(see page 565).
- A database system supported by the UMS; see the "Supported Environment" section of the [release notes](#)(see page 565).
- All installation requirements described under [HA: Installation Requirements](#)(see page 660) are fulfilled.
- The current version of the UMS is downloaded from the [IGEL Download Server](#)¹⁴¹.

- ⓘ For the first installation, it is advisable to use a server without an existing UMS installation.

Instructions

To install the UMS High Availability (HA) Extension on the first server, follow the instructions in the order given:

1. [Preparing the Database](#)(see page 662)
2. [Preparing the Servers](#)(see page 663)
3. [Starting the Installation](#)(see page 663)
4. [Defining the Database Connection](#)(see page 665)
5. [Checking the Installation](#)(see page 666)
6. [Saving the IGEL Network Token](#)(see page 666)

Preparing the Database

- Create a database schema and a user for the UMS. Use the relevant DBMS program and its documentation. See also [Connecting External Database Systems](#)(see page 289).

¹⁴¹ <https://www.igel.com/software-downloads/workspace-edition/>



Preparing the Servers

1. Verify that each server can "see" the other servers via the network.

⚠ All UMS Servers and UMS Load Balancers must reside on the same VLAN. Network traffic must be allowed over UDP broadcast port 6155, and TCP traffic and UDP broadcast traffic over port 61616. For more information on UMS ports, see [UMS Communication Ports](#)(see page 48). Note: IGEL UMS Server HA is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks.

2. Verify that the time on all servers is synchronized.

⚠ To avoid problems with your HA installation, make sure that the time on the servers of the HA network does not differ by more than one minute. After each manual time reset, the HA services on the relevant server must be restarted.

3. For Linux systems, make the directory `/root` writable for the user `root`.

Starting the Installation

1. Launch the UMS installer.

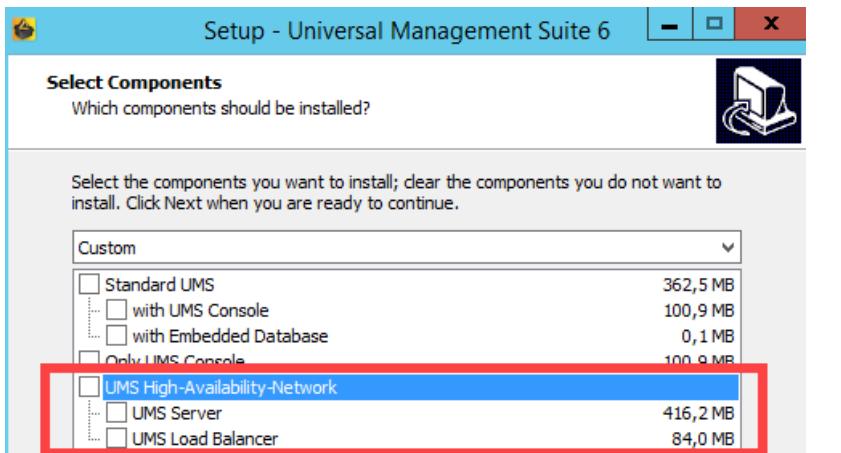
i You need administration rights to install the IGEL UMS HA.

2. Read and confirm the **License Agreement**.
3. Read the **Information** regarding the installation process.
4. Select a path for the installation.
5. Depending on your desired [HA network configuration](#)(see page 658), select the components to be installed: **UMS Server + UMS Load Balancer** or **UMS Server**.

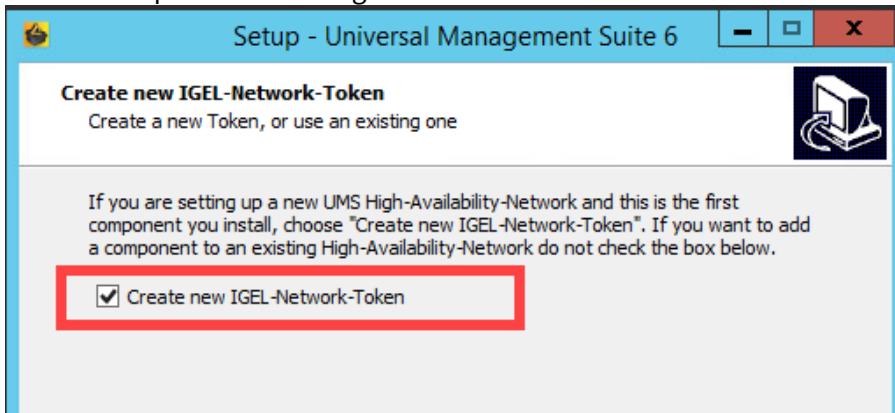
⚠ **Installing UMS Server and UMS Load Balancer on Separate Servers**

If you install HA network components on separate servers, **UMS Server** must always be installed first. In this case, the IGEL network token, which is required for the integration of further servers into the HA network, will be created. Additionally, the UMS Console and UMS Administrator applications, necessary for the further management of the installation, will be installed too. After configuring and enabling the database via the UMS Administrator, the UMS Server will be available in the HA network.

If you install an individual UMS Load Balancer, neither the IGEL network token nor UMS Console nor UMS Administrator will be installed. Only the option for uninstalling the UMS will then be set up in the Windows start menu.

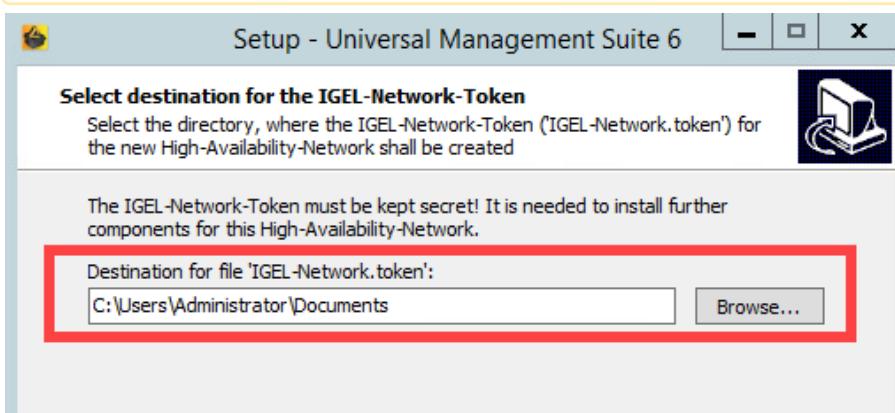


6. Confirm the system requirements dialog if your system fulfills them.
7. Select the **UMS data directory**, in which Universal Firmware Updates and files are to be saved.
8. Enable the option for creating an IGEL network token.



9. Specify a directory for saving the IGEL network token. The directory must be writeable for the administrator.

⚠ Be sure to keep the IGEL network token in a safe place! It will be needed for all subsequent server installations. If the IGEL network token is lost, the complete installation must be started again.





10. Optional: Under **Import existing keystore**, you can load the `tc.keystore` file from an existing UMS installation.

! This function can destroy your UMS installation. Do not import this file unless you know exactly what you are doing.
 11. If the internal Windows firewall is active on your host: Review the settings under **Windows firewall settings** and change them where necessary. Each port that is activated here will be set as rule in the Windows firewall. For more information about the usage of ports, see [UMS Communication Ports](#)(see page 48).
 12. Specify a folder name for the shortcut.
 13. Read the summary and start the installation process.
 14. Close the UMS installer once the installation is complete.
The UMS installer creates entries in the Windows software directory and the start menu. A shortcut for the UMS Console will also be placed on the desktop.
- i If [SQL Server AD Native](#)(see page 292) is used, you must also set the correct startup type and logon settings for the "IGEL RMGUIServer" service and restart the service. For details, see "[Configuring the UMS Server Windows Service](#)" under "[Setting Up the UMS for SQL Server AD Native](#)"(see page 299).

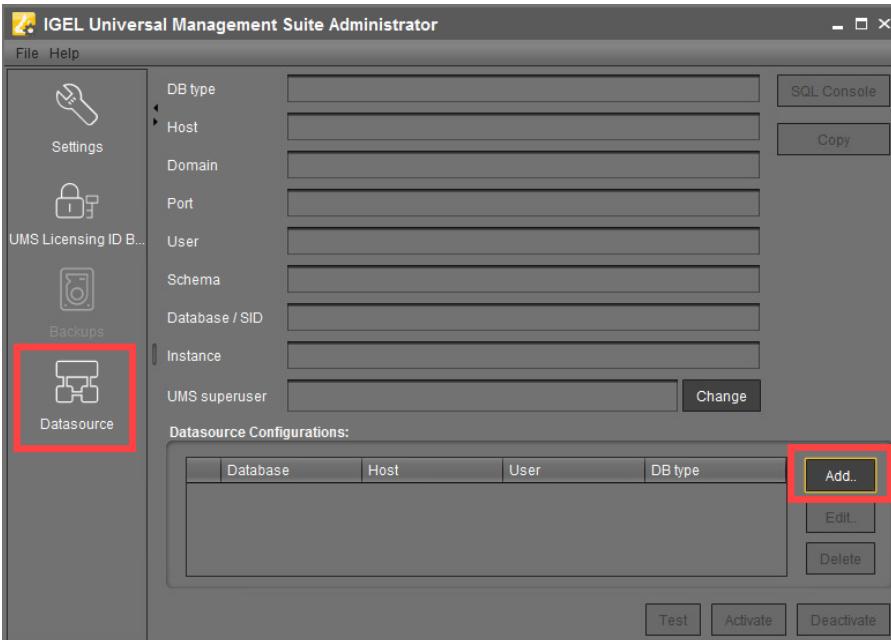
Defining the Database Connection

1. Open the UMS Administrator.

i Default path to the UMS Administrator:
Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`



2. Select **Datasource > Add.**



3. Enter the connection properties of the prepared database schema. See also [How to Set Up a Data Source in the IGEL UMS Administrator](#)(see page 543).
4. Click **Activate** to enable the data source. See also [Activating a Data Source](#)(see page 546).

Checking the Installation

1. Check if all processes are running. For the list of UMS HA processes, see [HA Services and Processes](#)(see page 691).
2. In the UMS Console, go to **UMS Administration > UMS Network** and check the items **Server** and **Load Balancer** if the complete UMS HA Extension has been chosen for the installation.

Process ID	Process Name	Timestamp	Service status	Mode
fa86e615-1d0c-4f79-a44d-39e4...	td-ums-srv2012	01.10.2020 16:15	Service is running	Normal Mode

Saving the IGEL Network Token

- Save the IGEL network token, i.e. the file `IGEL-Network.token`, on a storage medium which will be accessible when installing further HA servers (e.g. on the network or on a portable storage medium such as a USB stick). Always keep the IGEL network token well protected.

Next Step

>> Proceed with adding a further server to the HA installation, see [Adding Further Servers to the HA Network](#)(see page 667).



Adding Further Servers to the HA Network

Introduction

Further HA servers – with UMS Server, UMS Load Balancer, or both – can be installed in the same way as the first one. However, you do not need to create a new IGEL network token. Instead, you must select the network token created previously during the installation of the first server in an HA network.

In addition, a connection with the same database that is used by the first server must be established. The UMS HA network only works if all servers are connected to the same database.

Prerequisites

- A High Availability (HA) installation with a configured database, see [Installing the First Server in an HA Network](#)(see page 662).

⚠ The database connection should be defined during the installation of the first UMS Server in an HA network. In this case, all relevant configuration information is automatically copied to the additional UMS Servers.

- The IGEL network token created during the installation of the first server in the HA network, see [Installing the First Server in an HA Network](#)(see page 663).
- A server with the operating system supported by the UMS; see the "Supported Environment" section of the [release notes](#)(see page 565).
- All installation requirements described under [HA: Installation Requirements](#)(see page 660) are fulfilled.
- The same version of the UMS as for the first HA server is downloaded from the [IGEL Download Server](#)¹⁴².

Instructions

To add a new server to the UMS HA installation, follow the instructions in the order given:

1. [Preparing the Server](#)(see page 667)
2. [Preparing the IGEL Network Token](#)(see page 668)
3. [Starting the Installation](#)(see page 668)
4. [Checking the Installation](#)(see page 670)

Preparing the Server

1. Verify that the server can "see" the other servers via the network.

⚠ All UMS Servers and UMS Load Balancers must reside on the same VLAN. Network traffic must be allowed over UDP broadcast port 6155, and TCP traffic and UDP broadcast traffic over port 61616. For more information on UMS ports, see [UMS Communication Ports](#)(see page 48).

¹⁴² <https://www.igel.com/software-downloads/workspace-edition/>



Note: IGEL UMS Server HA is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks.

2. Verify that the time on all servers is synchronized.

- ⚠** To avoid problems with your HA installation, make sure that the time on the servers of the HA network does not differ by more than one minute. After each manual time reset, the HA services on the relevant server must be restarted.

3. For Linux systems, make the directory /root writable for the user root.

Preparing the IGEL Network Token

► If you have not yet done so, save the IGEL network token created during the installation of the first HA server, e.g. on a portable storage medium.

- i** If the path has not been changed, the file `IGEL-Network.token` can be found by default in the home directory of the administrator user on a UMS Server host.

- ⚠** If you have a fully functional UMS HA network already in use and simply want to enlarge it with one more HA server, make sure you use for the additional HA server installation the **current** IGEL network token. If you have not saved it:
- Restart the `IGEL_RMGUIServer` service (for the instruction, see [HA Services and Processes](#)(see page 691)) and use in this case the network token created upon the UMS Server startup from the directory:
Windows: `C:\Windows\System32\config\systemprofile\IGEL-Network.token`
Linux: `/root/IGEL-Network.token`

Starting the Installation

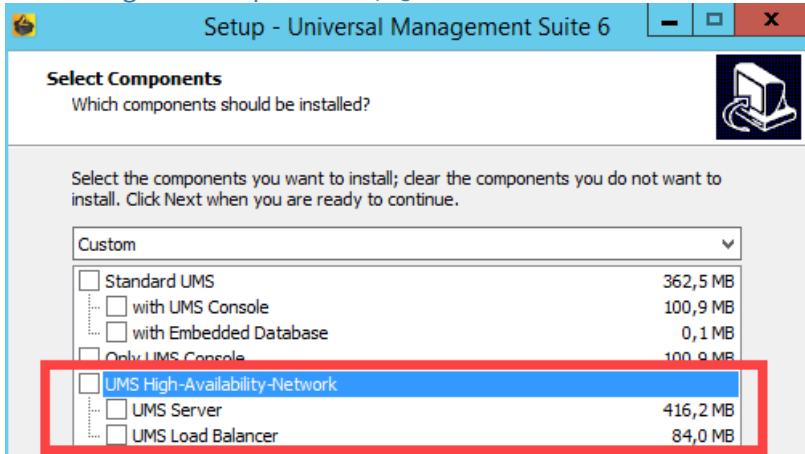
1. Launch the UMS installer.

- i** You need administration rights to install the IGEL UMS HA.

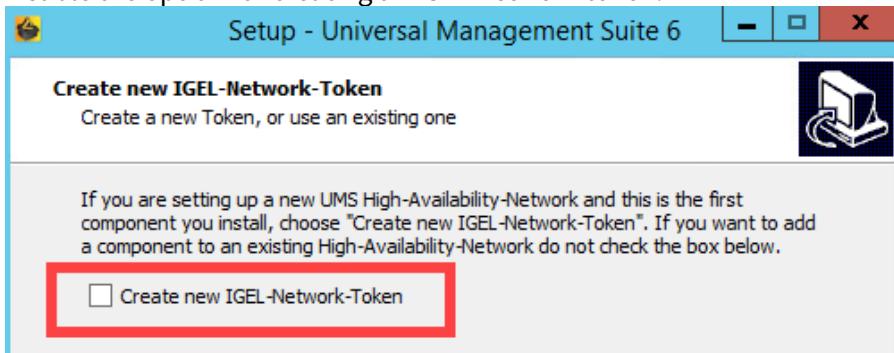
2. Read and confirm the **License Agreement**.
3. Read the **Information** regarding the installation process.
4. Select a path for the installation.



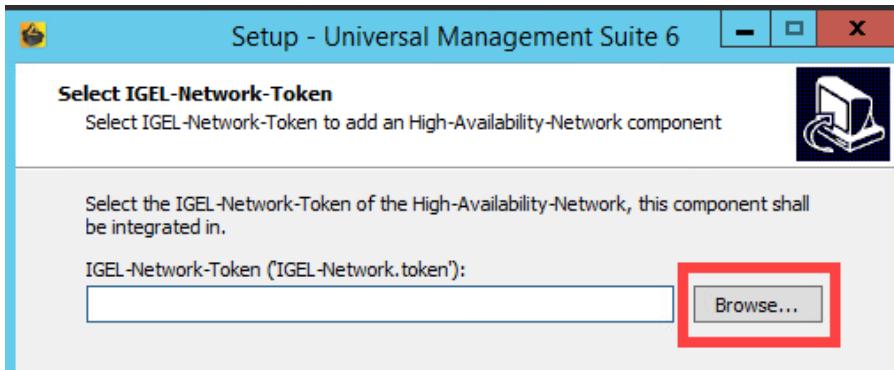
5. Select the components to be installed depending on your desired HA network configuration. See also [Configuration Options](#)(see page 658).



6. Confirm the system requirements dialog if your system fulfills them.
 7. Select the **UMS data directory**, in which Universal Firmware Updates and files are to be saved.
 8. Disable the option for creating an IGEL network token.



9. Select the IGEL network token to be used.



10. If the internal Windows firewall is active on your host: Review the settings under **Windows firewall settings** and change them where necessary. Each port that is activated here will be set as rule in the Windows firewall. For more information about the usage of ports, see [UMS Communication Ports](#)(see page 48).
 11. Specify a folder name for the shortcut.
 12. Read the summary and start the installation process.



13. Close the UMS installer once the installation is complete.

If you have included a UMS Server in the installation, the UMS installer creates entries in the Windows software directory and the start menu. The UMS Console and UMS Administrator applications are installed, and a shortcut for the UMS Console is placed on the desktop.

If you have installed an individual load balancer, only the option for uninstalling the UMS will be set up in the Windows start menu. No configuration on the load balancer is necessary. It connects automatically to the HA network during booting.

- i** If [SQL Server AD Native](#)(see page 292) is used, you must also set the correct startup type and logon settings for the "IGEL RMGUIServer" service and restart the service. This must be done on **ALL** UMS Server hosts. For details, see "[Configuring the UMS Server Windows Service](#)" under "[Setting Up the UMS for SQL Server AD Native](#)"(see page 299).

Checking the Installation

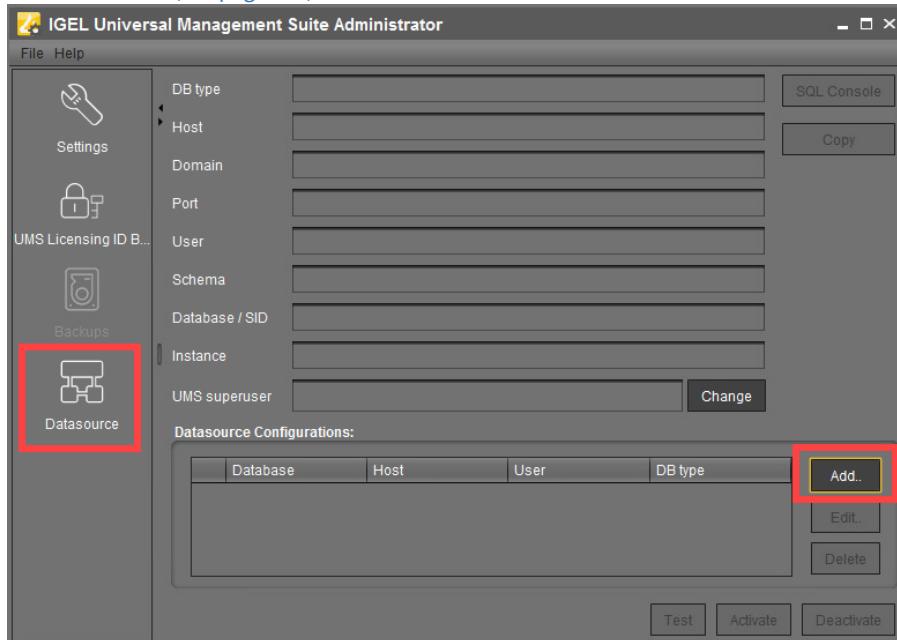
1. Check if all processes are running. For the list of UMS HA processes, see [HA Services and Processes](#)(see page 691).
2. If you have included a UMS Server in the installation, open **UMS Administrator > Datasource** and verify that the database connection has been successfully transferred from the already running UMS Server.

- i** Default path to the UMS Administrator:
Linux: /opt/IGEL/RemoteManager/RMAdmin.sh
Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe

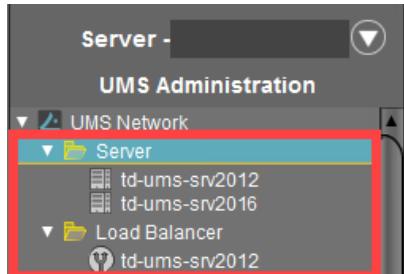
If the database connection has not been defined automatically, enter under **UMS Administrator > Datasource > Add** exactly the same database parameters you used during the installation of [the](#)



first HA server(see page 665) and click **Activate**.



3. In the UMS Console, go to **UMS Administration > UMS Network** and check the items **Server** and/or **Load Balancer**.



Additionally, you can use the feature for checking the HA installation, see [UMS HA Health Check](#)(see page 688).

For the future, you may also find it useful to read: [Creating a Backup](#)(see page 536) and [How to Detect Which Files Are Synchronized Automatically](#)(see page 159).

5.1.4 Updating the Installation of an HA Network

Use Case

You have a UMS High Availability (HA)(see page 657) installation and need to update it.

General Overview

There are two possible HA update procedures:



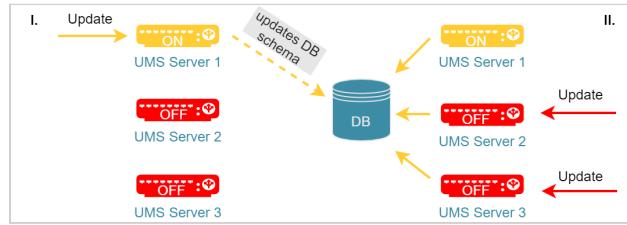
- With short downtime of the servers (see page 672) (recommended)
- Without downtime of the servers, but with automatic copying the productive database to a temporary database (see page 672), which generally results in longer update time

With Short Downtime

In this case, the update procedure generally looks as follows:

- Stop all UMS Servers except one (verify this in the server list of the UMS Console connected to the last running server).
- Update this UMS Server.
As soon as the update is complete, the productive database will be updated upon server startup.
- Update the remaining UMS Servers (simultaneously or one after another). When the update is complete, they will automatically connect to the productive database.
- Update other components like separate UMS Load Balancers and/or UMS Consoles.

For detailed instructions, see [Updating HA Installation: With Downtime of the Servers](#)(see page 673).



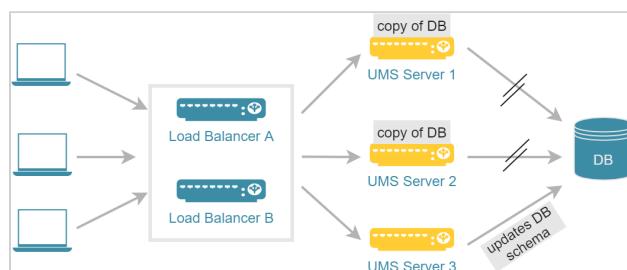
⚠ IGEL recommends using this HA update method due to a number of advantages:

- The update procedure is much faster.
- No database inconsistencies since no other servers and processes use the database during the update.
- Only short downtime. Note: Since there is no communication between the servers and devices (during the update of the first UMS Server), user-specific profiles cannot be supplied (IGEL Shared Workplace).

Without Downtime

In this case, the update procedure generally looks as follows:

- Update all UMS Servers to a new version, one server after another.
While being updated, a UMS Server disconnects itself from the productive database and stores a copy of it locally in an embedded Derby database. The copy is created for each server except the last. The last UMS Server also updates the schema of





the productive database. After this, all other UMS Servers connect themselves again to the original productive database.

2. Update other components like separate UMS Load Balancers and/or UMS Consoles.

For detailed instructions, see [Updating HA Installation: Without Downtime of the Servers](#)(see page 676).

- ⚠** By this update method, all UMS Servers can be addressed by the endpoint devices at any time during the update process, e.g. to supply user-specific profiles (IGEL Shared Workplace). However, note the following:
- The copying of the data from the productive database to the temporary database can take a lot of time.
 - Requests from devices can interfere with the copying process.
 - Changes in the temporary database are lost as soon as the servers switch back to the productive database when the update is complete.

- [Updating HA Installation: With Downtime of the Servers](#)(see page 673)
- [Updating HA Installation: Without Downtime of the Servers](#)(see page 676)

Updating HA Installation: With Downtime of the Servers

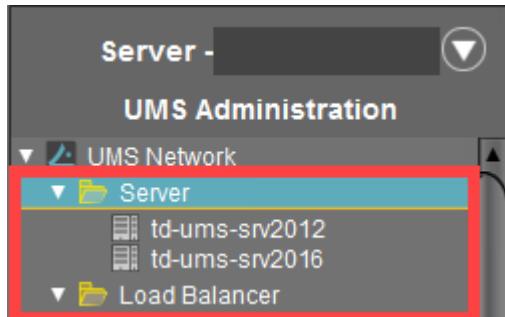
For a short overview of the High Availability (HA) update procedure, see [Updating the Installation of an HA Network](#)(see page 671).

To update the HA installation, follow these instructions in the order given.

Preparing the Update

Perform the following steps before updating a server:

1. Download the current version of IGEL Universal Management Suite from the [IGEL Download Server](#)¹⁴³and distribute the installer file to all systems with UMS components (UMS Server, UMS Load Balancer, UMS Consoles).
2. In the UMS Console, call up the list of UMS Servers and Load Balancers in the HA network under **UMS Administration > UMS Network** and check whether the listed components really exist in the network. Delete orphaned entries before starting the process for updating the components.



3. Create a backup of your database before starting the update installation. Use the backup procedures recommended by the DBMS manufacturer. See also [Creating a Backup](#)(see page 536).

 **Warning**

It is not possible to install a UMS version which is older than the current one. If you want to change to an older version, you will need to install a separate HA network and restore a database backup of the corresponding schema. This is also one of the reasons why you should back up the running system before updating the UMS HA network.

4. Verify that the time on all servers is synchronized.

 To avoid problems with your HA installation, make sure that the time on the servers of the HA network does not differ by more than one minute. After each manual time reset, the HA services on the relevant server must be restarted.

Updating UMS Servers

The main feature of this update method is that it checks at the beginning how many UMS Servers are "online". If the server where the update has been started is the only one active, no temporary database with a copy of the productive database is created and the productive database is updated immediately, i.e. as soon as the UMS Server starts after the update is complete. Therefore, it is necessary to leave ONLY ONE UMS Server running, i.e. the one you start the update procedure with. This can be any UMS Server within your HA network.

1. Stop all UMS Servers except the one, on which you are going to start the update. You can stop UMS Servers in the UMS Console under **UMS Administration > UMS Network > Server > [Server name] > Stop service** or in Windows Services, see [HA Services and Processes](#)(see page 691).
2. Verify that only one UMS Server is running and the others are stopped:
 - by checking the list of servers in the UMS Console under **UMS Administration > UMS Network > Server**
OR
 - with the following SQL statement:

```

select
    ep.epr_process_id,
    ep.epr_process_host,
    ep.epr_process_mode,
    ep.epr_service_status
from
    epr_processes ep
  
```

**where**

```
ep.epr_process_type = 'UMS_RMGUISERVER'
```

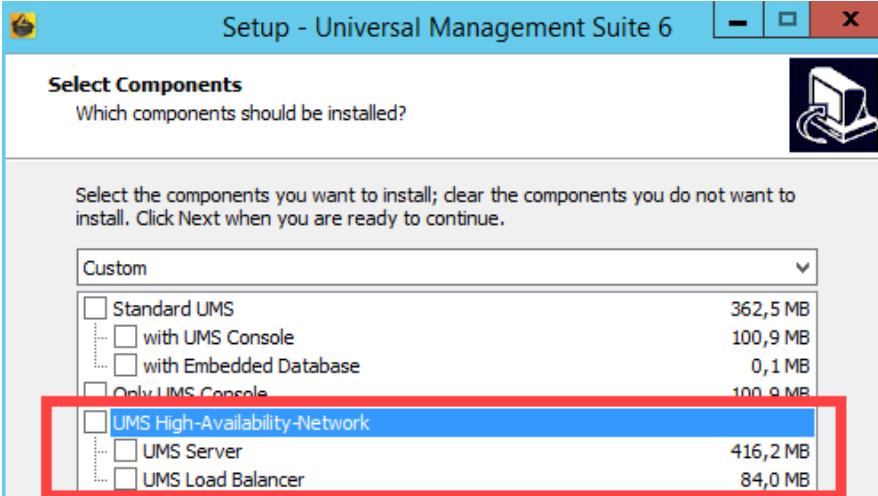
SERVICE_RUNNING must be shown only for the server you are about to update.
 SERVICE_STOPPED must be shown for all the other servers.

3. Launch the UMS installer.

i You need administration rights to update the IGEL UMS HA.

! When installing the UMS Server as a part of the HA network on Linux, the directory /root must be writable for the user root.

4. Read and confirm the **License Agreement**.
5. Read the **Information** regarding the installation process.
6. Verify the components to be installed. (In this example: HA network with UMS Server and UMS Load Balancer installed individually)



7. Confirm the system requirements dialog if your system fulfills them.
8. If the internal Windows firewall is active on your host: Review the settings under **Windows firewall settings** and change them where necessary. Each port that is activated here will be set as rule in the Windows firewall. For more information about the usage of ports, see [UMS Communication Ports](#)(see page 48).
9. Read the summary and start the installation process.
10. Close the UMS installer once the installation is complete.
 The UMS Server will start and update the database.

i If [SQL Server AD Native](#)(see page 292) is used, you must also set the correct startup type and logon settings for the "IGEL RMGUIServer" service and restart the service. This must be done on **ALL** UMS Server hosts. For details, see "[Configuring the UMS Server Windows Service](#)" under "[Setting Up the UMS for SQL Server AD Native](#)"(see page 299).

11. Open the UMS Console and go to **UMS Administration > UMS Network > Server** to verify that the server is



- successfully updated
- running
- in normal mode

Server	Process ID	Process Name	Timestamp	Service status	Mode
	fa86e615-1d0c-4f79-a44d-39e4...	td-ums-srv2012	01.10.2020 16:15	Service is running	Normal Mode

12. Update the remaining UMS Servers, either simultaneously or one after another, by repeating steps 3-11.

After the update, the servers will automatically start and connect to the productive database.

Updating Further Components

After updating the UMS Servers within the HA network, you have to update all other current UMS components, e.g. separate UMS Load Balancers and UMS Consoles.

1. In order to do this, run the UMS installer on the systems.
2. Verify the components to be installed.

- ⓘ You cannot connect to the UMS Server with a console version that is older than the version of the UMS Server.
- ⓘ Load balancers are able to interoperate with UMS Servers of newer versions, but they should have the same version as the UMS Servers for optimal performance.

See also [Load Balancer Is Not Stopping during the Update of the HA Installation](#)(see page 158).

Checking the Installation

1. Check if all processes are running. For the list of UMS HA processes, see [HA Services and Processes](#)(see page 691).
2. In the UMS Console, go to **UMS Administration > UMS Network** and check the items **Server** and **Load Balancer**.

All servers and load balancers must be:

- updated
- running
- in normal mode

Server	Process ID	Process Name	Timestamp	Service status	Mode
	fa86e615-1d0c-4f79-a44d-39e4...	td-ums-srv2012	01.10.2020 16:15	Service is running	Normal Mode

Updating HA Installation: Without Downtime of the Servers

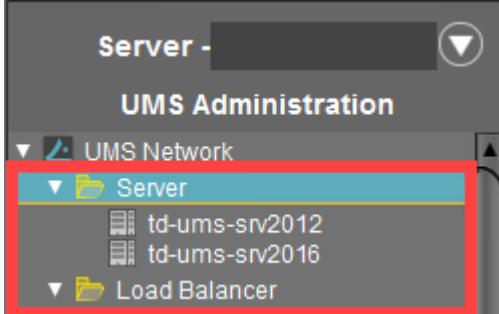
- ⚠ Before the update, see [Updating the Installation of an HA Network](#)(see page 671).

To update the HA installation, follow these instructions in the order given.

Preparing the Update

Perform the following steps before updating a server:

1. Download the current version of IGEL Universal Management Suite from the [IGEL Download Server](#)¹⁴⁴and distribute the installer file to all systems with UMS components (UMS Server, UMS Load Balancer, UMS Consoles).
2. In the UMS Console, call up the list of UMS Servers and Load Balancers in the HA network under **UMS Administration > UMS Network** and check whether the listed components really exist in the network. Delete orphaned entries before starting the process for updating the components.



3. Create a backup of your database before starting the update installation. Use the backup procedures recommended by the DBMS manufacturer. See also [Creating a Backup](#)(see page 536).

 **Warning**

It is not possible to install a UMS version which is older than the current one. If you want to change to an older version, you will need to install a separate HA network and restore a database backup of the corresponding schema. This is also one of the reasons why you should back up the running system before updating the UMS HA network.

4. Verify that the time on all servers is synchronized.

 To avoid problems with your HA installation, make sure that the time on the servers of the HA network does not differ by more than one minute. After each manual time reset, the HA services on the relevant server must be restarted.

Updating UMS Servers

In the update mode, the UMS Servers run with a local copy of the database. This ensures that they can answer requests from the devices and transfer configuration settings and profiles to the devices.

 In the update mode, you can connect to the servers via the UMS Console. All changes made in the UMS Console during this time will be lost after the update.

 **Warning**

¹⁴⁴ <https://www.igel.com/software-downloads/workspace-edition/>



Do not make changes in the productive database during the update process. This is because decoupled servers work with a copy of the database schema in the meantime. For this reason, the update of all components within the UMS HA network should be carried out immediately. Implement a test system for the first installation of new IGEL UMS versions and check their processes before transferring them to the productive system. This also applies to hotfixes, patches, etc. for server systems and databases.

Updating the First UMS Servers

You can select any UMS Server within the HA network to start the update procedure.

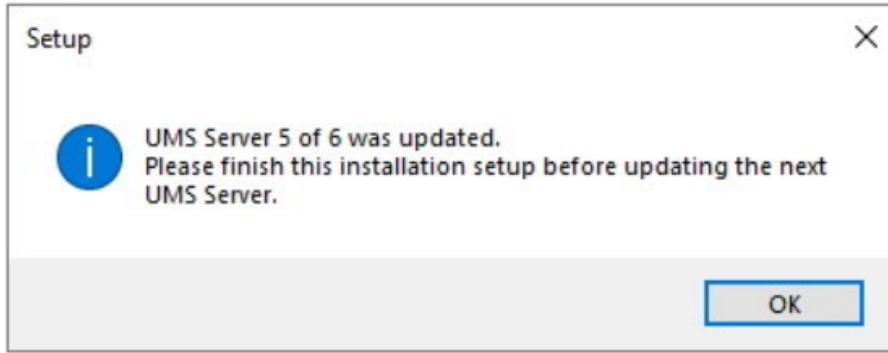
1. Launch the UMS installer.

i You need administration rights to update the IGEL UMS HA.

⚠ When installing the UMS Server as a part of the HA network on Linux, the directory /root must be writable for the user root.

2. Read and confirm the **License Agreement**.
3. Read the **Information** regarding the installation process.
4. Verify the components to be installed. (In this case: HA network with UMS Server and UMS Load Balancer installed individually)
5. Confirm the system requirements dialog if your system fulfills them.
6. If the internal Windows firewall is active on your host: Review the settings under **Windows firewall settings** and change them where necessary. Each port that is activated here will be set as rule in the Windows firewall. For more information about the usage of ports, see [UMS Communication Ports](#)(see page 48).
7. Read the summary and start the installation process.
During the installation, the UMS Server switches to update mode.
8. Confirm the message n of m servers updated.

Example:



9. Close the UMS installer once the installation is complete.

i If [SQL Server AD Native](#)(see page 292) is used, you must also set the correct startup type and logon settings for the "IGEL RMGUIServer" service and restart the service. This must be done on **ALL** UMS Server hosts. For details, see "[Configuring the UMS Server Windows Service](#)" under "[Setting Up the UMS for SQL Server AD Native](#)"(see page 299).



10. Continue with the update of the next UMS Server.

Updating the Last UMS Server

- ▶ Repeat steps [1-9\(see page 678\)](#) on the last UMS Server to be updated.

The last UMS Server updated renews the schema of the productive database after the installation. All other UMS Servers within the network which run in the update mode will be informed that the installation has finished. They will restart and reconnect themselves to the productive database. Afterwards, they will run in normal mode.

Updating Further Components

After updating the UMS Servers within the HA network, you have to update all other current UMS components, e.g. separate UMS Load Balancers and UMS Consoles.

1. In order to do this, run the UMS installer on the systems.
2. Verify the components to be installed.

- ⓘ You cannot connect to the UMS Server with a console version that is older than the version of the UMS Server.
- ⓘ Load balancers are able to interoperate with UMS Servers of newer versions, but they should have the same version as the UMS Servers for optimal performance.

See also [Load Balancer Is Not Stopping during the Update of the HA Installation\(see page 158\)](#).

Checking the Installation

1. Check if all processes are running. For the list of UMS HA processes, see [HA Services and Processes\(see page 691\)](#).
2. In the [UMS Administrator\(see page 529\)](#), go to **Datasource** to check if the database is activated.

- ⚠ If the server list has not been checked at the beginning of the update (see [Preparing the Update\(see page 677\)](#), step 2) and there have been more servers registered in the database than actually running, it might be the case that there is a server within the HA network that did not reconnect to the productive database.
In this case, you have to switch over the data source manually to the productive database.
The database schema will be renewed the first time an updated server connects to the productive database. Afterwards, all other servers within the network can be switched over to this database.

3. In the UMS Console, go to **UMS Administration > UMS Network** and check the items **Server** and **Load Balancer**.

All servers and load balancers must be:

- updated
- running
- in normal mode



Server	Process ID	Process Name	Timestamp	Service status	Mode
	fa86e615-1d0c-4f79-a44d-39e4...	td-ums-srv2012	01.10.2020 16:15	Service is running	Normal Mode

5.1.5 Switching from a Standard UMS Installation to an HA Installation

Use Case

You have a standard UMS installation, but you want to switch to a [High Availability\(see page 657\)](#) (HA) installation.

Prerequisites

- A standard UMS installation with either an embedded or an external database
- A set of servers with the operating system supported by the UMS; see the "Supported Environment" section of the [release notes\(see page 565\)](#).

⚠ It is highly recommended to use only new servers for the HA installation, i.e. without the existing UMS installation.

- A database system supported by the UMS; see the "Supported Environment" section of the [release notes\(see page 565\)](#).
- All installation requirements described under [HA: Installation Requirements\(see page 660\)](#) are fulfilled.
- The required version of the UMS is downloaded from the [IGEL Download Server](#)¹⁴⁵.

⚠ Do not use the UMS version older than the version of the existing UMS installation!

Instructions

The switch from a standard UMS installation to an HA installation involves the migration of the existing UMS Server to a new host and, in the case of the embedded database, the move to the external database.

The migration procedure generally involves the following steps:

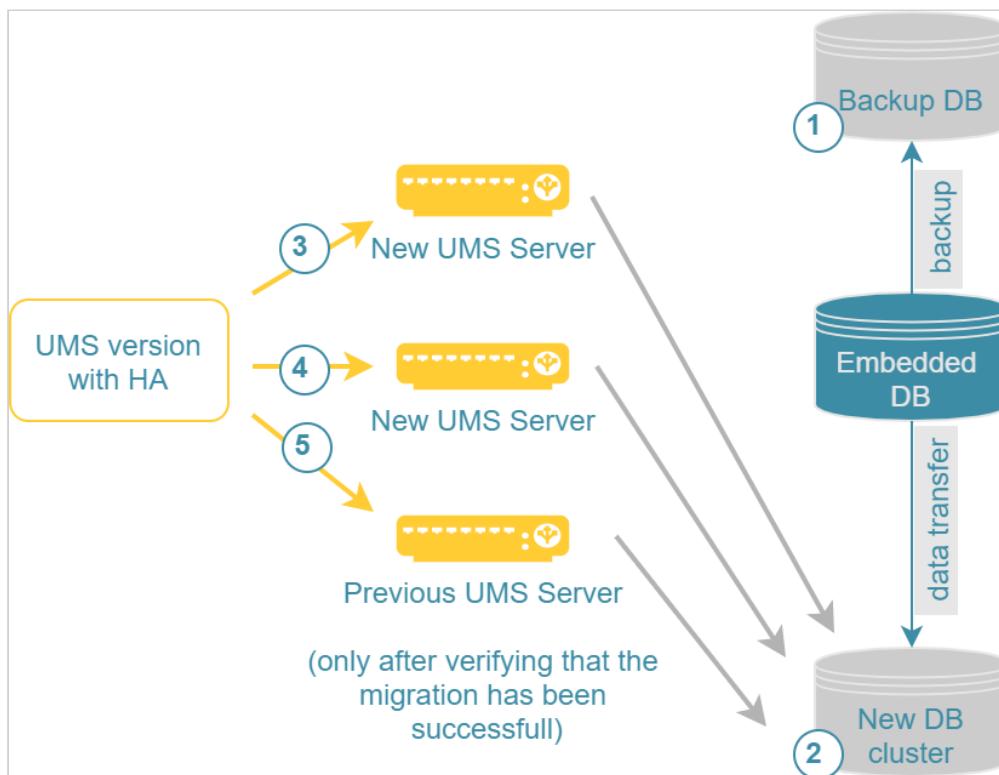
1. Backing up and, if necessary, cleaning existing data
2. If the embedded database is in use: Setting up an external database and transferring the data from the existing database to the new one
3. Installing the first HA server with the `tc.keystore` file of the previous UMS installation, connecting it to the external database and transferring the files from the previous UMS installation

✓ For the first HA server, take a new host machine, i.e. without the existing UMS installation. After you make sure that the migration has been successful, you can uninstall the old UMS Server and reinstall it with the HA extension.

¹⁴⁵ <https://www.igel.com/software-downloads/workspace-edition/>

4. Adding further components to the HA network, e.g. further UMS Servers, Load Balancers, UMS Console

Example with an Embedded DB



Detailed instructions are provided below. Follow them in the order given:

- Preparing the Migration(see page 681)
- Setting Up the New Database and Transferring Data (If the Embedded DB is in Use)(see page 683)
- Installing the First HA Server and Transferring the Data from the Existing UMS Server(see page 684)
- Installing Further HA Components(see page 687)

Preparing the Migration

Preparing New Servers

1. Verify that each server can "see" the other servers via the network.

⚠ All UMS Servers and UMS Load Balancers must reside on the same VLAN. Network traffic must be allowed over UDP broadcast port 6155, and TCP traffic and UDP broadcast traffic over port 61616. For more information on UMS ports, see [UMS Communication Ports](#)(see page 48). Note: IGEL UMS Server HA is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks.

2. Verify that the time on all servers is synchronized.



⚠ To avoid problems with your HA installation, make sure that the time on the servers of the HA network does not differ by more than one minute. After each manual time reset, the HA services on the relevant server must be restarted.

3. For Linux systems, make the directory /root writable for the user root.

Preparing the Existing System

Tip

The move provides an opportunity to remove any UMS database data which are no longer used. For example, you can

- delete endpoint devices that no longer exist
- delete profiles that are no longer used
- remove files and firmware updates that are no longer needed

It is highly recommended to create a backup before carrying out the cleanup (as a backup of the system running) and another one after the cleanup.

1. Create a backup before performing the move:
 - For the embedded database: Create a backup using the UMS Administrator tool, see [Creating a Backup](#)(see page 536). Include all options in the backup.
 - For external database systems: Use the backup procedures recommended by the DBMS manufacturer. For the backup of server configurations, use the UMS Administrator tool, see [Creating a Backup](#)(see page 536).
2. Save the following files, e.g. to a storage medium that can be accessed during UMS HA installation:

Certificates	<ul style="list-style-type: none"> • [IGEL installation directory]/rmtcserver/* It includes the tc.keystore file, which is necessary for the communication with the endpoint devices. The certificate of this keystore can also be exported via the UMS Console under UMS Administration > Global Configuration > Certificate Management > Device Communication > Export key pair
Device licenses (up to UMS 6.07; as of UMS 6.08, licenses are included in the database)	<ul style="list-style-type: none"> • [IGEL installation directory]/rmclient/cacerts • [IGEL installation directory]/rmguiserver/https_cert_chain.keystore • [IGEL installation directory]/rmguiserver/webapps/e08ce61-d6df-4d2b-b44a-14c1ec722c44

**Files and
firmware
updates**

- [IGEL installation directory]/rmguiserver/webapps/ums_filetransfer

3. Create a backup of the UMS Licensing ID using the UMS Administrator tool. For detailed instructions, see [Transferring or Registering the UMS Licensing ID](#)(see page 106).

Next Step

>> If you use the embedded database: [Setting Up the New Database and Transferring Data \(If the Embedded DB is in Use\)](#)(see page 683)

>> If you use the external database: [Installing the First HA Server and Transferring the Data from the Existing UMS Server](#)(see page 684)

Setting Up the New Database and Transferring Data (If the Embedded DB is in Use)

- i** The following steps are only required if your current UMS installation uses an embedded database.

If you use the embedded database, you have to move its data to the external database before you start with the installation of the first HA server.

1. Create a database schema and a user for the UMS. Use the relevant DBMS program and its documentation. See also [Connecting External Database Systems](#)(see page 289).
2. Open the UMS Administrator on the existing UMS Server.

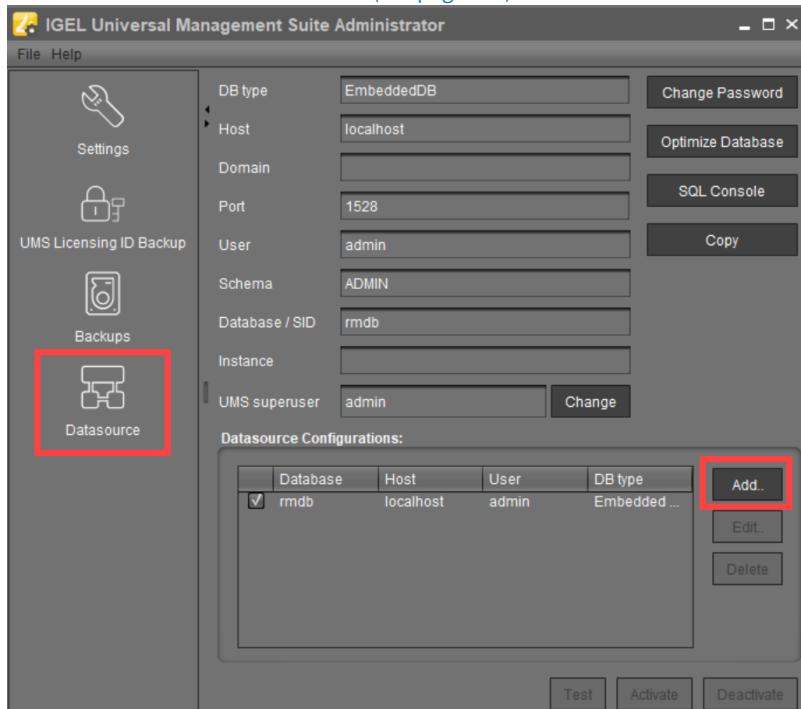
- i** Default path to the UMS Administrator:

Linux: /opt/IGEL/RemoteManager/RMAdmin.sh

Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe



3. Add the new database connection under **Datasource > Add**. See also [How to Set Up a Data Source in the IGEL UMS Administrator](#)(see page 543).



4. Select the embedded database (active datasource) and click **Copy** to copy its contents to the new database.
 5. Select the new database and click **Activate**. See also [Activating a Data Source](#)(see page 546).
 Now, the external database is set up as a datasource for your UMS.

For a concrete example of how to switch to an external database, see [Migrating a UMS Database From Embedded DB to Microsoft SQL Server](#)(see page 112).

Next Step

>> [Installing the First HA Server and Transferring the Data from the Existing UMS Server](#)(see page 684)

Installing the First HA Server and Transferring the Data from the Existing UMS Server

When all preparation steps have been made, you can start the migration.

Installing the First HA Server

► Start the UMS High Availability (HA) installation. For the instructions, see the "Starting the Installation" section under ["Installing the First Server in an HA Network"](#)(see page 663).

When asked for the keystore, use the file [IGEL installation directory]/rmtcserver/tc.keystore of the existing UMS installation:

**Import existing keystore (optional)**

Select a keystore file you want to use continuously



If you have been using the IGEL UMS, you can now import the 'tc.keystore' file for future usage. The communication with your Thin-Clients will work without further modifications, then.

Keystore file ('tc.keystore'):

[Browse...](#)**Transferring the Data from the Old UMS Server**

- Copy the files from the following folders to the new server – without the WEB-INF folder:

- [IGEL installation directory]/rmguiserver/webapps/ums_filetransfer

(i) Universal Firmware Updates

If you have used the UMS's integrated webserver to distribute the firmware updates, the updates that are still required should be manually transferred to the new server or the FTP server (if you configure it as the destination for the update files, see [Universal Firmware Update\(see page 493\)](#)). See also [How to Detect Which Files Are Synchronized Automatically\(see page 159\)](#).

Or you can simply download the required firmware updates anew.

- [IGEL installation directory]/rmguiserver/webapps/e08ce61-d6df-4d2b-b44a-14c1ec722c44 (only required if the old server has UMS version 6.07 or older)

Defining the Database Connection

1. Stop the Windows service IGEL_RMGUIServer on the old UMS Server.
2. Open the UMS Administrator on the HA server.

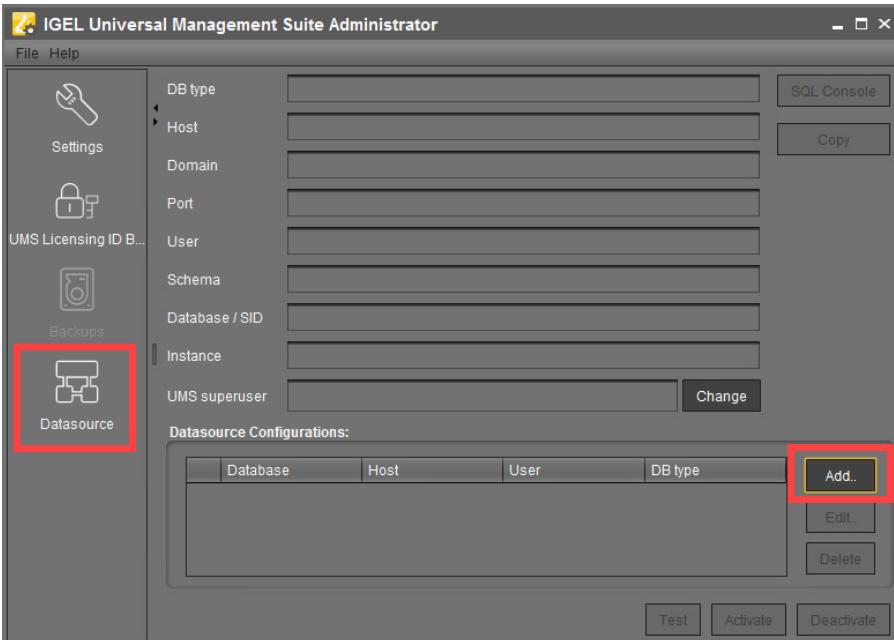
(i) Default path to the UMS Administrator:

Linux: /opt/IGEL/RemoteManager/RMAdmin.sh

Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe



3. Select **Datasource > Add**.



4. Enter the connection properties of the prepared database. See also [How to Set Up a Data Source in the IGEL UMS Administrator](#)(see page 543).
5. Click **Activate** to enable the data source. See also [Activating a Data Source](#)(see page 546).
The UMS Server will start automatically after that.

Checking the Installation

1. Check if all processes are running. For the list of UMS HA processes, see [HA Services and Processes](#)(see page 691)
2. In the UMS Console, go to **UMS Administration > UMS Network** and check the items **Server** and **Load Balancer** if the complete UMS HA Extension has been selected for installation. Check if there is an entry for the previous UMS Server among the listed components. If so, delete it.

Server		Server		
	UMS Administration	Process ID	Process Name	Timestamp
		fa86e615-1d0c-4f79-a44d-39e4...	td-ums-srv2012	01.10.2020 16:15
				Service is running
				Normal Mode

Transferring or Registering Your UMS Licensing ID

- Transfer the UMS Licensing ID of the previous UMS installation to the new server. Alternatively, you can register the new UMS Licensing ID, which was created during the installation of the HA server. For detailed instructions, see [Transferring or Registering the UMS Licensing ID](#)(see page 106).



Adjusting DHCP Tag and DNS Alias

- Adapt, if necessary, the **DHCP Tag** and the **DNS Alias** `igelrmserver` with the IP or FQDN of the new UMS Server. See [Registering Devices Automatically](#)(see page 312).

- i** The configuration of the DHCP tag and the DNS alias is not a setting that can be made within the IGEL software. You must configure these within your individual network environment on the corresponding DHCP and DNS servers.

Next Step

>> Proceed with installing the other components, i.e. further UMS Servers, UMS Load Balancers, or UMS Console: [Installing Further HA Components](#)(see page 687).

Installing Further HA Components

After the first HA server is installed and the data has been moved to it, you can install further components, i.e. further UMS Servers, Load Balancers, UMS Console.

1. Install further servers and check the installation. For the instructions, see [Adding Further Servers to the HA Network](#)(see page 667).
The data will automatically be synchronized between the HA servers, see [How to Detect Which Files Are Synchronized Automatically](#)(see page 159).
2. After all UMS Servers have been installed, update the host assignment for job execution. For the instructions, see [Updating Host Assignment for Job Execution](#)(see page 111).

- i** If you have used and adjusted the DNS alias and the DHCP option, the following step is NOT required since the device can resolve the name `igelrmserver` correctly.
In the local configuration, the device always remembers the IP of the UMS Server of its first registration. It is thus possible that the old IP address is displayed under **System > Remote Management**. Therefore, it makes sense to manually set an entry for remote administration after the migration:
 1. Create a profile in the UMS:
 - Go to **System > Remote Management** and click **Add**.
 - Under **UMS Server**, enter the IP of the new UMS Server.
 2. Apply this profile globally, to the entire structure.

5.1.6 Licensing the High Availability Extension

With the IGEL OS 11 Licensing Model

The High Availability Extension is included in the Workspace Edition and does not require an additional license.



Before IGEL OS 11

The High Availability Extension comes in packages of 50 licenses. These licenses are installed in the UMS. The UMS checks if the number of licenses is at least as high as the number of devices connected to the UMS.

Each version of the IGEL UMS contains five test licenses allowing you to evaluate the function free of charge and without having to register.

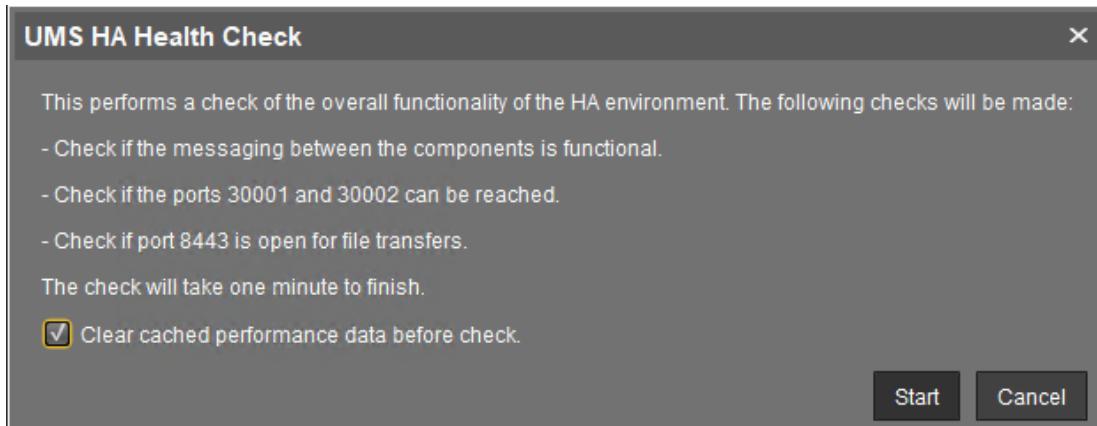
- ▶ Register the license file you receive in the UMS Console under **UMS Administration > Global Configuration > Licenses > UMS Licenses**.

- ⓘ An HA network only works with a license covering all managed devices registered in the UMS. A mixed mode (devices with HA support and devices without HA support) is not possible.

5.1.7 UMS HA Health Check

Menu path: Menu bar > **Help > UMS HA Health Check**

As of UMS version 6.05.100, you can perform an overall check of your High Availability environment with the **UMS HA Health Check** feature. It checks whether the interaction between the components of the HA system is working properly, in particular, whether the components can exchange messages and data:



- ⓘ The permission to use the **UMS HA Health Check** feature can be set under **System > Administrator accounts**, see [General Administrator Rights](#)(see page 512).

To check your HA environment:

1. Make sure the servers and the components installed on them are in normal operational mode.
2. In the menu bar, go to Help > **UMS HA Health Check**.
3. Disable the checkbox **Clear cached performance data before check** if you want the cached data from previous runs to be included in the analysis.

After the necessary data are collected and analyzed, a window opens where the results and corresponding recommendations are presented in a number of tabs. Each tab has a **Show Details** button that opens a detailed analysis report in HTML format. The description of each tab and the



HTML report can be found below.

UMS HA Health Check

Messaging	WebDav	Port 30001	Port 30002	Certificates	More Checks
Checked					
UMS GUI Server@HEX-02: - UMS GUI Server@HEX-01:					Transfer time 541ms OK
UMS GUI Server@HEX-02: - Load Balancer@HEX-02:					Transfer time 31ms OK
UMS GUI Server@HEX-02: - Load Balancer@HEX-01:					Transfer time -522ms OK
UMS GUI Server@HEX-02: - Watchdog@HEX-02:					Transfer time 734ms OK
UMS GUI Server@HEX-02: - Watchdog@HEX-01:					Transfer time 369ms OK
UMS GUI Server@HEX-01: - UMS GUI Server@HEX-02:					Transfer time 991ms OK
UMS GUI Server@HEX-01: - Load Balancer@HEX-02:					Transfer time 1209ms OK
UMS GUI Server@HEX-01: - Load Balancer@HEX-01:					Transfer time 610ms OK

Show Details **Next Tab** **Ok** **Cancel**

Messaging

This check detects whether the components are running and can exchange messages. It performs a ping test between the components of the HA installation on each server. The list shows the result with the indication of the transfer time for each combination of the components.

UMS HA Health Check

Messaging	WebDav	Port 30001	Port 30002	Certificates	More Checks
Checked					
UMS GUI Server@HEX-02: - Watchdog@HEX-01:					Transfer time -24ms OK
UMS GUI Server@HEX-01: - UMS GUI Server@HEX-02:					Transfer time 149ms OK
UMS GUI Server@HEX-01: - Load Balancer@HEX-02:					No messaging connection available Check firewall and the ti...
UMS GUI Server@HEX-01: - Load Balancer@HEX-01:					Transfer time 31ms OK
UMS GUI Server@HEX-01: - Watchdog@HEX-02:					Transfer time 103ms OK
UMS GUI Server@HEX-01: - Watchdog@HEX-01:					Transfer time 0ms OK
Load Balancer@HEX-02: - UMS GUI Server@HEX-02:					No messaging connection available Check firewall and the ti...
Load Balancer@HEX-02: - UMS GUI Server@HEX-01:					No messaging connection available Check firewall and the ti...

Show Details **Next Tab** **Ok** **Cancel**

The reasons why messaging between components is not possible are usually the following:

- One of the components is not running at all.



- The necessary ports, 61616 and 6155, are not open in the firewall. See [UMS Communication Ports](#)(see page 48).
- The system time on the servers differs a lot.
 - ⚠ To avoid problems with your HA installation, make sure that the time on the servers of the HA network does not differ by more than one minute. After each manual time reset, the HA services on the relevant server must be restarted.
- The IGEL network token differs between the components. For example, this can happen due to the generating of a new IGEL network token, instead of using the network token initially created during the installation of the first UMS Server when further UMS Servers / UMS Load Balancers are installed within a HA network.

WebDav

This check examines whether the UMS Servers can exchange files via WebDav.

Possible reasons for failure are the following:

- One of the components is not running at all.
- WebDav port 8443 is not open in the firewall.

Port 30001

Port 30001 is used for connections between the devices and the UMS Load Balancer. As the test cannot mimic a device, the UMS Servers try to connect to the UMS Load Balancer via port 30001.

Possible reasons for failure are the following:

- One of the components is not running at all.
- Port 30001 is not open in the firewall.

Port 30002

Port 30002 is used by the UMS Load Balancer for forwarding requests from the device to the UMS Server.

Possible reasons for failure are the following:

- One of the components is not running at all.
- Port 30002 is not open in the firewall.

Certificates

This check compares the certificates stored on the UMS Server with those stored on the UMS Load Balancer.

A possible reason for failure can be the following:

- Failure in communication between the components due to the differing IGEL network tokens, see the above section "[Messaging](#)(see page 690)".



More Checks

If other problems are detected, the corresponding results and recommendations are displayed here.

Detailed Report

A detailed report generated in HTML format upon the click on the **Show Details** button provides some additional information.

Tip for Contacting IGEL Support

If the recommendations provided did not help to resolve the problems, save the HTML report and send it to IGEL Support together with the archive with the support information, which can be created in the menu bar under **Help > Save support information**.

Roles: Based on the results, the check shows which roles are possible for the servers of the HA environment.

Example:

Process ID	Host	Roles
45ae09c1-4445-4cel-a7a9-0125d353a480	HEX-01	[WebdavServer, Server, HA, LoadBalancer, WebdavClient, Client]
f427828d-fe9b-4445-abea-0b42382dee35	HEX-02	[WebdavServer, Server, HA, LoadBalancer, WebdavClient, Client]
ums-broker-49951-1592214135973-0-0	HEX-01	[Server, HA, LoadBalancer, Client]
ums-broker-49993-1592214726620-0-0	HEX-02	[Server, HA, LoadBalancer, Client]
ums-watchdog-49953-1592214138113-1-0	HEX-01	[Server, HA, LoadBalancer]
ums-watchdog-49995-1592214730651-1-0	HEX-02	[Server, HA, LoadBalancer]

Config Info: Shows the configuration information as provided by the processes. For a UMS Load Balancer, i.e. UMS broker process, the known servers of this Load Balancer are shown.

Process Info: Provides an overview of the processes.

Certificate Fingerprints: Shows fingerprints of the certificates stored in the database on the UMS Server and the tc.keystore file on the UMS Load Balancer.

5.1.8 HA Services and Processes

A High Availability (HA) installation consists of several processes: Each node of the HA network has either the UMS Server or the UMS Load Balancer or both running, depending on the configuration you have chosen during the installation process of the UMS HA, see also [Configuration Options\(see page 658\)](#). In addition, the UMS Watchdog always runs on each node.

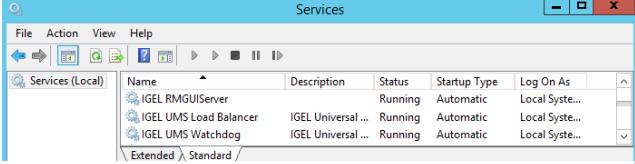
UMS Server	<ul style="list-style-type: none"> Handles all requests from the devices and the UMS Console. Talks to the devices. Executes jobs. Acts as a message broker for internal messages.
UMS Load Balancer	<ul style="list-style-type: none"> Forwards incoming requests from the devices to one of the UMS Servers with load balancing.



	The UMS Load Balancer has a list of running UMS Servers and distributes the requests to them sequentially.
UMS Watchdog	<ul style="list-style-type: none"> Monitors the run status of the UMS Server and the UMS Load Balancer running on the same server and forwards it to the UMS Servers. Starts or stops the UMS Server or the UMS Load Balancer on request from a UMS Server.

⚠ If both the UMS Server and the UMS Load Balancer are running on the same server, the UMS Server uses port 30002 and the UMS Load Balancer uses port 30001. If only the UMS Server is installed on a server, it always listens on port 30001. See [UMS Communication Ports](#)(see page 48).

The following table shows how you can find out which HA processes are running and how/where you can stop or start them.

Windows	Linux
Services:	<ul style="list-style-type: none"> For the list of running processes, use the command: <code>sudo ps -ef grep RemoteManager</code> where RemoteManager is the last part of the installation path; Adjust it if the installation path is different.
	Each process has two entries on the list.
The processes are normally stopped here.	<ul style="list-style-type: none"> For stopping the processes, use: <code>sudo systemctl stop igel-ums-watchdog</code> <code>sudo systemctl stop igel-ums-broker</code> <code>sudo systemctl stop igel-ums-server</code>
Task Manager:	<ul style="list-style-type: none"> For stopping the processes if the stop with the init scripts does not function: <code>sudo kill -9 xxxx</code> where the ID of the process can be seen in the output of <code>sudo ps -ef grep RemoteManager</code>
Emergency stop if the process cannot be stopped in the Services .	
cmd / Command Prompt:	
<pre>sc queryex "IGELRMGUIServer" sc queryex "IGEL UMS Load Balancer" sc queryex "IGEL UMS Watchdog"</pre>	
Emergency stop if the process cannot be stopped in the Services :	
<ul style="list-style-type: none"> <code>taskkill /PID xxxx /F</code> where the PID can be seen in the output of <code>sc queryex "Name of the process"</code> 	



5.2 Shared Workplace (SWP)

SWP

IGEL Shared Workplace (SWP) allows user-dependent configuration using profiles created in the IGEL Universal Management Suite and linked to the AD user accounts. In the process, user-specific profile settings are passed on to the device along with the device-dependent parameters. You will find an overview of the parameters that can be individually configured for a user under [Parameters Configurable in the User Profile](#)(see page 697).

5.2.1 Licensing with IGEL OS 11

For use with IGEL OS 11 devices, Shared Workplace requires a valid license from the IGEL Enterprise Management Pack (EMP). This license must be present on every IGEL OS 11 device on which Shared Workplace is to be used. When the license expires, users will no longer be able to login to a Shared Workplace session.

5.2.2 Licensing with IGEL OS 10

For use with IGEL OS 10 devices, Shared Workplace requires an add-on license for Shared Workplace. This license must be present on every IGEL OS 10 device on which Shared Workplace is to be used. The license is perpetual.

5.2.3 Typical Uses for Shared Workplace

- Workstations used for shift work or in call centers, where different staff members at a workstation need their own individual settings, e.g. session types or mouse-button settings for right/left-handed operation.
- Roaming environments, where users frequently switch workstations, such as in hospitals and at service/ticket counters, checkouts, or reception areas. After a user has logged in, the endpoint device licensed for Shared Workplace automatically configures itself. It does this via the UMS server using the individual or group profile stored in the UMS database. These profiles can easily be assigned to a user with the help of the IGEL Universal Management console using a convenient drag-and-drop procedure.

i In environments with an increasing number of Shared Workplace workstations, IGEL recommends using the [UMS High Availability Extension](#)(see page 657). The high level of UMS server availability achieved ensures that users receive their user-specific profile at all times.

-
- [SWP Configuration in the UMS Console](#)(see page 694)
 - [Parameters Configurable in the User Profile](#)(see page 697)
 - [Display Configuration for Shared Workplace \(SWP\)](#)(see page 698)



5.2.4 SWP Configuration in the UMS Console

In order to be able to use IGEL Shared Workplace, the following requirements must be met:

- Users who are to be given a specific profile must be set up in a Microsoft Active Directory.
- Devices which are to allow user logins must have a license for the IGEL Shared Workplace function. This can be transferred to the devices via the IGEL UMS license management system.

i If a device has been given a license for IGEL Shared Workplace, this cannot be canceled. However, the function can be disabled via the list of available services in the device configuration. Login via IGEL Shared Workplace is then disabled.

- Although not absolutely necessary, the use of the [High Availability Extension](#)(see page 657) for the IGEL Universal Management Suite is recommended for larger installations. This will ensure a high level of availability for the user profiles in the network.

i If you use IGEL Shared Workplace with IGEL Universal Desktop WES 7, bear in mind that the default password "**user**" must be set for the default user "**user**", otherwise it will not be possible to log in.

See also [Display Configuration for Shared Workplace \(SWP\)](#)(see page 698).

In this chapter, you can learn about:

- [Linking an Active Directory](#)(see page 694)
- [Assigning a User Profile](#)(see page 695)
- [Enabling IGEL Shared Workplace on the Thin Client](#)(see page 696)
- [User login](#)(see page 696)
- [Logout and Change of User](#)(see page 697)

The priority of user-specific profiles is dealt with in [Order of Effectiveness of Profiles in Shared Workplace](#)(see page 353). See also [Order of Effectiveness of Profiles](#)(see page 351).

Linking an Active Directory

To link an Active Directory in the UMS, proceed as follows:

1. Click on **Active Directory** in the **UMS Administration** area.
2. Click on **Add**.
The **Add Active Directory / LDAP Service** mask will open.
3. Enter the **domain name** and the access data.
4. Confirm your settings by clicking on **OK**.
Your Active Directory will now feature in the list.



Server - dokumentation.igel.local

UMS Administration

- ▼ UMS Network
- Server
- ▼ Global Configuration
 - Administrative Tasks
 - Active Directory / LDAP Configuration
 - Universal Firmware Update
 - License Configuration

Active Directory / LDAP Domains

Domain Name	Domain Controller	Page Size
UMS.TEST	172.30.200.1	1000

- ⓘ Other LDAP servers (*Novell eDirectory, OpenLDAP* etc.) cannot be used for *IGEL Shared Workplace* user authentication purposes.

Assigning a User Profile

Go to your Active Directory in the UMS navigation tree under **Server > Shared Workplace User**.



You can browse it or search for it by using this symbol:

- ▶ Select an object within the AD structure.

You will need to authenticate yourself vis-à-vis the Active Directory in order to do so.

- ▶ Assign the desired user profile to this object:

Server>Shared Workplace User>[Active Directory]>[Object]

Server - 172.30.251.2

/Shared Workplace Users/IGEL.LOCAL/PM

Managed Service Accounts
Office Scan
PM
Presales / Sales
Printer
QS

Filter

Name	Type	Account
Computer	OU	
Gruppen	OU	
User	OU	

Assigned objects

Name
LX_Languages

As with thin clients, a number of individual profiles can be assigned. In this case, indirectly as well as directly assigned profiles will be taken into account.

- ⓘ Right-click the name of a user account, to see the profile settings of a special thin client.



Enabling IGEL Shared Workplace on the Thin Client

You can configure the settings for Shared Workplace from the UMS via a profile or directly in the setup of the relevant thin client.

1. Go to **Configuration > Security > Login > IGEL Shared Workplace**.
2. Enable the **IGEL Shared Workplace** function.
3. Define the **link for logging off** from the system (only for thin clients with IGEL Linux).

The screenshot shows the UMS Configuration interface for a thin client named "IGEL-00E0C54EE5CE". The left sidebar has a "Security" section expanded, with "Logon" selected. Under "Logon", "Shared Workplace" is highlighted. The main panel shows three icons: Smartcard, Active Directory/Kerberos, and Shared Workplace (which is selected). Below these are two checkboxes: "Activate IGEL Shared Workplace" (checked) and "Skip IGEL Shared Workplace login if UMS server is unavailable". A section titled "Logoff shortcut locations:" contains four checkboxes: "Enable in Start Menu" (checked), "Enable on Desktop", "Enable in Desktop Context Menu", and "Enable in Application Launcher".

User login

If you have a license, you can easily log in to a thin client with *IGEL Shared Workplace*:

1. Boot the thin client.
A login window will appear.
2. Log in with your AD login data.
You will receive the profile settings recorded for you from the UMS.

i The thin client configuration which is active for the user logged in is the result of cumulating all profiles which have been assigned either directly or indirectly to the thin client or the user. See also [Prioritization of Profiles](#)(see page 350).



Logout and Change of User

Windows Embedded Standard

- ▶ Log out via the start menu.

IGEL Universal Desktop Linux

Under Linux, you can set up the following logout options:

- ▶ In the **Application Launcher**, define where you will place the buttons for logging off.
- ▶ Under **Security > Login > IGEL Shared Workplace** in the IGEL Setup, define a hotkey for logging off.

5.2.5 Parameters Configurable in the User Profile

Not all parameters available in an item of firmware can be configured on a user-specific basis.

The system settings which cannot be configured effectively by a user-specific profile are described below.

- ⓘ The UMS does not check whether the settings are effective.

The device-specific system settings for the IGEL operating systems which **cannot be configured effectively** are listed below. No check takes place in the IGEL UMS.

- [Universal Desktop Linux](#)(see page 697)
- [Universal Desktop Windows Embedded Standard](#)(see page 698)

UD Linux Device-specific Parameters

The following system settings are **not** configurable in the user profile:

- Network settings including those for the network drives
- Screen configuration for IGEL Linux v5 to 5.05.100 and for IGEL Linux v4 to 4.13.100.

- ⓘ Depending on the hardware used, display errors may occur if the user changes the resolution or rotates the screen even under IGEL Linux from Release 4.14.100. See the How-To document [Display Configuration for Shared Workplace](#)(see page 698).

- Touchscreen configuration
- Update settings
- Security settings
- Remote management
- Customer-specific partition
- Server for background images



- ⓘ With IGEL version 10.03.500 or higher, background images and the custom wallpaper server can be defined for each individual user via Shared Workplace.

- Customer-specific bootsplash
- Browser plug-ins
- SCIM entry methods, however, these can be enabled on a user-specific basis
- Three-button mouse emulation
- Appliance Mode (VMware View, Citrix XenDesktop and Spice)

UD W7 Device-specific Settings

The following system settings cannot be configured in the user profile:

- Language, standards and formats
- Network settings including those for the network drives
- Active Directory login
- USB device configuration
- List of the available features and Windows Services
- Update settings
- Setup session
- User and security settings
- File Based Write Filter
- Energy options
- Remote management
- Appliance Mode (VMware View and Citrix XenDesktop)

5.2.6 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 depend 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])
```

5.3 Asset Inventory Tracker (AIT)



For details, see [View Asset Information](#)(see page 395).

5.4 IGEL Management Interface (IMI)

See the documentation on this page: [IGEL Management Interface \(IMI\)](#)¹⁴⁶

5.5 Universal Customization Builder (UCB)



- [UCB Reference Manual](#)(see page 700)

¹⁴⁶ <https://kb.igel.com/display/igelimi>



5.5.1 UCB Reference Manual

With the Universal Customization Builder (UCB), IGEL Windows Embedded firmware can easily and reliably be expanded and adapted to meet your needs. For example, you may choose to install local device drivers or special applications. You can even set important Windows registry keys without having detailed knowledge of Shell or Windows scripting.

IGEL Customization Builder is part of the IGEL Universal Management Suite (UMS) (Windows only).

- [Overview\(see page 700\)](#)
- [Partial Update for IGEL Devices with Windows Embedded Standard\(see page 700\)](#)

Overview

Typical Usage Scenarios

- Supplementing local apps: Rolling out applications for local operations, e.g. checkout software for retailers and other sector-specific software, on a centralized basis
- Upgrading device drivers: For sector-specific peripherals or original drivers
- Setting registry keys: Individually adapting Windows Embedded Standard
- Kiosk systems: Equipping devices with special local applications or software clients in order to operate them independently of the company network, e.g. as time recording terminals

Features

- Simple procedures for generating, packing and rolling out firmware expansion packages for IGEL Windows Embedded (partial update).
- Predefined templates: Task-oriented for typical application scenarios
- Debugging: Automatic package creation with syntax checks
- Automatic versioning within customization projects
- Support for the packages created available from the IGEL support team

Testing Required

Before distributing changes to your actual systems, it is important to test partial updates on one or more devices to ensure that they are stable and function correctly.

Partial Update for IGEL Devices with Windows Embedded Standard

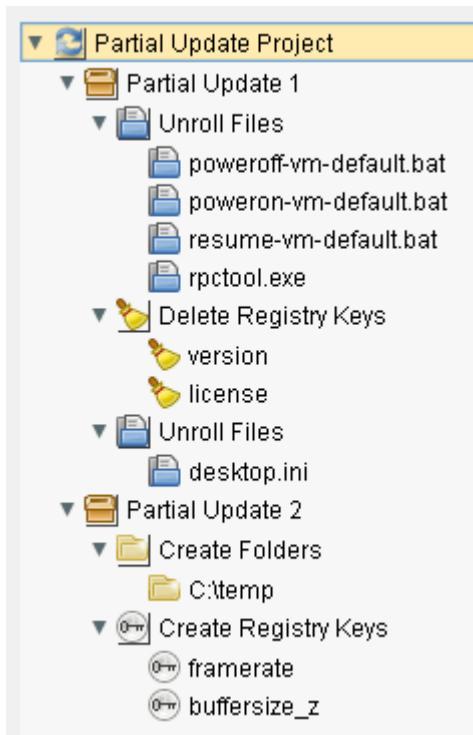
A partial update is a collection of tasks which are grouped together in a script. This script is sent to the devices together with the files that are to be distributed. The script is executed on the device and works through the pre-defined tasks.

Various tasks such as distributing files, setting up registry keys, executing commands and many others can be defined for a partial update. Similar tasks of the equivalent type are grouped together in sections. A project can



contain a number of partial updates with various sections and tasks. Using the import function, a number of partial updates can be brought together to form a project.

An example is shown here:



The following types of tasks (sections) are available in projects:

- Roll out file
- Create directory
- Set rights
- Delete file/directory
- Create registry key
- Roll out registry file
- Delete registry key
- Install application
- Execute command

When a project is being "built", all necessary scripts are generated and stored together with the required source files in a selectable project directory.

❗ Before distributing changes to your actual systems, it is important to test partial updates on one or more devices to ensure that they are stable and function correctly.

Project Functions

Launch the Universal Customization Builder in the UMS Console via **System > Universal Customization Builder**.

The following functions are available for a partial update project:

	<p>Create new project ([Ctrl+n])</p> <ul style="list-style-type: none">Opened projects are saved.The setup dialog opens.Enter a Project name.Select a Project directory for the project. A subfolder with this name will be created; this subfolder will contain all project files.Select Partial Update as the project type.Click OK.
	<p>Load project ([Ctrl+o])</p> <ul style="list-style-type: none">Opened projects are saved.The selection dialog opens.Select a project file (partial update project . ipu).Click Open.
	<p>Save current project ([Ctrl+s])</p> <ul style="list-style-type: none">Saves the project in its current state in the project directory.
	<p>Save current project as...</p> <ul style="list-style-type: none">The setup dialog opens.Enter a Project name.Select a Project directory for the project; a sub-folder bearing the project name and containing all project files will be set up in it.Click OK.A copy of the current project with all files will be saved under the new name in the selected directory.
	<p>Close current project ([Ctrl] + [0])</p> <p>The current project is saved and then closed.</p>
	<p>Import project ([Ctrl+i])</p> <ul style="list-style-type: none">The selection dialog opens.Select a project file (. ipu).Click Open.



	<ul style="list-style-type: none"> All parts of the selected project will be added to the current project.
	<p>Build project ([Ctrl+b])</p> <ul style="list-style-type: none"> The selection dialog opens. Select a destination directory for the partial update. Warning - All files in the destination directory will be deleted! Click Open. <p>All scripts and files to be sent to the device will be stored in the destination directory. Once the process has been completed successfully, the destination directory contains the finished partial update for distribution to the devices.</p>
	<p>Options</p> <p>Default project path: Select the URL of the current project path.</p>
	<p>Add new entity... ([Insert])</p> <ul style="list-style-type: none"> Sets up a new element depending on the current element type.
	<p>Delete entity... ([Delete])</p> <ul style="list-style-type: none"> Deletes the selected elements.
	<p>Move element upwards ([Page up])</p> <ul style="list-style-type: none"> Moves the selected element up one position.
	<p>Move element downwards ([Page Down])</p> <ul style="list-style-type: none"> Moves the selected element down one position.
	<p>Expand all entities</p> <ul style="list-style-type: none"> Opens all tree nodes.
	<p>Collapse all entities</p> <ul style="list-style-type: none"> Closes all tree nodes.

Transferring the Partial Update

To transfer partial updates to the system, proceed as follows:

- Launch the device configuration (locally or in the UMS).
- Select **System > Update > Partial Update**.
- Check the **Use IGEL Setup for configuring partial update settings** checkbox.
- Select a transfer **Protocol (HTTP, FTP, FILE)**.
- Specify the source server/path on the drive (destination directory for the partial update project).
- If necessary, enter the relevant login data.
- Click **Apply** to save the settings.
- Click **Search for Updates** in order to search the source for available updates (only locally on the device).



Available updates can then be installed directly. The device will reboot for this purpose. It will also reboot after the update has been installed.

In the UMS, you can launch the distribution of the partial update via the device's context menu (**Update & snapshot commands > Partial Update**) or set up a planned task that will perform the distribution on a scheduled basis.

5.6 Mobile Device Management Essentials (MDM)



⚠ MDM is not further developed by IGEL.

IGEL Mobile Device Management Essentials (MDM) is a feature introduced with UMS version 5.09.100 as a technical preview.

During the technical preview phase, only five devices can be managed simultaneously. This technical preview does not require licensing.

[MDM Basic Overview](#)(see page 704)

[MDM Setup Guide](#)(see page 715)

[Connecting Mobile Devices to the UMS](#)(see page 716)

5.6.1 Basic Overview

This guide gives an overview of how IGEL Mobile Device Management Essentials (MDM) lets you manage iOS mobile devices.

Configuring MDM in the UMS is detailed in the [MDM Setup Guide](#)¹⁴⁷.

Apple Push Notification Service (APNs)

The UMS and iOS mobile devices communicate with each other via the Apple Push Notification service (APNs).

Also, the IGEL Cloud Gateway (version 1.04.100 or higher) is required to provide a secure communication channel between the UMS and the iOS mobile devices connecting from outside the company network (see the [Communication Chart](#)(see page 707)).

¹⁴⁷ <https://kb.igel.com/display/endpointmgmt509/MDM+Setup+Guide>



The setup procedure can be outlined as follows:

1. Set up an ICG instance and connect it to the UMS, find detailed instructions in the [ICG Manual](#)(see page 704).
2. In the UMS, create a certificate-signing request for the Apple Push Certificates portal.
3. Log in with your Apple account to the Apple Push Certificates portal to generate a certificate for the UMS using the certificate-signing request.
4. Using the generated certificate, connect the UMS to the Apple Push Notification Service (APNs).
5. You are now ready start connecting iOS mobile devices to the UMS, this is also referred to as device enrollment.

For a detailed walk-through of these setup steps, see the [MDM Setup Guide](#)¹⁴⁸.

Connecting Devices

The iOS app **IGEL MDM Enrollment** is used to connect mobile devices to the UMS. The app is available free of charge from the app store.

For a detailed description of the device enrollment procedure, see [Connecting Mobile Devices to the UMS](#)(see page 716).

Managing Devices

New folder "Mobile Devices" in the UMS structure tree

Mobile devices that have been added to the UMS are listed in the new **Mobile Devices** folder.

Right-clicking on a mobile device listed there will open a context menu with object-specific commands.

The screenshot shows the UMS Administration interface. On the left, a tree view of the UMS structure includes categories like Master Profiles, Template Keys and Groups, Firmware Customizations, Thin Clients, and Mobile Devices (1). The 'Mobile Devices' category is expanded, showing a list containing 'iPhone8,2'. A red circle highlights the context menu options for this device, which are displayed on the right side of the screen. These options include Model Name, Organization Info, Build Version, Serialnumber, Last seen, Last command, and a Communication section with attributes like Phone Number, IMEI, MEID, ICCID, MAC (Ethernet), MAC (Wifi), MAC (Bluetooth), SIM Carrier Network, and Subscriber Carrier Network.

¹⁴⁸ <https://kb.igel.com/display/endpointmgmt509/MDM+Setup+Guide>



New profile type "Mobile Device" — mobile devices are manageable via profiles only

The new profile type "Mobile Device" has been introduced, since mobile devices are manageable via profiles only. The fact that you must use a profile to manage a mobile device means that, unlike with thin clients, double-clicking a mobile device object in the Mobile Devices folder will not open a configuration dialog; instead, you will have to create a profile and send the profile to the device or several devices.

In the **Profiles** folder of the UMS, mobile-device profiles can be distinguished from other types by the symbol.

- See [Creating Mobile Device Profiles](#)(see page 718).
- See [Sending Profiles to Mobile Devices](#)(see page 718).
- For general information on profiles, see [Profiles](#)¹⁴⁹.

5.6.2 MDM Manual

- [Prerequisites](#)(see page 706)
- [Supported Mobile Devices](#)(see page 706)
- [Communication Chart](#)(see page 707)
- [Supported Features](#)(see page 707)

Prerequisites

Prerequisites

- Universal Management Suite (UMS) 5.09.100 or higher
- IGEL Cloud Gateway (ICG) 1.04.100 or higher
- Any of the [supported mobile devices](#)(see page 706) with the IGEL MDM Enrollment iOS app installed

Supported Mobile Devices

The following iOS versions are supported:

- at least iOS 10.3
- iOS 11
- iOS 12.

The following mobile devices are supported:

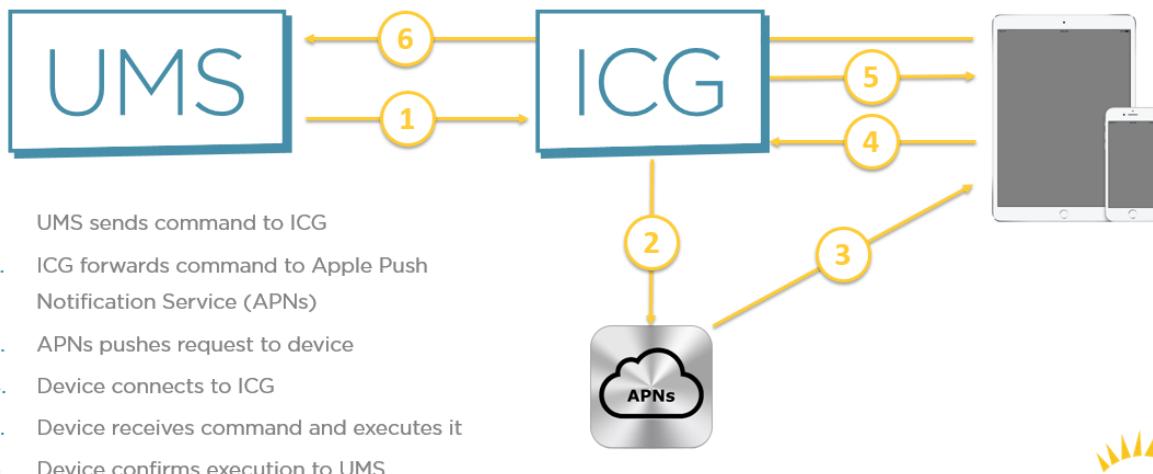
Device	Version(s)
Apple iPhone	5s and later
Apple iPad mini	2 and later
Apple iPad Pro	9.7 inch and later
Apple iPad Air	1 and 2

¹⁴⁹ <https://kb.igel.com/display/endpointmgmt/Profiles>



Communication Chart

The chart below shows the communication process between the UMS, the ICG, the Apple Push Notification Service and an iOS mobile device.



Supported Features

- i** Some features supported by IGEL MDM are only applicable if the device has been put into **supervised mode** beforehand with Apple's tools.
Please see next section which features require supervised mode.

- [Mobile Devices](#)(see page 707)
- [Context Menu](#)(see page 709)
- [Mobile Device Profile Settings](#)(see page 710)

Mobile Devices

Menu path: **UMS Console > UMS Administration > Global Configuration > Mobile Devices**

This section gives you an overview of the status of the IGEL Could Gateway (ICG) and its connection to the Apple Push Notification service.

Users can scan the QR code with the IGEL MDM App for iOS to enroll their devices. For more information, see [Connecting Mobile Devices to the UMS](#)(see page 716).



QR Code

- **Displayname:** The displayname
- **Host:** The host
- **Port:** The port
- **Apns Status:** Status of the connection to the Apple Push Notification service
- **Firmware available:** Shows if the firmware required for MDM is available
- **Enrollment URL:** The enrollment URL

Possible actions related to the QR code:

- **show:** Show the QR code in a separate window
- **send via email:** Send the QR code via email
- **save as jpg:** Save the QR code as JPG file
- **send as png:** Save the QR code

Apple iOS Devices

Menu path: **UMS Console > UMS Administration > Global Configuration > Mobile Devices > Apple iOS devices**

In this section, you can set up the required certificate for connecting the UMS to the Apple Push Notification Service. How you set up the certificate to connect the UMS with the Apple Push Notification Service is described in the [MDM Setup Guide](#)(see page 715).

You can perform the following actions:

Icon	Description
	Create a new certificate-signing request and save it as a *.csr file
	Open the Apple Push Certificate Portal at https://identity.apple.com in the system browser
	Import the Apple MDM Push Certificate (*.pem file)
	Create and save certificate-signing request for renewal



Icon	Description
	Show the certificate details of the Apple MDM Push Certificate
	Cut the certificate
	Delete the certificate

Status information:

Icon	Description
	Certificate successfully set up
	Waiting for certificate upload
	Incomplete / certificate error

You may further specify:

- **Enrollment profile displayname:** Displayname for the enrollment profile
- **Enrollment profile description:** Description of the enrollment profile
- **Adjust UMS-internal name with name on device**

Context Menu

Menu path: **UMS Console > Server [IP] tab > Mobile Devices > [mobile device]**

Right-click a mobile device icon in the UMS console navigation tree to open the context menu for the device.

- **Rename:** Give the device a new name
- **Delete:** Remove device from UMS
- **Copy:** Copy the device
- **Cut:** Cut the device
- **Access control:** Configure device permissions for UMS administrators
- **Clear 'Configuration Change Status' flag:** Resets configuration change flags (blue dot next to the symbols for the thin clients).
- **Send Configuration:** Sends the configuration of the UMS to the highlighted devices (this does not happen automatically!).
- **Refresh device information:** The system information will be refreshed.
- **Refresh security information:** The security information will be refreshed.
- **Device lock:** Locks the screen of the device.
- **Clear passcode:** Clears the existing passcode for the screen locker.



- **Shutdown** (Supervised only)
- **Restart** (Supervised only)
- **Reset to factory defaults:** Resets the device to factory defaults and erases its storage contents.

! **Warning**

Resetting the device to factory defaults will erase its storage contents.

- **Logging: Messages:** Opens the **Log Messages** window for messages.
- **Logging: Event Messages:** Opens the **Log Messages** window for event messages.

Mobile Device Profile Settings

- **i** Unlike thin clients, mobile devices can be configured only through profiles.

This section explains the settings available in a mobile device profile. They are also explained in the [Apple Profile Manager Help](#).¹⁵⁰

- [Restrictions](#)(see page 710)
- [Passcode](#)(see page 711)
- [Wi-Fi](#)(see page 711)
- [Mail](#)(see page 713)
- [Air](#)(see page 714)
- [System](#)(see page 714)

Restrictions

Menu path: **[mobile-device profile] > Restrictions**

- **i** Features marked as **(Supervised Only)** are only manageable if the device has been put into supervised mode.

Functionality

This page allows you to disable or enable various iOS features, very similiar to the **Settings > General > Restrictions** dialog on iOS.

Apps

Enable or disable select iOS apps such as iTunes or Safari. In supervised mode you can also create a whitelist OR a blacklist of apps, using their bundle identifiers, separated by semicolon.

Media

Set your region code and age ratings for movies, TV shows and apps.

¹⁵⁰ <https://help.apple.com/profilemanager/mac/5.3/?lang=en#/>



Passcode

Menu path: [Mobile device profile] > Code

In this area, you can change passcode settings.

- **Require Passcode on Device:** Enforce entering a passcode before using the device. (Default: enabled)
- **Allow Simple Values:** Permits users to use sequential or repeated characters in their passcodes. For example, “3333” or “DEFG”. (Default: enabled)
- **Require Alphanumeric:** Requires that the passcode contain at least one letter or number. (Default: disabled)
- **Minimum Passcode Length:** Specifies the minimum number of characters a passcode can contain.
- **Min Complex Chars:** Specifies the number of non-alphanumeric characters (such as \$ and !) the passcode must contain.
- **Maximum Passcode Age:** Requires users to change their passcode at the interval you specify. It can be set to --, or from 1 to 730 days.
- **Auto-Lock:** If the device isn’t used for the period of time you specify, it automatically locks. It can be set to --, or set to lock after 1 to 5 minutes. Enter the passcode to unlock the device.
- **Passcode History:** The device refuses a new passcode if it matches a previously used passcode. You can specify how many previous passcodes are remembered and compared. It can be set to --, or from 1 to 50 passcodes.
- **Grace Period for Device Lock:** Specifies how soon the device can be unlocked again after use, without reprompting again for the passcode.
- **Max Failed Attempts:** The number of failed passcode attempts that can be made before an iOS device is erased or locked.
If you don’t change this setting, after six failed attempts, the device imposes a time delay before a passcode can be entered again.
The time delay increases with each failed attempt. After the final failed attempt, all data and settings are securely erased from the iOS device. The device locks after the final attempt.
The passcode time delay begins after the sixth attempt, so if you set this value to 6 or lower, no time delay is imposed and the device is erased when the attempt limit is exceeded.

Wi-Fi

Menu path: [mobile-device profile] > Wi-Fi

Use the [+] icon to add a new Wi-Fi network.

Wifi Session

- **SSID:** Enter the SSID of the wireless network to connect to (must not contain spaces).
- **Hidden Network:** Defines if the network is hidden. (Default: Disabled)
- **Auto join:** Allow the device to automatically join the specified network. When this option is off, the user is asked to allow the connection. (Default: Enabled)
- **CaptiveBypass:** Users won’t have an opportunity to join networks that require agreements or other information prior to network access. (Default: Disabled)

Proxy



- **Proxy Type**
 - None
 - Manual: (Enter manually the connection details **Proxy Server**, **Proxy Server Port**, **Proxy Username** and **Proxy Password**)
 - Automatic: (Enter Proxy PacUrl). For Web Proxy Autodiscovery (WPAD) configurations leave the **Proxy Server URL** field empty, and the device will request the wpad.dat file using DHCP (via a 252 entry) or DNS (via an A Record with the name WPAD).
- **Proxy Server:** Hostname or IP of the server
- **Proxy Server Port:** Port of the server
- **Proxy Username:** Username of the server
- **Proxy Password:** Password of the server
- **Proxy PacUrl:** The proxy PAC URL
- **Proxy PAC Fallback allowed:** (Default: Disabled)

QoS

- **QoS Marking Policy:** You can restrict QoS marking, disable it, and approve specific apps for audio and video calls. Those apps must be configured to take advantage of QoS on Cisco corporate networks. You install this payload in a configuration profile which allows specific business apps to get priority. The Cisco network looks for these markings and provides the correlated service level. (Default: Disabled)
- **Allow QoS marking** (Default: Enabled)
- **QoS marking for audio/video calls** (Default: Disabled)
- **QoS Whitelisted Apps** (bundle identifiers, separated by semicolons) (Default: Disabled)

Network

- **Choose network type:**
 - standard
 - oldhotspot
 - passpoint
- **Displayed Operator Name:** Enter the name you want displayed for the Passpoint network.
- **Domain Name:** Enter the fully qualified domain name (FQDN) of the Passpoint service provider.
- **Roaming OIs:** HotSpot 2.0 organization identifiers
- **Roaming OIs:** Enter the six-digit hex code corresponding to one of the service provider's Passpoint network.
- **Real Names:** HotSpot 2.0 NAI real names (Default: Disabled)
- **Realm Names:** Enter the known Network Access Identifier (NAI) realm names.
- **MCC/MNCs:** HotSpot 2.0 MCC/MNCs
- **MCC/MNCs:** Enter the six-digit code combining the Mobile Country Code (MCC) and Mobile Network Configurations (MNC)
- **Roaming Enable:** Specify whether to connect to additional Passpoint networks pre-approved by the service provider. (Default: Disabled)

Security

- **Encryption Type:**
 - None
 - WEP
 - WPA



- WPA2
- Any: The network requires either WEP, WPA or WPA2 authentication when connecting to the network, but will not connect to non-authenticated networks.
- **Password:** Password for the network

Mail

Menu path: [mobile-device profile] > Mail

Use the [+] icon to add a new mail account.

- **Account Description:** Display name for the account
- **Account Type:**
 - EmailTypeIMAP
 - EmailTypePOP
- **Path Prefix:** Path prefix for the IMAP mail server.
- **Account Name:** Username on mail server
- **Email Address:** E-mail address
- **Prevent Move:** Mail messages cannot be moved between mail accounts. (Default: Disabled)
- **Disable Mail Recents Syncing:** Recently used addresses are not synced across devices. (Default: Disabled)
- **Allow Mail Drop:** Mail is not an option in the share sheet. (Default: Disabled)
- **Prevent App Sheet:** If set to true, this account will not be available for sending mail in third-party applications. (Default: Disabled)

Inbox

Menu path: [mobile-device profile] > Mail > [session name] > Inbox

- **Mail Server:** Hostname or IP address
- **Port:** Port number for incoming mail (Default: 993)
- **Username:** The username used to connect to the server for incoming mail
- **Incoming Mail Server Authentication:** The authentication method for the incoming mail server
Possible values:
 - None
 - Password
 - MD5 Challenge-Response
 - NTLM
 - HTTP MD5 Digest
- **Password:** The password for the incoming mail server authentication
- **Use SSL:** Defines whether incoming mail is received through an SSL-encrypted connection (Default: Enabled)

Outbox

Menu path: [mobile-device profile] > Mail > [session name] > Outbox

- **Mail Server:** Hostname or IP address
- **Port:** Port number for outgoing mail (Default: 587)
- **Username:** The username used to connect to the server for outgoing mail



- **Incoming Mail Server Authentication:** The authentication method for the outgoing mail server
Possible values:
 - None
 - Password
 - MD5 Challenge-Response
 - NTLM
 - HTTP MD5 Digest
- **Password:** The password for the outgoing mail server authentication
- **Outgoing Password Same as Incoming:** Defines if for SMTP authentication the same password is used as for POP/IMAP authentication. (Default: Disabled)
- **Use SSL:** Defines if mail is sent via an SSL-encrypted connection (Default: Enabled)

Air

Menu path: [mobile-device profile] > Air

AirPrint

- **Printer:** Use printers (Default: Disabled)
- **IP Address:** Enter IP addresses of printers, separated by semicolons
- **Resource Path:** Enter the resource paths corresponding to the IP addresses above, separated by semicolons

System

Menu path: [mobile-device profile] > System > Registry

In the registry, you can change firmware parameters directly.

 Changes to the registry should be made by experienced users only, because you can easily make misconfigurations.

- **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 want 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 **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.

5.6.3 MDM How-Tos

- [MDM Setup Guide](#)(see page 715)
- [Connecting Mobile Devices to the UMS](#)(see page 716)
- [Creating Mobile Device Profiles](#)(see page 718)
- [Sending Profiles to Mobile Devices](#)(see page 718)

MDM Setup Guide

Prerequisites

- UMS 5.09.100 or higher
- ICG 1.04.100 or higher

i You need an **Apple account** (Apple ID and password). If you do not have one, please create an account at <https://appleid.apple.com>.

This how-to explains the necessary steps to set up IGEL Mobile Device Management Essentials (MDM) in the UMS. Perform the steps in the given order.

Step 1: Import the iOS Firmware Metadata File

Import the iOS firmware metadata into the UMS:

1. Download **IGEL Firmware for iOS <version>.xml**.

⚠ MDM is not further developed by IGEL. Only the profile for enabling the management of devices with iOS 10.3 is available.
Direct download link: [IGEL Firmware for iOS¹⁵¹](#).

2. Start the **UMS Console**.
3. In the upper left, click **System** and select **Import ... > Import Firmwares**.
4. In the file chooser dialog, select the **IGEL Firmware for iOS <version>.xml** file.
5. Click **Open**.

The firmware will be imported. Upon success, a confirmation window will appear.

Step 2: Connect the UMS to the Apple Push Service

(1) Generate a certificate-signing request for the Apple Certificates Portal:

1. Start the **UMS Console**.
2. Go to **UMS Administration > Global configuration > Mobile Devices > Apple iOS devices**.
You will find the status message set to **Incomplete**.

¹⁵¹https://publicbuilds.blob.core.windows.net/files/IGEL_UNIVERSAL_MANAGEMENT_SUITE/MDM/IGEL%20Firmware%20for%20iOS%2010.3.11.xml.zip



3. Click the icon (**Create and Save Certificate Signing Request for MDM Apple Push Certificate**).

You will be prompted to save a *.csr file, which contains the generated certificate-signing request.

4. Save the *.csr file to a location you can remember.

When completed, the status message will change to **Waiting for upload of the Apple MDM Push Certificate**.

Now you need to create an Apple MDM Push Certificate and import it, as described in the next two steps (2) and (3).

(2) Generate an Apple Push Certificate in the Apple Push Certificates Portal:

1. Open the Apple Push Certificates Portal at <https://identity.apple.com/pushcert/> and log in with your Apple ID and password.
2. Click **Create a Certificate**.
3. Accept the **Terms & Conditions**.
4. Upload the certificate-signing request (*.csr file) which you created in step (1).
5. Download the resulting push certificate (*.pem file) to a location you can remember.

(3) Import the Apple Push Certificate in the UMS Console to connect the ICG with the Apple Push Service.



- Click the icon (**Import Apple MDM Push Certificate**) to import the MDM Apple Push Certificate into the UMS.

When the certificate was successfully imported, the status message will change to **Complete - Certificate expires at [date]**.

Via the ICG, the UMS will try to establish a connection to the Apple Push Service.

Info When the connection between the ICG and the Apple Push Service was successfully established, in the UMS, under **UMS Administration > Global configuration > Mobile Devices**, the **Appns Status** field will be **Connected**.

You are now ready to start connecting mobile devices to the UMS, see [Connecting Mobile Devices to the UMS](#)(see page 716).

Connecting Mobile Devices to the UMS

Prerequisites

- UMS 5.09.100 or higher
- Any of the devices listed under [Supported Devices](#)(see page 706)
- The IGEL iOS app IGEL MDM Enrollment must be installed on your device.

Info The **IGEL MDM Enrollment** app is available free of charge from the Apple App Store.



- The UMS must be connected to the Apple Push Service, see the [MDM Setup Guide](#)(see page 715).

This how-to explains the necessary steps to connect iOS mobile devices to the UMS using the IGEL Mobile Device Enrollment app.

Steps

To connect a mobile device to the UMS, proceed as follows:

1. Switch on your mobile device and start the **IGEL MDM Enrollment** app.

You will be presented with a screen to choose between **Scan QR-Code** and **Manual Input**:



2. Tap **Scan QR-Code**:

3. With your mobile device's cam, scan the QR code under **UMS Administration > Global Configuration > Mobile Devices**.

i If for any reason you cannot use your mobile device's cam, please use **Manual Input** and manually enter the connection details available under **UMS Administration > Global Configuration > Mobile Devices**. The required format is `https://[host or IP]:port`

4. Click **Enroll**.

Your device's default browser (usually Apple Safari) will open a link to automatically download the MDM profile file.

i When presented an HTTPS error, select **Show details > Visit website**.

5. Accept all warnings and allow installing the enrollment profile ("Remote Management").

i If you receive the error "Profile Installation Failed", see the troubleshooting article [Profile Installation Fails When Connecting Mobile Device to the ICG](#)(see page 718).



6. In the UMS Console, reload the navigation tree.
Your mobile device is now listed in the **Mobile Devices** folder.

Creating Mobile Device Profiles

This how-to assumes that you have set up IGEL Mobile Device Management Essentials (MDM). If not, see [MDM Basic Overview](#)(see page 704).

To create a mobile device profile, proceed as follows:

1. Right-click **Profiles** in the UMS structure tree; from the context menu, choose **New Mobile Device Profile**.
2. Enter a **Profile Name**
3. Enter a **Profile Description**
4. For **Based on**, choose **IGEL Firmware for iOS 10.3.x**
5. Click **OK**.
The settings window for the profile will open.
6. In the settings window, you can make settings and apply them immediately (send the configuration to mobile devices), or click **Save** and apply settings later.

For a general overview of UMS profiles, see [Creating Profiles](#)(see page 335).

Sending Profiles to Mobile Devices

This how-to assumes that you have set up IGEL Mobile Device Management Essentials (MDM). If not, see [MDM Basic Overview](#)¹⁵².

To send a profile to a mobile device, proceed as follows:

1. Assign a profile to a device by dragging and dropping the profile onto the mobile-device object in the **Mobile Devices** tree node.
2. Right-click the device and select **Send Configuration**.

5.6.4 MDM Troubleshooting

- [Profile Installation Fails When Connecting Mobile Device to the ICG](#)(see page 718)

Profile Installation Fails When Connecting Mobile Device to the ICG

Issue

You are trying to connect a mobile device to the UMS as described under [Connecting Mobile Devices to the UMS](#)(see page 716).

You can download the profile for MDM, but its installation fails.

¹⁵² <https://kb.igel.com/display/endpointmgmt509/Basic+Overview+MDM>



Solution

This issue occurs because you already installed a profile in the past.

When you try to install a new profile, the old one is not automatically overwritten.

You have to manually delete the old profile.

To do this, on your mobile device, go to **Settings > General > Device Management** and delete the old profile.



6 UMS Web App

The UMS Web App is a web-based user interface to the UMS Server, introduced with Universal Management Suite version 6.05.100. The installation of the UMS Web App is optional and handled via the [UMS installer](#)(see page 260).

As an early feature set, the UMS Web App can now be used only in addition to the Java-based [UMS Console / UMS Web App](#)(see page 257).

A currently limited range of functions will constantly be expanded. The main features include:

- configurable search functionality
- managing the directory tree and moving devices
- shadowing of devices and various device commands (power control, update, sending/receiving settings, reset to factory defaults, etc.)
- assigning objects to devices and directories
- managing the profile directory tree and editing profile properties
- monitoring the status of the UMS network
- logging of actions performed in the UMS Web App

The UMS Web App and the UMS Console share the same database, user rights, and certificates.

- Changes made in the UMS Console are immediately available in the UMS Web App, and vice versa. They are searchable after the next reindexing, which is executed every hour.

- [Basic Overview](#)(see page 721)
- [Important Information](#)(see page 727)
- [Installation](#)(see page 729)
- [Supported Environment](#)(see page 731)
- [How to Log In to the IGEL UMS Web App](#)(see page 732)
- [UMS Web App Manual](#)(see page 732)

6.1 Video

See also the video illustrating the basic UMS Web App features.



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=wV_lhRa-2D8&feature=youtu.be



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

<https://www.youtube.com/watch?v=-hsI5W9PTuE&feature=youtu.be>



6.2 Basic Overview

These are the basic features currently implemented for the UMS Web App.

6.2.1 Devices

1

Directory Tree

Devices (2)

- Augsburg (2)
- techdoc (2)
- RD (2)**

Bremen (0)

2

RD

Filter objects

Name
td-RD01
td-RD02

3A

RD

Assign object Reboot Shutdown Wake up

Properties

Name: RD Number of contained devices: 2

Directory Path: Devices / Augsburg / techdoc / RD

4

Screensaver

11.04.100.rc9.01

1

Directory Tree

Devices (2)

- Augsburg (2)
- techdoc (2)
- RD (2)**

Bremen (0)

2

RD

Filter objects

Name	Unit ID	MAC Address
td-RD01	05641000E583142622	UC5-LX
td-RD02	00E0C520986A	UD3-LX 51

3B

td-RD02

Shadow Assign object Reboot Shutdown

Properties

Name: td-RD02 Unit ID: 00E0C520986A MAC Address: 00E0C520986A

Last IP: Product: IGEL OS 11

Version: 11.05.100.01 Last Contact: Jul 8, 2021, 10:23 AM

Directory Path: Devices / Augsburg / techdoc / RD

Custom Properties

Department: DeviceAttribute_Subdepartments

Technical Documentation: KB

4

3B

3B

3B

1 Directory Tree

Shows all created directories.

- Creating new directories
- Renaming directories
- Deleting empty directories
- Moving directories: drag & drop or [Ctrl + X], [Ctrl + V]
- Copying directories: [Ctrl] + drag & drop or [Ctrl + C], [Ctrl + V]



		<ul style="list-style-type: none"> Moving devices to another directory: drag & drop Bulk actions (for all devices in the selected directory)
2	Device list	<p>Shows all devices directly contained in the directory selected in the Directory Tree.</p> <ul style="list-style-type: none"> Filtering devices by Name, Product ID, Unit ID, Version, and IP Address Sorting devices by Name, Product ID, Unit ID, Version, and IP Address Paging for the navigation in the device list Defining the number of devices to be displayed on one page
3A	Directory information	<p>Shows details and assigned objects for the directory selected in the Directory Tree.</p> <ul style="list-style-type: none"> Filtering the assigned objects by the object type, direct / indirect type of assignment, free text entry Detaching directly assigned objects
3B	Device information	<p>Shows details for the device selected in the device list.</p> <ul style="list-style-type: none"> The status of the device (online, offline, unknown) Renaming the device (Advanced) system information <ul style="list-style-type: none"> Adding / editing / deleting customizable system information, incl. device attributes License information, user login history Assigned objects <ul style="list-style-type: none"> Filtering the assigned objects by the object type, direct / indirect type of assignment, free text entry Detaching directly assigned objects Jumping to the assigned profile / master profile
4	Device commands	<p>Executed for the selected individual directory / device.</p> <ul style="list-style-type: none"> Power control commands (reboot, shutdown, suspend, wakeup) Shadowing (VNC), secure shadowing, shadowing over ICG Updating, sending / receiving settings, etc. Assigning objects, e.g. profiles, firmware updates, etc.
	Messages	<p>Shows information regarding the successful or unsuccessful execution of commands.</p> <ul style="list-style-type: none"> Automatically deleted at the reloading of the page in the browser



6.2.2 Search

1	Configurable search mask	<ul style="list-style-type: none"> Adding/removing search parameters. Search criteria are linked with logical AND. The last search configuration is saved.
2	Configurable search result list	<ul style="list-style-type: none"> Selecting device properties to be displayed by adding / removing columns (Table View) Sorting devices Paging
3	Export Data	Exporting search results in a CSV format
4	Search tags	Show the search parameter values specified in the search mask
5	Table View	The devices found are presented in the table form.



		<ul style="list-style-type: none">• Adding / removing columns• Paging for the navigation in the search result list• Defining the number of devices to be displayed on one page• Sorting within any selected column
	Card View	<p>The devices found are presented in the card form.</p> <ul style="list-style-type: none">• Collapsible / expandable device cards• Paging for the navigation in the search result list• Defining the number of devices to be displayed on one page• Sorting devices by Name, Product ID, Unit ID, Version, and IP Address <p>For each selected device, device information and device commands are shown.</p>



6.2.3 Configuration

1	Configuration Tree	<p>Shows all created profile directories and subdirectories.</p> <ul style="list-style-type: none"> Creating new directories Renaming directories Deleting empty directories Moving directories: drag & drop or [Ctrl + X], [Ctrl + V] Moving profiles to another directory: drag & drop
2	Profile list	<p>Shows all profiles contained in the directory selected in the Configuration Tree.</p> <ul style="list-style-type: none"> Filtering profiles by Name and Version Sorting profiles by Name and Version Paging for the navigation in the profile list Defining the number of profiles to be displayed on one page



3	Directory information	Shows details for the directory selected in the Configuration Tree .
4	Profile information	Details for the profile selected in the profile list <ul style="list-style-type: none"> Editing profile properties, e.g. profile name, firmware version it is based on, etc.
A	Activated Settings	Shows all configuration settings activated in the selected profile.
B	Template Key Relation	Shows template keys used in the profile.
C	Contained Files	Shows all files assigned to the selected profile. <ul style="list-style-type: none"> Quick assignment of the file to the selected profile Detaching assigned files from the profile
D	Assigned Devices	Shows all devices the selected profile is assigned to. <ul style="list-style-type: none"> Quick assignment of the device / device directory to the selected profile Detaching the device / device directory from the profile Jumping to the assigned device

6.2.4 Network

The screenshot shows the IGEL UMS 6 interface with the following numbered elements:

- 1: A list of available UMS Servers, UMS Load Balancers, and IGEL Cloud Gateways (ICG).
- 2: A detailed view of the selected UMS Server (192.168.30.110) showing its state as "running".
- 3: A detailed view of the UMS Server Details for the selected server.
- 4: A line graph titled "Requests" showing successful, waiting, and failed requests over time.

1 List of all available UMS Servers / UMS Load Balancers / IGEL Cloud Gateways (ICG)



2	<ul style="list-style-type: none"> Status of the selected UMS Server / UMS Load Balancer / IGEL Cloud Gateway (running, not running, unknown) Status of UMS Server / ICG connections (connected, disconnected, unknown) Number of currently connected devices (only for the ICG)
3	Details for the selected UMS Server / UMS Load Balancer / IGEL Cloud Gateway
4	Statistics for the device requests

6.2.5 Logging

The screenshot shows the UMS Web App interface with the 'LOGGING' tab selected. On the left, there is a search panel with fields for Logtime, Severity, Username, Category, Action, Message, and Name of the Affected Object. The main area displays a table of log entries with columns for Logtime, Username, Severity, Category, Action, Name of the Affected Object, Message, and Origin. The log entries show various system actions such as Device assignments, shutdowns, and URL file attachments.

Logtime	Username	Severity	Category	Action	Name of the Affected Object	Message	Origin
11/4/20, 4:14:07 PM	ike	Information	Assignment	Device: assign / detach template ...	td-RD02	Template value Language EN wa...	Webapp
11/4/20, 1:22:28 PM	ike	Information	Assignment	Directory: assign / detach url file	RD	URL file https://\$serverhostname...	Webapp
11/3/20, 8:03:24 PM	ike	Information	Assignment	Directory: assign / detach url file	RD	URL file https://\$serverhostname...	Webapp
11/3/20, 8:00:30 PM	ike	Information	Device	Shutdown	td-RD02	OK	Webapp
11/3/20, 3:35:52 PM	ike	Information	Assignment	Device: assign / detach template ...	td-RD02	Template value Language EN wa...	Webapp
11/3/20, 3:35:38 PM	ike	Information	Assignment	Device: assign / d	Device: assign / detach template value	URL file https://\$serverhostname...	Webapp
11/3/20, 3:34:39 PM	ike	Information	Assignment	Device: assign / detach url file	td-RD02	URL file https://\$serverhostname...	Webapp
11/2/20, 7:48:18 PM	ike	Information	Device	Shutdown	td-RD04	OK	Webapp

1	Configurable search mask	<ul style="list-style-type: none"> Adding/removing parameters for log searching. Search criteria are linked with logical AND. The last search configuration is saved.
2	Search tags	Show the search parameter values specified in the search mask
3	Log list	<p>Shows log messages for the actions performed in the UMS Web App.</p> <ul style="list-style-type: none"> Paging for the navigation in the log list Defining the number of log messages to be displayed on one page Sorting within any selected column Tooltips for detailed information
4	Clear data	Deletes log messages

6.3 Important Information

⚠ Take notice of the following information regarding the UMS Web App.



6.3.1 Login

- The login data of the database user are not accepted for the UMS Web App. For how to log in to the UMS Web App, see [How to Log In to the IGEL UMS Web App](#)(see page 732).

6.3.2 Permissions

- The UMS Web App and the UMS Console share the same permissions. For detailed information on access rights in the IGEL UMS, see [Create Administrator Accounts](#)(see page 508).
- There are some permissions only applicable to the UMS Web App – "Delete Log Messages" and "Device Bulk Action". They can be set in the UMS Console under **System > Administrator accounts > New / Edit > General - WebApp**.
- Read permissions to a directory enable access to devices in this directory; permissions only to devices are not sufficient.

6.3.3 Synchronization between the UMS Console and the UMS Web App

- Changes made in the UMS Console are immediately available in the UMS Web App, and vice versa.
- Changes made in the UMS Console are searchable not immediately, but after the next reindexing, which is executed every hour.
- Changes to profile settings made in the UMS Console as well as settings for the newly created profiles are displayed in the UMS Web App under **Configuration > [Profile name] > Activated Settings** not immediately, but after the next reindexing: this reindexing is executed with a one-day interval.

6.3.4 Logging

- Currently, only logs for actions performed in the UMS Web App are displayed.
- Log files for the UMS Web App can also be found in `/rmguiserver/logs/wums*`

6.3.5 Shadowing (VNC)

- Shadowing over ICG is only possible with IGEL Cloud Gateway version 2.02 or higher.
- For secure shadowing, newly registered devices need to boot several times until the certificate for the SSL tunnel is transferred to the UMS.

6.3.6 Certificate

- By default, browsers do not accept the self-signed certificate used by the UMS Server and display a security warning. For how to solve the problem, see [UMS Web App: The Browser Displays a Security Warning \(Certificate Error\)](#)(see page 187).



6.3.7 Bulk Actions

- The simultaneous selection of several devices or directories is currently not possible. If you want to execute bulk commands, you can do it now only by selecting an individual directory.

6.3.8 Supported Resolution

- The minimal supported resolution is 768 px.

6.3.9 Installation

- In case of using the UMS Web App in a HA environment, the UMS Web App does not necessarily have to be installed on every UMS Server. The UMS Console and the UMS Web App can be installed on different servers.
- If the UMS Web App starts with a 404 system error right after the installation of the UMS, see [UMS Web App: "404 - System Error" Message](#)(see page 205).

6.3.10 RAM and Disk Space Requirements

- The increase of the RAM and disk space is required due to the implemented Elasticsearch engine. For the minimum requirements, see [Installation Requirements for the IGEL UMS](#)(see page 258).

6.4 Installation

To work with the UMS Web App, it has to be enabled during the UMS installation procedure.

⚠ Take notice that the installation of the UMS Web App requires additional disk space and RAM, see [Installation Requirements for the IGEL UMS](#)(see page 258).

ⓘ High Availability

In a HA environment, the UMS Web App does not necessarily have to be installed on each UMS Server. If you choose, however, to install the application on several UMS Servers, you can use it on all of them. The data will be synchronized.

The UMS Console and the UMS Web App can be installed on different servers.

To install the UMS Web App, proceed as follows:

6.4.1 Windows

- In the UMS installer, activate **UMS Web App (early feature set)**. For detailed information, see [IGEL UMS Installation under Windows](#)(see page 283) or [Updating under Windows](#)(see page 288).



Setup - Universal Management Suite 6

Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Custom

<input checked="" type="checkbox"/> Standard UMS	358,1 MB
<input checked="" type="checkbox"/> with UMS Console	96,4 MB
<input checked="" type="checkbox"/> with Embedded Database	0,1 MB
<input type="checkbox"/> Only UMS Console	96,4 MB
<input type="checkbox"/> UMS High-Availability-Network	411,7 MB
<input type="checkbox"/> UMS Server	84,0 MB
<input type="checkbox"/> UMS Load Balancer	
<input checked="" type="checkbox"/> UMS Web App (early feature set)	321,7 MB

Current selection requires at least 793,6 MB of disk space.

< Back Next > Cancel

When the installation is complete, you can open the UMS Web App in your browser at <https://<server>:8443/webapp/#/login>. See also [How to Log In to the IGEL UMS Web App](#)(see page 732).

Setup - Universal Management Suite 6

Completing the Universal Management Suite 6 Setup Wizard

Please notice, the UMS Web App provides a subset of the UMS feature set. For more information please visit the IGEL Knowledge Base:
<https://kb.igel.com/ums/webapp/en>

The URL to access the UMS Web App is composed as follows:
<https://<server>:8443/webapp/#/login>

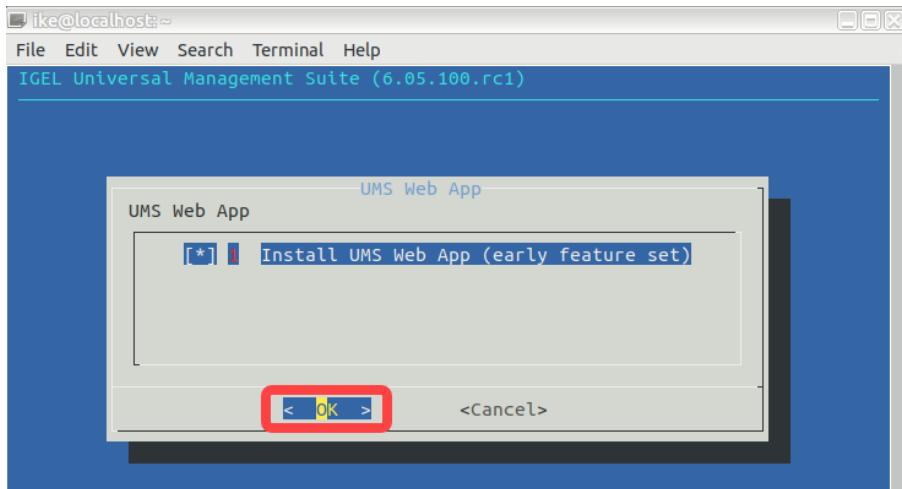
Open UMS Web app in browser

Finish



6.4.2 Linux

- In the UMS installer, select **Install UMS Web App (early feature set)**. For detailed information, see [IGEL UMS Installation under Linux](#)(see page 261) or [Updating under Linux](#)(see page 286).



When the installation is complete, you can open the UMS Web App in your browser at <https://<server>:8443/webapp/#/login>. See also [How to Log In to the IGEL UMS Web App](#)(see page 732).

6.5 Supported Environment

For information on the supported servers and databases, see the section "Supported Environment" in the [release notes](#)(see page 565).

6.5.1 Supported Browsers

The UMS Web App officially supports the following browsers:

- Google Chrome (version 83 or higher)
- Firefox (version 74 or higher)
- Internet Explorer (version 11 or higher)
- Edge (version 83 or higher)

6.5.2 Supported Resolution

- Min. 768 px

(i) If you want to use the UMS Web App on mobile devices, note that the min. supported width for the responsive design is 768 px.



6.6 How to Log In to the IGEL UMS Web App

The IGEL Universal Management Suite (UMS) [Web App](#)(see page 720) is a web-based user interface to the UMS Server, introduced with UMS version 6.05.100.

The following article describes how to open and log in to the UMS Web App.

6.6.1 How to Access the IGEL UMS Web App

To open the IGEL UMS Web App:

- ▶ In the web browser, open the URL [https ://<server>:8443/webapp/#/login](https://<server>:8443/webapp/#/login).¹⁵³

⚠ "8443" is the default GUI server port, see "GUI server port" under [Settings for IGEL UMS Administrator](#)(see page 530). For detailed information on the UMS ports, see [UMS Communication Ports](#)(see page 48). If you have changed the GUI server port, adjust the URL accordingly.

OR

- ▶ In the symbol bar of the UMS Console, click the icon .

6.6.2 Login Data for the IGEL UMS Web App

To log in to the IGEL UMS Web App, you can use:

- The credentials of the UMS superuser, which can be changed in the **UMS Administrator > Datasource > UMS superuser**. See [Changing the UMS Superuser](#)(see page 547).
- The additionally created administrator account, which can be added in the **UMS Console > System > Administrator accounts**. See [Create Administrator Accounts](#)(see page 508).

⚠ The login data of the database user are not accepted for the UMS Web App.

- i** UMS Web App implements login brute-force protection:
- After several failed login attempts, the user account will be temporarily blocked. This includes also accounts that do not exist.
 - To prevent probing, dynamic login delay (milliseconds) is implemented. This is required since the response time could be an indicator of the (non-)existence of an account.

6.7 UMS Web App Manual

This reference manual describes the UMS Web App interface:

¹⁵³ <https://localhost:8443/webapp>.



- **Menu Bar**(see page 733)
- **Search**(see page 734)
- **Devices**(see page 737)
- **Configuration**(see page 748)
- **Network**(see page 752)
- **Logging**(see page 754)

6.7.1 Menu Bar

The menu bar comprises the following options:

Search		Search for devices according to the selected parameters
Devices		Shows all devices registered on the UMS Server and their details.
Configuration		Shows all standard profiles (see page 331) and their details as well as devices and device folders assigned to them.
Network		Shows all connected UMS Servers, UMS Load Balancers, and IGEL Cloud Gateways, their details, and statistical information.
Logging		Shows log messages for the actions performed in the UMS Web App.
		<p>Opens Messages window which shows information regarding the successful or unsuccessful execution of commands. The messages are automatically deleted at the reloading of the UMS Web App page in the browser.</p> <ul style="list-style-type: none"> • A successfully executed command is marked with . • A failed command is marked with a warning symbol .



- A partially failed command is marked with a warning symbol .

► Click a message to view details.

Messages				
Time	Description	Result		
Nov 5, 2020, 4:32:31 PM	Send settings to device	 OK		
Nov 5, 2020, 4:31:58 PM	Reboot device	 The action failed partly.		
10 ▾ 1 – 2 of 2 < < > >				
Time	Description	Unit Id	Device Name	Result
Nov 5, 2020, 4:31:37 PM	Reboot device	85641000E583142622	td-RD01	 Connection timed out: connect
Nov 5, 2020, 4:31:37 PM	Reboot device	00E0C520986A	td-RD02	 OK

 Help	The UMS Web App documentation on kb.igel.com ¹⁵⁴ and details of the current version of the Universal Management Suite.
 English	Language settings for the user interface
	Logout from the UMS Web App

6.7.2 Search

Menu path: UMS Web App > **Search**

-  Changes made in the UMS Console or in the local Setup are searchable in the UMS Web App after the next reindexing, which is executed every hour.

-  The last search configuration is automatically saved and restored on the next visit of the **Search** area.

In the **Search** area, you can search for devices according to the configured search parameters. When no values are specified in the search mask, all devices registered in the UMS are shown.

¹⁵⁴ <http://kb.igel.com>



The screenshot shows two views of the UMS Web App interface for the 'DEVICES' section.

Top View:

- Search Mask (1):** On the left, a search form with fields for Device Name, Unit ID, Product ID (set to 'UD3'), Version, Comment, MAC Address, and Last IP. A red '1' is placed above the search mask.
- Search Result (2):** A table showing one result: td-RD02, 00E0C520986A, UD3-LX 51, 11.05.100.01. A red '2' is placed above the search result table.
- Table View Options (3):** A dropdown menu on the right side of the table header. It includes 'Table View' (selected), 'Card View' (disabled), and a 'Select columns' section. A red dashed arrow points from the top of the 'Select columns' section down towards the table.
- Card View Options (4):** A dropdown menu on the right side of the table header. It includes 'Table View' (disabled), 'Card View' (selected), and a 'Select columns' section. A red arrow points from the bottom of the 'Select columns' section towards the card view area.

Bottom View:

- Search Mask (1):** Same as the top view.
- Search Result (2):** A table showing one result: td-RD02, 00E0C520986A, UD3-LX 51, 11.05.100.01. A red '2' is placed above the search result table.
- Card View Options (3):** A dropdown menu on the right side of the table header. It includes 'Table View' (disabled), 'Card View' (selected), and a 'Select columns' section. A red arrow points from the bottom of the 'Select columns' section towards the card view area.
- Device Detail View (4):** On the right, a detailed view for the selected device 'td-RD02'. It shows tabs for 'Properties' (selected) and 'Custom Properties'. Under 'Properties', there are sections for 'Department' (td-RD02), 'Technical Documentation' (DeviceAttribute_Subdepartments KB), and 'System Information' (Battery Level, CPU Speed, CPU Type, Flash Size). A red arrow points from the bottom of the 'Select columns' section towards this detail view.

1	Search mask	<p>Search Parameters: Adds / removes criteria for the search. Search criteria are linked with logical AND.</p> <p>To remove a value, click and then Search. This updates the search result list.</p>
2	Search tags	<p>Show the search parameter values specified in the search mask. If you switch to another area, e.g. Devices, and back, the search tags will remind you that the previous search configuration is still active.</p>
3	Table View	<p>Search results are displayed in the table form.</p> <ul style="list-style-type: none"> Adding / removing columns for the search result list Paging for the navigation in the search result list Defining the number of devices to be displayed on one page



		<ul style="list-style-type: none"> Sorting within any selected column
	Card View	<p>Search results are displayed in the card form.</p> <ul style="list-style-type: none"> Paging for the navigation in the search result list Defining the number of devices to be displayed on one page Sorting devices by Name, Product ID, Unit ID, Version, and IP Address <p>For each selected device, device information and device commands are shown. For detailed information, see Devices(see page 737).</p>
4	Export Data	<p>Opens an Exporting search results dialog where the parameters for the CSV export file can be configured. Columns selected under Select columns in the Table View are automatically included in the export file if not disabled manually in the Exporting search results dialog. For more information on exporting search results, see Exporting Search Results(see page 736).</p>

Exporting Search Results

Menu path: UMS Web App > **Search**

The results of a search query can be saved as a CSV file.

To export search results, proceed as follows:

1. Perform a search query.

i If no values are specified for search parameters, all devices registered in the UMS will be included in the export file.

2. Switch to the  **Table View**.



3. Click **Export data**.

The **Exporting search results** dialog opens.

Filtering parameters
dev Select All

<input checked="" type="checkbox"/> Device Name	<input type="checkbox"/> DeviceAttribute_Subdepartm
<input type="checkbox"/> Device Type	<input type="checkbox"/> Device Serial Number

Separator for CSV export
 ; , | ^ Save as: search-data-export_2021-07-08

Export Cancel

4. Select the desired parameters.

For quick filtering, enter the name of the parameter under **Filtering parameters**.

5. Select the required delimiter under **Separator for CSV export**.

6. Click **Export**.

The export file is automatically downloaded in a few seconds.

6.7.3 Devices

Menu path: UMS Web App > **Devices**

Device changes made in the UMS Console are immediately available in the UMS Web App, and vice versa.

In the **Devices** area, you can manage devices registered on the UMS Server. All devices registered on the UMS Server are shown.

You can structure the **Devices** area by creating directories and subdirectories. When doing so, you should bear in mind that each device can only be stored in a single directory.

Avoid placing too many devices in one folder, see [Performance Optimizations](#)(see page 251).



Directory Level

Device Level

1	Directory Tree Shows all created directories and subdirectories with the specification of the number of devices assigned to them. <ul style="list-style-type: none"> • Creating a Directory(see page 742) • Renaming a Directory(see page 744) • Deleting a Directory(see page 744) • Moving a Device Directory(see page 743) • Copying a Device Directory(see page 743) • Moving Devices(see page 745)
2	Device list Shows all devices directly contained in the directory selected in the Directory Tree . <ul style="list-style-type: none"> • Filtering devices by Name, Product ID, Unit ID, Version, and IP Address



		<ul style="list-style-type: none"> • Sorting devices by Name, Product ID, Unit ID, Version, and IP Address • Paging for the navigation in the device list • Defining the number of devices to be displayed on one page
3A	Directory information	<p>Details for the directory selected in the Directory Tree</p> <p>[Directory Name]: The name of the selected directory</p> <p>Properties: Properties of the selected directory, e.g. the full Directory Path, Number of contained devices</p> <p>Assigned Objects: Directly and indirectly assigned objects, e.g. profiles, firmware updates, etc. For details, see Assigning Objects(see page 746).</p>
3B	Device information	<p>Details for the device selected in the device list</p> <p>Status display: The status of the selected device. For icons showing the device's status, see "Status Displays(see page 740)" under Devices(see page 737).</p> <p>[Device Name]: The name of the selected device. It does not need to be identical to the name of the device in the network. The name of a device does not need to be unique and can be used a number of times.</p> <p>To rename the device, click , type a new name, and press [Enter].</p> <p>Properties: Properties of the selected device, e.g. Last IP, MAC Address, Unit ID, Last Contact(see page 177), etc.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> The unit ID serves as a unique identifier in the UMS. With IGEL devices, IGEL zero clients, devices converted with the IGEL UDC/OSC, and devices with the IGEL UMA, the unit ID is set to the MAC address of the device.</p> </div> <p>[Directory Path]: Full directory path for the selected device</p> <p>Custom Properties: Allows changing such customizable properties as Site, Department, device attributes (currently configured only in the UMS Console under UMS Administration > Global Configuration ></p>



[Device Attributes](#)(see page 463). To edit the properties, click .

System Information: Shows such properties as **CPU Type**, **Memory Size**, **Device Type**, etc. To copy a property's value, click .

Assigned Objects: Directly and indirectly assigned objects, e.g. profiles, firmware updates, etc. For details, see [Assigning Objects](#)(see page 746).

The following sections are displayed only if there are data available for the section.

Licenses: Details on the licenses for the selected device. The section is available for the IGEL OS 11 devices only. To copy a value, click .

User Login History: Shows up to 10 last user logins if the logging is enabled. For details on the logging activation, see the section "User Login History" under [Device](#)(see page 384).

4	Device commands	<p>Device commands, e.g. power control commands, firmware update, etc., are executed for an individual directory or an individual device. The status of the command execution is shown under Messages(see page 733) .</p> <ul style="list-style-type: none"> ▶ Click to view all available device commands. <p>For details on the device commands, see "Device Commands(see page 741)" below.</p>
---	-----------------	---

Status Displays

The UMS monitors the status of the devices by regularly sending UDP packets. In accordance with the preset, this occurs every 3 seconds. For information on how to change the interval for the online check, see [Devices](#)(see page 382).

When the device is connected via IGEL Cloud Gateway (ICG), a cloud symbol icon is added to the device.



- The exclamation mark indicates that changes have not yet been transferred to the device:

td-RD01

Icons for an IGEL OS Device

The following icons show the status of an IGEL OS device:

	The device is online.
	The device is offline.
	The status of the device is unknown.

Icons for a UD Pocket

The following icons show the status of a UD Pocket:

	The UD Pocket is online.
	The UD Pocket is offline.
	The status of the UD Pocket is unknown.

Device Commands

The following commands can be executed for an individual device as well as for an individual directory (with the exception of shadowing).

	Shadow	Shadowing / secure shadowing / shadowing over ICG (with ICG 2.02 or higher): Launches a VNC session for the highlighted device if shadowing is enabled for this device, see Shadow¹⁵⁵ . For details on shadowing in the UMS, see Shadowing (VNC) (see page 399) and UMS and Devices: Secure Shadowing (see page 68).
	Assign object	Assigns / detaches an object, e.g. a profile, a file, etc. For details, see Assigning Objects (see page 746).
	Reboot	Restarts the highlighted device.
	Shutdown	Shuts down the highlighted device.

¹⁵⁵ <https://kb.igel.com/display/igelos1104/Shadow>



Wake up	Starts the highlighted device via the network (Wake-on-LAN).
Suspend	Puts the highlighted device into suspend mode.
Send settings	Sends the configuration of the UMS to the highlighted device.
Receive settings	Reads the local configuration of the highlighted device to the UMS.
Reset to factory defaults	Resets the highlighted device to the factory defaults.
Update	Carries out a firmware update on the highlighted IGEL OS device.
Update on shutdown	Updates the firmware when the highlighted IGEL OS device is shut down.
Refresh system information	Refreshes the system information for the highlighted device.
Refresh license information	Refreshes the license information for the highlighted device.

- If a user does not have sufficient rights, the command icons are grayed out. For information on permissions in the UMS, see [Access Rights](#)(see page 509).

- [Creating a Directory](#)(see page 742)
- [Copying a Device Directory](#)(see page 743)
- [Moving a Device Directory](#)(see page 743)
- [Renaming a Directory](#)(see page 744)
- [Deleting a Directory](#)(see page 744)
- [Moving Devices](#)(see page 745)
- [Assigning Objects](#)(see page 746)

Creating a Directory

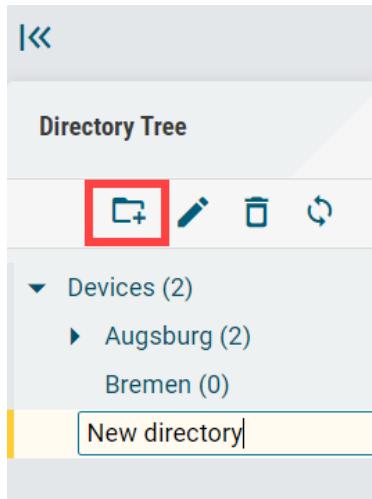
Menu path: UMS Web App > **Devices**

You can create as many directories and subdirectories as you want in order to group the devices together. When you create sub-directories, the devices organized in it form subgroups of a group.

- A device that is unequivocally identified by its MAC address can only be stored in a single directory, i.e. only as a member of a single group.

To create a directory or subdirectory, proceed as follows:

1. In the **Directory Tree**, select a directory, e.g. "Devices".
2. Click .
3. Enter a name for the new directory.



4. Press [Enter].
The new directory will be displayed below the selected directory in the **Directory Tree**.

You can now move devices to this new directory.

Copying a Device Directory

Menu path: UMS Web App > **Devices**

You can copy a device directory and paste it into any directory. Only an empty directory as well as the subdirectories contained in it will be copied; devices cannot be copied.

To copy a device directory, proceed as follows:

1. In the **Directory Tree**, click on the directory that you want to copy.
2. Press [Ctrl + C].
3. Click on the directory in which you would like to paste the copy of the directory.
4. Press [Ctrl + V].
5. Confirm the **Copy directory** dialog.
A new device directory that has the same name as the original directory will be created. The new directory will contain newly created copies of the subdirectories contained in the original directory.

 You can copy a device directory also via drag & drop while holding down the [Ctrl] key.

Moving a Device Directory

Menu path: UMS Web App > **Devices**

When moving a device directory to another directory, the directory itself, its subdirectories, and devices contained in them will be moved.



To move a device directory, proceed as follows:

1. In the **Directory Tree**, click on the directory that you want to move.
2. Click [Ctrl + X].
3. Click on the directory in which you would like to move the directory.
4. Click [Ctrl + V].

The **Move directory** dialog opens.

⚠ If profiles are indirectly assigned to a device or revoked as a result of the device being moved to a different directory, its configuration too will change. The new configuration can take effect either immediately or when the device is next rebooted.

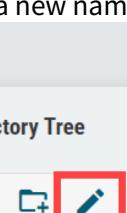
5. Select when you want the changes to take effect and confirm this by clicking on **Move**.

i You can move a directory also by dragging and dropping it to another directory.

Renaming a Directory

Menu path: UMS Web App > **Devices**

To rename a directory or subdirectory, proceed as follows:

1. In the **Directory Tree**, select a directory you want to rename, e.g. "Bremen".
2. Click .
3. Enter a new name for the directory.

4. Press [Enter].

Deleting a Directory

i Difference to the UMS Console

In the UMS Web App, only directories that do not contain any devices can be deleted.



! There is currently NO recycle bin support. If you delete a directory, it will be permanently removed.

To delete a directory, proceed as follows:

1. In the **Directory Tree**, select the directory that is to be deleted.
2. Click .

The screenshot shows the 'Directory Tree' section of the UMS web app. It displays a hierarchical list of devices under 'Devices (2)'. Under 'Augsburg (2)', there is 'techdoc (2)' which contains 'HS (0)', 'OS5 (0)', and 'RD (2)'. A red box highlights the delete icon (a trash can) located at the top of the tree view.

i If a directory is deleted, all subdirectories contained in it will be deleted too.

3. Confirm the **Delete directory** dialog.

Moving Devices

Since a device can only be stored in a single directory, you cannot copy devices, but only move them.

Devices are moved via drag & drop:

1. In the **Directory Tree**, select a directory that contains the device to be moved.
2. Select the relevant device.

The screenshot shows the UMS web app interface. On the left, the 'Directory Tree' sidebar shows 'Devices (2) > Augsburg (2) > techdoc (2) > RD (2)'. On the right, the main panel shows a list of devices in the 'RD' directory. Two devices are listed: 'techdocRD1' and 'techdocRD2'. A red arrow points from the 'RD' entry in the Directory Tree to the 'techdocRD2' device in the list.

Name	Serial Number	Location
techdocRD1	00E0C520986A	UD3-LX 51
techdocRD2	85641000E583142622	JC5-LX



3. Drag the device to the directory required and drop it.
The **Move device** dialog opens.
4. Select when you want the changes to take effect.

⚠ If profiles are indirectly assigned to a device or revoked as a result of the device being moved to a different directory, its configuration too will change. The new configuration can take effect either immediately or when the device is next rebooted.

5. Confirm that you wish to move the device by clicking on **Move**.

Assigning Objects

Menu path: UMS Web App > **Devices**

- To assign an object, select the desired directory / device and click **Assign object**.

i It is not possible to assign an object to the root directory.

The screenshot shows the 'Assign Object to Device' dialog. At the top, the device name 'td-RD02' is displayed with a red '1' above it. Below the title bar are several icons and a search bar labeled 'Filter objects'. The main interface is divided into two panes:

- Assignable Objects (Left Pane, Red '2'):** A list of objects available for assignment. It includes 'Browser' (orange shield icon), 'Wallpaper' (purple shield icon with a red minus sign and a small '5'), 'BackgroundWallpaper: /usr/share/pixmaps/wallpaper' (neutral icon), 'BackgroundWallpaper: /usr/share/pixmaps/UD_BG...' (yellow icon), and 'BackgroundWallpaper: /usr/share/pixmaps/UD_BG...' (yellow icon). A 'Firmware Customization' section is also visible.
- Assignments (Right Pane, Red '3'):** A list of objects currently assigned to the device. It includes 'Background' (green shield icon), 'Energy options' (orange shield icon), and 'BackgroundWallpaper: /usr/share/pixmaps/UD_BG_16x...' (orange icon).

In the center, there are two large blue arrows: a downward-pointing arrow on the left and an upward-pointing arrow on the right, both with red '5' above them. At the bottom right are 'Save' and 'Cancel' buttons.

1	Name of the directory / device	Name of the directory / device to which the object is assigned
---	--------------------------------	--



2	Assignable objects	<p>Shows all objects that can be assigned to the directory / device.</p> <p>The following objects can be assigned:</p> <ul style="list-style-type: none"> : Profiles. For details, see Profiles(see page 331). : Master profiles. For details, see Master Profiles(see page 359). : Firmware customizations. For details, see Firmware Customizations(see page 375). : Template keys and value groups. For details, see Template Profiles(see page 361). : Files. For details, see Files(see page 430). : Firmware updates. For details, see Universal Firmware Update(see page 433).
3	Assignments	Shows all objects directly assigned to the directory / device.
4	Filter	<div style="display: flex; align-items: center;"> <input style="width: 100px; margin-right: 10px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; font-size: 14px; font-weight: bold; outline: none;" type="text" value="11"/> x X </div> <p>Filters the objects under Assignable objects and Assignments according to</p> <ul style="list-style-type: none"> the selected object type the entry in the text field <p>The above filter criteria are linked with the operator <i>AND</i>.</p> <p>► Click to remove all filters.</p>
5	Assigning / detaching object	To assign / detach the selected object, you can use the arrow buttons or drag & drop.

Assigned Objects

Objects can be assigned directly or indirectly:

- Directly assigned objects have been assigned to an individual device or directory.
- Indirectly assigned objects have been "inherited" via the directory structure.

► To view all assigned objects, i.e. directly and indirectly assigned objects, select the desired directory / device and go to **Assigned Objects**.



1	<p>Filters the assigned objects according to</p> <ul style="list-style-type: none"> the selected object type the entry in the text field direct or indirect assignment type <p>The above filter criteria are linked with the operator <i>AND</i>.</p> <p>► Click to remove all filters.</p>
2	For indirectly assigned objects only: Specifies the path to the directory the object assignment is inherited from.
3	For directly assigned objects only: Detaches the object from the directory / device.

6.7.4 Configuration

Menu path: UMS Web App > **Configuration**

In the **Configuration** area, you can manage profiles. Currently, only managing standard and master profiles is possible. For more information on profiles and master profiles, see [Profiles](#)(see page 331) and [Master Profiles](#)(see page 359).

⚠ Currently, the creation of profiles and the change of configuration settings are possible ONLY in the UMS Console. Settings activated for the newly created profiles as well as setting changes are displayed in the UMS Web App not immediately, but after the next reindexing, which is executed, in this case, with a one-day interval.

ⓘ Master profiles have to be first enabled in the UMS Console under **UMS Administration > Global Configuration > UMS Features**, see [Enabling Master Profiles](#)(see page 360).



You can structure profiles by creating directories and subdirectories.

1

Configuration Tree

- Profiles (16)
 - Firmware (9)
 - Languages (4)
 - Desktop (2)**
 - Sessions (1)
- Master Profiles (2)
 - Browser (2)
 - New directory (0)

2

Profiles / Desktop

Desktop

Background	11.05.100.rc5.01
Screensaver	11.04.100.rc9.01

3

Number of contained devices
2

1

Configuration Tree

- Profiles (16)
 - Firmware (9)
 - Languages (4)
 - Background**
 - Screensaver
- Master Profiles (2)
 - Browser (2)
 - New directory (0)

2

Profiles / Desktop

Background

Properties	Based on	Id
Name Background	11.05.100.rc5.01	76924
Directory Path Profiles / Desktop		

4

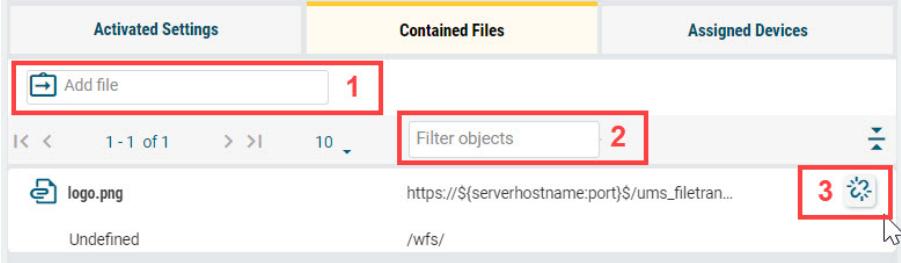
Activated Settings A	Template Key Relation B	Contained Files C	Assigned Devices D
Key	Display name	Value	
① windowmanager.defaulttheme.wallpaper	Wallpaper (1st monitor)	①	
① x.xserver1.standbytime	Standby Time	5	
① x.xserver1.standbytime.bat	Standby Time	3	

1	Configurations on Tree	Shows all created profile directories and subdirectories with the specification of the number of profiles assigned to them. <ul style="list-style-type: none"> To create a profile directory, click To rename a profile directory, click To delete a profile directory, click To move a profile directory to another directory, select the relevant directory and move it per drag & drop to the desired directory or use [Ctrl + X], [Ctrl + V]. To move the profile to another directory, navigate to the relevant profile in the profile list and move it per drag & drop to the desired directory.
2	Profile list	Shows all profiles contained in the directory selected in the Configuration Tree . <ul style="list-style-type: none"> Filtering profiles by Name and Version Sorting profiles by Name and Version Paging for the navigation in the profile list Defining the number of profiles to be displayed on one page



3	Directory information	<p>Details for the directory selected in the Configuration Tree.</p> <p>[Directory Name]: The name of the selected directory</p> <p>Properties: Properties of the selected directory, e.g. the full Directory Path, Number of contained devices</p>
4	Profile information	<p>Details for the profile selected in the profile list</p> <p>[Profile Name]: The name of the selected profile</p> <p>Properties: Properties of the selected profile, e.g. its Name, Version it is based on, etc. To edit the properties, click .</p> <div data-bbox="346 714 1060 1221" style="border: 1px solid #ccc; padding: 10px;"> <p> Edit properties</p> <p>Name Screensaver</p> <p>Description</p> <p>Sessions Do NOT overwrite sessions</p> <p>Version IGEL OS 11 11.04.100.rc9.01</p> <p style="text-align: right;"> Save  Cancel</p> </div> <div data-bbox="362 1275 1410 1397" style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <p> Overwrite sessions option should be activated only in exceptional cases. With this option, you can override free instances(see page 334) of all other profiles. For more information, see New Profile - Options(see page 338).</p> </div> <p>ID: Profile ID. If several profiles are assigned to a device on an equal basis, the newer profile with the higher profile ID has priority. For more information on prioritization of profiles, see Order of Effectiveness of Profiles(see page 351) and Prioritization of Profiles(see page 350).</p> <p>[Directory Path]: Full directory path for the selected profile</p>



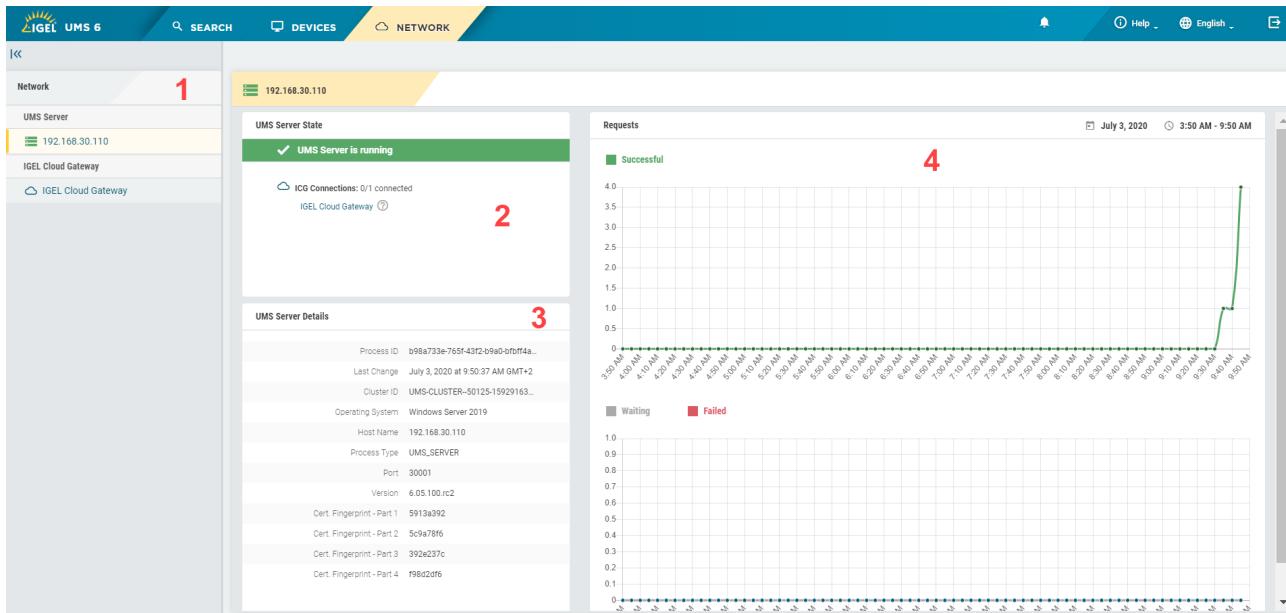
A	Activated Settings	<p>Shows all configuration settings activated in the selected profile.</p> <p>Key: Key of the configuration parameter ► Click the i-icon to open the tooltip.</p> <p>Display name: Name of the configuration parameter as displayed in the IGEL Setup and the configuration dialog in the UMS Console.</p> <p>Value: A value set for the parameter. All password values are anonymized. ► If a parameter receives a value from a template key (see Template Profiles(see page 361)), click to jump to the corresponding template key.</p>
B	Template Key Relation	<p>Shows template keys used in the profile, see Template Profiles(see page 361) and Using Template Keys in Profiles(see page 370).</p> <p>Template Key: Name of the template key</p> <p>Parameter: Key of the configuration parameter for which a template key is configured</p> <p>Template Expression: A template key configured</p> <p>Examples of template expressions: https://\igel.\\${Country} – template key configuring the starting page of the browser session SSH on \\${MAC} – static template key configuring the name for the SSH session, which will be composed of "SSH on" and the MAC address of the endpoint device </p>
C	Contained Files	<p>Shows all files assigned to the selected profile. Files should be first added in the UMS Console. For details on the file transfer, see Files(see page 430).</p>  <p>1: Allows to quickly add the file to the profile. To use the option, you should already know the file name or its part.</p> <p>2: Filters the files added to the profile according to the entered string.</p> <p>3: Detaches the selected file from the profile.</p>



D	Assigned Devices	Shows all devices the selected profile is assigned to.
		<p>1: Allows to quickly assign the selected profile to the device or device directory. To use the option, you should already know the name of the device / device directory or its part.</p> <p>2: Filters the devices / device directories assigned to the selected profile. The filter criteria are linked with the operator AND.</p> <ul style="list-style-type: none"> ▶ Click to remove all filters. <p>3: Detaches the selected device / device directory from the profile.</p> <p>4: Jumps to the corresponding device and shows all Assigned Objects for it.</p>

6.7.5 Network

Menu path: UMS Web App > **Network**





1	List of all available UMS Servers / UMS Load Balancers / IGEL Cloud Gateways (ICG)
2	<ul style="list-style-type: none"> • Status of the selected UMS Server / UMS Load Balancer / IGEL Cloud Gateway, see "Status Displays(see page 753)" below. • Status of UMS Server / ICG connections (connected, disconnected, unknown) • Number of currently connected devices (only for the ICG)
3	Details for the selected UMS Server / UMS Load Balancer / IGEL Cloud Gateway
4	Statistics for the device requests

Status Displays

UMS Server

The following icons show the status of the installed UMS Servers.

	The UMS Server is running.
	The UMS Server is not running.
	The status of the UMS Server is unknown (e.g. when a new server is being propagated in the network).
	The user is not authorized to view details for the UMS Server.
	The UMS Server is being updated.

UMS Load Balancer

The following icons show the status of the installed UMS Load Balancers.

	The Load Balancer is running.
	The Load Balancer is not running.
	The status of the UMS Load Balancer is unknown (e.g. when a new load balancer is being propagated in the network).
	The user is not authorized to view details for the Load Balancer.

IGEL Cloud Gateway

The following icons show the status of the installed IGEL Cloud Gateways.

	The IGEL Cloud Gateway is running.
	The IGEL Cloud Gateway is not running.



	The status of the IGEL Cloud Gateway is unknown.
	The user is not authorized to view details for the IGEL Cloud Gateway.

6.7.6 Logging

Menu path: UMS Web App > **Logging**

In the **Logging** area, you can search for log messages according to the configured search parameters. The last search configuration is automatically saved and restored on the next visit of the **Logging** area.

When no values are specified in the search mask, all available log messages are shown.

Log messages are available if

- logging is enabled in the UMS Console under **UMS Administration > Global Configuration > Logging**. See [Logging\(see page 500\)](#).
- a user has sufficient rights. For details on where you can define permissions, see [General Administrator Rights\(see page 512\)](#) and [Access Rights in the Administration Area\(see page 520\)](#).

Only log messages for the actions performed in the UMS Web App are currently displayed. Logs of the UMS Console are not included.

The screenshot shows the UMS Web App interface with the 'LOGGING' tab selected. The search mask at the top includes fields for Logtime (set to Nov 1, 2020 - Nov 4, 2020), Severity, Username, Category, Action (set to Shutdown, Directory: assign / detach url file, Device: assign / detach url file, directory: assign / detach template value, Device: assign / detach template value), and Message. A red arrow points to the 'Logtime' field. The search results table below shows log entries from Nov 14, 2020, to Nov 13, 2020, with columns for Logtime, Username, Severity, Category, Action, Name of the Affected Object, Message, and Origin. A red box highlights the 'Clear data' button in the top right of the table header. A red number '3' is located at the bottom center of the table.

1	Search mask	Search criteria for the logs (linked with logical AND) To remove a value, click and then Search . This updates the search results.
2	Search tags	Show the search parameter values specified in the search mask. If you switch to another area, e.g. Devices , and back, the search tags will remind you that the previous search configuration is still active.
3	Log list	Shows all logs that match the search criteria. <ul style="list-style-type: none"> • Paging for the navigation in the log list • Defining the number of log messages to be displayed on one page



		<ul style="list-style-type: none">• Sorting within any selected column• Tooltips, useful in case of truncations
4	Clear data	<p>Deletes the logs that are older than the number of days set.</p> <p>⚠ To delete the logs, a user must have the right "Delete Log Messages", see General Administrator Rights(see page 512). Directly after the deletion of logs, a message "No matching logs found" appears. Wait for the next reindexing to view the updated list of the log messages. However, you can immediately view and search for new logs, i.e. logs for actions performed after the deletion procedure.</p>

⚠ It is recommended to delete unnecessary logs regularly to avoid problems with insufficient disk space.



7 Fact Sheets

7.1 UMS Web App

