



IGEL OS Reference Manual



- [What Is New in 11.08.200?](#)(see page 3)
- [IGEL Workspace Edition](#)(see page 4)
- [Bluetooth Assistant](#)(see page 8)
- [Setup Assistant for IGEL OS](#)(see page 9)
- [Boot Procedure](#)(see page 22)
- [The IGEL OS Desktop](#)(see page 32)
- [Setup](#)(see page 42)
- [Sessions](#)(see page 47)
- [Accessories](#)(see page 499)
- [User Interface](#)(see page 636)
- [Network](#)(see page 688)
- [Devices](#)(see page 753)
- [Security](#)(see page 795)
- [System](#)(see page 823)



What Is New in 11.08.200?

The release notes for the latest release of IGEL OS 11.08.200 can be found on our download server at www.igel.com/software-downloads/workspace-edition/¹ as well as in the Knowledge Base under Notes for Release 11.08.200.

Composite USB Redirection

It is now possible to configure the redirection of composite USB devices, see [Native USB Redirection for Citrix Sessions in IGEL OS](#)(see page 71).

Dynamic e911 Support

For Citrix sessions, support for dynamic emergency calling with MS Teams has been added. See [Unified Communications](#)(see page 85).

App Protection for the Citrix Workspace App

A registry key for activating the app protection feature has been added, see [StoreFront Login](#)(see page 53).

Dynamic Default Printer Selection

You can configure IGEL OS to automatically set the currently connected printer as the default printer. This feature works with USB printers. See [Dynamic Selection of the Default Printer on IGEL OS](#).

Teradici PCoIP Is Now HP Anyware PCoIP

Teradici PCoIP has been renamed to HP Anyware PCoIP; see [PCoIP Sessions with the HP Anyware Client in IGEL OS](#)(see page 447).

Smart Virtual Background Support for the Zoom Client

A virtual background can now be used with the Zoom client; see [Zoom Client Selection in IGEL OS](#)(see page 496), section "Smart Virtual Background Support".

¹ <https://www.igel.com/software-downloads/workspace-edition/>



IGEL Workspace Edition

IGEL devices comprise the latest hardware and an embedded operating system based on IGEL Linux.

The firmware included with every IGEL Workspace product is multifunctional and contains a wide range of protocols allowing access to server-based services.

Management software: Universal Management Suite

For optimum management of your IGEL devices, the IGEL Universal Management Suite (UMS) is available on our [download page](#)².

- ⓘ With the IGEL Universal Management Suite, you can configure devices in the same way as in the devices' local setup.

- [Supported Formats and Codecs](#)(see page 5)
- [IGEL Devices Supported by IGEL OS 11](#)(see page 6)

² <https://www.igel.com/software-downloads/igel-universal-management-suite/>



Supported Formats and Codecs

As supplied, IGEL OS 11 supports the following multimedia formats and codecs:

- Ogg/Vorbis
- Ogg/Theora
- WAV
- FLAC
- Multimedia Codec Pack (MMCP); enabled by the Workspace Edition, see [IGEL Softwarelizenzen - Übersicht](#)

The MMCP includes the following codecs:

Supported Formats	Supported Codecs
AVI	MP3
MPEG	AAC
ASF (restricted under Linux)	WMA stereo
WMA	WMV 7/8/9
WMV (restricted under Linux)	MPEG 1/2
MP3	MPEG4
OGG	H.264

i AC3 is not licensed.



IGEL Devices Supported by IGEL OS 11

Core Requirements for IGEL OS 11

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

i RAM size higher than 2 GB is recommended if you use any of the following:

- Unified Communications optimizations (uses a client-side media engine)
- High-resolution graphics output
For details on the supported graphics-related characteristics of IGEL devices, see [Graphics on IGEL Devices](#) or, for older devices, [Graphics on Legacy IGEL Devices](#).
- More than two monitors

- Storage: 2 GB minimum; ≥ 4 GB recommended

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

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

IGEL Devices Supported by IGEL OS 11

IGEL UD (Universal Desktop)

Product Line	Device Type	Hardware ID	64 Bit	Memory (RAM)	Storage	HW Video Acceleration
UD2	D220	40	Yes	2 GB	4 GB	Yes
UD2	M250C	50	Yes	2 GB	4 GB	Yes
UD2	M250C	51 / 52*** (see page 7)	Yes	2 GB	8 GB	Yes
UD3* (see page 7)	M340C	50	Yes	2 GB	4 GB	Yes
UD3	M340C	51	Yes	2 GB	4 GB	Yes
UD3	M350C	60	Yes	4 GB	8 GB	Yes
UD5* (see page 7)	H830C	50	Yes	2 GB	4 GB	Yes



Product Line	Device Type	Hardware ID	64 Bit	Memory (RAM)	Storage	HW Video Acceleration
UD6	H830C	51	Yes	2 GB	4 GB	Yes
UD7	H850C	10	Yes	4 GB	4 GB	Yes
UD7 ^{**(see page 7)}	H850C	11	Yes	4 GB	4 GB	Yes
UD7	H860C	20	Yes	8 GB	8 GB	Yes
UD9 ^{*(see page 7)}	TC215B	40 / 41 (Touch)	Yes	2 GB	4 GB	Yes

* IGEL UD3-LX 50 and UD5-LX 50 are officially supported up to IGEL OS 11.05, incl. private builds. IGEL UD9-LX 40 / 41 (Touch) devices are officially supported up to IGEL OS 11.07.910.

** As of December 2019, IGEL UD7 model H850C is equipped with the AMD Secure Processor; for further information, see UD7 Model H850C.

*** IGEL UD2-LX 52 is supported with IGEL OS 11.06.140 and later.

IGEL Zero

i Note on IZ Devices

The IZ devices listed below can be upgraded to IGEL OS 11. To upgrade your IZ devices to IGEL OS 11, please contact your IGEL sales representative. See also <https://www.igel.com/os11migration/>.

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



Bluetooth Assistant

A Bluetooth Assistant starts before the actual Setup Assistant. This tests whether a USB mouse and/or a USB keyboard are available. If not, it searches for unconnected Bluetooth devices and helps you connect them.

The assistant starts with a window in which a timeout expires for a few seconds. During this time you can still cancel the wizard.

On the following setup pages you can make settings related to Bluetooth:

Bluetooth Tool:

Path: [Accessories > Bluetooth Tool](#)(see page 583)

Here you define the start options for the **Bluetooth Tool** session.

USB Access Control:

Path: [Devices > USB Access Control](#)(see page 785)

If you have USB access control enabled, you should make sure that you explicitly allow the connection to your Bluetooth devices via a class rule or device rule.

Bluetooth

Path: [Devices > Bluetooth](#)(see page 784)

Bluetooth must be activated here so that you can work with Bluetooth devices.

If you activate **Tray Icon**, you can start the Bluetooth tool via an icon in the system bar.

- ⓘ If you want to disable the Bluetooth Assistant in general, put the file `.igel_skip_bt-autopairing` in the directory `/wfs/user/`
The assistant will be skipped.

For more information about enabling Bluetooth services, see [Bluetooth](#)(see page 784).



Setup Assistant for IGEL OS

When you start an unconfigured device, you will be welcomed by the **Setup Assistant** for IGEL OS. This assistant takes you through the most important initial configuration steps.

- ⓘ The Setup Assistant starts automatically after booting IGEL OS if all the following requirements are met:
- The device is not yet configured.
 - No IP address for the Universal Management Suite (UMS) was transferred using the DHCP option 224.
 - No UMS can be accessed under the DNS name `igelrmserver`.

Buttons

Next

Go to the next configuration step.

Back

Go back to the previous step.

Cancel

Exit the setup assistant without saving changes to the configuration. Changes to the time and date will however remain effective.

Skip

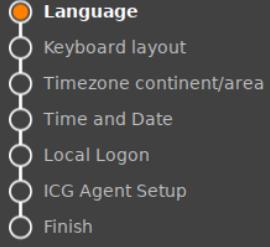
This button is shown if the current configuration step can be omitted. If you click on **Skip**, nothing will change during the configuration step. If the configuration is edited, the button will switch to **Next**.

- ⓘ Instead of clicking **Skip**, the **ESC** key can also be clicked to skip this configuration step.

Language



Language



The sidebar contains the following options:

- Language (selected)
- Keyboard layout
- Timezone continent/area
- Time and Date
- Local Logon
- ICG Agent Setup
- Finish

WELCOME!

The IGEL setup assistant helps you with the configuration of your IGEL device.

NOTE: During this process, the client may receive new remote settings.
In this case, the IGEL setup assistant will be closed and all changes made reset.

Select the language for the user interface.

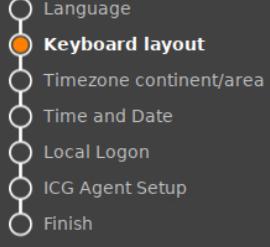
Language

English

Cancel Back Next

Here you can select the language for the user interface

Keyboard Layout



The sidebar contains the following options:

- Language
- Keyboard layout** (selected)
- Timezone continent/area
- Time and Date
- Local Logon
- ICG Agent Setup
- Finish

Select the keyboard layout of your keyboard.

Keyboard layout

English(US)

Cancel Back Next



Select the keyboard layout. The selected layout applies for all parts of the system including emulations, window sessions and X11 applications.

Time Zone Continent/Area

A screenshot of the "Timezone continent/area" setup window. On the left, there is a sidebar with a tree view of setup options: Language, Keyboard layout, Timezone continent/area (which is selected and highlighted in orange), Time and Date, Local Logon, ICG Agent Setup, and Finish. The main panel has a title "Timezone continent/area" and a sub-instruction "Choose a timezone according to your location." It contains two dropdown menus: "Timezone continent/area" set to "General" and "Location" set to "UTC". At the bottom right are three buttons: "Cancel", "Back", and "Next".

The screenshot shows the "Timezone continent/area" configuration screen. The sidebar on the left lists various setup categories, with "Timezone continent/area" being the active selection. The main area displays a message to choose a timezone and includes dropdown menus for selecting the continent/area and location. Navigation buttons for "Cancel", "Back", and "Next" are visible at the bottom right.

Select the continent/area for your location.

Possible values:

- **General***
Under **Location**, you can select a GMT time zone.
- **Africa... Pacific:**
Under **Location**, you can select a city for the selected continent/area.

Location

Select your location or time zone.

- i** Location: Summer time adjustment is taken into account here. Example: If you select "Berlin", the device will switch between summer time and normal time in accordance with the German adjustment rules. Time zone: The GMT time zones specify by how many hours the time zone for a particular location differs from the Greenwich time zone. The preceding symbol is used in accordance with the POSIX format. Examples: For New York City, select "GMT+5" which means "5 hours west of Greenwich". For Moscow, select "GMT-3" which means "3 hours east of Greenwich".



Time and Date

A screenshot of the "Time and Date" setup window. On the left, a sidebar lists steps: Language, Keyboard layout, Timezone continent/area, Time and Date (which is selected and highlighted in orange), Local Logon, ICG Agent Setup, and Finish. The main window title is "Time and Date" and contains the instruction "Enter the correct time and date." Below this is a "Date" section with a calendar for December 2021. The 17th is selected and highlighted with a blue border. Below the calendar is a "Time" section with a digital clock showing "10:36" and increment buttons. A checkbox labeled "Use NTP time server" is present, followed by a text input field. At the bottom are "Cancel", "Back", and "Next" buttons.

Language
Keyboard layout
Timezone continent/area
Time and Date
Local Logon
ICG Agent Setup
Finish

Time and Date

Enter the correct time and date.

Date

Sun	Mon	Tue	Wed	Thu	Fri	Sat
28	29	30	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

Time

10:36 - +

Use NTP time server

Cancel Back Next

Date

Select the current date.

Time

Set the current local time.

Use NTP time server

The device uses the NTP time server that is entered in the field. You can specify multiple NTP time servers separated by spaces. Example: 0.de.pool.ntp.org 1.de.pool.ntp.org

- i** To configure an NTP server via a UMS profile, edit **Use NTP time server** and **NTP time server** under **System > Time and Date**. For details on profiles, see Using Profiles.

Next

Sets the system clock according to what is entered above.



Mobile Broadband

Basic mode*

Country

The country of your provider.

Provider

Provider (the possible options depend on what you choose for **Country**).

APN/Plan

APN/Plan (the possible options depend on what you select for **Provider**).

For more configuration options, click the **Expert Mode** button.

Expert mode

Enabled

Determines if the settings made in the expert mode are used. (Default: Enabled)

APN

APN (Access Point Name) for your network connection. If you do not know the APN, ask your mobile communications operator for it.

Network ID

Network ID for your network connection. If you do not know the network ID, ask your mobile communications operator for it.

Number

Access number for your network connection. If you do not know the access number, ask your mobile communications operator for it.



User name

User name for your network connection. If you do not know the user name, ask your mobile communications operator for it.

Password

Password for your network connection. If you do not know the password, ask your mobile communications operator for it.

PIN

PIN for the SIM card used.

Wireless

This configuration step is available if a WLAN adapter was found when starting the device. The device will search for available WLAN access points as soon as the configuration step is opened. The WLAN access points found will be listed. You can then connect to your desired WLAN access point.

- ⓘ If you carry out the WLAN configuration and exit the Setup Assistant by selecting **Finish**, the connection will be saved and WLAN will be permanently enabled. If you skip this configuration step or cancel the configuration, WLAN will not be permanently enabled.
If no Wi-Fi adapter is found, please check if:
 1. There is a Hardware Switch on your device.
 2. There is a BIOS Setting that disables Wi-Fi, if Ethernet is connected.
 3. There is a BIOS update for your Endpoint.

Wireless regulatory domain

In the first selection menu, select the world region (example: **Europe**) in which you are situated and in the second one the country (example: **United Kingdom**).

: Searches again for WLAN access points.

: Opens a dialog which allows you to enter the WLAN name (SSID) of a hidden WLAN access point.

(Name of a WLAN access point in the list): Click on your desired WLAN access point and enter your access data in the dialog.

Once the connection is established, the symbol will be shown in the **Connected** column.

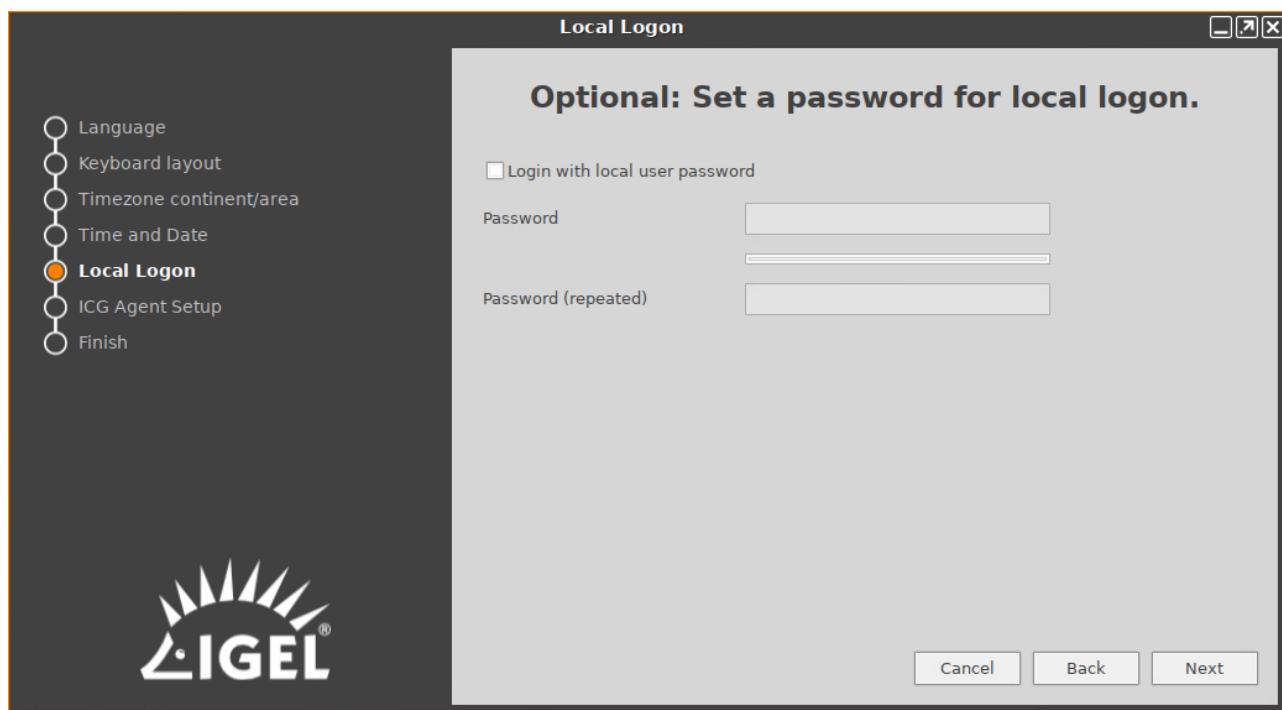


Connectivity

This page is shown if for any reason no network connectivity is available.

Follow the instructions on the screen.

Local Logon



This step is optional. If you want to configure a local user password later, see [Local User](#)(see page 812).

Login with local user password

A login screen is shown upon the start of the device, and a local user password set under **Password** is used to log in.

Password

Enter the desired password. The checker shown below assesses the strength of the password.



Password (repeated)

Repeat the password.

Activate Your IGEL OS in the Setup Assistant

In this step, you select the method for licensing your IGEL OS endpoint device. If the device has no license yet, the following options are available:

- **Continue with Starter License**
- **Request Full Feature 90-day Evaluation**
- **Alternative License Deployment** (Mostly needed if no IGEL UMS / ICG is in use.)
- **Managed License Deployment** (Preferred if you use a IGEL UMS)

If the device already has a license, the following options are available:

- **Keep using the current license**
You can continue with **Next**
- **Manual license update**
The procedure is the same as that for **Manual license deployment**.

The options are described in detail further below.

Continue with Starter License

With the IGEL OS Starter License, you can use the endpoint device immediately. For details on the features supported by the IGEL OS Starter License, see [IGEL Softwarelizenzen - Übersicht](#). If the device is not managed by the IGEL Universal Management Suite (UMS), an End User License Agreement (EULA) must be accepted.

⚠️ IMPORTANT: NO Multi-Media Codec Pack (MMCP) included, there is no Unified Communication or general performance optimization available.

Request Full Feature 90-day Evaluation

With this evaluation license, all features of IGEL OS 11 are available for a fixed period. This period starts when the device has received the demo license.

i For a demo license, you must accept the EULA to continue with setting up and using your device.

1. Make your choice as required and fill in all fields.
2. Activate the checkbox near **I agree to the terms + conditions and privacy policy**.



3. Click **ACTIVATE YOUR OS 11.**

Your device fetches a demo license from IGEL.

Alternative License Deployment

You can deploy a license via HTTP download from a specific URL, via FTP, or from a USB memory stick.

To deploy a license from a URL:

1. Enter the complete URL of the license file in the text field, including the protocol.
2. Click **Install**.

To deploy a license via FTP:

1. Click **FTP**.
2. Define the access data for your FTP server:

- Host/Port:
URL of the FTP server on which the license file is located

- User
User for accessing the FTP server

- Password
Password associated with the **User**

3. Click **Browse**.
4. In the dialog, go to the license file and select it.
5. Click **Install**.

To deploy a license from a USB memory stick.

1. Click **File**.
2. Connect the USB flash drive that contains the license to the device.
3. Under **Storage Device**, select the USB flash drive that contains the license.



4. Click **Browse**.
5. In the dialog, go to the license file, select it and click **Open**.
6. Click **Install**.

Managed License Deployment

The device will request a license from the UMS. If the device is outside the company network, the IGEL Cloud Gateway (ICG) will be used for connecting the device to the UMS. In this case, ICG access must be set up; see below, ICG Agent Setup.

 Please note that the device will not immediately receive a license in this step.

Troubleshooting: Proxy Configuration

If you get an error at this stage of the wizard, you may need to configure a proxy.

1. Click **Proxy configuration** in the upper right of the wizard to get to the proxy configuration dialog.
2. Edit the proxy settings as required:
 - Use proxy server
Activate this if a proxy is required.
 - HTTP Proxy
Address of the HTTP proxy
 - Port
Port of the HTTP proxy
 - SSL Proxy
Address of the SSL proxy



- Port

Port of the SSL Proxy

- SOCKS Host

Address of the SOCKS Host

- Port

Port of the SOCKS host

- User name

User name for authentication

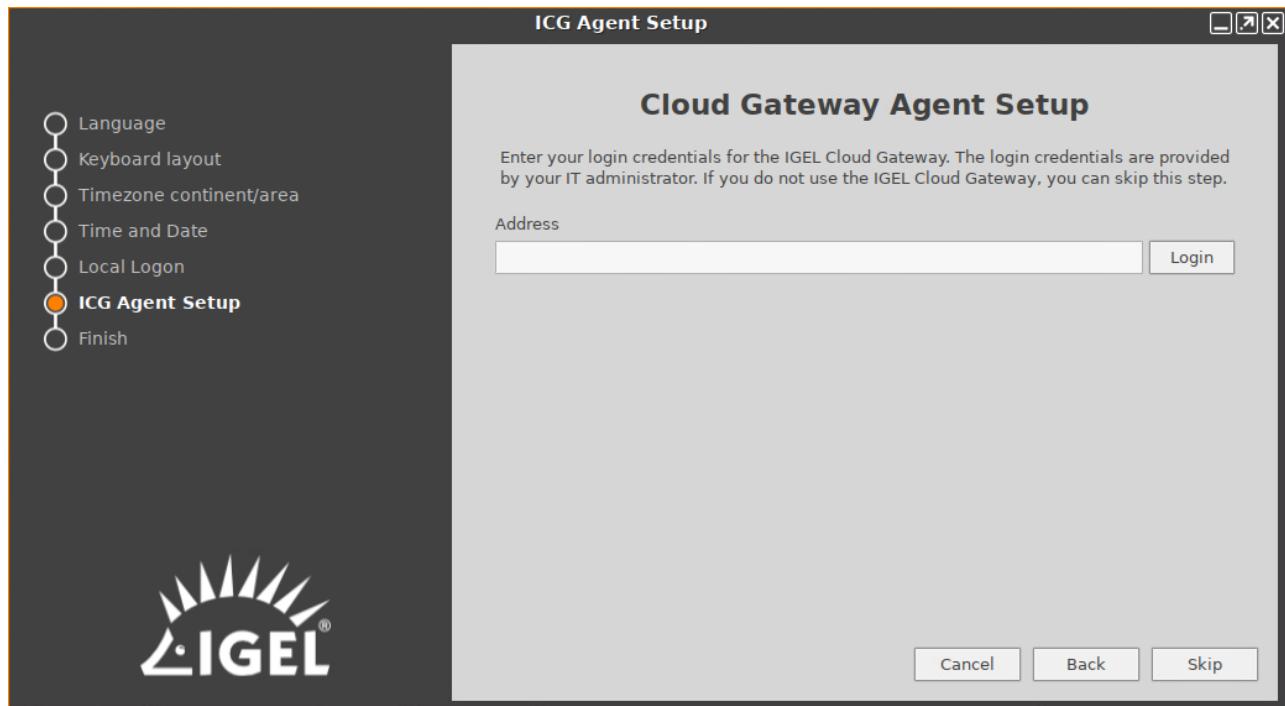
- Password

Password for authentication

i **User name** and **Password** are the credentials for all proxy types configurable here (HTTP, SSL and SOCKS).



Cloud Gateway Agent Setup



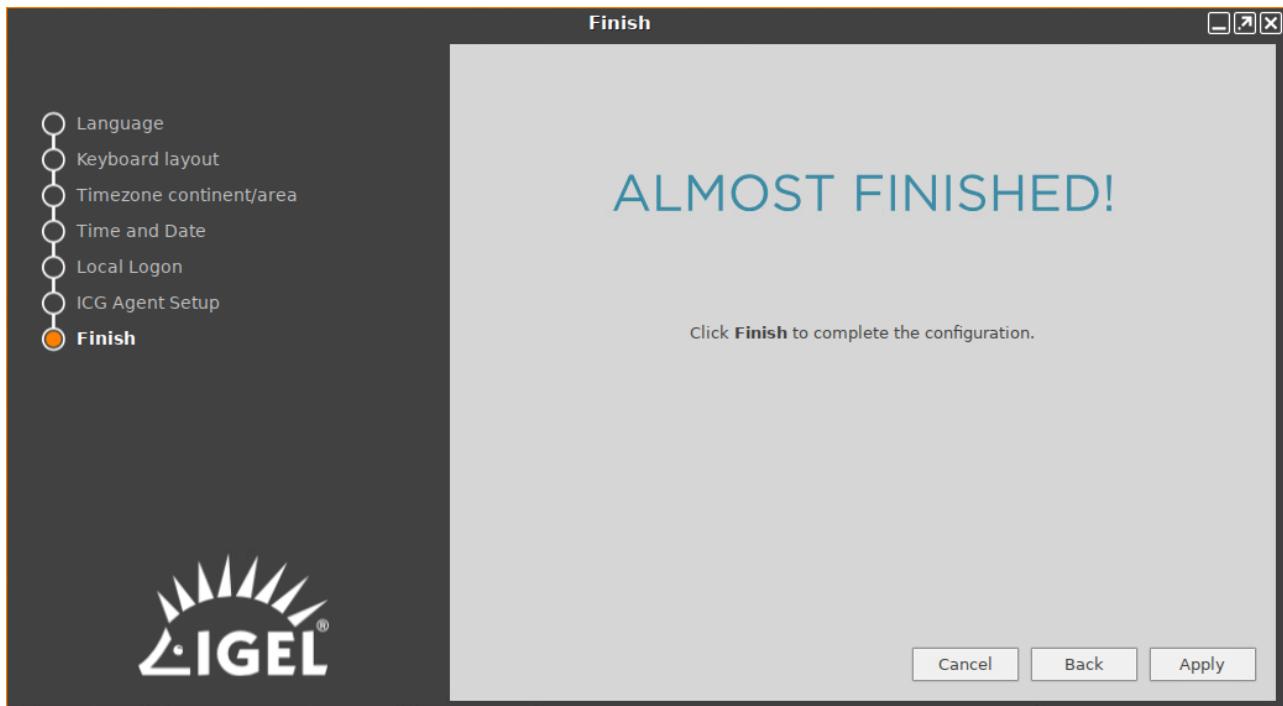
If your system administrator has given you access data for IGEL Cloud Gateway, you can connect the device to the gateway here.

You will find instructions for this under [Using ICG Agent Setup](#)(see page 621).

Otherwise, do not touch this page and click on **Skip** or **Next**.



Finish



Saves all settings and closes the Setup Assistant. If you have changed the language, the GUI X11 graphics system will restart; the screen will go black for a short time. If you have a UD Pocket Demo, a restart is required to finish the activation.

*IGEL OS system default



Boot Procedure

The quick installation procedure is complete.

- ▶ Restart the system in order to start the boot procedure.
-

- [Boot Menu](#)(see page 23)
- [Network Integration](#)(see page 30)
- [X-Server](#)(see page 31)



Boot Menu

During the boot procedure, a boot menu is available on request. Via this menu, you can access system parameters or reset the device to the factory defaults if the device is configured incorrectly or you experience problems when booting.

- ▶ During the boot procedure, press the [Esc] key repeatedly in rapid succession in the second stage loader when the "loading kernel" message is shown on the screen.

A menu with four boot options as well as an option for resetting the device to the default factory settings will appear:

- **Quiet boot:** Normal start (default)
- **Verbose boot:** Start with system messages and an interactive root shell
- **Emergency boot (setup only):** Setup only
- **Failsafe boot with CRC check:** Start with an integrity check of the operating system
- **Reset to factory defaults:** Reset the client to factory defaults
- **Custom boot command:** Boot with configurable command line options



Quiet Boot

Quiet boot is the default boot mode. In this mode, all kernel messages are disabled and the graphical user interface is started.



Verbose Boot

Unlike in **Quiet boot** mode, the boot messages are shown in **Verbose boot** mode. The boot procedure also pauses before the graphics system and the user session start.

This gives you an opportunity to open a root shell and interactively execute debugging commands (such as `ifconfig` etc.).

- ❖ Use the root shell only if you have adequate knowledge of Linux or if you are instructed to do so by the IGEL Helpdesk and are given appropriate guidance. Incorrect use can destroy the operating system.

Proceed as follows:

1. Select **Verbose boot** from the boot menu.
2. Wait until the boot messages stop at `Reached target IGEL Network Online`.
3. Open a virtual console with the key combination [Ctrl]+[Alt]+[F11] or [Ctrl]+[Alt]+[F12].
4. Log in by pressing [Return] and enter the root password if necessary.
5. Go through the desired individual commands.
6. Now enter the following command to continue the normal boot procedure:
`systemctl default`
The graphical user session will start.



Emergency Boot

During an **Emergency Boot**, the device is started without network drivers and with a resolution of 640 x 480 - 60 Hz. The setup is then opened directly.

This option is useful if, for example, you have selected an excessively high screen resolution or a wrong mouse type and these settings can no longer be changed in the normal setup.

- ▶ Close the setup window to shut down the system or restart it.
Unlike with a reset, the setup will open with the actual settings.



Failsafe Boot - CRC Check

During a **Failsafe boot**, a check of the file system is carried out first. The device then starts in **Verbose mode**.

This option is helpful if you no longer have a bootable system after a firmware update. The **Failsafe boot** checks where the problem is. If need be, an old version will be booted and you will need to repeat the firmware update.



Reset to Factory Defaults

⚠ If you select **Reset to factory defaults**, all personal settings on the device (including your password and the sessions you have configured) will be lost.

i A warning message will appear on the screen before the procedure is carried out. If the device is protected by an administrator password, you will be prompted to enter this password.

Do you know the password?

1. Confirm the warning message.
2. Enter the password. You have three attempts.

Do you not know the password?

1. Confirm the warning message.
2. When you are prompted to enter the password, press the Enter key three times.
3. Press [c].
The Terminal Key will appear.
4. Contact us using license@igel.com³.
5. Enter the Terminal Key shown, the firmware version, and your contact details.
IGEL will send you a so-called Reset to Factory Defaults Key specially for your device. To ensure that the process is as straightforward and yet as secure as possible, each key is valid for just one device.
See also Resetting a Device with Unknown Administrator Password.

⚠ You can also reset your device to factory defaults in the UMS Console under **Devices > Other commands > Reset to Factory Defaults**, see Devices.

³ <mailto:license@igel.com>



Custom Boot Command

If you select **Custom boot command**, preconfigured options will be placed on the kernel command line. This allows you for example to investigate and rectify problems with specific hardware components.

- ⚠ The Custom boot command is merely a temporary solution – it is not an everyday booting method. It must therefore be selected manually in the boot menu.

To configure the options for the Custom boot command, proceed as follows:

1. Open a **local terminal** and log in as `root`.
2. Enter the following command to bring up the current options:
`bootreg get /dev/igfdisk boot_cmd`
3. Save your desired options with the following command:
`bootreg set /dev/igfdisk boot_cmd "<Your Options>"`
4. Check the options that you have entered:
`bootreg get /dev/igfdisk boot_cmd`

- ⓘ If you would like to delete options for the Custom boot command, leave an empty string of characters in their place: `bootreg set /dev/igfdisk boot_cmd ""`



Network Integration

Once the kernel has been loaded, the network can be configured.

There are three possible ways of integrating the terminal into the network environment.

Depending on the terminal settings, choose between

- **DHCP**,
- **BOOTP**,
- **manually configured IP address**.

i The network interface can be stopped and restarted on the Linux Console (accessible via [Ctrl]+[Alt]+[F11]) with this command: `/etc/init.d/network stop /etc/init.d/network start`



X-Server

The final step in the boot procedure involves starting the **X-Server** and the local **windowmanager**.



The IGEL OS Desktop

You can operate the device via the taskbar and the *IGEL* menu.



The following items can be found in the taskbar at the bottom of the screen:

1		Opens the <i>IGEL</i> menu.
2	Quick Start Panel	
		Application Launcher: Opens a dialog window with start symbols for sessions.
		Setup: Opens the <i>IGEL</i> setup.



		Symbol for sessions: Launches a session.
③	Window bar	
		Window buttons Allows you to switch between open windows.
④	System tray	
		CPU power plan: Changes the power saving settings.
		Volume control
		Allows you to remove a USB stick safely
		Local network connection
		Time / date

The *IGEL* menu offers the following areas and functions:

- **Sessions:** Allows you to launch sessions
- **System:** Allows you to launch system programs
- **About:** Shows all relevant system information
- **Search window:** Allows you to find sessions and functions in the start menu
- Allows you to shut down the device
- Allows you to restart the device

-
- Application Launcher(see page 35)
 - Sessions(see page 37)
 - System(see page 38)
 - License(see page 39)



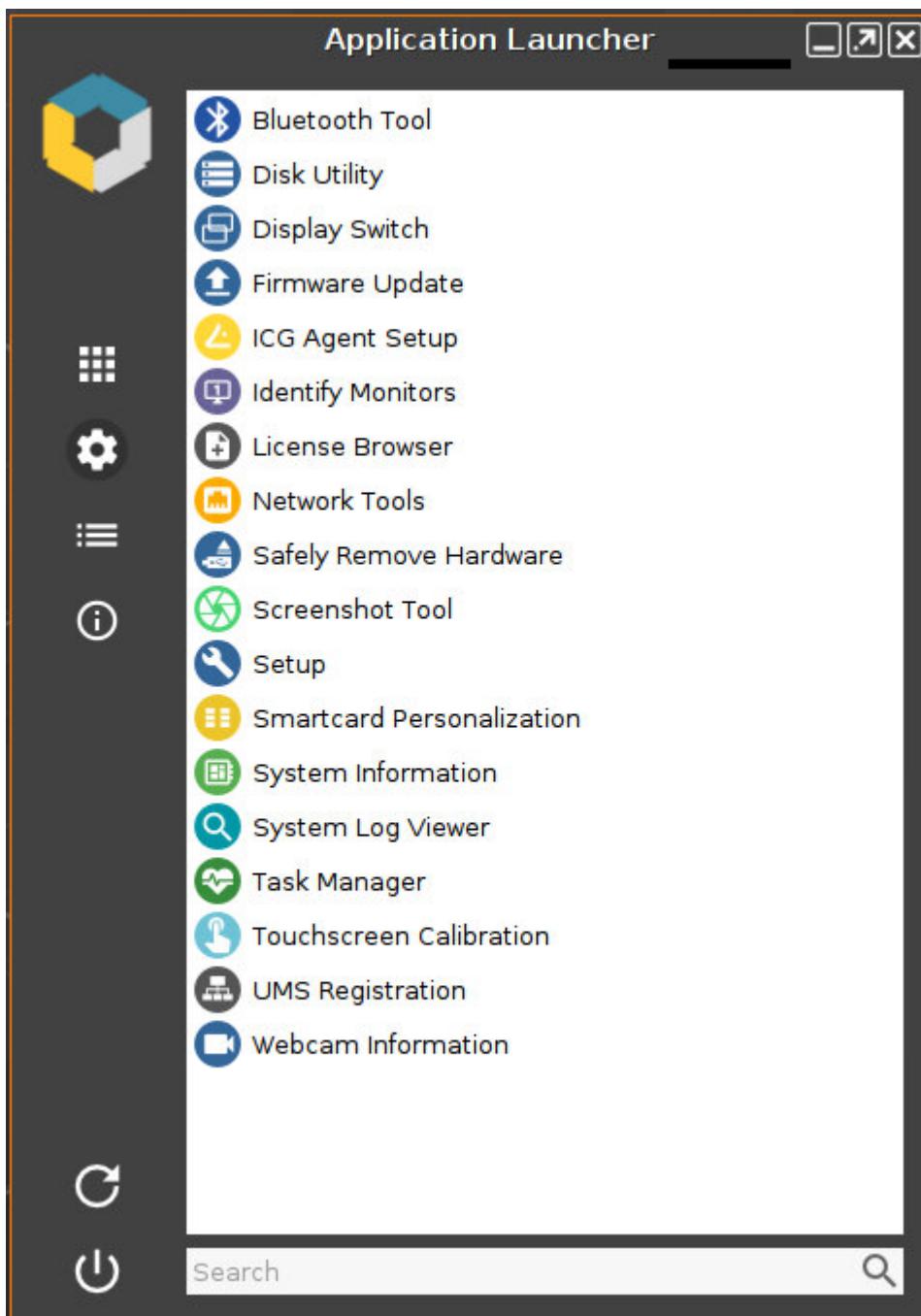
- [About Window](#)(see page 40)
- [Restart and Shutdown](#)(see page 41)



Application Launcher

To launch the **Application Launcher**, proceed as follows:

- ▶ Click on in the Quick Start Panel or in the start menu.





The sub-areas of the Launcher provide access to:

	Listing of the sessions (see page 37) that have been set up
	Listing of the most important tools (see page 38)
	License declarations (see page 39) for the components used
	The About Window (see page 40) with information about the system
	Restart
	Shut down
	Search field for fast access to the components

You will find information regarding the configuration under [Application Launcher](#)(see page 535).



Sessions

All sessions created are shown in a list of applications if they are enabled for the main session page.

- ▶ To open an application, double-click on it or click on **Run**.

Alternatively, you can launch sessions via icons on the desktop, in the quick launch bar or from the Start menu and context menu.

Applications can also be launched automatically and a key combination (hotkey) can be defined.

It is also possible, to build a file structure for the sessions in the application launcher. Therefor, in the setup page **Desktop Integration** of the relevant application you have to define a folder in the application launcher.

- The available options for launching a session can be defined under **Desktop Integration** in the session configuration.



System



Under **System**, you can execute various tools including the firmware updating tool with the pre-set update information.

The following tools are available:

- **Identify Monitors:** Shows the screen's number and manufacturer details.
- **Screenshot Tool:** Takes photos of the screen content.
- **Bluetooth Tool:** Starts the Bluetooth tool.
- **Firmware Update:** Carries out the update with the settings made during the setup.
- **Safely Remove Hardware:** Removes external storage devices without a risk of losing data.
- **Disk Utility:** Shows information regarding connected USB drives.
- **Network Tools:** Provides detailed information on the network connection and offers a number of problem analysis tools such as ping or traceroute.
- **Setup:** Launches the IGEL Setup.
- **System Information:** Shows information regarding hardware, the network and connected devices.
- **System Log Viewer:** Shows system log files "live" and allows you to add your own logs.
- **Task Manager:** Manages all processes.
- **Touchscreen Calibration:** Allows a connected touchscreen monitor to be calibrated.
- **UMS Registration:** Logs the device on to a UMS server (access data for the server are required).
- **Webcam Information:** Shows data relating to a connected webcam and allows the camera to be tested.



License



Under **License** you will find the following:

- The licenses for the components used in the UD system
- Information on the provision of source code, e.g. under GPL



About Window

In the **About** window, accessible via the icon, you will find the following data:

- **Product:** Information regarding the installed firmware
 - Copyright
 - Firmware Release Date
 - Firmware Version
 - Product ID
 - Product Name
 - Website
- **License Information:** Expiration dates of available licenses
- **Network:** Computer name, hardware address, and IP address of the device
 - Local Name
 - Default Gateway (only with valid network connection)
 - DNS Server (only with valid network connection)
 - Universal Management Suite
- **Interface [number name]:**
 - Description
 - Hardware Address
 - IP Address

If the network status changes, the details will automatically be updated. To force an update, click on .

- **Hardware:**
 - Boot Mode
 - CPU Model
 - Device Type
 - Flash Size
 - Graphic Chipset
 - Memory Size
 - Total Operating Time
 - Unit ID (equal to MAC address (UD, UDC) or serial number (UD Pocket))
- **Licensed Features:** List with all firmware features for which a license is available

You can copy individual entries via the context menu (right mouse button).



Restart and Shutdown





Setup

With the help of the setup, you can change the system configuration and session settings.

- ⓘ Any changes you have made in the UMS take precedence and may no longer be able to be changed. A lock symbol before a setting indicates that it cannot be changed.

-
- [Starting the Setup](#)(see page 43)
 - [End the Setup](#)(see page 44)
 - [Quick Setup](#)(see page 45)
 - [Setup Search](#)(see page 46)



Starting the Setup

You can open the setup in the following ways:

- Double-click in the **Application Launcher**
- or click on **Run**.
- Double-click on the desktop (if available based on the settings).
- Select **Setup** in the desktop context menu (if available based on the settings).
- Select **System > gear icon Setup** in the start menu.
- Click on in the Quick Start Panel.
- Launch the setup using the keyboard command [Ctrl]+[Alt]+[s], or in the Appliance Mode using [Ctrl]+[Alt]+[F2].

You can configure how the setup can be launched under **Accessories**. The options described above as well as combinations thereof are available.



End the Setup

In order to end the setup again, you have the following options:

- ▶ Click on **Apply** if you have finished configuring a setup area and would like to save your settings without closing the setup program.
- ▶ Click on **Cancel** if you have not made any changes and would like to abort the setup.
- ▶ Click on **OK** to save your changes and exit the setup.



Quick Setup

As administrator, you prepare the setup for the user. If you want to give the user the option of defining their own settings in certain areas of the setup, you can prepare a quick setup. A quick setup is a slimmed down version of the setup. It only displays areas the user is allowed to change.

To create a quick setup session, proceed as follows:

1. Enable the password for the administrator in IGEL Setup under **Security > Password**.

i If users are to be allowed to edit parts of the setup only with a password, enable the password for the setup user too.
2. Under **Accessories > Quick Settings**(see page 521), define the name and options for calling up the quick setup.
3. Under **Accessories > Quick Settings > Page Authorizations**,(see page 523) enable those areas to which the user is to have access.

i You can set up a hotkey to start quick setup in appliance mode. Instructions for setting up the hotkey can be found under [Quick Settings](#)(see page 521).



Setup Search

The **Search** function enables you to find parameter fields or parameter values within the setup.

1. To start a **search**, click on the button below the tree structure.
2. Enter the text to be searched for and the search details.
3. Select one of the hits.
4. Click on **Show result** and you will be taken to the relevant setup page.

The parameter or value found will be highlighted as shown below.

A screenshot of the IGEL Setup software interface. On the left, there's a sidebar with a tree structure. Under the 'Search' section, the 'Language' option is selected. Below it, several checkboxes are listed: 'Search in labels' (checked), 'Search in current values', 'Consider case', and 'Compare whole text'. A large 'Search' button is located below these checkboxes. To the right, the main configuration pane shows language settings. It includes dropdown menus for 'Language' (set to English) and 'Keyboard layout' (set to German). There's also a checkbox for 'Show indicator in taskbar'. Under 'Input language', a dropdown menu is set to 'Follows Keyboard layout'. In the 'Standards and formats' section, a dropdown menu is set to 'Follows Input language', which is highlighted with a yellow box. At the bottom left of the main pane, a message box displays '10 Hit(s)' and a list of three items, all of which are highlighted with yellow boxes: 'Language: "Language"', 'Language: "Follows Input langu...', and 'Language: "Input language"'.

Configuration

Search

Search string

Language

Search in labels

Search in current values

Consider case

Compare whole text

Search

10 Hit(s)

Language: "Language"

Language: "Follows Input langu..."

Language: "Input language"

Language

Keyboard layout

Show indicator in taskbar

Input language

Standards and formats



Sessions

Menu path: **Sessions > Sessions Summary**

In this area, you will find an overview of all available sessions.

Add: Adds a session from the selection of available session types.

Filter: Filters sessions shown in the list according to the string of characters entered.

- [Copy Session](#)(see page 48)
- [Global Session Options](#)(see page 49)
- [Citrix](#)(see page 50)
- [RDP Global](#)(see page 111)
- [RDP Session](#)(see page 140)
- [Remote Desktop Web Access](#)(see page 155)
- [Horizon Client Global](#)(see page 169)
- [Horizon Client Session](#)(see page 200)
- [Appliance Mode](#)(see page 213)
- [AppliDis](#)(see page 224)
- [Evidian AuthMgr](#)(see page 233)
- [NoMachine NX Client](#)(see page 245)
- [X Sessions](#)(see page 266)
- [Parallels Client Global](#)(see page 274)
- [Parallels Client Session](#)(see page 280)
- [PowerTerm Selection in IGEL OS](#)(see page 293)
- [PowerTerm Session](#)(see page 294)
- [IBM iAccess Client](#)(see page 298)
- [ThinLinc Global](#)(see page 321)
- [ThinLinc Session](#)(see page 328)
- [SSH Session](#)(see page 342)
- [VNC Viewer Sessions](#)(see page 350)
- [Firefox Browser Global](#)(see page 360)
- [Firefox Browser Session](#)(see page 389)
- [Chromium Browser Global Session in IGEL OS](#)(see page 396)
- [Chromium Sessions](#)(see page 415)
- [Media Player Global](#)(see page 420)
- [Media Player Session](#)(see page 425)
- [VoIP Client](#)(see page 433)
- [PCoIP Sessions with the HP Anyware Client in IGEL OS](#)(see page 447)
- [AVD Global](#)(see page 454)
- [AVD Session](#)(see page 460)
- [Amazon WorkSpaces](#)(see page 476)
- [deskMate Session](#)(see page 486)
- [Unified Communications](#)(see page 495)



Copy Session

You can copy a session in the setup. The copy of the session has all the properties of the original session and is located in the same folder as the original session.

To copy a session, proceed as follows:

1. In the setup, open the menu path **Sessions > [Session Type] > [Session Type] Sessions**.
Example: **Sessions > RDP > RDP Sessions**
The existing sessions are shown.
2. Highlight the session that you want to copy.
3. In the **[Session Type] Sessions** area, click . Alternative: Open the context menu of the session by right-click and select **Copy**.
A copy of the session will be created.



Global Session Options

Menu path: **Setup > Sessions > Global Session Options**

- **Network notification on session start:** If when launching sessions no network is available, a notification will be shown.
 - Network notification is enabled (default)
 - Network notification is disabled
- **Notification delay:** Time in seconds after which the notification is shown. (default: 15)
Possible values:
 - 1 ... 120 seconds
- **Delay session start at boot time to apply new UMS settings:** If new settings were made in the UMS, the device may receive them during the boot procedure.
 - The session start will be delayed until the settings have been transferred or the time limit has been exceeded.
- **Timeout:** Delay in seconds. (default: 10)
Possible values:
 - 1 ... 120 seconds



Citrix

Menu path: **Setup > Sessions > Citrix**

- Citrix Client Selection in IGEL OS(see page 51)
- Citrix Global(see page 52)
- Citrix StoreFront(see page 91)
- Citrix Self-Service(see page 105)



Citrix Client Selection in IGEL OS

When configuring Citrix sessions in IGEL OS, you can specify which version of Citrix Workspace App will be used for all StoreFront connections.

Menu path: **Sessions > Citrix > Citrix Client Selection**

Citrix client version

Selects the Citrix client version to be used for Citrix sessions.

For the included Citrix client versions, see the "Component Versions" section in the IGEL OS release notes.

⚠ When using UMS profiles for configuration, make sure the firmware version the profile is **based on** matches the firmware actually installed on the device (see [Creating Profiles](#)). If they do not match and the client version selected via the profile is not included in the firmware, the client version will fall back to default.

i After changing the **Citrix client version**, check the settings under:

- **Citrix > Citrix StoreFront > Server**
- **Citrix > Citrix StoreFront > Login**



Citrix Global

Menu path: **Sessions > Citrix > Citrix Global**

This section describes global Citrix settings which apply for all Citrix sessions. Most of these settings can be either carried over or overwritten in the individual sessions.

- i** Please note that a number of configuration options depend on the version of the Citrix Receiver selected.

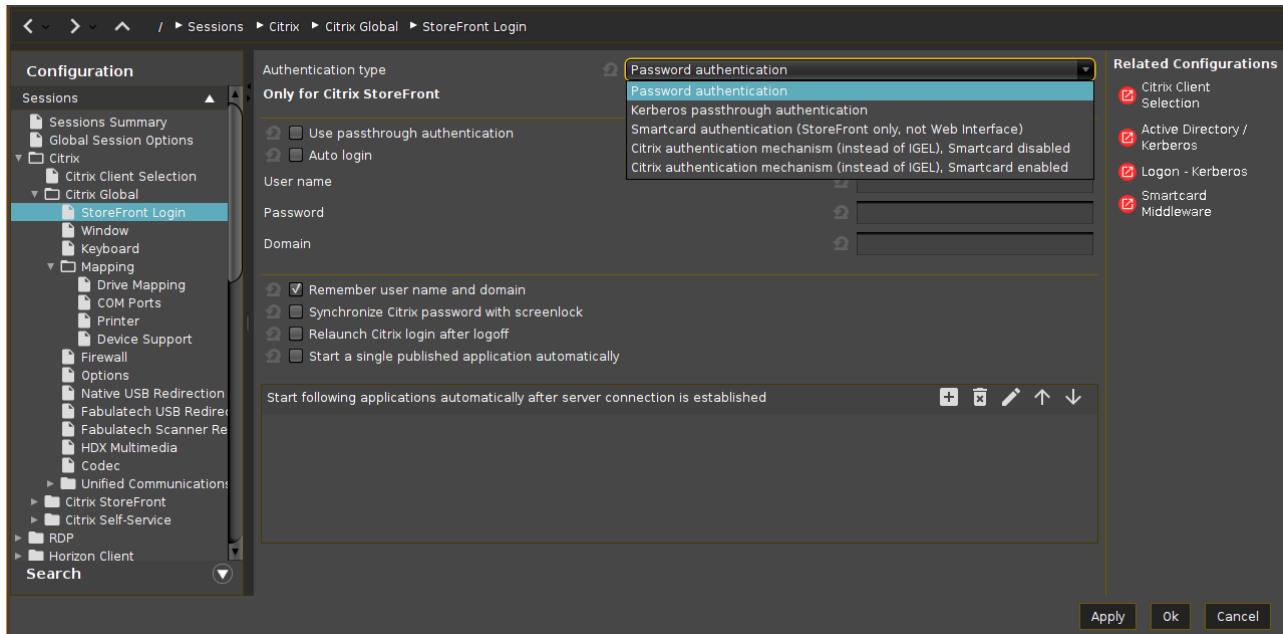
If there are problems with the logging in to a Citrix Storefront session because of the expired password, see [Login Failed because of the Expired AD Password](#).

- [StoreFront Login](#)(see page 53)
- [Window](#)(see page 56)
- [Keyboard](#)(see page 58)
- [Mapping](#)(see page 59)
- [Firewall](#)(see page 67)
- [Options for an IGEL OS Citrix Session](#)(see page 68)
- [Native USB Redirection for Citrix Sessions in IGEL OS](#)(see page 71)
- [Fabulotech USB Redirection](#)(see page 75)
- [Fabulotech Scanner Redirection](#)(see page 79)
- [HDX Multimedia Settings for an IGEL OS Citrix Session](#)(see page 80)
- [Codec](#)(see page 83)
- [Unified Communications Settings for Citrix Sessions in IGEL OS](#)(see page 85)

StoreFront Login

In this area, you can globally configure login options for Citrix sessions in IGEL OS. For individual sessions, login options can be defined under **Sessions > Citrix > Citrix StoreFront > Login**.

Menu path: **Sessions > Citrix > Citrix Global > StoreFront Login**



Authentication type

Depending on the Citrix client version, the following types are available:

- **Password authentication:** Suitable for on-premises connections; connections via Citrix NetScaler or to a cloud environment may cause problems.
- **Kerberos passthrough authentication:** Uses local login data for listing and launching applications. The option enables single sign-on if login with AD/Kerberos is configured on the device, see [Active Directory/Kerberos](#)(see page 807).
- **Smartcard authentication (StoreFront only, not Web Interface):** Authentication via smartcard will only work with StoreFront, not with Web Interface. For configuration details, see Citrix StoreFront.
- **Citrix authentication mechanism (instead of IGEL), Smartcard disabled:** Recommended for cloud environments and Citrix NetScaler.
- **Citrix authentication mechanism (instead of IGEL), Smartcard enabled:** Recommended for cloud environments and Citrix NetScaler.

- ⓘ** If you have set an authentication type with smartcard, select the type of card on the [Smartcard](#)(see page 817) page. You may find it also helpful to read the how-to Smartcard Authentication in IGEL OS.



Depending on the selected authentication type, the following options are available:

Use passthrough authentication

- Cached login data are used for listing and starting applications. For more information, see Passthrough Authentication.
- No passthrough authentication. (Default)

Auto login

- Uses the login data preset on this page when connecting to the server.
- Do not log in automatically. (Default)

User name

Can only be filled in with password authentication.

Password

Can only be filled in with password authentication.

⚠ Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

Domain

Can only be filled in with password authentication.

Remember username and domain

- Saves the user name and domain from the last login. (Default)
- The user name and domain will not be saved.

Synchronize Citrix password with screenlock

- Synchronizes the [screenlock password](#) (see page 666) with that of the Citrix application. You can use this option if you want, for example, to use the user's AD password to unlock the screen.
- No synchronization (Default)

Relaunch Citrix login after logoff

- Automatically shows the login dialog again after logging out.
- Does not start the login procedure again. (Default)



Start a single published application automatically

This parameter is relevant if exactly 1 published application is provided for the user whose login is configured here.

- The published application is started when the user has logged in.
- The published application is not started on login. (Default)

Start following applications automatically after server connection is established

A list of applications to be started in the session.

To edit the list, proceed as follows:

- Click on to create a new entry. In the **Add** dialog, give the name of the application.

Application names are case-sensitive.
You can also enter part of the name followed by an asterisk (*).

- Click on to remove the selected entry.
- Click on to move the entry upwards.
- Click on to move the entry downwards.

After a successful login, the associated desktop icon for each available application will be placed on the device desktop. All applications whose name matches one of the names given in the **Start following applications automatically after server connection is established** area will then be launched.

App Protection Feature for the Citrix Workspace App

To strengthen the security of your Citrix environment, you can use the app protection feature in IGEL OS 11.08.200 or higher. It provides anti-keylogging and anti-screen-capturing functionalities. For more information on this feature and the required server-side settings, see <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/secure/app-protection.html>.

To activate the feature on IGEL OS, go to **System > Registry** and enable the following registry key:

Parameter	Citrix App Protection
Registry	<code>ica.appprotection</code>
Value	<code>false / true</code>
Note	The feature is supported for Citrix Workspace app version 22.07 and higher; for how to change the version, see Citrix Client Selection in IGEL OS (see page 51).



Window

Menu path: **Sessions > Citrix > Citrix Global > Window**

Under **Window**, you can configure the following settings:

Multimonitor full-screen mode

Possible options:

- Restrict full-screen session to one monitor
- [Expand full-screen session across all monitors](#)
- Expand the session over a self-selected number of monitors

ⓘ Select this setting if you do not want to span the session across all monitors, but only across a certain number of monitors. Under **Monitor selection, specify the relevant monitors.**

StoreFront start monitor: This setting is available if you selected **Restrict full-screen session to one monitor** for **Multimonitor full-screen mode**.

Monitor selection: This setting is available if you selected **Expand the session over a self-selected number of monitors** for **Multimonitor full-screen mode**.

Example

Sample configuration: If you have 4 monitors and want to expand your session across monitor 2, 3, and 4 you have to insert `2,3,4` or `2,4`.

Embed systray icons into window manager taskbar: Specifies if an application icon is shown in the local taskbar.

- On
- Off

Citrix connection bar

Possible options:

- Off
- On
- Factory default is "/*": The Citrix connection bar is enabled or disabled by the server.

Control bar for Citrix sessions

The in-session control bar is present in Citrix sessions. For details, see [In-Session Control Bar](#)(see page 661).

Screen Pinning

You can run multiple Citrix desktop sessions simultaneously on different monitors. In this section, you assign one or more monitors to each session.

If a desktop session is not assigned to monitors, the default settings in the general section of this Setup page apply to it.

⚠ This feature works only with desktop sessions; published applications cannot be controlled.



- For each Citrix desktop session, click to configure a corresponding monitor setup. The following parameters must be set:

Citrix session name: Name of the desktop session as displayed in the browser, desktop, or Self-Service. The session name is provided by the server. The wildcards "*" (any number of any characters) and "?" (any single character) can be used.

Example

With three desktop sessions that are named "Desktop2019", "DesktopW10", and "DesktopD10", you can assign settings like so, for instance:

- "Desktop*": The settings are assigned to all three desktops.
- "Desktop?10": The settings are assigned to "DesktopW10" and "DesktopD10".
- "DesktopW10": The settings are assigned to "DesktopW10".

Multimonitor full-screen mode: Defines how the desktop sessions are distributed over the monitors. For the arrangement of the monitors and their numbering, go to **User Interface > Display** (see [Display Settings in IGEL OS](#)(see page 637)).

Possible options:

- Restrict full-screen session to one monitor: The desktop session is displayed on the monitor that is selected under **Desktop session start monitor**.
- Expand full-screen session across all monitors: The desktop session uses all monitors.
- Expand the session over a self-selected number of monitors: The monitors can be selected with **Monitor selection**.

Desktop session start monitor: The desktop session is displayed on the selected monitor.

Monitor selection: Selects one or several monitors on which this desktop session is to be displayed. This setting is available if you selected **Expand the session over a self-selected number of monitors**.

Example

Sample configuration: If you have 4 monitors and want to expand your session across monitor 2, 3, and 4 you have to insert `2,3,4` or `2,4`.



Keyboard

Menu path: **Setup > Sessions > Citrix > Citrix Global > Keyboard**

On the **Keyboard** page, you can define alternative key combinations for hotkeys commonly used during ICA sessions. In *Windows* for example, the key combination [Alt]+[F4] closes the current window. This key combination works in ICA sessions too. All key combinations with [Alt] which are not used by the *X Window Manager* function in the familiar way during an ICA session.

The following settings can be configured:

- **Keyboard layout**
 - default: The local keyboard setting will be used in ICA too.
 - Other Countries
- **Input language**:
 - default: The local keyboard setting will be used in ICA too.
 - Other Countries
- **Mapping Ctrl+Alt+End to Ctrl+Alt+Del for Citrix sessions**
 - The user can use the combination [Ctrl]+[Alt]+[End] to change the password instead of [Ctrl]+[Alt]+[Del] when the corresponding prompt message appears.
 - No mapping (default)
- **Keyboard mapping file**: You can choose between two alternatives.
 - generic: Sends language-independent scancodes from the keyboard to the computer.
 - Linux: Sends language-specific scancodes.

The key alternatives are restricted to [Ctrl]+[Shift]+[Key] by default. However, you can change the settings by clicking on the Hotkey Modifier drop-down field and/or hotkey symbol for the relevant key combination.

- Possible keys: [F1] – [F12], [Plus], [Minus], [Tab]
- Possible modifiers: [Shift], [Ctrl], [Alt], [Alt]+[Ctrl], [Alt]+[Shift], [Ctrl]+[Shift]
- **Toggle SpeedScreen**: Key combination for switching *SpeedScreen* (client reacts immediately to keyboard inputs or mouse clicks) on and off alternately.



Mapping

Menu path: **Setup > Sessions > Citrix > Citrix Global > Mapping**

Locally connected devices such as printers or USB storage devices can be made available in ICA sessions.

- [Drive Mapping \(Citrix\)](#)(see page 60)
- [COM Ports](#)(see page 62)
- [Printer](#)(see page 64)
- [Device Support](#)(see page 65)



Drive Mapping (Citrix)

Menu path: **Setup > Sessions > Citrix > Citrix Global > Mapping > Drive Mapping**

Through drive mapping, each directory mounted on the device (including CD-ROMs and disk drives) is made available to you during *ICA* sessions on *Citrix* servers.

In this area, you can specify which drives and paths are mapped during the logon. This applies for all *ICA* sessions.

- **Drive mapping:**

Citrix servers can access the device's local drives. (default)

To manage the **Drive Mapping** list, proceed as follows:

- ▶ Click on to create a new entry.
- ▶ Click on to remove the selected entry.
- ▶ Click on to edit the selected entry.
- ▶ Click on to copy the selected entry.

Local (USB) devices which are to be used for drive mapping purposes must first be set up as storage devices.

Before you unplug a hotplug storage device from the device, you must safely remove it. Otherwise, data on the hotplug storage device can be damaged. Depending on the configuration, there is one or several possibilities to safely remove a hotplug storage device:

- Click on in the task bar. The taskbar is not available in a fullscreen session.
- Click on in the in-session control bar. Depending on the configuration, the in-session control bar may be available in a fullscreen session. For further information, see In-session Control Bar.
- Function **Accessories > Safely Remove Hardware** with further starting possibilities; amongst other things, a hotkey can be defined here.
If the following warning is displayed: **Volume(s) still in use. Dont' remove the device.**, then the hotplug storage device must not be removed. First, exit the program concerned or close all files or directories that reside on the hotplug storage device.

Add Drive Mapping

- **Enable:**

The drive will be made available in the session.

- **Drive to map:** DOS-style drive letters on the Citrix Server.



- ⓘ If the drive letter you have selected is no longer available on the Citrix server, the specified directory or local drive will be given the next free letter during the logon.

- **Local drive path:** Unix path name of the local directory to which the mapping is to refer.

- ⓘ If you map a locally connected device, use the pre-defined path names available in the drop-down field.

- **Read access**

Possible options:

- yes
- no
- ask user: The read access right is queried when each ICA session is accessed for the first time.

- **Write access**

Possible options:

- yes
- no
- ask user: The write access right is queried when each ICA session is accessed for the first time.



COM Ports

Menu path: **Setup > Sessions > Citrix > Citrix Global > Mapping > COM Ports**

- **COM port mapping**

Enables the mapping of serial devices connected to the device to the serial interfaces of the Citrix server. (Default)

i If you would like to use signature pads, you must enable them beforehand under **User Interface > Input > Signature Pad**(see page 680).

To manage the list of **COM port devices**, proceed as follows:

- ▶ Click to create a new entry.
- ▶ Click to remove the selected entry.
- ▶ Click to edit the selected entry.
- ▶ Click to copy the selected entry.

Add

- **COM port device:** Allows you to select from all serial and USB interfaces on the device.

Possible values:

- "COM 1"
- "COM 2"
- "COM 3"
- "COM 4"
- "USB COM 1": For UD3-LX60 devices (mainboard: M350C), this port must be used instead of "COM 1".
- "USB COM 2"
- "USB COM 3"
- "USB COM 4"

- **Detect Devices...:** Opens a dialog allowing you to select the device file. 3 device files are available for each device; the **Description** column shows the type of device file:

- (GENERIC) [device designation]: Generic type. The name of the device file ends in a consecutive number which depends on the boot procedure or the order of insertion.
Example: `/dev/ttyUSB0`
- (BY PORT) [device designation]: According to USB port. The device file is in the `/dev/usbserial/` directory. The name of the device file ends in the number of the USB port that the device is plugged into. Example: `/dev/usbserial/ttyUSB_P12`
- (BY USBID) [device designation]: According to USB ID. The device file is in the `/dev/usbserial/` directory. The name of the device file ends as follows: `_V[Vendor ID]_P[Product ID]`. Example: `/dev/usbserial/ttyUSB_V067b_P2303`
- (Virtual) [device designation]: Virtual device; used for signature pads for example. Example: `/dev/ttyVST0`



- i If your device has an additional multiport PCI card, more than 2 connections may be available.



Printer

Menu path: **Setup > Sessions > Citrix > Citrix Global > Mapping > Printer**

You can set up a printer for ICA sessions here.

- **Client printer mapping:** With this function, the locally connected device printer is made available for your ICA sessions, provided that it was not disabled on the server side.
- **Set another default printer:**
 - Allows you to specify a default printer for the client which differs from the one defined in the printer setup.
 - Do not set another default printer. (default)
- **Default printer:** Print queues used on the device to specify the default printer for the session. `lp` is the locally configured default printer.
- **Default printer driver:** Windows driver name for the printer which is automatically set up. Enter one of the universal drivers or your own driver name here.
Possible values:
 - Citrix PCL4 universal driver (old)
 - Citrix Universal Printer
 - Citrix XPS Universal Printer
 - User entry

i See also <https://support.citrix.com/article/CTX140208>.

i The printers must be set up on the **Devices > Printers > CUPS > Printer** page and must be enabled there for mapping in ICA sessions, see ICA sessions.

Because the device merely places incoming print jobs in a queue, you need to install the printer on the server.



Device Support

Menu path: **Setup > Sessions > Citrix > Citrix Global > Mapping > Device Support**

In this area, you can enable virtual ICA channels for communicating with various devices connected to the device.

The devices supported are listed in the [IGEL Third Party Hardware Database](#)⁴.

DriveLock channel: The virtual DriveLock channel is implemented on the device. The channel must also be installed on the Citrix server.

DriveLock can read hardware data from local USB devices and transfer these data to the Citrix server with the help of the Virtual ICA Channel Extension. From *IGEL Linux Version 10.03.500*, this is also possible with SATA devices. When using whitelists, rules based on the hardware properties of the connected drive (e.g. manufacturer details, model and serial number) are taken into account.

Important information regarding DriveLock can be found in the FAQ Using DriveLock with IGEL Devices.

- A virtual channel for DriveLock is enabled.
- No virtual channel for DriveLock is enabled. (Default)

deviceTRUST channel

- A virtual channel for deviceTRUST is enabled.
- No virtual channel for deviceTRUST is enabled. (Default)

Crossmatch DigitalPersona fingerprint channel

- A virtual channel for Crossmatch DigitalPersona is enabled.
- No virtual channel for Crossmatch DigitalPersona is enabled. (Default)

Diktamen Channel for Dictation

- A virtual channel for Diktamen is enabled..
- No virtual channel for Diktamen is enabled. (Default)

Grundig MMC-Kanal for dictation with Grundig devices

- A virtual channel for communication with Grundig devices is enabled.
- No virtual channel for communication with Grundig devices is enabled. (Default)

Nuance channel for dictation: Virtual audio channel for dictation devices. Dictation microphones from Grundig, Philips and Olympus are supported.

ⓘ This channel is only responsible for audio transmission. The channel for dictation device operating elements is manufacturer-specific and must be enabled separately.

- The Nuance audio channel is enabled.
- The Nuance audio channel is not enabled. (Default)

Olympus Channel for dictation

- A virtual channel for communication with Olympus devices is enabled.
- No virtual channel for communication with Olympus devices is enabled. (Default)

⁴ <https://www.igel.com/linux-3rd-party-hardware-database/>

**signotec signature pad channel**

- A virtual channel for communication with signotec signature pads is enabled.
 No virtual channel for communication with signotec signature pads is enabled. (Default)

StepOver signature pad channel

- A virtual channel for communication with StepOver signature pads is enabled.
 No virtual channel for communication with StepOver signature pads is enabled. (Default)

Philips speech channel for dictation

- A virtual channel for communication with Philips dictation devices is enabled.
 No virtual channel for communication with Philips dictation devices is enabled. (Default)

DPM server drive: Via this drive, the Philips PocketMemo dictation device makes the voice recordings available to the server. (Default: P)

- i** The dictation device is automatically assigned to the selected drive letter. Ensure that no other Hotplug storage device is assigned to this drive letter. Further information can be found under [Hotplug storage device](#)(see page 779) and [Drive mapping](#)(see page 60).

SpeechAir server drive: Via this drive, the Philips SpeechAir dictation device makes the voice recordings available to the server. (Default: S)

- i** The dictation device is automatically assigned to the selected drive letter. Ensure that no other Hotplug storage device is assigned to this drive letter. Further information can be found under [Hotplug storage device](#)(see page 779) and [Drive mapping](#)(see page 60).

Kofax SPVC signature pad channel

- The Kofax SPVC signature pad channel is enabled.
 The Kofax SPVC signature pad channel is not enabled. (Default)

Lakeside SysTrack channel

- The Lakeside SysTrack channel is enabled.
 The Lakeside SysTrack channel is not enabled. (Default)



Firewall

Menu path: **Setup > Sessions > Citrix > Citrix Global > Firewall**

In this area, you can configure the following firewall settings:

Alternative address

- Allows you to use a proxy or Secure Gateway server as an alternative address for connections via a firewall.
 Do not use an alternative address (default)

SOCKS / Secure Proxy

Proxy type

- None (Direct Connection)
- SOCKS: A proxy that uses the SOCKS protocol
- Secure (HTTPS): An HTTP proxy with TLS/SSL encryption.

Proxy server: Name or IP address of the proxy server

Proxy port: TCP port of the proxy server (default: 1080)

Secure Gateway (Relay Mode)

Secure gateway address: If you would like to use a Citrix Secure Gateway in relay mode, you must give the full DNS name – the IP address is not sufficient in this case.

Port: TCP port of the gateway (default: 443)



Options for an IGEL OS Citrix Session

In this area, you can optimize the general behavior and performance for Citrix sessions in IGEL OS.

Menu path: **Sessions > Citrix > Citrix Global > Options**

Use server redraw

- The Citrix server is responsible for refreshing the screen content.
- Do not use server redraw.*

Disable Windows alert sounds

- Switches off the Windows warning sounds.
- The warning sounds remain enabled.*

Backing store

- The X Server temporarily stores hidden window content.
- Window content is not stored.*

Deferred screen update mode

- Enables delayed updates from the local video buffer on the screen. The local video buffer is used if the seamless Windows mode or HDX latency reduction is used.
- No delayed update.*

Cache size in kB

Default: 1024

Minimum bitmap size in bytes

The minimum size of the bitmap files that are to be stored in the cache. (Default: 1024)

Persistent cache path

The directory where the files are to be stored locally. (Default: \$ICAROOT/cache)

- ⚠ Do not make the cache too big; otherwise, you run the risk of the device having too little storage space for its own system and other applications. You may have no alternative but to equip your device with additional RAM.



Scrolling control

Depending on the speed of your network or the response time of your server, there may be a delay between you letting go of the mouse button on a scroll bar and the scrolling actually stopping (e.g. when using Excel). Changing this value may help. (Default: 100)

Audio bandwidth limit in StoreFront sessions

- **High***
- **Medium**
- **Low**

i Higher quality requires more network and computing resources.

Auto reconnect

Automatically attempt to reconnect if the connection is terminated.*

Do not attempt to reconnect.

Maximum retries

Default: 3

Delay in seconds before reconnecting

Default: 30

Allow Kerberos passthrough authentication in StoreFront sessions

Kerberos passthrough authentication is allowed.*

Kerberos passthrough authentication is not allowed.

i This point concerns Citrix XenApp in Version 6.5 and older.

CGP address

- **Use server address**
- **Text input**
- **disabled***

Multistream sessions

Support multistream ICA.

Do not support multistream ICA.*



* IGEL OS system default



Native USB Redirection for Citrix Sessions in IGEL OS

USB devices can be permitted or prohibited during a Citrix session on the basis of rules. Sub-rules for specific devices or device classes are also possible. The use of rules is described under [USB Access Control](#)(see page 785). See also [How to Configure Citrix Native USB Redirection](#).

An overview and best-practice recommendations for the use of webcams can be found under [Webcam Redirection and Optimization in IGEL OS](#).

Menu path: **Sessions > Citrix > Citrix Global > Native USB Redirection**

The screenshot shows the 'Configuration' interface with the 'Sessions' tree selected. Under 'Citrix Global', 'Native USB Redirection' is highlighted. The main pane displays 'Class Rules' and 'Device Rules'. A modal window titled 'Add' is open over the 'Device Rules' table, showing fields for Rule (Allow), Vendor ID (Deny), Product ID (Allow), Extra Config (Connect), and Name (Policy Rule). Buttons for 'OK' and 'Cancel' are at the bottom of the modal.

Native USB redirection

- Native USB redirection is enabled globally.
- Native USB redirection is disabled. (Default)

- ⓘ Enable either **native USB redirection** or **Fabulatech USB redirection**, but not both together.
- ⓘ Disable USB redirection if you use DriveLock. Further information can be found under [Using DriveLock with IGEL Devices](#).

Default rule

This rule will apply if no special rule was configured for a class or a device.

- **Deny (Default)**



- **Allow**

Tip

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

Class Rules

Class rules apply to USB device classes and sub-classes.

To manage rules, proceed as follows:

- ▶ Click to create a new entry.
- ▶ Click to remove the selected entry.
- ▶ Click to edit the selected entry.
- ▶ Click to copy the selected entry.

Add class rule:

Rule:

- **Deny:** No automatic redirect of a device
- **Allow:** Automatic redirect of a device only after a session starts
- **Connect:** Automatic redirect of a device when a session starts

In the case of **Connect** or **Allow**, the device is automatically redirected when it is unplugged and plugged in during a session, see <https://docs.citrix.com/en-us/citrix-workspace-app-for-linux/configure-xenapp.html#usb>.

Class ID: Selection list

Sub-class ID: Selection list

Name: Free text entry

Device Rules

Device rules apply to specific USB devices.

Add device rule:

Rule:

- **Deny:** No automatic redirect of a device
- **Allow:** Automatic redirect of a device only after a session starts
- **Connect:** Automatic redirect of a device when a session starts



i In the case of **Connect** or **Allow**, the device is automatically redirected when it is unplugged and plugged in during a session, see <https://docs.citrix.com/en-us/citrix-workspace-app-for-linux/configure-xenapp.html#usb>.

⚠ If you have problems with device redirection after the update to Citrix Workspace App 22.07 or higher, try to change the rule to **Connect**.

i **Composite USB Redirection**

In IGEL OS 11.08.200 and higher, you can configure composite USB redirection which is needed for multifunctional devices that use different interfaces. Examples of such composite USB devices are dictation microphones or Bloomberg keyboards which comprise a keyboard, fingerprint reader, an audio device, USB hub, etc.

To redirect the entire composite device to the session, only **Vendor ID** (`vid`) and **Product ID** (`pid`) must be added.

If you need to split the composite device and redirect only the child interfaces that use a generic USB channel, you must also add filter parameters `split` and `intf` under **Extra Config**. For more information on composite USB redirection and sample device rules, see <https://docs.citrix.com/en-us/citrix-workspace-app-for-linux/configure-xenapp.html#usb>.

Vendor ID: Hexadecimal manufacturer number

Product ID: Hexadecimal device number

i **Getting USB Device Information**

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see [Using “System Information” Function\(see page 592\)](#).

System Information example:



Devices - USB Devices - System Information

Information View Help

Refresh Generate Report Copy to Clipboard Synchronize

Computer

- Summary
- Operating System
- Security
- Kernel Modules
- Boots
- Languages
- Memory Usage
- Filesystems
- Display
- Environment Variables

Devices

- System DMI
- Processor
- Graphics Processors
- Monitors
- Memory Devices
- PCI Devices
- USB Devices**
- Network
- Interfaces

Done.

001:001 Linux 2.0 root hub
 002:001 Linux 1.1 root hub
 002:002 VMware Virtual Mouse
 002:003 VMware Virtual USB Hub
 002:004 **logitech** 960 Headset

Device Information

Product [0x0002] 2.0 root hub
 Vendor [0x1d6b] Linux Foundation
Linux
 Device EHCI Host Controller
 Manufacturer Linux 5.12.19 ehci_hcd
Linux
 Max Current 0 mA
 USB Version 2.00
 Speed 480 Mb/s

Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb` :

Local Terminal

File Edit View Terminal Tabs Help

```
root@ITC005056930CAD:~# lsusb | grep -i logitech
Bus 002 Device 004: ID 046d:0a45 Logitech, Inc. 960 Headset
root@ITC005056930CAD:~#
```

Extra Config: Allows to add `split` and `intf` parameters to split the composite USB device(see page 73).
 Example:

`CONNECT: vid=047F pid=C039 split=1 intf=03 # Allow HID device and connect automatically.`

Name: Free text entry



Fabulatech USB Redirection

Menu path: **Sessions > Citrix > Citrix Global > Fabulatech USB Redirection**

Redirection for USB devices can be allowed or denied during a Citrix session on the basis of rules. Sub-rules for specific devices or device classes are also possible. The use of rules is described under [USB Access Control](#)(see page 785).

- ⓘ For the Fabulatech USB Redirection, a server-side component is required. We recommend the USB for Remote Desktop IGEL Edition; see <http://www.usb-over-network.com/partners/igel/>.

Fabulatech USB Redirection

Fabulatech USB Redirection is enabled for all Citrix sessions.

- ⓘ Enable either **Native** or **Fabulatech USB Redirection** – not both together. Disable USB redirection if you use DriveLock.
- ⓘ Ensure that no other Hotplug storage device (USB stick) is connected if a session is started with Fabulatech USB Redirection. Otherwise, the hotplug storage device will not be securely removed when the session starts, and this could lead to data loss. With IGEL Linux Version 10.02.x the Hotplug storage device is already insecurely removed when the Fabulatech USB Redirection is enabled.

Default rule: This rule will apply if no special rule was configured for a class or a device.

- Deny
- Allow

Tip

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

Class Rules

Class rules apply to USB device classes and sub-classes.

Managing rules:

- Create a new entry
- Remove the selected entry
- Edit the selected entry
- Copy the selected entry

Class rule properties:

Rule:



- **Allow:** Devices that have the properties defined here are redirected by the Fabulatech USB Redirection.
- **Deny:** Devices that have the properties defined here are not redirected.

Class ID: Device class

Subclass ID: Subclass relating to the specified device class

Name: Free text entry

Override serial: Serial number that will appear in the session

Override name: Device name that will appear in the session

Postpone

- The USB device is only removed from the system (endpoint device) when the session starts.
 The USB device is no longer shown immediately after the system is booted.

i This setting is only effective if the **Takeaway** parameter is enabled.

Takeaway

- The USB device may be removed from the system (endpoint device).
 The USB device may not be removed.

No Reset

- The device will not be automatically reset after the connection with the session has been terminated.
 The device will be reset after the connection with the session has been terminated.

Device Rules

A device rule applies to a specific device that is identified by its serial number.

Device rule settings:

Rule:

- Allow
- Deny

Vendor ID: Hexadecimal manufacturer number

Product ID: Hexadecimal device number

i Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see [Using “System Information” Function\(see page 592\)](#).

System Information example:



Devices - USB Devices - System Information

Information View Help

Refresh Generate Report Copy to Clipboard Synchronize

Computer

- Summary
- Operating System
- Security
- Kernel Modules
- Boots
- Languages
- Memory Usage
- Filesystems
- Display
- Environment Variables

Devices

- System DMI
- Processor
- Graphics Processors
- Monitors
- Memory Devices
- PCI Devices
- USB Devices**

Network

Interfaces

Done.

Device Information

Product [0x0002] 2.0 root hub
Vendor [0x1d6b] Linux Foundation
Linux
Device EHCI Host Controller
Manufacturer Linux 5.12.19 ehci_hcd
Linux
Max Current 0 mA
USB Version 2.0
Speed 480 Mb/s

The device **002:004 logitech 960 Headset** is highlighted with a red box.

Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb` :

Local Terminal

```
File Edit View Terminal Tabs Help
root@ITC005056930CAD:~# lsusb | grep -i logitech
Bus 002 Device 004: ID 046d:0a45 Logitech, Inc. 960 Headset
root@ITC005056930CAD:~#
```

Name: Free text entry

Override serial: Serial number that will appear in the session.

Override name: Device name that will appear in the session.

Postpone

The USB device is only removed from the system (endpoint device) when the session starts.

The USB device is no longer shown immediately after the system is booted.



i This setting is only effective if the **Takeaway** parameter is enabled.

Takeaway

- The USB device may be removed from the system (endpoint device).
- The USB device may not be removed.

No Reset

- The device will not be automatically reset after the connection with the session has been terminated.
- The device will be reset after the connection with the session has been terminated.



Fabulatech Scanner Redirection

Menu path: **Sessions > Citrix > Citrix Global > Fabulatech Scanner Redirection**

Redirection for a Fabulatech scanner can be allowed during a Citrix session.

Fabulatech Scanner for Remote Desktop

Fabulatech Scanner for Remote Desktop is enabled.

- i For more information, see Citrix Fabulatech Scanner Redirection in IGEL OS.



HDX Multimedia Settings for an IGEL OS Citrix Session

HDX multimedia redirection improves the playback of audio and video content during a Citrix session.

Hardware acceleration for multimedia playback is available on specific devices. For further information, see [Hardware Video Acceleration on IGEL OS](#).

See also an overview and best-practice recommendations for the use of webcams under [Webcam Redirection and Optimization in IGEL OS](#).

Menu path: **Sessions > Citrix > Citrix Global > HDX Multimedia**

The screenshot shows the 'Sessions' configuration menu. Under 'Citrix Global', the 'HDX Multimedia' option is selected and highlighted in blue. The right-hand panel displays several configuration options for HDX Webcam redirection:

- Multimedia redirection**: Checked.
- HDX RealTime Webcam redirection**: Unchecked.
- Automatic HDX webcam configuration**: Checked.
- Resolution grade**: Set to 'Normal'.
- HDX Webcam frame rate**: Set to 5.
- HDX Webcam quality**: Set to 16.
- HDX Webcam width**: Set to 352.
- HDX Webcam height**: Set to 288.
- HDX Webcam delay time**: Set to 2000.
- HDX Webcam delay type**: Set to 1.
- HDX RealTime Media Engine**: Checked.
- Please note: With an enabled Browser Content Redirection in Citrix, any h.264 multimedia content within Firefox (incl. video playback) is not functional anymore. These two features cannot be used simultaneously.
- Browser content redirection**: Unchecked.

Multimedia redirection

- Multimedia data are sent to the device and decoded there.*
 Multimedia data are decoded on the server.

HDX RealTime Webcam redirection

- Redirection is enabled.
 Redirection is disabled.*

Automatic HDX webcam configuration

- The endpoint device detects the characteristics of the webcam and derives 6 different quality levels from these characteristics. The user can choose a quality level with the **Resolution grade** parameter.*
 The webcam must be configured manually using **HDX Webcam frame rate** and the subsequent parameters. For information on how to determine the capabilities of the webcam, see [Using Webcam Information](#)(see page 617).

Resolution grade

Possible options:

- **Very low**
- **Low**



- **Normal***
- **High**
- **Very high**
- **Best:** The highest resolution that is possible while maintaining a fluent video replay

HDX Webcam frame rate

The frame rate that is requested from the webcam. (Default: 5)

HDX Webcam quality

The image quality requested from the webcam. Range: 1-63. (Default: 16)

HDX Webcam width

The image width requested from the webcam. (Default: 352)

HDX Webcam height

The image height requested from the webcam. (Default: 288)

HDX Webcam delay time

Time to wait before the webcam is opened, in milliseconds. (Default: 2000)

HDX Webcam delay type

Possible options:

- **0:** No delay
- **1*:** If the time interval since the last closing of the webcam is less than the defined delay time (**HDX Webcam delay time**), the delay length is the remaining time.
- **2:** The delay time is as defined by **HDX Webcam delay time**.

HDX RealTime Media Engine

The HDX RealTime Media Engine is enabled and significantly improves the performance of Lync / Skype for Business.*

The HDX RealTime Media Engine is not used.

Browser content redirection (If enabled, Firefox will lose H.264 multimedia support)

i Please note: With an enabled **Browser content redirection** in Citrix, any H.264 multimedia content within Firefox (incl. video playback) is not functional anymore. These two features cannot be used simultaneously.

The browser content is redirected from the server to the device, e.g. to reduce the load on the server. This setting has an effect on the hardware video acceleration with Chromium or Firefox; see How Can I Use H.264 Hardware Acceleration for Chromium or Firefox Browsers on IGEL OS Endpoint Devices?

Sessions



Browser content redirection is disabled.*

*IGEL OS system default



Codec

Menu path: **Setup > Sessions > Citrix > Citrix Global > Codec**

- **Graphical codec:** Decoding method for the transferred screen content
 - Automatic: Automatically selects the appropriate codec according to the performance of the hardware.
 - H.264 Deep Compression Codec:
 - High image quality is possible, with lower network load
 - Without available hardware acceleration it is very CPU intensive.

i At the Citrix Server following policies must be set:

- **Use video codec for compression** must be enabled.
- **For the entire screen**: Text tracking should be enabled if bandwidth is not a problem to increase readability in Office applications
- **For actively changing regions**: Citrix Receiver 13.6+ required, otherwise JPEG fallback will be loaded
- **Use video codec when preferred**: If **For actively changing regions** is selected by Citrix, a Citrix receiver 13.6+ must be activated, otherwise JPEG fallback is loaded.

- JPEG:
 - High image quality possible, with high network load
 - Moderate CPU load

Additional parameters for H.264 Deep Compression Codec

These parameters are relevant if **Automatic** or **H.264 Deep Compression Codec** is selected.

- **Accelerated H.264 Deep Compression Codec**
 - Enables hardware-accelerated decoding with H.264, which reduces CPU load.
 - Uses the software implementation of H.264 and results in a greater CPU load. (default)
- For more information, read the Setting up Citrix Sessions with Hardware-Accelerated H.264 Deep Compression Codec How-To.

Following options are available in combination with H.264 Deep Compression Codec:

- **Text tracking:**
 - Loss-free depiction of texts (default)

Text is displayed sharper, especially if "Visual Quality" is set to Low/Medium. Recommended for office applications, but requires a higher available bandwidth. With bad connection and EDT over UDP it can lead to missing text parts.
- **Small frames feature:**
 - Pixel-perfect depiction of lines etc. (default)

This feature allows efficient processing when only a small part of the screen changes over time (for example, when a cursor flashes on an otherwise stable background).



Additional parameters for JPEG

These parameters are relevant if **JPEG** is selected.

- **JPEG direct-to-screen decoding**
 Decodes image tiles directly without using a bitmap cache.
 No JPEG direct-to-screen decoding (default)
- **JPEG batch decoding**
 Enables batch processing and delayed XSync. (default)



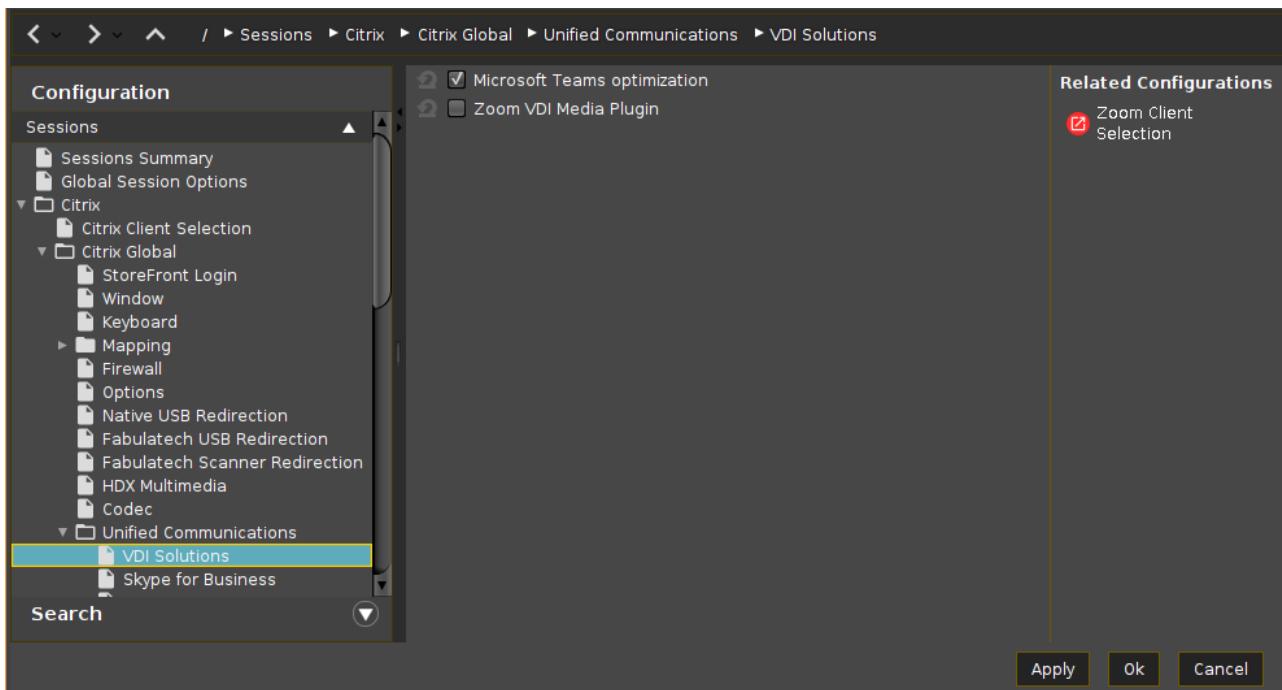
Unified Communications Settings for Citrix Sessions in IGEL OS

This article shows you how to use the Citrix session-related unified communications settings in IGEL OS. It is necessary to set some additional parameters in IGEL OS to leverage the Citrix-related multimedia enhancements. These parameters and their functions are explained below.

Menu path: **Sessions > Citrix > Citrix Global > Unified Communications**

VDI Solutions

Menu path: **Sessions > Citrix > Citrix Global > Unified Communications > VDI Solutions**



Microsoft Teams optimization

⚠ Server and Network Requirements

Microsoft Teams optimization requires additional configuration on the Citrix VDI Desktop image, as well as some additional network configurations.

For more information, see <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/multimedia/opt-ms-teams.html>.

- The audio and video streams for Microsoft Teams are redirected to the endpoint devices. Audio and video data are not processed by the server.*
- The audio and video streams for Microsoft Teams are not redirected.



i Dynamic e911 Support

IGEL OS 11.08.200 and higher supports dynamic emergency calling with MS Teams for Citrix sessions. When Microsoft Calling Plans, Operator Connect, and Direct Routing are used, the feature allows you to configure and route emergency calls like 999, 911, etc. and to notify security staff. The notification is provided based on the current location of the Citrix Workspace app running on the endpoint device. For more information on dynamic emergency calling in Citrix and the required server-side settings, see <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/multimedia/opt-ms-teams.html#microsoft-phone-system>.

To enable dynamic emergency calling in IGEL OS, go to **System > Registry** and activate the following registry key:

Parameter	Citrix Support for dynamic e911
Registry	<code>ica.emergencycalling</code>
Value	false / true
Note	The feature is supported for Citrix Workspace app version 21.12 and higher; for how to change the version, see Citrix Client Selection in IGEL OS (see page 51).

Zoom VDI Media Plugin

⚠ Server and Network Requirements

Zoom optimization requires additional configuration on the Citrix VDI Desktop image, as well as some additional network configurations.

For more information, see <https://support.zoom.us/hc/en-us/articles/201362163-Mass-Installation-and-Configuration-for-Windows>.

- The audio and video streams for Zoom are redirected to the endpoint devices. Audio and video data are not processed by the server.
- The audio and video streams for Zoom are not redirected.*

- i** The **Zoom VDI Media Plugin** version must be equal to or less than the version of the server-side Zoom VDI application; a plugin with a higher version is not supported. Zoom recommends updating the Zoom plugin after updating the Zoom VDI application since new features can require an updated plugin. For more information, see the Zoom article [VDI backwards compatibility](#)⁵. You can select the Zoom VDI Media Plugin version under **Sessions > Unified Communications > Zoom Client Selection > Zoom client version**.

Skype for Business

Menu path: **Sessions > Citrix > Citrix Global > Unified Communications > Skype for Business**

⁵ <https://support.zoom.us/hc/en-us/articles/360041602711-VDI-backwards-compatibility>

A screenshot of the Citrix Configuration software interface. The left sidebar shows a tree view of configuration categories: Global Session Options, Citrix (Citrix Client Selection, Citrix Global, StoreFront Login, Window, Keyboard, Mapping, Firewall, Options, Native USB Redirection, Fabulotech USB Redirection, Fabulotech Scanner Redirection, HDX Multimedia, Codec), Unified Communications (VDI Solutions, Skype for Business, Cisco), Citrix StoreFront, Citrix Self-Service, and a Search bar. The "Skype for Business" node under "Unified Communications" is selected and highlighted with a blue background. The main pane shows a checkbox labeled "HDX RealTime Media Engine" which is checked. At the bottom right of the main pane are three buttons: "Apply", "Ok", and "Cancel".

The screenshot shows the configuration path: Sessions > Citrix > Citrix Global > Unified Communications > Skype for Business. The "HDX RealTime Media Engine" checkbox is checked.

⚠ Server and Network Requirements

Skype for Business optimization requires additional configuration on the Citrix VDI Desktop image, as well as some additional network configurations.

For more information, see <https://docs.citrix.com/en-us/hdx-optimization/current-release.html>.

The HDX RealTime Media Engine is required for using Skype for Business in a Citrix session.

HDX RealTime Media Engine

- The HDX RealTime Media Engine is active.*
 The HDX RealTime Media Engine is not active.

Cisco

Menu path: **Sessions > Citrix > Citrix Global > Unified Communications > Cisco**

Here you can activate or deactivate the virtual desktop optimization for Cisco Webex and define settings for the Cisco JVDI client.



Cisco Webex Meetings VDI

This virtual desktop optimization contains a media engine and redirects the audio and video streams so that they are exchanged directly between the endpoint devices and Webex Meetings cloud, without going through the hosted virtual desktop in the datacenter.

⚠ The Cisco Webex Meetings VDI plugin and your server-side application should have the same version. For details on backward compatibility, see [Webex Meetings VDI Release Notes](#)⁶.

To select the version of the Cisco Webex Meetings plugin:

1. In the UMS configuration dialog or the local Setup, go to **Sessions > Unified Communications > Cisco Webex Meetings VDI Selection > Cisco Webex Meetings client version**.
(If you do not see the corresponding version in the UMS configuration dialog, but it is listed in the release notes, please update the firmware your profile is based on.)
2. Select the desired version and click **Apply** or **Ok**.

For further information, see the Cisco documentation for Webex Meetings:

- General information: <https://help.webex.com/en-us/nfjsqzbb/Cisco-Webex-Meetings-Virtual-Desktop-Software>

⁶https://help.webex.com/en-us/article/glj57y/Release-Notes-for-Cisco-Webex-Meetings-Virtual-Desktop-Software-Release-42.x#Cisco_Reference.dita_fcb4e1d7-dbef-4bab-8842-9b1a8f84a9e5



- Administration guide: https://www.cisco.com/c/en/us/td/docs/collaboration/webex_vdi/admin_webex_b_admin-cisco-wmvdi-40-8.html⁷
- Installation: https://www.cisco.com/c/en/us/td/docs/collaboration/webex_vdi/admin_webex_b_admin-cisco-wmvdi-40-8/webex_m_wvdi-software-installation.html

The Cisco Webex Meetings VDI solution is enabled.

The Cisco Webex Meetings VDI solution is disabled.*

Cisco Webex VDI

This virtual desktop optimization contains a media engine and redirects the audio and video streams so that they are exchanged directly, without going through the hosted virtual desktop in the datacenter.

For further information, see the Cisco documentation for Webex VDI:

- General information: https://www.cisco.com/c/dam/en_us/solutions/collaboration/docs/cisco-webex-teams-solution-overview.pdf
- Overview about the supported versions: https://help.webex.com/en-us/ntp1us7/Webex-VDI-Release-Notes#Cisco_Reference.dita_13d9aace-b6f9-41dc-a6e0-9f7a48834060
- Administration guide: [Administration - Webex App | Installation and Automatic Upgrade](#)⁸
- Installation: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/vdi/wbx-teams-vdi-deployment-guide.pdf

The Cisco Webex VDI solution is enabled.

The Cisco Webex VDI solution is disabled.*

Cisco JVDI Client

For the vendor documentation for the Cisco JVDI client, see [Deployment and Installation Guide for Cisco Jabber Softphone for VDI Release 14.0](#)⁹.

The Cisco JVDI Client is enabled.

The Cisco JVDI Client is disabled.*

- i** If you do not see the option **Cisco JVDI Client**, check if the **Cisco JVDI Client** is enabled under **System > Firmware Customization > Features**. Reboot the device if required.
If you have reduced the IGEL OS feature set before and cannot activate **Cisco JVDI Client**, see Adapting IGEL OS 11.04 or Higher for Devices with Small Storage.

Audio

⁷<https://eur03.safelinks.protection.outlook.com/>

⁸<https://help.webex.com/en-US/article/nw5p67g/Webex-App-%7C-Installation-and-Automatic-Upgrade>
⁹https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jvdi/14_0/dig/jvdi_b_deploy-install-jvdi-14-0/jvdi_b_deploy-install-jvdi-12-9_chapter_010.html



Default volume

Headphone volume control. (Default: 80%)

Default microphone volume

Microphone volume control. (Default: 80%)

Default ring volume

Ringtone volume control. (Default 100%)

Internal sound card

Here you have the possibility to define a sound card. If you leave the field empty, the default sound card of the system is used.

For further information, see Sound Preferences.

Video

You can set the Cisco JVDI Client to use the default resolutions of the camera or to use a user-defined set of resolutions. Separate configurations for cameras with and without hardware acceleration are possible.

Allow default resolutions (for cameras without hardware resolution)

The default resolutions of the camera are used.*

A user-defined set of resolutions is used. You can add a resolution by clicking in the **Camera** area and selecting the desired resolution.

Allow default resolutions (for cameras with hardware resolution)

The default resolutions of the camera are used.*

A user-defined set of resolutions is used. You can add a resolution by clicking in the **Hardware Accelerated Camera** area and selecting the desired resolution.

Related Topics

[Webcam Redirection and Optimization in IGEL OS](#)

[Which Unified Communication Solutions Does IGEL OS Support?](#)

*IGEL OS system default



Citrix StoreFront

Menu path: **Sessions > Citrix > Citrix StoreFront**

Most of the settings were already configured under Citrix Global.

- [Server](#)(see page 92)
- [Login Settings for Citrix StoreFront in IGEL OS](#)(see page 93)
- [Appearance](#)(see page 96)
- [Reconnect](#)(see page 97)
- [Refresh](#)(see page 99)
- [Logoff](#)(see page 101)
- [Desktop Integration](#)(see page 103)



Server

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront > Server**

- **Server location:** You can set up up to 5 Citrix master browsers per domain. If the first browser is not available, the second will be queried and so on. Please note that multiple farms can be searched. You can therefore specify addresses for a number of server farms.
- To manage the list, proceed as follows:
 - Click on to create a new entry.
 - Click on to remove the selected entry.
 - Click on to edit the selected entry.
 - Click on to copy the selected entry.

Add

- **Protocol:**
 - https://
- **Citrix Store site address:** Server name or IP address of the server
- **Port:** Network port on which the service is available (default: 443)
- **Path to Store:** (default: Citrix/Store)
- **Store name:** Name of the Citrix store

Domains

- To manage the list of **domains**, proceed as follows:
 - Click on to create a new entry.
 - Click on to remove the selected entry.
 - Click on to edit the selected entry.
 - Click on to copy the selected entry.

Handling of domain in login window:

- normal
- locked
- hidden



Login Settings for Citrix StoreFront in IGEL OS

In the **Login** area, you can define session-specific login options. Login options for Citrix sessions can also be configured in IGEL OS globally under **Citrix > Citrix Global > StoreFront Login**.

Menu path: **Sessions > Citrix > Citrix StoreFront > Login**

Authentication type

Depending on the Citrix client version, the following types are available:

- **Password authentication:** Suitable for on-premises connections; connections via Citrix NetScaler or to a cloud environment may cause problems.
- **Kerberos passthrough authentication:** Uses local login data for listing and launching applications. The option enables single sign-on if login with AD/Kerberos is configured on the device, see [Active Directory/Kerberos](#)(see page 807).
- **Smartcard authentication (StoreFront only, not Web Interface):** Authentication via smartcard will only work with StoreFront, not with Web Interface. For configuration details, see Citrix StoreFront.
- **Citrix authentication mechanism (instead of IGEL), Smartcard disabled:** Recommended for cloud environments and Citrix NetScaler.
- **Citrix authentication mechanism (instead of IGEL), Smartcard enabled:** Recommended for cloud environments and Citrix NetScaler.



- i** If you have set an authentication type with smartcard, select the type of card on the [Smartcard](#)(see page 817) page. You may find it also helpful to read the how-to Smartcard Authentication in IGEL OS.

Depending on the selected authentication type, the following options are available:

Use passthrough authentication

- Cached login data are used for listing and starting applications. For more information, see Passthrough Authentication.
- No passthrough authentication. (Default)

Auto login

- Uses the login data preset on this page when connecting to the server.
- Do not log in automatically. (Default)

User name

Can only be filled in with password authentication.

Password

Can only be filled in with password authentication.

- ⚠** Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

Domain

Can only be filled in with password authentication.

Remember username and domain

- Saves the user name and domain from the last login. (Default)
- The user name and domain will not be saved.

Synchronize Citrix password with screenlock

- Synchronizes the [screenlock password](#)(see page 666) with that of the Citrix application. You can use this option if you want, for example, to use the user's AD password to unlock the screen.
- No synchronization (Default)

Relaunch Citrix login after logoff

- Automatically shows the login dialog again after logging out.



Does not start the login procedure again. (Default)

Start a single published application automatically

This parameter is relevant if exactly 1 published application is provided for the user whose login is configured here.

The published application is started when the user has logged in.

The published application is not started on login. (Default)

Start following applications automatically after server connection is established

A list of applications to be started in the session.

To edit the list, proceed as follows:

- Click on to create a new entry. In the **Add** dialog, give the name of the application.

Application names are case-sensitive.
You can also enter part of the name followed by an asterisk (*).

- Click on to remove the selected entry.
- Click on to move the entry upwards.
- Click on to move the entry downwards.

After a successful login, the associated desktop icon for each available application will be placed on the device desktop. All applications whose name matches one of the names given in the **Start following applications automatically after server connection is established** area will then be launched.

App Protection Feature for the Citrix Workspace App

To strengthen the security of your Citrix environment, you can use the app protection feature in IGEL OS 11.08.200 or higher. It provides anti-keylogging and anti-screen-capturing functionalities. For more information on this feature and the required server-side settings, see <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/secure/app-protection.html>.

To activate the feature on IGEL OS, go to **System > Registry** and enable the following registry key:

Parameter	Citrix App Protection
Registry	<code>ica.appprotection</code>
Value	<code>false / true</code>
Note	The feature is supported for Citrix Workspace app version 22.07 and higher; for how to change the version, see Citrix Client Selection in IGEL OS (see page 51).



Appearance

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront > Appearance**

- **Show applications in the start menu**

- Applications will appear in the start menu (default)
- Applications will not appear in the start menu

- **Show in the start menu**

- All: All Citrix applications will be shown in the start menu.
 - Follow server settings

- **Resize icons for the start menu**

- The size of icons for the start menu will automatically be adjusted. (default)

Automatic scaling can prolong the logon procedure.

- **Apply display filter to start menu entries**

- Only the applications selected in the display filter will be shown in the start menu.
- Do not use display filter (default)

- **Show applications in the Application Launcher**

- Applications will be shown in the Application Launcher. (default)

- **Apply display filter to Application Launcher entries**

- Only the applications selected in the display filter will be shown in the Application Launcher.
- Do not use display filter (default)

- **Show applications on desktop**

- The applications will be shown on the desktop. (default)

- **Keep folder structure on desktop**

- The Citrix sessions are shown in their directory structure on the desktop.
- The directory structure is not shown. (default)

- **Show desktop shortcuts**

- All: All Citrix applications will be shown in the Desktop Launcher.
 - Follow server settings

- **Apply display filter to desktop icons**

- Desktop icons are created only for the applications selected in the display filter (see below). (default)

- **Display filter: Show only the following applications.** In the **Add** dialog, enter the name of the application that is to be shown on the desktop.

To manage the list, proceed as follows:

- Click on to create a new entry.
 - Click on to remove the selected entry.
 - Click on to edit the selected entry.

- **Enable following applications in quick start panel:** In the **Add** dialog, enter the name of the application that is to be shown in the quick start panel.



Reconnect

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront > Reconnect**

- **Automatic reconnection at logon**
 - Connection will take place when logging on.
 - Do not reconnect (default)
- **Connect to**

Possible values:

 - Active and terminated sessions
 - Terminated sessions only
 - Ask user
- **Automatic reconnection from menu/desktop**
 - Reconnect
 - Do not reconnect (default)
- **Connect to**

Possible values

 - Active and terminated sessions
 - Terminated sessions only
 - Ask user
- **Reconnect session name:** Session name (default: Reconnect)

Starting Methods for Sessions

- **Start menu:** If this option is enabled, the session can be launched from the start menu.
- **Application Launcher:** If this option is enabled, the session can be launched with the Application Launcher.
- **Desktop:** If this option is enabled, the session can be launched with a program launcher on the desktop.
- **Quick start panel:** If this option is enabled, the session can be launched with the quick start panel.
- **Start menu's system icon:** If this option is enabled, the session can be launched with the start menu's system icon.
- **Application Launcher's system icon:** If this option is enabled, the session can be launched with the Application Launcher's system icon.
- **Desktop context menu:** If this option is enabled, the session can be launched with the desktop context menu.
- **Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.
- **Path in the Application Launcher:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.
- **Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.



- **Password protection:** Specifies which password will be requested when launching the session.
Possible values:
 - **None:** No password is requested when launching the session.
 - **Administrator:** The administrator password is requested when launching the session.
 - **User:** The user password is requested when launching the session.
 - **Setup user:** The setup user's password is requested when launching the session.
- **Hotkey:**
 The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.
- **Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`. Here, you will find the available modifiers and the associated key symbols:
 - (No modifier) = `None`
 - = `Shift`
 - `[Ctrl]` = `Ctrl`
 - = `Super_L`
 - `[Alt]` = `Alt`

Key combinations are formed as follows with | :

- `Ctrl +` = `Ctrl|Super_L`

- **Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`



Refresh

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront > Refresh**

Refresh Session Name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
-  = `Shift`
- `[Ctrl]` = `Ctrl`
-  = `Mod4`

 When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows key` = `Ctrl|Super_L`

Key: Key for the hotkey

-  To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`



Logoff

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront > Logoff**

- **Logoff session name:** Session name (default: Logoff)

Starting Methods for Session

- **Session name:** Name for the session

! The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

- **Start menu:**
 - The session can be started with the start menu. (Default)
 - The session cannot be found in the start menu.
- **Application Launcher:**
 - The session can be started with the Application Launcher. (Default)
 - The session cannot be found in the Application Launcher.
- **Desktop:**
 - The session can be started with a program starter on the desktop. (Default)
 - The session does not have a program starter on the desktop.
- **Quick start panel:**
 - The session can be started with the quick start panel.
 - The session cannot be found in the quick start panel. (Default)
- **Start menu's system icon:**
 - The session can be started with the start menu's system icon.
 - The session cannot be found in the start menu's system icon. (Default)
- **Application Launcher's system icon:**
 - The session can be started with the Application Launcher's system icon.
 - The session cannot be found in the Application Launcher's system icon. (Default)
- **Desktop context menu:**
 - The session can be started with the desktop context menu.
 - The session cannot be found in the desktop context menu. (Default)
- **Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.
- **Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.
- **Password protection:** Specifies which password will be requested when launching the session.
Possible values:
 - **None:** No password is requested when launching the session.
 - **Administrator:** The administrator password is requested when launching the session.



- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.
- **Hotkey:** A hotkey with which the session can be started is defined. It consists of modifiers and a key.
- **Modifiers:** One or two modifiers for the hotkey:
 - None
 - = Shift
 - [Ctrl] = Ctrl
 - = Super_L
 - [Alt] = Alt

Modifiers can be combined by using the pipe character | :

- [Ctrl]+ = Ctrl|Super_L

- **Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard . Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the character string for the **Key** field. Example: Tab in (keysym 0xff09, Tab)



Desktop Integration

Menu path: **Sessions > Citrix > Citrix StoreFront > Desktop Integration**

Login session name: Session name.

The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.



Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- = `Ctrl`
- = `Mod4`

ⓘ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- = `Alt`

Key combinations are formed as follows with | :

- `Ctrl` + = `Ctrl|Super_L`

Key: Key for the hotkey

- ⓘ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.



Citrix Self-Service

Menu path: **Sessions > Citrix > Citrix Self-Service**

The Citrix Self-Service interface allows access to Citrix Virtual Desktops and Apps via Self-Service UI.

- [Server](#)(see page 106)
- [Options](#)(see page 108)
- [Desktop Integration](#)(see page 109)



Server

Menu path: **Setup > Sessions > Citrix > Citrix Self-Service > Server**

To manage the list, proceed as follows:

- ▶ Click on to create a new entry.
- ▶ Click on to remove the selected entry.
- ▶ Click on to edit the selected entry.
- ▶ Click on to copy the selected entry.

Server: Web Interface

Add:

- **Protocol:**
 - <http://>
 - <https://>
- **Server:** Name or IP address of the server
- **Server port:** Port on which the service is available (default: [80 \(http\)](http://), [443 \(https\)](https://))
- **Path to config.xml file:** (default: [Citrix/PNAgent/config.xml](#))
- **Store Name:** Name for the store

Server: StoreFront

Add:

- **Protocol:**
 - <http://>
 - <https://>
- **Server:** Name or IP address of the server
- **Server port:** Port on which the service is available (default: [80 \(http\)](http://), [443 \(https\)](https://))
- **Path to the store** (default: [Citrix/Store](#))
- **Store Name:** Name for the store

Server: StoreFront Legacy Mode

Add:

- **Protocol:**
 - <http://>
 - <https://>
- **Server:** Name or IP address of the server



- **Server port:** Port on which the service is available (default: [80 \(http\)](#), [443 \(https\)](#))
- **Path to the config.xml file** (default: [Citrix/Store/PNAgent/config.xml](#))
- **Store Name:** Name for the store



Options

Menu path: **Setup > Sessions > Citrix > Citrix Self-Service > Server > Options**

- **Display mode:** Display type for the Self-Service user interface

Possible values:

- Window
- Full screen

i In full screen mode, the IGEL desktop will not be available.

- **Multi user**

The user data on the client will be deleted after logging off or terminating Self-Service. (default)

- **Reconnect after logon:**

The Self-Service user interface reconnects automatically to applications and desktops after being launched.

The Self-Service user interface does not reconnect automatically.

- **Reconnect to apps after starting an application:**

The Self-Service user interface will attempt to reconnect to ongoing sessions if an application is launched or the store is reloaded.

The Self-Service user interface will not attempt to reconnect. (default)



Desktop Integration

Self-Service session: Name for the Self-Service session. (Default: Self-Service)

! The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.



Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

ⓘ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with | :

- `Ctrl` + = `Ctrl|Super_L`

Key: Key for the hotkey

- ⓘ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.



RDP Global

Menu path: **Setup > Sessions > RDP > RDP Global**

This section describes the procedure for configuring the global RDP settings. This configuration applies for all RDP sessions.

- ⓘ The protocol version cannot be configured manually. The version used by the server is automatically recognized and used.

-
- [Gateway](#)(see page 112)
 - [Local Logon](#)(see page 114)
 - [Window](#)(see page 115)
 - [Keyboard](#)(see page 117)
 - [Mapping](#)(see page 118)
 - [Performance](#)(see page 126)
 - [Options](#)(see page 130)
 - [Native USB Redirection](#)(see page 131)
 - [Fabulotech USB Redirection](#)(see page 134)
 - [Fabulotech Scanner Redirection](#)(see page 138)
 - [Multimedia](#)(see page 139)

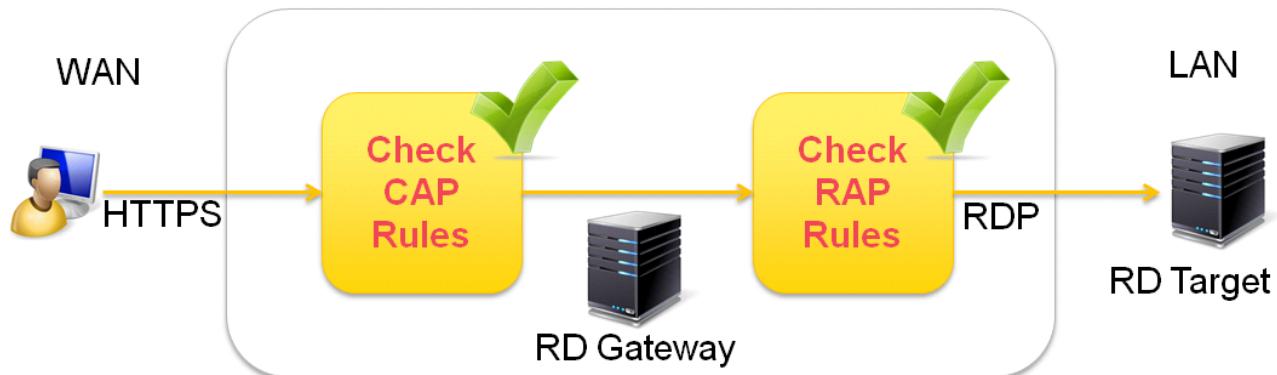
Gateway

Menu path: **Setup > Sessions > RDP > RDP Global > Gateway**

Via Microsoft Remote Desktop Gateway, you can access remote Windows systems.

The gateway translates between the internal *Remote Desktop Protocol* (RDP) and the external HTTPS connection.

Access to the Remote Desktop environment is provided via the browser. The browser establishes a secure connection to the gateway. From here, the connection query is forwarded to the target system. In the process, pre-defined *Connection Access Policies* and *Resource Access Policies* (CAP and RAP) for access control are evaluated.



Enable gateway support:

- Gateway support is enabled and you can configure the following settings:
- Gateway support is disabled. (default)

- **Gateway address**

Info **RD gateway** requires Microsoft Windows Server 2008R2 or Server 2012 with various restrictions for each server version.

The following Windows Server editions can preferably be used as gateway servers:

Server 2008R2 Standard (restricted to 250 RD Gateway connections)

Server 2008R2 Enterprise

Server 2008R2 Datacenter

Server 2012 Standard

Server 2012 Datacenter

Server 2012 Essential (restricted to the RD Gateway role)

Server 2012R2 Standard

Server 2012R2 Essential (restricted to the RD Gateway role)

Info RD Gateway is not supported in the IGEL RDP Legacy Mode.

- **Use other logon data for RD gateway**



- Uses custom data that can be defined below rather than the session access data.
- Uses the session access data. (default)

- **Gateway user name:** User name when logging on to the gateway
- **Gateway password:** Password when logging on to the gateway
- **Gateway domain:** Domain in which the gateway is located



Local Logon

Menu path: **Setup > Sessions > RDP > RDP Global > Local Logon**

In this area, you can prepopulate user data. As a result, you can avoid users possibly having to log in a number of times.

- ⓘ You can also use **Local logon** to freely select the server in the logon window of an RDP session.

- **Use local login window**

The RDP login window is used on the terminal side to set the user name and domain when a connection to the terminal server is established for the first time. (default)

You can configure the following presets:

- **Preset login information**

The login window is prepopulated with the user name and domain. (default)

- **Type:** Here, you can prepopulate the user name and domain in the logon window.

Possible values:

- Set user/domain from last login
- Set user/domain from session setup

- **Show domain**

Shows the domain entry in the logon window. (default)

- **Set client name to user name**

The name of the client for the RDP connection will be set to the user name. This setting may help to resolve reconnection problems during load balancing. (default)

- **Relaunch mode**

The RDP login window is displayed in restart mode and cannot be closed.

The RDP window will not be displayed in restart mode. (default)

- **Enable network authentication**

Enables network authentication via NTLM. Smartcards are not supported here. (default)

- **Domains:** Allows you to add domains which are to be available. If you enter a number of domains, these will be shown in the **Domains** drop-down area in the login module.

To manage the list of domains, proceed as follows:

- ▶ Click to create a new entry.
- ▶ Click to remove the selected entry.
- ▶ Click to edit the selected entry.
- ▶ Click to copy the selected entry.



Window

Menu path: **Sessions > RDP > RDP Global > Window**

In this area, you can configure the window for RDP sessions.

You can change the following settings:

Number of Colors: Specifies the color depth.

Possible values:

- 256
- Thousands
- Millions

Window size: Specifies the width and height of the window.

- Full-screen: The session is shown on the full screen. The device's taskbar is not visible.
- Work area: The session is shown on the full screen, minus the area needed by the device's taskbar.
- Numeric details: The session is shown in the selected resolution or on the selected percentage of the screen area.

Desktop scale factor: Specifies the desktop scaling in percent. Select a value from the selection list or enter a percentage value manually.

(i) Desktop scaling is supported from Windows Server 2012 or higher and from Windows 8.1 or higher.

Possible values:

- Automatic: The resolution set under **User Interface > Display > Options > Monitor-DPI** will be used for the RDP session.
- Numeric details: The display will be magnified by the factor given here. Value range: 100% - 500%

(i) Set the **Desktop scale factor** to a fixed value of 100% to allow server-side desktop scaling take effect. All values other than 100% overwrite the server-side setting.

Enable Display Control

The window size can be changed during the session. (Default)

(i) If the window size is to be changed during the session, at least Windows 8.1 or Windows Server 2012 R2 must be running on the server.

(i) It is not possible to change the window size during the session if **Window size** is set to **full-screen** or **workarea**.

Control Bar for RDP-Sessions

A control bar for minimizing and closing a full-screen session will be shown.

No control bar will be shown. (Default)



- ⓘ If the symbol bar is enabled, a session will be shown on one monitor only, even if **Multimonitor fullscreen mode** is set to **Expand full-screen session across all monitors**.

Multimonitor full-screen mode - If more than one monitor is connected to the terminal:

- Restrict full-screen session to one monitor
- Display full-screen session on all monitors
- Expand full-screen session across all monitors



Keyboard

Menu path: **Setup > Sessions > RDP > RDP Global > Keyboard**

Configure how the keyboard reacts within RDP sessions. The following options are available:

- **Enable clipboard**
 You can use the clipboard. (default)
- **Input language:** Here, you can determine which language is used for auto-correction in the RDP session. This is independent of the keyboard layout. The "Default" setting corresponds to the system setting. (default: Default).
- **Override local window manager keyboard shortcuts**
 All keyboard entries, including those which would otherwise be processed by the local window manager, will be sent straight to the Windows server.
 The keyboard shortcuts of the local window manager will not be overridden. (default)



Mapping

Menu path: **Sessions > RDP > RDP Global > Mapping**

In this area, you can make available locally connected devices such as printers or USB storage devices in RDP sessions.

- [Drive Mapping](#)(see page 119)
- [COM Ports](#)(see page 120)
- [Printers](#)(see page 122)
- [Device Support](#)(see page 123)
- [Audio](#)(see page 125)



Drive Mapping

Menu path: **Sessions > RDP > RDP Global > Mapping > Drive Mapping**

Through drive mapping, connected mass storage devices can be made available in the session. Specify which folders or drives are mapped during the login.

Enable Drive Mapping

Drive mapping is enabled. (Default)

- i** Local (USB) devices which are to be used for drive mapping purposes must first be set up as devices. See [Storage Hotplug](#)(see page 779).

- !** Before you unplug a hotplug storage device from the endpoint device, you must safely remove it. Otherwise, data on the hotplug storage device can be damaged. Depending on the configuration, there is one or several possibilities to safely remove a hotplug storage device:
- Click on ▲ in the task bar. The taskbar is not available in a fullscreen session.
 - Click on ▲ in the in-session control bar. Depending on the configuration, the in-session control bar may be available in a fullscreen session. For further information, see [In-Session Control Bar](#)(see page 661).
 - Function **Accessories > Safely Remove Hardware** with further starting possibilities; amongst other things, a hotkey can be defined here.
If the following warning is displayed: **Volume(s) still in use. Don't remove the device**, then the hotplug storage device must not be removed. First, exit the program concerned or close all files or directories that reside on the hotplug storage device.

Drive Mapping: List of mapped drives.

To set up drive mapping, proceed as follows:

1. Click **[+ Add** to bring up the mapping window.
2. Click **Enabled** to enable the drive connection.
3. Select a **Drive to map** from the list under which the local device or the folder is to be mapped.

- i** If the drive letter you have selected is no longer available on the server, the specified directory or local drive will be given the next free letter during the login.

4. Give the **Local Drive Path** of the local directory to which the mapping is to refer.

- i** If you map a locally connected device, use the pre-defined path names available in the drop-down field. The directories in question are those on which the devices are mounted by default during the boot procedure (e.g. `/autofs/floppy` for an integrated floppy drive).



COM Ports

Menu path: **Setup > Sessions > RDP > RDP Global > Mapping > Serial Connections**

As with locally connected mass storage devices, you can also map the device's local serial connections (COM ports) during an RDP session:

- **Enable COM port mapping:**
 COM port mapping is enabled. (default)
- **Server COM Port starts with:** Specifies the lowest device number that is used on the server for mapping. Possible values:
 - COM 1 to COM 6. (default: COM1)
- **COM Port Devices:** List with mapped local serial devices.
Click to add a serial device.
 - **COM Port Device:**
Possible values:
"COM 1"
"COM 2"
"COM 3"
"COM 4"
"USB COM 1": For UD3-LX60 devices (mainboard: M350C), this port must be used instead of "COM 1".
"USB COM 2"
"USB COM 3"
"USB COM 4"
- **Detect Devices....**: Opens a dialog allowing you to select the device file. 3 device files are available for each device; the **Description** column shows the type of device file:
 - (GENERIC) [device designation]: Generic type. The name of the device file ends in a consecutive number which depends on the boot procedure or the order of insertion.
Example: `/dev/ttyUSB0`
 - (BY PORT) [device designation]: According to the USB port. The device file is in the `/dev/usbserial/` directory. The name of the device file ends in the number of the USB port that the device is plugged into. Example: `/dev/usbserial/ttyUSB_P12`
 - (BY USBID) [device designation]: According to USB ID. The device file is in the `/dev/usbserial/` directory. The name of the device file ends as follows: `_V[Vendor ID]_P[Product ID]`. Example: `/dev/usbserial/ttyUSB_V067b_P2303`
 - (Virtual) [device designation]: Virtual device; used for signature pads for example. Example: `/dev/ttyVST0`

If your device has an additional multiport PCI card, more than 2 connections may be available.



- i** If you would like to use signature pads, you must enable them beforehand under **User Interface > Input > Signature Pad**(see page 680).



Printers

Menu path: **Setup > Sessions > RDP > RDP Global > Mapping > Printers**

In this area, you can configure printer mapping.

Enable Client Printer Mapping

The locally connected device printer is made available for your RDP sessions, provided that it was not disabled on the server-side. (default)

i The printers must be set up on the **Devices > Printer > CUPS > Printers - Configure CUPS Printers in IGEL OS**(see page 756) page and must be enabled there for mapping in RDP sessions.

i Because the device merely places incoming print jobs in a queue, you need to install the printer on the server.



Device Support

Menu path: **Setup > Sessions > RDP > RDP Global > Mapping > Device Support**

In this area, you can enable virtual RDP channels for communicating with various devices connected to the device.

The devices supported are listed in the [IGEL Third Party Hardware Database¹⁰](#).

- **Enable plugin support**

Communication between connected devices and the relevant server applications is enabled.

The individual channels must also be enabled.

Communication between connected devices and server applications is not enabled. (Default)

ⓘ When using DriveLock, ensure that the use of USB devices is not universally restricted; see Devices > USB Access Control.

- **DriveLock channel:** The virtual DriveLock channel is implemented on the device. The channel must also be installed on the RDP server.

DriveLock can read hardware data from local USB devices and transfer these data to the server with the help of the virtual RDP channel extension. From IGEL Linux Version 10.03.500 this is also possible with SATA devices. When using whitelists, rules based on the hardware properties of the connected drive (e.g. manufacturer details, model and serial number) are taken into account.

Important information regarding DriveLock can be found in the Using DriveLock with IGEL Devices FAQ.

A virtual channel for DriveLock is enabled.

No virtual channel for DriveLock is enabled. (Default)

- **Diktamen channel for dictation**

A virtual channel for Diktamen is enabled.

No virtual channel for Diktamen is enabled. (Default)

- **deviceTRUST channel**

A virtual channel for deviceTRUST is enabled..

No virtual channel for deviceTRUST is enabled. (Default)

- **Grundig MMC channel for dictation with Grundig devices**

A virtual channel for communication with Grundig devices is enabled.

No virtual channel for communication with Grundig devices is enabled. (Default)

- **Olympus channel for dictation**

A virtual channel for communication with Olympus dictation devices is enabled.

No virtual channel for communication with Olympus dictation devices is enabled. (Default)

- **Philips speech channel for dictation**

A virtual channel for communication with Philips dictation devices is enabled.

No virtual channel for communication with Philips dictation devices is enabled. (Default)

- **DPM server drive:** Via this drive, the Philips PocketMemo dictation device makes the voice recordings available to the server. (Default: P)

¹⁰ <https://www.igel.com/linux-3rd-party-hardware-database/>



- Information:** The dictation device is automatically assigned to the selected drive letter. Ensure that no other Hotplug storage device is assigned to this drive letter. Further information can be found under Hotplug storage device and Drive mapping.
- SpeechAir server drive:** Via this drive, the Philips SpeechAir dictation device makes the voice recordings available to the server (default: S)
- Information:** The dictation device is automatically assigned to the selected drive letter. Ensure that no other Hotplug storage device is assigned to this drive letter. Further information can be found under Hotplug storage device and Drive mapping.
- Lakeside SysTrack channel**
 The Lakeside SysTrack channel is enabled.
 The Lakeside SysTrack channel is not enabled. (Default)
- Enable smartcard**
 The device's smartcard reader will appear within the RDP session. Applications can access the reader and the smartcards it contains. (Default)
 The device's smartcard reader will not appear within the RDP session.



Audio

Menu path: **Setup > Sessions > RDP > RDP Global > Mapping > Audio**

In this area, you can configure the settings for local audio transmission.

- **Enable client audio**

Possible values:

- On: Audio will be transmitted.
- Off: No audio will be transmitted.

- **Audio quality mode**

Possible values:

- Automatic
- High: High audio quality is favored.
- Medium: Medium audio quality is favored.
- Dynamic

- **Audio compression**

Possible values:

- Automatic
- On: Compressed audio data will be accepted.
- Off: Compressed audio data will not be accepted.

- **Audio recording**

The microphone will be diverted to the session.

The microphone will not be diverted to the session. (Default)



Performance

Menu path: **Setup > Sessions > RDP > RDP Global > Performance**

In this area, you can configure settings in order to improve the performance of the RDP session.

Enable RemoteFX

Remote FX is enabled. (Default)

RemoteFX codec mode

Possible options:

- Use server setting
- Optimized for LAN
- Optimized for WAN
- Legacy mode

Hardware accelerated codecs AVC420/AVC444 (H.264)

Possible options:

- Automatic: H.264 is activated automatically if supported by the device's hardware.
- On: H.264 is activated, regardless of hardware support.

i For testing purposes only; this option can lead to display flaws.

- Off: H.264 is deactivated.

► You can disable graphics functions which are not absolutely necessary.

Graphics settings that you can disable in order to improve performance:

Disable wallpaper

Desktop background is disabled.

Desktop background is enabled. (Default)

Don't show contents of window while dragging

Window content will be hidden.

Window content will be shown. (Default)

Disable menu and window animation

Menu and window animation is disabled.

Menu and window animation is enabled. (Default)

Disable themes

Themes are disabled.

Themes are enabled. (Default)

Disable cursor shadow

Cursor shadow is disabled.



Cursor shadow is enabled. (Default)

Disable cursor settings

Cursor settings are disabled. No "unnecessary" mouse movements will be sent.

Cursor settings are enabled. (Default)

Enable font smoothing

Font smoothing is enabled.

Font smoothing is disabled. (Default)

Compression

- i** In low-bandwidth environments, you should use **compression** in order to reduce network traffic. Note that the use of compression reduces the burden on the network but does use CPU power.

Data are compressed.

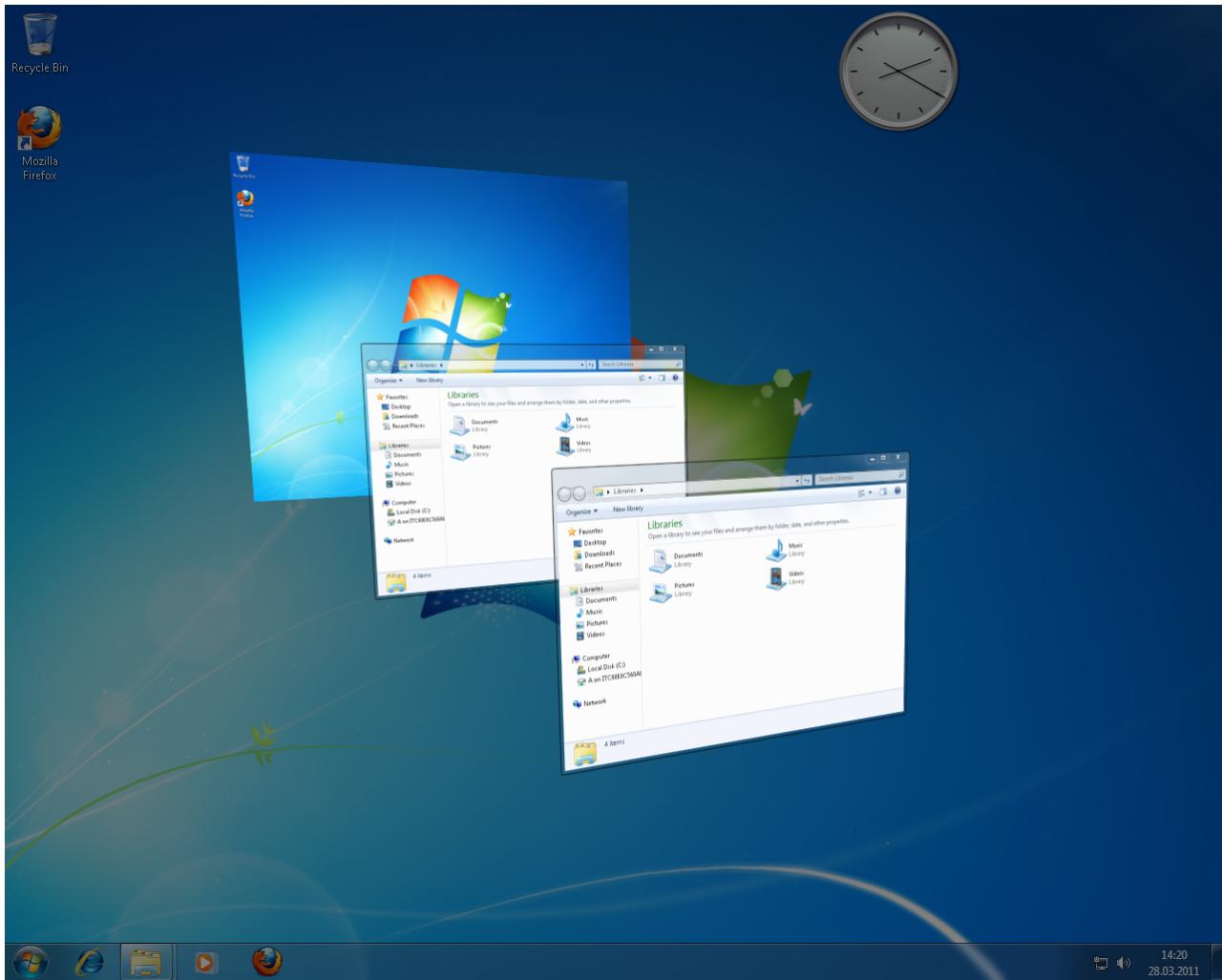
Data flow is not compressed. (Default)

RemoteFX Support

Menu path: **Setup > Sessions > RDP > RDP Global > Performance > RemoteFX Support**

With the Service Pack 1 for *Windows Server 2008 R2*, local system functions such as *Windows Aero* or 3D display can be made available in RDP sessions too.

In order to do this, the RemoteFX extension for RDP must be enabled. You can configure the relevant settings under **RDP Global > Performance** or in the corresponding session settings.



- i** Globally enabling Remote FX is not recommended as conventional RDP sessions may also be affected by this. With RemoteFX, all graphics effects available under Performance are enabled. This may slow down the session as a result. It is better to enable the function only for individual sessions which establish a connection to appropriately equipped servers.



Further information on Remote FX and the server-related requirements is available from Microsoft at [https://technet.microsoft.com/en-us/library/dd736539\(ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd736539(ws.10).aspx)¹¹.

- ⓘ In the IGEL Registry, you can configure the number of frames sent by the server without confirmation under the key `rdp.winconnect.remotefx-ack`. The default value is 1. A value of 2 or 3 can lead to improved performance in networks with high latency.

¹¹ [http://technet.microsoft.com/en-us/library/dd736539\(ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd736539(ws.10).aspx)



Options

Menu path: **Setup > Sessions > RDP > RDP Global > Options**

In this area, you can configure the following settings:

- **Inverted cursor color**

Possible values:

- Black
- White
- Dotted

 You can also configure your own values `custom: ,`. The colors must be given in the ARGB8888 format, e.g. 0xFF000000.

- **Reset license**

The Microsoft license will be removed from the device. The device must then be restarted.
 The license will not be removed. (default)

- **Reset confirmed server certificates**

All confirmed server certificates will be deleted from the client.
 The certificates will not be deleted. (default)

- **Client name:** Client name for terminal service identification.

Possible values:

- Special client name: Specify a special client name in the next field.
- MAC address: Use the MAC address of the computer as the client name
- Computer name: Use the name of the computer

- **Custom client name:** If you have opted for a special client name, you can enter the name here. If the field remains empty, the MAC address of the client will be used automatically.

- **Verify server certificate**

The server certificate will be verified if the connection is TLS-encrypted. (default)



Native USB Redirection

Menu path: **Sessions > RDP > RDP Global > Native USB Redirection**

USB devices can be permitted or prohibited during an RDP session on the basis of default rules. Sub-rules for specific devices or device classes are also possible. The use of rules is described under [USB Access Control](#)(see page 785).

- ⓘ Enable either **Native** or **Fabulatech USB Redirection** – not both together. For details on **Fabulatech USB Redirection**, see [Fabulatech USB Redirection](#)(see page 134).

- ⓘ Disable USB redirection if you use DriveLock. Further information can be found under Using DriveLock with IGEL Devices.

Enable native USB redirection

Native USB redirection is enabled and you can define default rules below.

Native USB redirection is not enabled. (Default)

Default rule

Possible values:

- Deny
- Allow

Tip

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

Class Rules

Class rules apply to USB device classes and sub-classes.

To manage rules, proceed as follows:

- ▶ Click to create a new entry.
- ▶ Click to remove the selected entry.
- ▶ Click to edit the selected entry.
- ▶ Click to copy the selected entry.

Add a class rule:

Rule:

- Deny
- Allow

Class ID: Selection list



Subclass ID: Selection list

Name: Free text entry

Device Rules

Device rules apply to specific USB devices.

Add a device rule:

Rule:

- Allow
- Deny

Vendor ID: Hexadecimal manufacturer number

Product ID: Hexadecimal device number

Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see [Using “System Information” Function\(see page 592\)](#).

System Information example:



Devices - USB Devices - System Information

Information View Help

Refresh Generate Report Copy to Clipboard Synchronize

Computer

- Summary
- Operating System
- Security
- Kernel Modules
- Boots
- Languages
- Memory Usage
- Filesystems
- Display
- Environment Variables

Devices

- System DMI
- Processor
- Graphics Processors
- Monitors
- Memory Devices
- PCI Devices
- USB Devices**
- Network
- Interfaces

Done.

001:001 Linux 2.0 root hub
 002:001 Linux 1.1 root hub
 002:002 VMware Virtual Mouse
 002:003 VMware Virtual USB Hub
 002:004 **logitech** 960 Headset

Device Information

Product [0x0002] 2.0 root hub
 Vendor [0x1d6b] Linux Foundation
Linux
 Device EHCI Host Controller
 Manufacturer Linux 5.12.19 ehci_hcd
Linux
 Max Current 0 mA
 USB Version 2.00
 Speed 480 Mb/s

Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:

Local Terminal

File Edit View Terminal Tabs Help

```
root@ITC005056930CAD:~# lsusb | grep -i logitech
Bus 002 Device 004: ID 046d:0a45 Logitech, Inc. 960 Headset
root@ITC005056930CAD:~#
```

Name: Free text entry

See also an overview and best-practice recommendations for the use of webcams under Webcam Redirection and Optimization in IGEL OS.



Fabulatech USB Redirection

Menu path: **Sessions > RDP > RDP Global > Fabulatech USB Redirection**

Redirection for USB devices can be allowed or denied during an RDP session on the basis of rules. Sub-rules for specific devices or device classes are also possible. The use of rules is described under [USB Access Control](#)(see page 785).

- ⓘ For the Fabulatech USB redirection, a server-side component is required. We recommend the USB for Remote Desktop IGEL Edition; see <http://www.usb-over-network.com/partners/igel/>.

Fabulatech USB Redirection

- Fabulatech USB redirection is enabled for all RDP sessions.
 Fabulatech USB redirection is disabled. (Default)

- ⓘ Enable either **Native** or **Fabulatech USB Redirection** – not both together. Disable USB redirection if you use DriveLock.
- ⓘ Ensure that no other Hotplug storage device (USB stick) is connected if a session is started with Fabulatech USB redirection. Otherwise, the Hotplug storage device will not be securely removed when the session starts, and this could lead to data loss. With IGEL Linux Version 10.02.x the Hotplug storage device is already insecurely removed when the Fabulatech USB redirection is enabled.

Default rule: This rule will apply if no special rule was configured for a class or a device.

- **Deny**
- **Allow**

Tip

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

Class Rules

Class rules apply to USB device classes and sub-classes.

To manage rules, proceed as follows:

- ▶ Click to create a new entry.
- ▶ Click to remove the selected entry.
- ▶ Click to edit the selected entry.
- ▶ Click to copy the selected entry.

Class rule properties:

**Rule:**

- Allow: Devices that have the properties defined here are redirected by the Fabulatech USB redirection.
- Deny: Devices that have the properties defined here are not redirected.

Class ID: Device class**Subclass ID:** Subclass relating to the specified device class**Name:** Free text entry**Override serial:** Serial number that will appear in the session**Override name:** Device name that will appear in the session**Postpone**

- The USB device is only removed from the system (endpoint device) when the session starts.
 The USB device is no longer shown immediately after the system is booted. (Default)

This setting is only effective if the **Takeaway** parameter is enabled.

Takeaway

- The USB device may be removed from the system (endpoint device).
 The USB device may not be removed. (Default)

No Reset

- The device will not be automatically reset after the connection with the session has been terminated.
 The device will be reset after the connection with the session has been terminated. (Default)

Device Rules

A device rule applies to a specific device that is identified by its serial number.

Device rule settings:

Rule:

- Allow
- Deny

Vendor ID: Hexadecimal manufacturer number**Product ID:** Hexadecimal device number

Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see [Using “System Information” Function\(see page 592\)](#).

System Information example:



Devices - USB Devices - System Information

Information View Help

Refresh Generate Report Copy to Clipboard Synchronize

Computer

- Summary
- Operating System
- Security
- Kernel Modules
- Boots
- Languages
- Memory Usage
- Filesystems
- Display
- Environment Variables

Devices

- System DMI
- Processor
- Graphics Processors
- Monitors
- Memory Devices
- PCI Devices
- USB Devices**
- Network
- Interfaces

Done.

001:001 Linux 2.0 root hub
 002:001 Linux 1.1 root hub
 002:002 VMware Virtual Mouse
 002:003 VMware Virtual USB Hub
 002:004 **logitech 960 Headset**

Device Information

Product [0x0002] 2.0 root hub
 Vendor [0x1d6b] Linux Foundation
Linux
 Device EHCI Host Controller
 Manufacturer Linux 5.12.19 ehci_hcd
Linux
 Max Current 0 mA
 USB Version 2.0
 Speed 480 Mb/s

Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb` :

Local Terminal

```
File Edit View Terminal Tabs Help
root@ITC005056930CAD:~# lsusb | grep -i logitech
Bus 002 Device 004: ID 046d:0a45 Logitech, Inc. 960 Headset
root@ITC005056930CAD:~#
```

Name: Free text entry

Override serial: Serial number that will appear in the session

Override name: Device name that will appear in the session

Postpone

The USB device is only removed from the system (endpoint device) when the session starts. (Default)

The USB device is no longer shown immediately after the system is booted.



i This setting is only effective if the **Takeaway** parameter is enabled.

Takeaway

- The USB device may be removed from the system (endpoint device). (Default)
- The USB device may not be removed.

No Reset

- The device will not be automatically reset after the connection with the session has been terminated. (Default)
- The device will be reset after the connection with the session has been terminated.



Fabulatech Scanner Redirection

Menu path: **Sessions > RDP > RDP Global > Fabulatech Scanner Redirection**

Redirection for a Fabulatech scanner can be allowed during an RDP session.

Fabulatech Scanner for Remote Desktop

Fabulatech Scanner for Remote Desktop is enabled.

 For more information, see RDP Fabulatech Scanner Redirection.



Multimedia

Menu path: **Setup > Sessions > RDP > RDP Global > Multimedia**

In this area, you can enable video redirection in order to allow optimized video playback in remote sessions.

- **Video redirection**

- Use video redirection. The device renders the video data.
- Do not use video redirection. (default)

From *IGEL Linux 5.06.100*, hardware acceleration for multimedia playback is available on certain devices. You will find more detailed information in the FAQ Hardware Video Acceleration on IGEL OS.

.



RDP Session

Menu path: **Sessions > RDP > RDP Sessions**

You can set up your own RDP sessions here.

The following configuration pages offer you detailed setup options for the RDP session:

- [Server](#)(see page 141)
- [Gateway](#)(see page 142)
- [Logon](#)(see page 143)
- [Window](#)(see page 144)
- [Keyboard](#)(see page 146)
- [Mapping](#)(see page 147)
- [Performance](#)(see page 148)
- [Options](#)(see page 149)
- [USB Redirection](#)(see page 150)
- [Multimedia](#)(see page 151)
- [Desktop Integration](#)(see page 152)



Server

Menu path: **Sessions > RDP > RDP Sessions > [Session Name] > Server**

In this area, you can change the information regarding the server connection.

- Choose between **Server** and **RemoteApps mode**.

Server

Server: Name or IP address of the server.

RDP port: The RDP TCP/IP port which is used for the connection. (Default: 3389)

Collection: The name of the Remote Desktop Services (RDS) collection to connect to.

- ⓘ Instead of the collection name, it is also possible to specify under **Collection** the token that directs the RDP client to a specific RDS collection. The token format is `tsv://MS Terminal Services Plugin.1.RDS collection name`. For more information, see [What Is the String for Token-Based Load Balancing?](#).

Application: Start application for the terminal server session.

Command line parameter for the executed program: Command line parameter with which you would like to call up your own application in the RemoteAPP mode.

Changeable server URL on local login

- The server can be entered freely when the user logs in locally. Local login must be enabled in order to do this.
- The terminal server's login window will be shown. When using local login, the device's login window will be shown. (Default)

- ⓘ If the **Passthrough Authentication** option is enabled, the session with the local login data for the terminal user, e.g. from the domain login, is used. However, this setting will be overridden by the **Local Login** global parameter. You should not therefore use both options at the same time.

Enable RemoteApp Mode

Like the published applications of a Citrix server, MS Windows Server 2008 offers the option of passing on RemoteApps to the device.

Detailed instructions regarding server configuration can also be found on the Microsoft website: [TS RemoteApp Step-by-Step Guide](#)¹².

On the client side, only a few parameters need to be configured after enabling the RemoteApp mode.

- ⓘ Please note that the name of the application to be launched must be preceded by two pipe characters (||), e.g. `||Excel`.

¹² [https://technet.microsoft.com/en-us/library/cc730673\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc730673(v=ws.10).aspx)



Gateway

Menu path: **Setup > Sessions > RDP > RDP Sessions > [Session Name] > Gateway**

Here, you can specify custom gateway details for your RDP session.

- **Enable gateway support**

- Global setting: The settings from **RDP Global > Gateway** will be carried over.
- Session setting: Here, you can configure custom settings. The entry options correspond to those under **RDP Global > Gateway**(see page 112).
- Off: No gateway support

- **Gateway address**

Info: RD Gateway requires Microsoft Windows Server 2008R2 or Server 2012 with various restrictions for each server version.

The following Windows Server editions can preferably be used as gateway servers:

Server 2012 Standard

Server 2012 Datacenter

Server 2012 Essential (restricted to the RD Gateway role)

Server 2012R2 Standard

Server 2012R2 Essential (restricted to the RD Gateway role)

Server 2016

Server 2019

Info: RD Gateway is not supported in the IGEL RDP Legacy Mode.

- **Use other credentials for RD Gateway authentication:**

Uses custom data that can be defined below rather than the session access data.

- **Gateway user name**
- **Gateway password**
- **Gateway domain**



Logon

Menu path: **Sessions > RDP > RDP Sessions > [Session Name] > Logon**

Here, you can specify session-specific settings for login.

Use passthrough authentication for this session

This option can be used if the local device login takes place via Kerberos or Shared Workspace. The login data saved temporarily when logging in to the device will be used for the user name and password.

The login data are not passed on. (Default)

User name: Name of the user

Password: Password of the user

⚠ Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

Domain: Windows domain



Window

Menu path: **Setup > Sessions > RDP > RDP-Sessions > [Session Name] > Fenster**

Here, you can specify the settings for the RDP session window.

- **Number of colours**

Possible values:

- Global setting
- 256
- Thousands
- Millions

- **Window size**

Possible values:

- Global setting
- Fullscreen: The session is shown on the full screen. The thin client's taskbar is not visible.
- Workarea: The session is shown on the full screen, minus the area needed by the thin client's taskbar.
- Numeric details: The session is shown in the selected resolution or on the selected percentage of the screen area.

- **Desktop scale factor:** Specifies the desktop scaling in percent. This function is available from IGEL Linux Version 10.02.

Desktop scaling is supported from Windows Server 2012 or higher and from Windows 8.1 or higher.

Possible values:

- Global setting (default)
- Automatic: The resolution set under **Setup > User Interface > Display > Options > Monitor-DPI** will be used for the RDP session.
- Numeric details: The display will be magnified by the factor given here. Value range: 100% - 500%

- **Display resolution**

Possible values:

- Same as window size
- Value selection: The session runs on the server side with the screen resolution selected here. The session will be shown on the thin client in the screen resolution set with the **Window size** parameter. If the screen resolution on the server side is smaller than the **Window size**, the display will be magnified accordingly and anti-aliasing may be used. Example: Applications that only work or work optimally with a specific screen resolution.

- **Start monitor:** Specifies the monitor on which the session is to start.

- No configuration
- Selects a specific monitor

- **Multi-monitor fullscreen mode:** This setting is relevant if more than one monitor is connected to the terminal:

- Global setting



- Restrict fullscreen session to one monitor.
- Display fullscreen session on all monitors.
- Expand fullscreen session across all monitors.



Keyboard

Menu path: **Setup > Sessions > RDP > RDP Sessions > [Session Name] > Keyboard**

Here, you can specify session-specific keyboard settings.

- **Keyboard map**

Possible values:

- Automatic
- Country name

- **Override local window manager keyboard shortcuts**

Possible values:

- Global setting
- On
- Off



Mapping

Menu path: **Setup > Sessions > RDP > RDP Sessions > [Session Name] > Mapping**

- **Enable COM port mapping**
 - Global setting:
 - On
 - Off
- **Enable drive mapping**
 - Global setting from **RDP Global > Mapping > Drive Mapping**
 - On
 - Off
- **Enable printer mapping**
 - Global setting from **RDP Global > Mapping > Printers**
 - On
 - Off
- **Enable plugin support**
 - Global setting from **RDP Global > Mapping > Drive Support**
 - Off
- **Enable client audio**
 - Global setting from **RDP Global > Mapping > Audio**
 - On
 - Off
- **Audio quality mode**
 - Global setting from **RDP Global > Mapping > Audio**
 - Automatic
 - High: High audio quality is favored.
 - Medium: Medium audio quality is favored.
 - Dynamic
- **Audio compression**
 - Global setting from **RDP Global > Mapping > Audio**
 - Automatic
 - On
 - Off
- **Audio capture**
 - Global setting from **RDP Global > Mapping > Audio**
 - On
 - Off
- **Enable clipboard**
 - Global setting from **RDP Global > Keyboard**
 - On
 - Off



Performance

Menu path: **Setup > Sessions > RDP > RDP Sessions > [Session Name] > Performance**

- **Enable RemoteFX**
 - Global setting from **RDP Global > Performance**
 - On
 - Off
- **Hardware accelerated codecs AVC420/AVC444 (H.264)**
 - Global setting from **RDP Global > Performance**
 - On
 - Off
- **Disable wallpaper**
 - Global setting from **RDP Global > Performance**
 - On
 - Off
- **Do not show contents of window while dragging**
 - Global setting from **RDP Global > Performance**
 - On
 - Off
- **Disable menu and window animation**
 - Global setting from **RDP Global > Performance**
 - On
 - Off
- **Disable themes**
 - Global setting from **RDP Global > Performance**
 - On
 - Off
- **Disable cursor shadow**
 - Global setting from **RDP Global > Performance**
 - On
 - Off
- **Disable cursor settings**
 - Global setting from **RDP Global > Performance**
 - On
 - Off
- **Enable font smoothing**
 - Global setting from **RDP Global > Performance**
 - On
 - Off
- **Compression**
 - Global setting from **RDP Global > Performance**
 - On
 - Off



Options

Menu path: **Setup > Sessions > RDP > RDP Sessions > [Session Name] > Options**

Here, you can specify the name and symbol for the RDP client.

- **Client name:** Specifies the name that is sent to the terminal server for identification purposes.
Possible values:
 - Global setting: The setting from **RDP Global > Options** will be carried over.
 - Custom client name: The name given under **Custom client name** will be used as the client name.
 - MAC address: The MAC address of the computer will be used as the client name.
 - Host name: The name of the device specified under **Setup > Network > LAN Interfaces > Terminal name** will be used as the client name. See [LAN Interfaces](#)(see page 689).
- **Custom client name:** Custom client name; if the field is empty, the MAC address will be used.
- **Collection:** The name of the Remote Desktop Services (RDS) collection to connect to.
 - Instead of the collection name, it is also possible to specify under **Collection** the token that directs the RDP client to a specific RDS collection. The token format is `tsv://MS Terminal Services Plugin.1.RDS collection name`. For more information, see [What Is the String for Token-Based Load Balancing?](#).
- **Icon name:** File name of the icon without file extension. (Default: `rdp`)



USB Redirection

Menu path: **Sessions > RDP > RDP Sessions > [Session Name] > USB Redirection**

Native USB redirection

- Global setting: The settings from **RDP Global > Native USB Redirection** will be carried over.
- On: Native USB redirection is enabled.
- Off: Native USB redirection is disabled.

Further information regarding the global settings can be found under [Native USB Redirection](#)(see page 131).



Multimedia

Menu path: **Setup > Sessions > RDP > RDP Sessions > [Session Name] > Multimedia**

- **Enable video redirection**

- Global setting: The setting from **RDP Global > Multimedia** will be used.
 - On: Video redirection is enabled.
 - Off: Video redirection is disabled.

Further information regarding the global settings can be found under [Multimedia](#).



Desktop Integration

Menu path: **Sessions > RDP > RDP Sessions > [Session Name] > Desktop Integration**

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.



Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

ⓘ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with | :

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

- ⓘ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.



- The session is started automatically, even when no network is available.



Remote Desktop Web Access

Menu path: **Sessions > RDP > Remote Desktop Web Access**

With Web Access for Remote Desktop (Web Access for RD), users can access RemoteApp and a Remote Desktop connection via the start menu on a computer or via a web browser.

RemoteApps and Remote Desktop connections therefore provide a modified view of RemoteApp programs and virtual desktops for users.

More information on Web access for Remote Desktop can be found under [Microsoft Technet - Web Access for RDP¹³](#).

The settings for launching the session are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

¹³ <http://technet.microsoft.com/en-us/library/cc731923.aspx>



Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

ⓘ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows key` = `Ctrl|Super_L`

Key: Key for the hotkey

ⓘ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.



Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

-
- [Server](#)(see page 158)
 - [Authentication](#)(see page 162)
 - [Appearance](#)(see page 163)
 - [Logoff](#)(see page 164)
 - [Desktop Integration](#)(see page 166)



Server

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Server**

In this area, you can specify the server configuration.

The Web Access page for *Windows Server 2012* and *Windows Server 2012 R2* can also be used on a Linux endpoint device in the *Firefox* browser. See [Via Browser\(see page 161\)](#).

Server configuration

Possible values:

- "[Predefined configuration](#)": You can define several server connections with the same user access data. The user must enter their access data and the domain in the login window. See [Predefined Configuration\(see page 159\)](#).
- "Ask user": The connection is preconfigured on the server side. The user only needs to enter their corporate e-mail address. See [Ask User\(see page 160\)](#).

Server location: These settings are needed if **Server configuration** is set to "Predefined configuration".

Protocol

Possible values:

- "http://"
- "[https://](#)"

RD Web Access Server: Name of the Web Access server

Path to web portal (Default: `/rdweb/feed/webfeed.aspx`)

Enable gateway support

Possible values:

- "Global settings"
- "Session settings"
- "Off"

Gateway address: If you would like to carry over the session settings, you must also specify the gateway address.

Domains: Domain of the Web Access server

-
- [Predefined Configuration\(see page 159\)](#)
 - [Ask User\(see page 160\)](#)
 - [Via Browser\(see page 161\)](#)



Predefined Configuration

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Server**

To predefine settings, proceed as follows:

1. Go to **Sessions > RDP > Remote Desktop Web Access > Server**.
2. Under **Server configuration**, select **Predefined configuration**.
3. Create a new session. See the [Server\(see page 158\)](#) section regarding the session settings.
4. Select a login option under **Remote Desktop Web Access > Authentication**.
If you have selected **Predefined configuration**, the **Passthrough authentication** mode will be available for logging in in addition to the normal user authentication process.
5. Under [Desktop Integration\(see page 166\)](#) and [Logoff\(see page 164\)](#), you can specify how you would like to log in and off.

i You must make a setting for the login icon because this is not preconfigured and you will not otherwise have access to the Web Access logon.

The applications can be provided in the Application Launcher, in the start menu, in the quick start panel, or on the desktop. Under [Appearance\(see page 163\)](#), you can choose from the list of available applications for display on the desktop or in the quick start panel.

Ask User

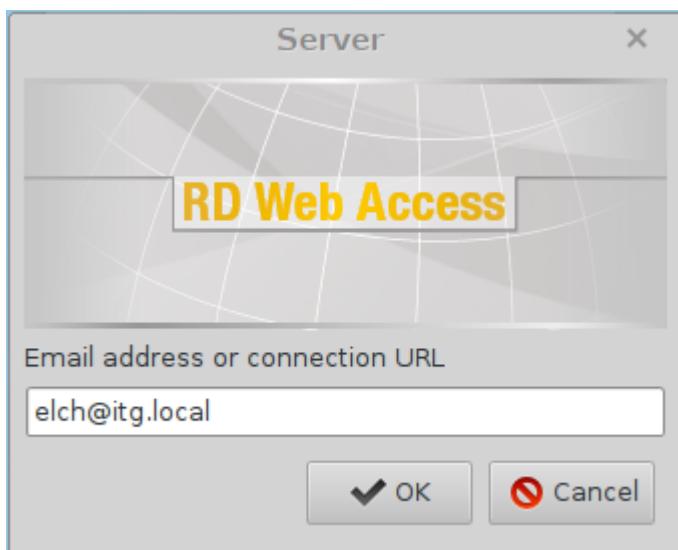
Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Server**

With this logon method, the network connections connected with the user name on the server side must be preconfigured and it must be possible to query them via DNS.

To configure access via **Ask user**, proceed as follows:

- ▶ Select **Ask user** under **RD Web Access > Server > Server configuration** menu.

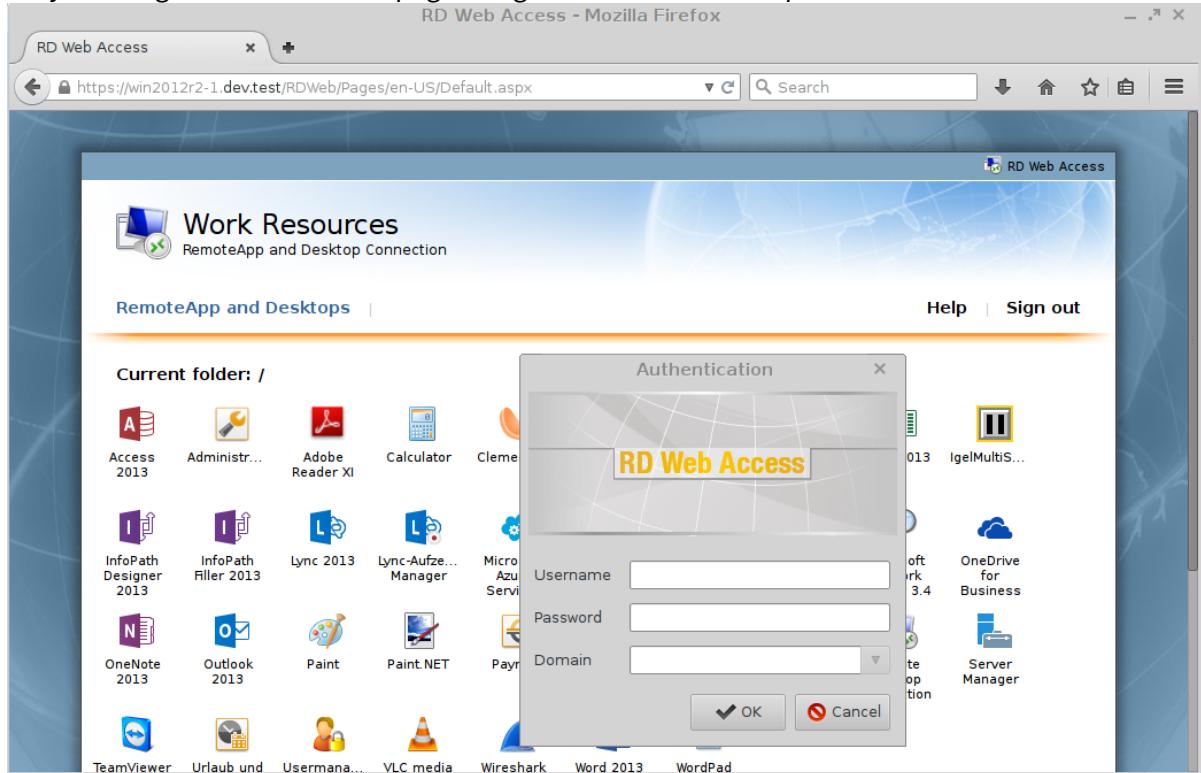
The user is given a login window in which they enter their e-mail address consisting of @ :



Via Browser

The Web Access page for *Windows Server 2012* and *Windows Server 2012 R2* can also be used on a Linux thin client in the *Firefox* browser.

- The user only needs the corresponding URL which is entered in the address bar.
- They then log in on the browser page using their user name and password.



If the user clicks one of the applications offered by Web Access, the thin client will open a logon mask and then a *Remote Desktop* session for the application chosen.



Authentication

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Authentication**

You can change login settings on the server and select applications that are launched automatically after logging in.

- i** The login settings on the server are only effective if **Sessions > RDP > Remote Desktop Web Access > Server > Server configuration** is set to **Predefined configuration**. Further information can be found under [Server](#)(see page 158).

Authentication mode: Specifies how the user authenticates themselves on the server.

Possible values:

- "Passthrough authentication": This option can be used if the local endpoint device login takes place via Kerberos or Shared Workspace. The login data saved temporarily when logging in to the device will be used for the user name and password.
- "Auto logon": The login data in **Username**, **Password**, and **Domain** will be used to log in.
- "User logon

Username: User name when logging in to the server

Password: Password when logging in to the server

Domain: Domain in which the user name and password are valid

Save username and domain from the last login

Possible options:

- "Yes": The username and domain from the last login will be saved.
- "No": The username and domain from the last login will not be saved.
- "LegacySessions > RDP > RDP Global > Local Logon > Preset login information is enabled. If it is enabled, the saved data of **Local Logon** will be used also for RD Web Access.

To select an application for automatic launching, proceed as follows:

1. Click **[+]** in the **Start following applications automatically after server connection is established** area.
2. In the **Add** dialog, enter the name of the application. (Example: Word 2013)

- i** You can also enter part of the name followed by an asterisk (*). If you enter e.g. Word*, all available versions of Microsoft Word as well as Microsoft WordPad will be opened.

3. Click on **Ok**.
- After a successful login, the associated desktop icon for each available application will be placed on the device desktop. All applications whose name matches one of the names given in the **Start following applications automatically after server connection is established** area will then be launched.



Appearance

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Appearance**

In this area, you can decide where you would like to display Remote Desktop Web Access applications:

Show applications in start menu

The applications are shown in the start menu. (Default)

Apply display filter to start menu entries

Only the applications listed in the display filter will be shown in the start menu.

All applications will be shown in the start menu. (Default)

Show applications in Application Launcher

The applications are shown in Application Launcher. (Default)

Apply display filter to Application Launcher entries

Only the applications listed in the display filter will be shown in the Application Launcher.

All applications will be shown in the Application Launcher. (Default)

Show applications on desktop

The applications will be shown on the desktop. (Default)

Apply display filter to desktop icons

Only the applications listed in the display filter will be shown on the desktop.

All applications will be shown on the desktop. (Default)

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Display filter: Show only the following applications

- ▶ Via +, you can add applications to the display filter and determine display options for this selected group.

Enable following applications in Quick Start Panel

- ▶ Via +, you can specify applications which will be added to the quick start panel.



Logoff

Menu path: **Setup > RDP > Remote Desktop Web Access > Logoff**

Here, you can specify how you would like to log off from the application.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`



Desktop Integration

Menu path: **RDP > Remote Desktop Web Access > Desktop Integration**

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.



Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network



- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.



Horizon Client Global

Menu path: **Sessions > Horizon Client > Horizon Client Global**

In this area, you can define the global settings for Horizon Client sessions.

The following setting is carried over from the global settings for RDP sessions if "RDP" is selected as a **preferred desktop protocol**, see [Server Options for Horizon Sessions in IGEL OS\(see page 170\)](#) and [Connection Settings\(see page 203\)](#):

- **Number of colors;** see [Window\(see page 115\)](#)

 - [Server Options for Horizon Sessions in IGEL OS\(see page 170\)](#)
 - [Local Logon Options for Horizon Client in IGEL OS\(see page 172\)](#)
 - [Window\(see page 174\)](#)
 - [USB Redirection\(see page 175\)](#)
 - [Fabulotech USB Redirection for IGEL OS\(see page 178\)](#)
 - [Fabulotech Scanner Redirection\(see page 186\)](#)
 - [Serial Port Redirection\(see page 187\)](#)
 - [Drive Mapping\(see page 188\)](#)
 - [Multimedia\(see page 189\)](#)
 - [Performance\(see page 190\)](#)
 - [Smartcard Middleware Settings for VMware Horizon Sessions in IGEL OS\(see page 191\)](#)
 - [Unified Communications Settings for VMware Horizon Sessions in IGEL OS\(see page 194\)](#)



Server Options for Horizon Sessions in IGEL OS

In this area, you can specify the settings for the connection between the server and the VMware Horizon Client that is built into IGEL OS.

Menu path: **Sessions > Horizon Client > Horizon Client Global > Server Options**

Preferred desktop protocol

The selected option is preferred by the client when negotiating the connection protocol. If the server does not accept the connection protocol preferred by the client, the connection protocol preferred by the server will be used.

Possible values:

- **Server setting:** The client does not provide the server details of a preferred connection protocol. The connection protocol preferred by the server is used.*
- **RDP:** The client tells the server that it prefers RDP as the connection protocol.
- **PCoIP:** The client tells the server that it prefers PCoIP as the connection protocol.
- **VMware Blast:** The client tells the server that it prefers VMware Blast as the connection protocol.

i Hardware video acceleration can be used for VMware Blast. Information regarding hardware video acceleration on IGEL devices can be found under Hardware Video Acceleration on IGEL OS. If no hardware video acceleration is available, rendering will take place via software, without acceleration.

High Color Accuracy Mode

Enables H.264 encoding with High Color Accuracy in VMware Blast Sessions. The Horizon Client uses high color accuracy only if the agent supports it. On mobile devices that are running on battery, this feature might reduce battery life and performance.

- High color accuracy is allowed.
 High color accuracy is not allowed.*

Kiosk mode

- Horizon client sessions are held in kiosk mode.

✓ As an alternative, you can also use the [Appliance Mode](#)(see page 213).

- Horizon client sessions are held in normal mode.*

Server certificate verification mode

Specifies what will happen if server certificate verification fails.



Possible values:

- **Reject if verification fails**
- **Warn if verification fails***

See also Deploying Trusted Root Certificates in IGEL OS.

- **Allow unverifiable connections**

Action to take in case there are running applications from previous sessions

Specifies the start behavior of an **application**-type session if applications from a previous session are still running. The session type is defined under **Sessions > Horizon Client > Horizon Client Session > [Session Name] > Connection Settings > Session Type**.

Possible values:

- **Ask to reconnect to open applications:** When the session starts, the user is asked whether they want to re-establish the connection. If the connection is reestablished, the applications running will be available. The applications will have the same status as when the connection was terminated.*
- **Reconnect automatically to open applications:** The connection will be re-established automatically. The application running will be available. The application will have the same status as when the connection was terminated.
- **Do not ask to reconnect and do not reconnect:** The connection will not be re-established.

*IGEL OS system default



Local Logon Options for Horizon Client in IGEL OS

Using **Local Logon** settings, described in this article, you can prepopulate user data for VMware Horizon sessions. As a result, you can avoid users possibly having to log in a number of times.

Menu path: **Sessions > Horizon Client > Horizon Client Global > Local Logon**

Local Logon Configuration for VMware Horizon

The screenshot shows the 'Configuration' screen under 'Sessions'. The left sidebar lists categories like Sessions Summary, Global Session Options, Citrix, RDP, and Horizon Client (with sub-options like Server Options, Local Logon, Window, USB Redirection, and Fabulotech USB Redirection). The 'Local Logon' option is selected. The main panel displays several configuration options:

- Use local login window**: A checked checkbox.
- Preset login information**: A checked checkbox.
- Type**: A dropdown menu set to "Set user/domain from last login".
- Show domain**: A checked checkbox.
- Exit on disconnect or when an error occurs**: An unchecked checkbox.
- Domains**: A table with one row labeled "Domain".

Use local login window

- The local login window of the endpoint device will be used to log in to the server. If you use the local login window, you can prepopulate login information.
 The local login window will not be used.*

Preset login information

- Login information will appear automatically in the login window. With **Type**, you can specify the source of the login information.*

Type

- Set user/domain from last login:** The login information from the last session will appear automatically in the login window.*
- Set user/domain from session setup:** Session-specific login information will appear automatically in the login window. The session-specific login information is described under [Connection Settings](#)(see page 203).

Show domain

- The domain will be shown in the login window.*



Relaunch mode

- The login window is shown in relaunch mode and cannot be closed.
- The login window is not shown in relaunch mode.*

Exit on disconnect or when an error occurs

- The session will be ended completely when the connection is terminated.
- The connection overview will be shown when the connection is terminated.*

Domain

This is how you can work with the domain list:

- ▶ Click to add a new domain.
- ▶ Click to remove the selected domain.
- ▶ Click to edit the selected domain.
- ▶ Click to copy the selected domain.

Further settings options can be found under **Security > Active Directory / Kerberos**(see page 814) and **Security > Logon > Active Directory / Kerberos**(see page 807).

*IGEL OS system default



Window

Menu path: **Sessions > Horizon Client > Horizon Client Global > Window**

Window size: Specifies the width and height of the window.

Possible options:

- "Full-screen": The session is shown on the full screen. The device's taskbar is not visible.
- "Work area": The session is shown on the full screen, minus the area needed by the device's taskbar.
- Numeric details: The session is shown in the selected resolution or on the selected percentage of the screen area.

Multimonitor full-screen mode - If more than one monitor is connected to the terminal:

- "Restrict full-screen session to one monitor"
- "Display full-screen session on all monitors"
- "Expand full-screen session across all monitors": The same as "Display full-screen session on all monitors"



USB Redirection

Menu path: **Sessions > Horizon Client > Horizon Client Global > USB Redirection**

In this area, you can enable and configure USB redirection for specific devices. A USB composite device can be split into its components (interfaces). Example: USB dictation device that is split into the components loudspeaker, microphone, storage device/drive, and control buttons.

- ⓘ Ensure that the power supplied by the USB connection is adequate for the device.

- ⓘ If USB redirection is enabled, drive mapping should be disabled; see [Drive Mapping\(see page 188\)](#). Otherwise, USB redirection can cause a storage device to be removed from the drive mapping. This is the case if the **Automatically connect when inserted** option is enabled.

You can change the following settings:

USB Redirection

- On
- Off

Automatically connect at startup

USB devices that were inserted before the start of the session are available in the session. (default)

Automatically connect when inserted

USB devices that are inserted during the session are available in the session. (default)

Default rule: This rule will apply if no special rule was configured for a class or a device.

- Allow
- Deny

Tip

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

Automatic splitting of composite USB devices

A USB composite device will automatically be split into its individual components (interfaces). The class rules will be applied to these individual devices.

The device will not be split into its components.

Creating a Class Rule

1. To create a new rule, click in the **Class Rules** area.
2. Choose a **Rule**. The rule specifies whether the use of the device class defined here is allowed or prohibited.



3. Under **Family**, select the class of device for which the rule should apply. Examples: **Audio, Printer, Smartcard, Storage Devices**.
4. Under **Name**, give a name for the rule.
5. Click on **Ok**.
6. Click on **Apply or Ok**.
The rule is active.

Creating a Device Rule

i When a rule is defined, at least one of the properties **Vendor ID** or **Product ID** must be given.

1. To create a new rule, click **[+]** in the **Device Rules** area.
2. Choose a **Rule**. The following rules are available:
 - Deny: The device will not be redirected via USB redirection.
 - Allow: The device will be redirected via USB redirection.
 - Split: A USB composite device will automatically be split into its individual components (interfaces).
 - No auto-split: A USB composite device will not be split.
3. Give the **Vendor ID** of the device as a hexadecimal value.
4. Give the **Product ID** of the device as a hexadecimal value. The product ID can contain asterisks '*', each asterisk representing one hexadecimal digit. If the field is left empty, any product ID is matched.

i Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see [Using “System Information” Function](#)(see page 592).

System Information example:



Devices - USB Devices - System Information

Information View Help

Refresh Generate Report Copy to Clipboard Synchronize

Computer

- Summary
- Operating System
- Security
- Kernel Modules
- Boots
- Languages
- Memory Usage
- Filesystems
- Display
- Environment Variables

Devices

- System DMI
- Processor
- Graphics Processors
- Monitors
- Memory Devices
- PCI Devices
- USB Devices**

Network

- Interfaces

Done.

001:001 Linux 2.0 root hub
 002:001 Linux 1.1 root hub
 002:002 VMware Virtual Mouse
 002:003 VMware Virtual USB Hub
 002:004 **logitech** 960 Headset

Device Information

Product [0x0002] 2.0 root hub
 Vendor [0x1d6b] Linux Foundation
Linux
 Device EHCI Host Controller
 Manufacturer Linux 5.12.19 ehci_hcd
Linux
 Max Current 0 mA
 USB Version 2.00
 Speed 480 Mb/s

Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:

Local Terminal

File Edit View Terminal Tabs Help

```
root@ITC005056930CAD:~# lsusb | grep -i logitech
Bus 002 Device 004: ID 046d:0a45 Logitech, Inc. 960 Headset
root@ITC005056930CAD:~#
```

5. Only for USB composite devices: Under **Interface Exclude List**, enter a list of interfaces that are to be excluded from USB redirection. The individual interfaces are separated by spaces. Example: "0 1".
6. Under **Name**, give a name for the rule.
7. Click on **Ok**.
8. Click on **Apply** or **Ok**.
The rule is active.

See also an overview and best-practice recommendations for the use of webcams under Webcam Redirection and Optimization in IGEL OS.



Fabulatech USB Redirection for IGEL OS

For Fabulatech USB redirection, a special Fabulatech server component (USB for Remote Desktop Igel Edition) must be installed on the Horizon VDI desktop. Please note that licenses must be purchased from Fabulatech to enable this functionality.

More detailed information about the function can be found on the Fabulatech partner site: <http://www.usb-over-network.com/partners/igel/>.

Important Notes

- Enable either native USB redirection or Fabulatech USB Redirection – not both together.
- Disable USB redirection if you use DriveLock.
- Ensure that no other hotplug storage device (USB memory stick) is connected before you enable Fabulatech USB redirection. Otherwise, the hotplug storage device is insecurely removed.
- Generally, Fabulatech USB Redirection might not be the ideal solution for each use case. For details, refer to the general device redirection recommendations of your terminal server or VDI vendor.

Menu path: **Sessions > Horizon Client > Horizon Client Global > Fabulatech USB Redirection**

Fabulatech USB Redirection

Fabulatech USB Redirection is used.

Fabulatech USB Redirection is not used.*

Default rule

This rule will apply if no special rule was configured for a class or a device.

Possible options:

- Deny*
- Allow

Tip

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

Class Rules

Class rules apply to USB device classes and sub-classes.

Managing rules:



- Create a new entry.
- Remove the selected entry.
- Edit the selected entry.
- Copy the selected entry.

The class rule properties are described in the following.

Rule

Possible options:

- Deny: Devices that have the properties defined here are not redirected.
- Allow: Devices that have the properties defined here are redirected by the **Fabulotech USB Redirection.***

Class ID

Device class

Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see [Using “System Information” Function\(see page 592\)](#).

System Information example:



Devices - USB Devices - System Information

Information View Help

Refresh Generate Report Copy to Clipboard Synchronize

Computer

- Summary
- Operating System
- Security
- Kernel Modules
- Boots
- Languages
- Memory Usage
- Filesystems
- Display
- Environment Variables

Devices

- System DMI
- Processor
- Graphics Processors
- Monitors
- Memory Devices
- PCI Devices
- USB Devices**
- Network
- Interfaces

Done.

001:001 Linux 2.0 root hub
 002:001 Linux 1.1 root hub
 002:002 VMware Virtual Mouse
 002:003 VMware Virtual USB Hub
 002:004 **logitech** 960 Headset

Device Information

Product [0x0002] 2.0 root hub
 Vendor [0x1d6b] Linux Foundation
Linux
 Device EHCI Host Controller
 Manufacturer Linux 5.12.19 ehci_hcd
Linux
 Max Current 0 mA
 USB Version 2.00
 Speed 480 Mb/s

Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:

Local Terminal

File Edit View Terminal Tabs Help

```
root@ITC005056930CAD:~# lsusb | grep -i logitech
Bus 002 Device 004: ID 046d:0a45 Logitech, Inc. 960 Headset
root@ITC005056930CAD:~#
```

Subclass ID

Subclass relating to the specified device class

i Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see [Using “System Information” Function\(see page 592\)](#).



System Information example:

Devices - USB Devices - System Information

Information View Help

Refresh Generate Report Copy to Clipboard Synchronize

Computer

- Summary
- Operating System
- Security
- Kernel Modules
- Boots
- Languages
- Memory Usage
- Filesystems
- Display
- Environment Variables

Devices

- System DMI
- Processor
- Graphics Processors
- Monitors
- Memory Devices
- PCI Devices
- USB Devices**

Network

Interfaces

Done.

Device Information

Product [0x0002] 2.0 root hub
 Vendor [0x1d6b] Linux Foundation
Linux
 Device EHCI Host Controller
 Manufacturer Linux 5.12.19 ehci_hcd
Linux
 Max Current 0 mA
 USB Version 2.00
 Speed 480 Mb/s

Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:

Local Terminal

File Edit View Terminal Tabs Help

```
root@ITC005056930CAD:~# lsusb | grep -i logitech
Bus 002 Device 004: ID 046d:0a45 Logitech, Inc. 960 Headset
root@ITC005056930CAD:~#
```

Name

Free text entry

Override serial

Serial number that will appear in the session



Override name

Device name that will appear in the session

Postpone

- The USB device is only removed from the system (endpoint device) when the session starts.
 The USB device is no longer shown immediately after the system is booted.*

i This setting is only effective if the **Takeaway** parameter is enabled.

Takeaway

- The USB device may be removed from the system (endpoint device).
 The USB device may not be removed.*

No Reset

- The device will not be automatically reset after the connection with the session has been terminated.
 The device will be reset after the connection with the session has been terminated.*

Device Rules

A device rule applies to a specific device that is identified by its serial number.

The device rule settings are described in the following.

Rule

Possible options:

- Deny: The device will not be redirected via Fabulatech USB Redirection.
- Allow: The device will be redirected via Fabulatech USB Redirection.*

Vendor ID

Hexadecimal manufacturer number

i Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see [Using “System Information” Function\(see page 592\)](#).

System Information example:



Devices - USB Devices - System Information

Information View Help

Refresh Generate Report Copy to Clipboard Synchronize

Computer

- Summary
- Operating System
- Security
- Kernel Modules
- Boots
- Languages
- Memory Usage
- Filesystems
- Display
- Environment Variables

Devices

- System DMI
- Processor
- Graphics Processors
- Monitors
- Memory Devices
- PCI Devices
- USB Devices**
- Network
- Interfaces

Done.

001:001 Linux 2.0 root hub
 002:001 Linux 1.1 root hub
 002:002 VMware Virtual Mouse
 002:003 VMware Virtual USB Hub
 002:004 **logitech** 960 Headset

Device Information

Product [0x0002] 2.0 root hub
 Vendor [0x1d6b] Linux Foundation
Linux
 Device EHCI Host Controller
 Manufacturer Linux 5.12.19 ehci_hcd
Linux
 Max Current 0 mA
 USB Version 2.00
 Speed 480 Mb/s

Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:

Local Terminal

File Edit View Terminal Tabs Help

```
root@ITC005056930CAD:~# lsusb | grep -i logitech
Bus 002 Device 004: ID 046d:0a45 Logitech, Inc. 960 Headset
root@ITC005056930CAD:~#
```

Product ID

Hexadecimal device number

i Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see [Using “System Information” Function\(see page 592\)](#).



System Information example:

Devices - USB Devices - System Information

Information View Help

Refresh Generate Report Copy to Clipboard Synchronize

Computer

- Summary
- Operating System
- Security
- Kernel Modules
- Boots
- Languages
- Memory Usage
- Filesystems
- Display
- Environment Variables

Devices

- System DMI
- Processor
- Graphics Processors
- Monitors
- Memory Devices
- PCI Devices
- USB Devices**

Network

Interfaces

Done.

Device Information

Product [0x0002] 2.0 root hub
Vendor [0x1d6b] Linux Foundation
Linux
Device EHCI Host Controller
Manufacturer Linux 5.12.19 ehci_hcd
Linux
Max Current 0 mA
USB Version 2.00
Speed 480 Mb/s

The device **002:004 logitech 960 Headset** is highlighted with a red box.

Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:

Local Terminal

```
File Edit View Terminal Tabs Help
root@ITC005056930CAD:~# lsusb | grep -i logitech
Bus 002 Device 004: ID 046d:0a45 Logitech, Inc. 960 Headset
root@ITC005056930CAD:~#
```

Name

Free text entry

Override serial

Serial number that will appear in the session.



Override name

Device name that will appear in the session.

Postpone

- The USB device is only removed from the system (endpoint device) when the session starts.*
- The USB device is no longer shown immediately after the system is booted.

i This setting is only effective if the **Takeaway** parameter is enabled.

Takeaway

- The USB device may be removed from the system (endpoint device).*
- The USB device may not be removed.

No Reset

- The device will not be automatically reset after the connection with the session has been terminated.*
- The device will be reset after the connection with the session has been terminated.

*IGEL OS system default



Fabulatech Scanner Redirection

Menu path: **Sessions > Horizon Client > Horizon Client Global > Fabulatech Scanner Redirection**

You can enable or disable Fabulatech scanner redirection.

Fabulatech Scanner for Remote Desktop

Fabulatech scanner redirection is enabled.



Serial Port Redirection

Serial Port Redirection

With the serial port redirection feature, you can redirect locally connected serial (/dev/ttyS) ports, such as built-in RS232 ports or USB-to-Serial adapters, to their RDS-hosted desktops.

- Serial Port Redirection is enabled.
- Serial Port Redirection is disabled. (Default)



Drive Mapping

Menüpfad: **Horizon Client > Horizon Client Global > Drive Mapping**

Through drive mapping, connected mass storage devices can be made available in the session. Specify which folders or drives are mapped during the login.

Enable Drive Mapping

Drive mapping is enabled. (Default)

- ⓘ Local (USB) devices which are to be used for drive mapping purposes must first be set up as devices. See [Storage Hotplug](#)(see page 779).

- ⚠ Before you unplug a hotplug storage device from the endpoint device, you must safely remove it. Otherwise, data on the hotplug storage device can be damaged. Depending on the configuration, there is one or several possibilities to safely remove a hotplug storage device:
 - Click on ▲ in the task bar. The taskbar is not available in a fullscreen session.
 - Click on in the in-session control bar. Depending on the configuration, the in-session control bar may be available in a fullscreen session. For further information, see [In-Session Control Bar](#)(see page 661).
 - Function **Accessories > Safely Remove Hardware** with further starting possibilities; amongst other things, a hotkey can be defined here.
 If the following warning is displayed: **Volume(s) still in use. Don't remove the device**, then the hotplug storage device must not be removed. First, exit the program concerned or close all files or directories that reside on the hotplug storage device.

- **Drive Mapping:** List of mapped drives.

To set up drive mapping, proceed as follows:

1. Click **[+ Add]** to bring up the mapping window.
2. Click **Enabled** to enable the drive connection.
3. Select a **Drive to map** from the list under which the local device or the folder is to be mapped.

- ⓘ If the drive letter you have selected is no longer available on the server, the specified directory or local drive will be given the next free letter during the login.

4. Give the **Local Drive Path** of the local directory to which the mapping is to refer.

- ⓘ If you map a locally connected device, use the pre-defined path names available in the drop-down field. The directories in question are those on which the devices are mounted by default during the boot procedure (e.g. `/autofs/floppy` for an integrated floppy drive).



Multimedia

Menu path: **Sessions > Horizon Client > Horizon Client Global > Multimedia**

You can change the following multimedia settings:

VMware Multimedia Redirection

Possible values:

- Off: The server renders the multimedia data and sends the individual images to the client.
- On: The client renders the multimedia data supplied by the server.

Real Time Audio Video (RTAV):

Specifies the redirection of video data from the client USB webcam.

Possible values:

- Off: The client does not forward the webcam data as video data.

i With USB redirection, data from the webcam can be forwarded to the server even if RTAV is disabled. For an overview and best-practice recommendations for the use of webcams, see Webcam Redirection and Optimization in IGEL OS.

- On: The client forwards the webcam data as video data.



Performance

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Global > Performance**

In this area, you can optimize the performance of *Horizon Client* sessions.

You can change the following settings:

PCoIP client-side image cache size: Specifies the size of the cache for images. Caching parts of the display reduces the amount of data to be transferred.

Possible values:

- 50 MB
- 100 MB
- 150 MB
- 200 MB
- 250 MB
- 300 MB

Larger cache sizes of 250 MB or more should only be used if at least 2 GB RAM or more is available.

Lakeside SysTrack

The Lakeside SysTrack is enabled.

The Lakeside SysTrack is not enabled. (Default)

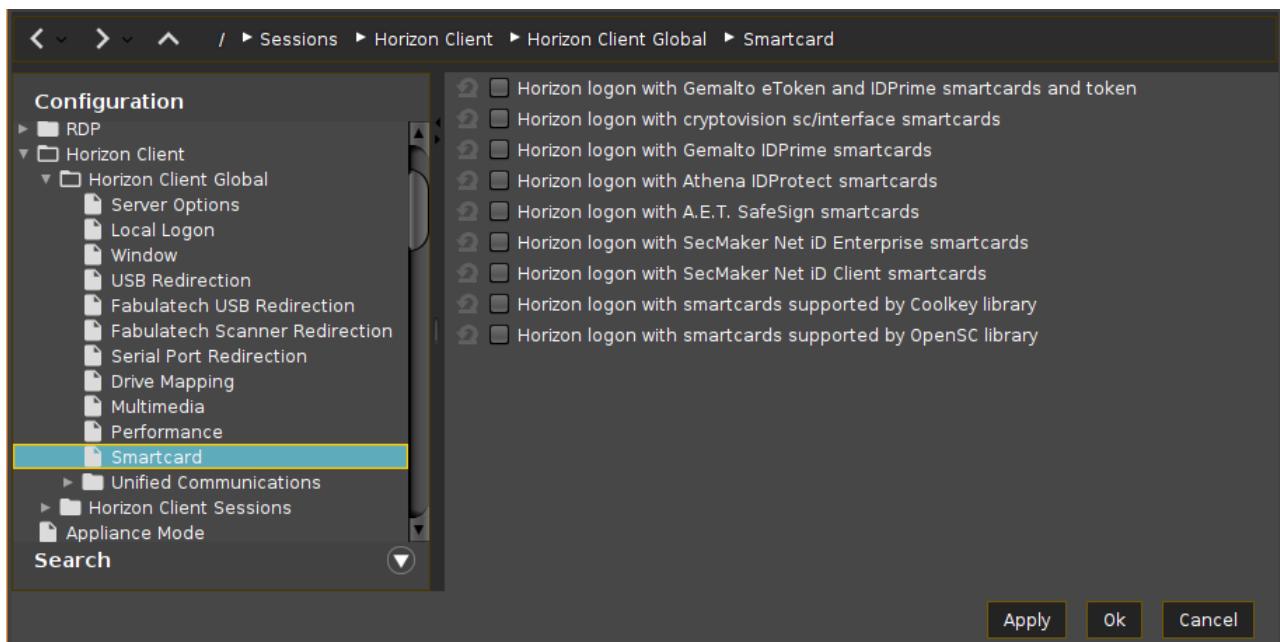


Smartcard Middleware Settings for VMware Horizon Sessions in IGEL OS

When configuring login with a smartcard, you have to define smartcard middleware to be used. In this area of the IGEL Setup, you select the middleware (PKCS#11 module) which matches your card or your token. If you want to use your own PKCS#11 library with VMware Horizon, see Using a Custom PKCS#11 Library.

For more information on smartcard authentication in IGEL OS, see the how-to Smartcard Authentication in IGEL OS.

Menu path: **Sessions > Horizon Client > Horizon Client Global > Smartcard**



Horizon logon with Gemalto eToken and IDPrime smartcards and token

- The middleware for Gemalto/SafeNet eToken, IDPrime smartcards and tokens is used.
 The middleware for Gemalto/SafeNet eToken, IDPrime smartcards and tokens is not used.*

Horizon logon with cryptovision sc/interface smartcards

- The middleware for cryptovision sc/interface smartcards is used.
 The middleware for cryptovision sc/interface smartcards is not used.*

Horizon logon with Gemalto IDPrime smartcards

- (i)** Activate this Gemalto middleware if you want to use Gemalto common criteria devices in unlinked mode.



- The middleware for Gemalto IDPrime smartcards is used.
- The middleware for Gemalto IDPrime smartcards is not used.*

Horizon logon with Athena IDProtect smartcards

- The middleware for Athena IDProtect smartcards is used.
- The middleware for Athena IDProtect smartcards is not used.*

Horizon logon with A.E.T. SafeSign smartcards

- The middleware for A.E.T. SafeSign Smartcards is used.
- The middleware for A.E.T. SafeSign Smartcards is not used.*

Horizon logon with SecMaker Net iD Enterprise smartcards

- The SecMaker Net iD Enterprise middleware, formerly known as "SecMaker Net iD", is used.
- The SecMaker Net iD Enterprise middleware is not used.*

Horizon logon with SecMaker Net iD Client smartcards

- The SecMaker Net iD Client middleware is used. SecMaker Net iD Client is the next generation of Net iD Enterprise, see <http://docs.secmaker.com/net-id-client/latest/index.html>.
- The SecMaker Net iD Client middleware is not used.*

Horizon logon with smartcards supported by Coolkey library

- The Coolkey middleware is used.
- The Coolkey middleware is not used.*

Horizon logon with smartcards supported by OpenSC library

- The OpenSC middleware is used.
- The OpenSC middleware is not used.*

Horizon logon with smartcards supported by 90meter library

Licensed Feature

This feature requires an add-on license; see Add-On Licenses. Please contact your IGEL sales representative.

- The 90meter middleware is used.



The 90meter middleware is not used.*

* IGEL OS system default



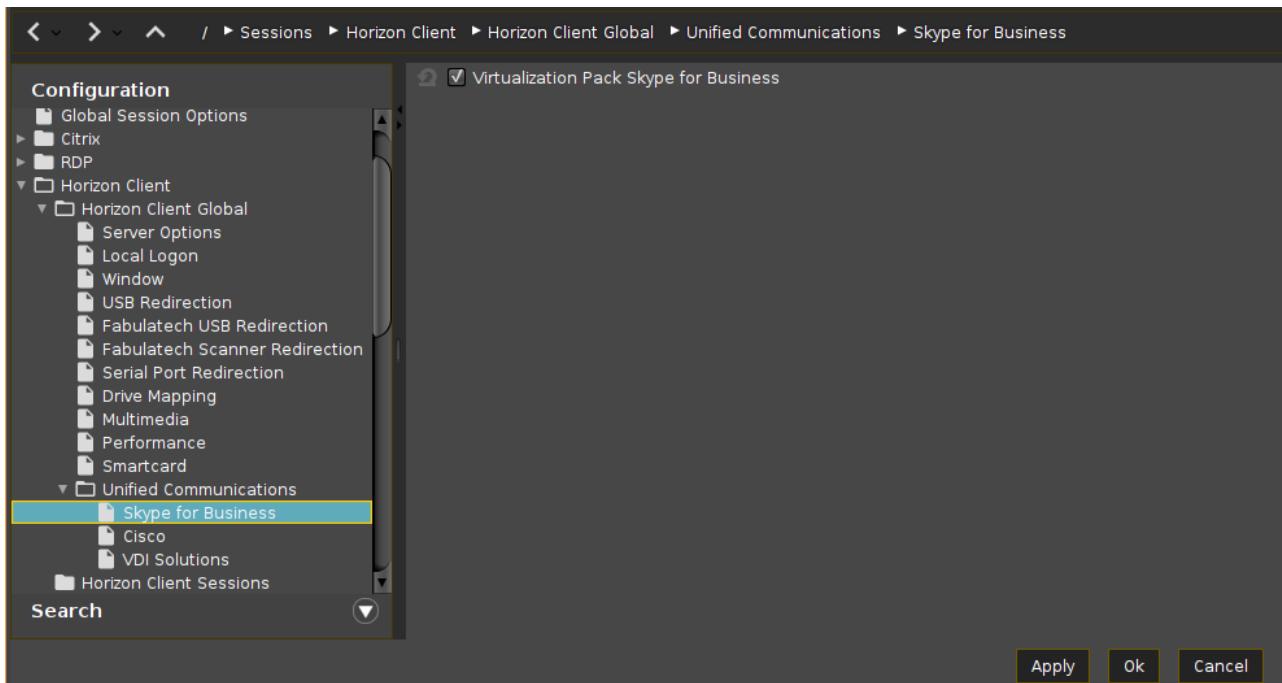
Unified Communications Settings for VMware Horizon Sessions in IGEL OS

This article shows you how to use the IGEL OS unified communications settings for VMware Horizon sessions. It is necessary to set some additional parameters in IGEL OS to leverage the VMware Horizon-related multimedia enhancements. These parameters and their functions are explained below.

Menu path: **Sessions > Horizon Client > Horizon Client Global > Unified Communications**

Skype for Business

Menu path: **Sessions > Horizon Client > Horizon Client Global > Unified Communications > Skype for Business**



⚠ Server and Network Requirements

Skype for Business optimization requires additional configuration on the server side. For more information, see the VMware article [Configuring VMware Virtualization Pack for Skype for Business¹⁴](#).

Virtualization Pack Skype for Business

- The Virtualization Pack Skype for Business is active.*
- The Virtualization Pack Skype for Business is not active.

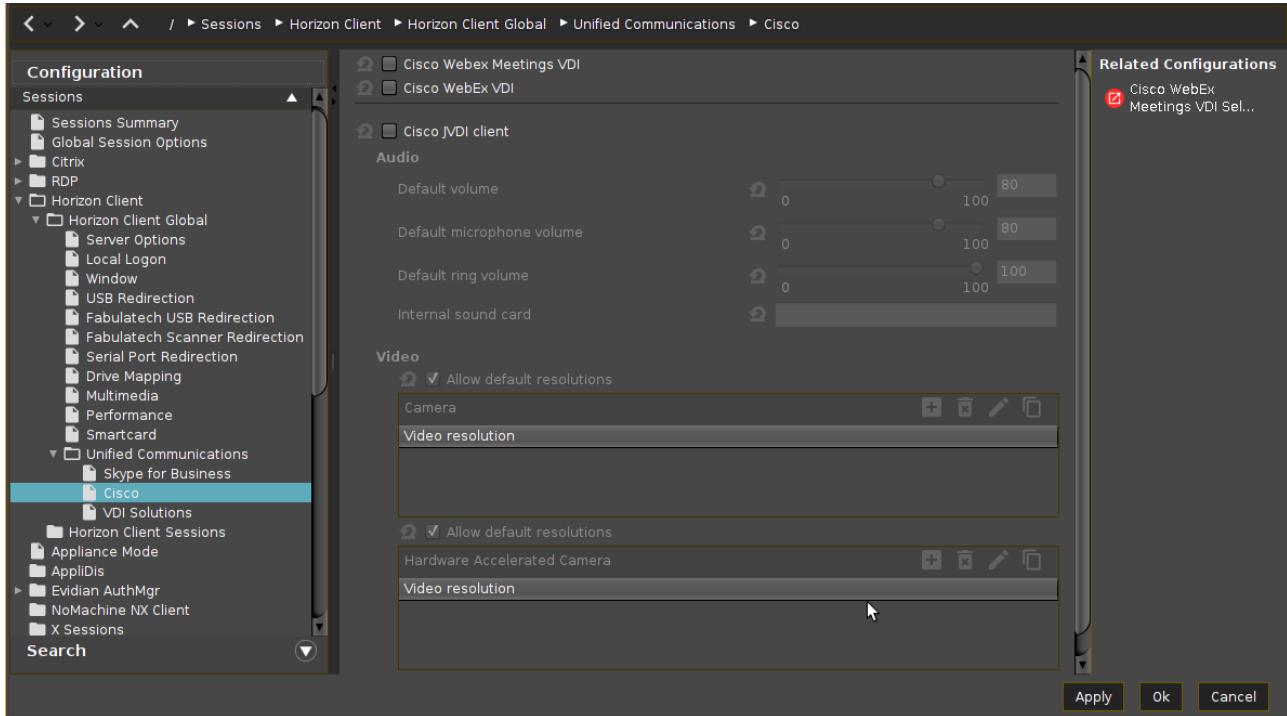
¹⁴<https://docs.vmware.com/en/VMware-Horizon-7/7.13/horizon-remote-desktop-features/GUID-ABE8ACEE-02DE-4F1C-99D8-6B589E1762E9.html>



Cisco

Menu path: **Sessions > Horizon Client > Horizon Client Global > Unified Communications > Cisco**

Here you can activate or deactivate the virtual desktop optimization for Cisco Webex and define settings for the Cisco JVDI client.



Cisco Webex Meetings VDI

This virtual desktop optimization contains a media engine and redirects the audio and video streams so that they are exchanged directly between the endpoint devices and Webex Meetings cloud, without going through the hosted virtual desktop in the datacenter.

⚠ The Cisco Webex Meetings VDI plugin and your server-side application should have the same version. For details on backward compatibility, see [Webex Meetings VDI Release Notes¹⁵](#).

To select the version of the Cisco Webex Meetings plugin:

1. In the UMS configuration dialog or the local Setup, go to **Sessions > Unified Communications > Cisco Webex Meetings VDI Selection > Cisco Webex Meetings client version.**
(If you do not see the corresponding version in the UMS configuration dialog, but it is listed in the release notes, please update the firmware your profile is based on.)
2. Select the desired version and click **Apply** or **Ok**.

¹⁵ https://help.webex.com/en-us/article/glj57y/Release-Notes-for-Cisco-Webex-Meetings-Virtual-Desktop-Software-Release-42.x#Cisco_Reference.dita_fcb4e1d7-dbef-4bab-8842-9b1a8f84a9e5



For further information, see the Cisco documentation for Webex Meetings:

- General information: <https://help.webex.com/en-us/nfjsqzbb/Cisco-Webex-Meetings-Virtual-Desktop-Software>
- Administration guide: [https://www.cisco.com/c/en/us/td/docs/collaboration/webex_vdi/admin/webex_b_admin-cisco-wmvdi-40-8.html¹⁶](https://www.cisco.com/c/en/us/td/docs/collaboration/webex_vdi/admin/webex_b_admin-cisco-wmvdi-40-8.html)
- Installation: https://www.cisco.com/c/en/us/td/docs/collaboration/webex_vdi/admin/webex_b_admin-cisco-wmvdi-40-8/webex_m_wvdi-software-installation.html

The Cisco Webex Meetings VDI solution is enabled.

The Cisco Webex Meetings VDI solution is disabled.*

Cisco Webex VDI

This virtual desktop optimization contains a media engine and redirects the audio and video streams so that they are exchanged directly, without going through the hosted virtual desktop in the datacenter.

For further information, see the Cisco documentation for Webex VDI:

- General information: https://www.cisco.com/c/dam/en_us/solutions/collaboration/docs/cisco-webex-teams-solution-overview.pdf
- Overview about the supported versions: https://help.webex.com/en-us/ntpplus7/Webex-VDI-Release-Notes#Cisco_Reference.dita_13d9aace-b6f9-41dc-a6e0-9f7a48834060
- Administration guide: [Administration - Webex App | Installation and Automatic Upgrade¹⁷](#)
- Installation: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/vdi/wbx-teams-vdi-deployment-guide.pdf

The Cisco Webex VDI solution is enabled.

The Cisco Webex VDI solution is disabled.*

Cisco JVDI Client

For the vendor documentation for the Cisco JVDI client, see [Deployment and Installation Guide for Cisco Jabber Softphone for VDI Release 14.0¹⁸](#).

The Cisco JVDI Client is enabled.

The Cisco JVDI Client is disabled.*

i If you do not see the option **Cisco JVDI Client**, check if the **Cisco JVDI Client** is enabled under **System > Firmware Customization > Features**. Reboot the device if required.

¹⁶ https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.cisco.com%2Fc%2Fen%2Fus%2Ftd%2Fdocs%2Fcollaboration%2Fwebex_vdi%2Fadmin%2Fwebex_b_admin-cisco-wmvdi-40-8.html&data=04%7C01%7Cfeeney%40igel.com%7Cbbb4ae6a9db34ec84a0b08d88cee6ac9%7C3f04441122ea4ba182dfd85e25879b4f%7C0%7C0%7C637414302911303723%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQljoV2luMzliLCJBtil6lk1haWwiLCJXVCi6Mn0%3D%7C1000&sdata=NrHywiQaoFcqcl5f%2FCRgK2BJw7%2BFfWirNQNj4MYTz0s%3D&reserved=0

¹⁷ <https://help.webex.com/en-US/article/nw5p67g/Webex-App-%7C-Installation-and-Automatic-Upgrade>

¹⁸ https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jvdi/14_0/dig/jvdi_b_deploy-install-jvdi-14-0/jvdi_b_deploy-install-jvdi-12-9_chapter_010.html



If you have reduced the IGEL OS feature set before and cannot activate **Cisco JVDI Client**, see Adapting IGEL OS 11.04 or Higher for Devices with Small Storage.

Audio

Default volume

Headphone volume control. (Default: 80%)

Default microphone volume

Microphone volume control. (Default: 80%)

Default ring volume

Ringtone volume control. (Default 100%)

Internal sound card

Here you have the possibility to define a sound card. If you leave the field empty, the default sound card of the system is used.

For further information, see [Sound Preferences](#)(see page 539).

Video

You can set the Cisco JVDI Client to use the default resolutions of the camera or to use a user-defined set of resolutions. Separate configurations for cameras with and without hardware acceleration are possible.

Allow default resolutions (for cameras without hardware resolution)

The default resolutions of the camera are used.*

A user-defined set of resolutions is used. You can add a resolution by clicking **[+]** in the **Camera** area and selecting the desired resolution.

Allow default resolutions (for cameras with hardware resolution)

The default resolutions of the camera are used.*

A user-defined set of resolutions is used. You can add a resolution by clicking **[+]** in the **Hardware Accelerated Camera** area and selecting the desired resolution.

VDI Solutions

Menu path: **Sessions > Horizon Client > Horizon Client Global > Unified Communications > VDI Solutions**



The screenshot shows the 'Sessions' configuration screen in the IGEL OS interface. The navigation path is: / > Sessions > Horizon Client > Horizon Client Global > Unified Communications > VDI Solutions. The 'Configuration' pane on the left lists several sections: Global Session Options, Citrix, RDP, Horizon Client (with sub-options like Horizon Client Global, Unified Communications, and VDI Solutions), and Horizon Client Sessions. The 'VDI Solutions' option is highlighted with a blue selection bar. The 'Related Configurations' pane on the right shows 'Zoom Client Selection' with a red warning icon. At the bottom right are three buttons: 'Apply', 'Ok', and 'Cancel'.

HTML5 multimedia redirection

⚠ Server and Browser Requirements

HTML5 multimedia redirection requires additional configuration on the server side. For more information, see the VMware article [Configuring HTML5 Multimedia Redirection](#)¹⁹.

HTML5 multimedia content is redirected from a remote desktop to the endpoint devices.*

HTML5 multimedia content is not redirected.

Microsoft Teams optimization

⚠ Server and Network Requirements

Microsoft Teams optimization requires additional configuration on the server side. For more information, see the VMware articles [Microsoft Teams Optimization with VMware Horizon](#)²⁰ and [Configuring Media Optimization for Microsoft Teams](#)²¹.

The audio and video streams for Microsoft Teams are redirected to the endpoint devices. Audio and video data are not processed by the server.*

The audio and video streams for Microsoft Teams are not redirected.

¹⁹<https://docs.vmware.com/en/VMware-Horizon-7/7.13/horizon-remote-desktop-features/GUID-6A68ECA4-6B9C-43C5-B437-D39B71005BAD.html>

²⁰<https://techzone.vmware.com/resource/microsoft-teams-optimization-vmware-horizon>

²¹<https://docs.vmware.com/en/VMware-Horizon/2106/horizon-remote-desktop-features/GUID-F68FA7BB-B08F-4EFF-9BB1-1F9FC71F8214.html>



Zoom VDI Media Plugin

⚠ Server and Network Requirements

Zoom optimization requires additional configuration on the server side. For more information, see the Zoom articles [Getting started with VDI²²](#) and [Mass deployment with preconfigured settings for Windows²³](#).

The audio and video streams for Zoom are redirected to the endpoint devices. Audio and video data are not processed by the server.

The audio and video streams for Zoom are not redirected.*

i The **Zoom VDI Media Plugin** version must be equal to or less than the version of the server-side Zoom VDI application; a plugin with a higher version is not supported. Zoom recommends updating the Zoom plugin after updating the Zoom VDI application since new features can require an updated plugin. For more information, see the Zoom article [VDI backwards compatibility²⁴](#).

You can select the Zoom VDI Media Plugin version under **Sessions > Unified Communications > Zoom Client Selection > Zoom client version**.

Related Topics

[Webcam Redirection and Optimization in IGEL OS](#)

[Which Unified Communication Solutions Does IGEL OS Support?](#)

*IGEL OS system default

²² <https://support.zoom.us/hc/en-us/articles/360031096531-Erste-Schritte-mit-VDI>

²³ <https://support.zoom.us/hc/en-us/articles/201362163-Mass-Installation-and-Configuration-for-Windows>

²⁴ <https://support.zoom.us/hc/en-us/articles/360041602711-VDI-backwards-compatibility>



Horizon Client Session

Menu path: **Sessions > Horizon Client > Horizon Client Sessions > [Session Name]**

You can configure one or more Horizon Client sessions.

The settings for launching the session are described below.

Session name: Name for the session.

The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.



- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.



No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.

-
- [Connection Settings](#)(see page 203)
 - [Window](#)(see page 204)
 - [Mouse and Keyboard](#)(see page 205)
 - [Mapping](#)(see page 206)
 - [Performance](#)(see page 207)
 - [Options](#)(see page 208)
 - [Multimedia](#)(see page 209)
 - [Desktop Integration](#)(see page 210)



Connection Settings

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Connection Settings**

In this area, you can specify the settings for the connection between the *Horizon Client* and the server.

- **Server URL:** URL of the *VMware Horizon* server
- **Use passthrough authentication for this session**
 - The user name and password are temporarily saved and used for authentication purposes in this session.
 Passthrough authentication is not used. (default)
- **User name:** User name when logging on to the *VMware Horizon* server
- **User password:** Password when logging on to the *VMware Horizon* server
- **Domain:** Domain when logging on to the *VMware Horizon* server
- **Session type:** Specifies whether the session contains a desktop or an individual application.
Possible values:
 - Desktop: The session contains a desktop.
 - Application: The session contains an individual application.
- **Desktop name:** Specifies a name for the desktop. This option is available if **Session Type** is set to "Desktop".
- **Application:** Application that is launched during the session. This option is available if **Session Type** is set to "Application".
- **Autoconnect**
 - When the session starts, the connection to the desktop or application will automatically be established. For this to be possible, the name of the desktop or application must be defined.
 When the session starts, the overview will be shown. (default)
- **Preferred desktop protocol:** The selected option is preferred by the client when negotiating the connection protocol.
Possible values:
 - Global setting
 - Server setting
 - RDP
 - PCoIP
 - VMWare Blast
- **Enable kiosk mode**
 - Global setting
 - On
 - Off

Further settings options can be found under [AD/Kerberos Configuration](#)(see page 814) and [AD/Kerberos](#)(see page 807).



Window

Menu path: **Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Window**

In this area, you can change the way in which the session is displayed.

Window size: Specifies the width and height of the window.

Possible values:

- Global setting: The window size is carried over from the global settings for Horizon Client sessions, see [Window\(see page 174\)](#).
- Fullscreen: The session is shown on the full screen.
- User selection
- Numeric details: The session is shown in the selected resolution or on the selected percentage of the screen area.

Number of colors: Specifies the color depth.

- Global setting: The color depth is carried over from the global settings for RDP sessions, see [Window\(see page 115\)](#).
- 256
- Thousands
- Millions

Start monitor: Specifies the monitor on which the session is shown.



Mouse and Keyboard

Menu path: **Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Mouse and Keyboard**

In this area, you can define the settings for the mouse and keyboard.

Disable Mouse Motion Events

The mouse pointer will only be shown locally on the thin client. If the user moves the mouse over a session item, no reaction of the item will be shown.

Further settings options can be found in the user interface setup area under [Language\(see page 662\)](#) as well as [Keyboard\(see page 672\)](#) and [Additional keyboard layouts\(see page 673\)](#).



Mapping

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Mapping**

In this area, you can specify the data transmission between the thin client and *Horizon Client* session.

- ⓘ These settings only apply to RDP-based sessions.
▶ Check whether **Sessions > Horizon Client Sessions > Horizon Client Session > Connection Settings > Preferred Connection Protocol** selection is set to "RDP".

- **Enable Client Audio**
 - [Global setting](#)
 - On - enhanced
 - On - secure
 - Off
- **Enable Clipboard**
 - [Global setting](#)
 - On
 - Off
- **Enable Printer Mapping**
 - [Global setting](#)
 - On
 - Off
- **Enabling COM Port Mapping**
 - [Global setting](#)
 - On
 - Off
- **Enable Drive Mapping**
 - [Global setting](#)
 - On
 - Off
- **Enable USB Redirection**
 - [Global setting](#)
 - Off

Further settings options can be found in the RDP Global setup area under Drive Mapping, COM Ports, [Printers](#)(see page 122), Audio, Keyboard and in the Devices area under [Printer](#)(see page 754).



Performance

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Performance**

In this area, you can save system resources by disabling certain visual functions of the user interface.

- **Disable wallpaper:**
 - On: No desktop background image is shown.
- **Do not show contents of window while dragging:**
 - On: The content of a window will not be shown while the window is being moved.
- **Disable menu and window animation:**
 - On: Transitions for menus and windows will not be animated.
- **Disable themes:**
 - On: No optional desktop theme can be used.
 - Off: An optional desktop theme can be used.
- **Disable cursor shadow:**
 - On: The mouse pointer will be shown without a shadow.
 - Off: The mouse pointer will be shown with a shadow.
- **Disable cursor settings**
 - On: The mouse pointer settings cannot be changed.
 - Off: The mouse pointer settings can be changed.
- **Enable font smoothing:**
 - Global setting: The setting under Sessions > Horizon Client > Horizon Client Global will be used.
 - On: Edges will be smoothed when text is displayed.
 - Off: Edges will not be smoothed when text is displayed.

Further settings options can be found in the Horizon Global setup area under [Performance\(see page 190\)](#) and in the RDP Global area under [Performance\(see page 126\)](#).



Options

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Options**

In this area, you can change the following settings:

- **Working directory:** Directory that is used after logging on
- **Compression:**
 - Global setting: The setting from **Setup > Sessions > Horizon Client > Horizon Client Global** will be carried over.
 - On: The data flow between the client and server will be compressed.
 - Off: The data flow will not be compressed.
- **Enforce TLS-encrypted connections:**
 - Global setting: The setting from **Setup > Sessions > Horizon Client > Horizon Client Global** will be carried over.
 - On: Encryption of the connection with TLS will be forced.
 - Off: Encryption will not be forced.
- **Network level authentication:**
 - On: The user will authenticate themselves on the network level (network layer authentication) in order to establish an RDP connection.

i If network level authentication is enabled, the local logon window is used. This also applies if the **Use local logon window** option under **Setup > Sessions > Horizon Client > Horizon Client Global > Local Logon** is disabled.

- Off: Conventional authentication

Further settings options can be found in the RDP Global setup area under [Options](#)(see page 130), [Performance](#)(see page 126) and in the Horizon Global area under [Local Logon Options for Horizon Client in IGEL OS](#)(see page 172).



Multimedia

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Multimedia**

You can change the following multimedia setting:

- **Enable VMware multimedia redirection**

Possible values:

- Global setting: The setting under **Sessions > Horizon Client > Horizon Client Global** will be used.
- off: The server renders the multimedia data and sends the individual images to the client.



Desktop Integration

Menu path: **Sessions > Horizon Client > Horizon Client Sessions > [Session name] > Desktop Integration**

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.



Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

Sessions



- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.



Appliance Mode

Menu path: **Sessions > Appliance Mode**

In the appliance mode, only one specific session is accessible. You can activate the appliance mode for one of the following session types (if available on your system):

- VMware Horizon(see page 215)
- Browser(see page 216)
- Citrix Self-Service(see page 217)
- RHEV/Spice(see page 218)
- Imprivata(see page 219)
- RDP MultiPoint Server(see page 222)
- XDMCP for This Display(see page 223)

ⓘ The system hotkey [Ctrl]+[Alt]+[S] for launching the setup application does not work in the appliance mode. Use [Ctrl]+[Alt]+[F2] instead.

ⓘ You can set up a hotkey to start quick setup in appliance mode.

By default, access to other applications is not possible in appliance mode. However, these applications can be made available by activating **Appliance Mode Access** at the corresponding **Desktop Integration** page:

- ICA Connection Center(see page 500)
- Task Manager(see page 557)
- Application Launcher(see page 535)
- Firmware Update(see page 602)
- Quick Settings(see page 521)
- Sound Preferences(see page 539)
- Disk Utility(see page 593)
- Commands(see page 576)
- Webcam Information(see page 614)
- Touchscreen Calibration(see page 553)
- Screen Lock/Saver(see page 663)
- Monitor Calibration(see page 573)
- Network Tools(see page 578)
- Screenshot Tool(see page 564)
- System Information(see page 589)
- Bluetooth Tool(see page 583)
- Display Switch
- Identify Monitors(see page 610)
- System Log Viewer(see page 545)
- Local Terminal(see page 504)
- SSH Session(see page 342)
- Custom Application(see page 850)
- Mobile Device Access(see page 599)



- [Open VPN](#)(see page 722)
- [OpenConnect VPN](#)(see page 728)
- [genucard](#)(see page 731)

Additionally, the in-session control bar can be used in an appliance mode session. With the in-session control bar, the user can eject a USB drive, start the wireless manager, start the Mobile Device Access USB tool and end the session. For further information, see [In-Session Control Bar](#)(see page 661).



VMware Horizon

Menu path: **Sessions > Appliance Mode > VMware Horizon**

Server URL: URL of the VMware Horizon server.

User name: User name when logging on to the VMware Horizon server.

User password: Password when logging on to the VMware Horizon server.

⚠ Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

Domain: Domain when logging on to the VMware Horizon server.

Desktop name: Desktop that is to be launched automatically.

Autoconnect

The desktop given in **Desktop name** is launched automatically.

Network level authentication

- **on:** The user will authenticate themselves on the network level (network layer authentication) in order to establish an RDP connection.
- **off:** Conventional authentication.

i If network level authentication is enabled, the local login window is used. This also applies if the **Use local login window** option under **Sessions > Horizon Client > Horizon Client Global > Local Logon** is disabled.



Browser

Menu path: **Sessions > Appliance Mode > Browser**

When this appliance mode is active, the Firefox browser is started to establish a connection with a session, e.g. a Citrix XenDesktop session. With a Citrix session, the browser is restarted after the session has been closed.

- ⓘ If your session requires an on-screen keyboard, you can jump to the relevant configuration page via the link **On-screen keyboard** on the right-hand side. See also [On-Screen Keyboard](#)(see page 568).

Web URL: URL for the session



Citrix Self-Service

Menu path: **Sessions > Appliance Mode > Citrix Self-Service**

- ⓘ At least Citrix Receiver Version 13 is required.

Self-Service delivery server URL: Server address including the `https://` prefix.

- ⓘ In the appliance mode, only one server can be used for Self-Service.

Multi User (StoreFront servers only)

The user data on the client will be deleted after logging off or terminating Self-Service.

Reconnect after logon

The Self-Service GUI reconnects automatically after being launched.

Reconnect to apps after starting an application

The Self-Service GUI will attempt to reconnect to ongoing sessions if an application is launched or the store is reloaded.



RHEV/Spice

Menu path: **Sessions > Appliance Mode > RHEV/Spice**

Connection Broker: URL of the Connection Broker.



Imprivata

Menu path: **Sessions > Appliance Mode > Imprivata**

Imprivata offers digital security solutions for healthcare organizations. For more information, see [imprivata.com](https://www.imprivata.com)²⁵.

- ⓘ Enable the following in the Setup if you use Imprivata versions above 6.3: **System > Registry > imprivata.gain_permission.**

Set the URL to the server: URL address of the single sign-on server.

Path to the appliance: Path to the application on the single sign-on server. (Default: `sso/servlet/getembeddedloader?arch=amd64`)

Enable component's logging

Log files will be generated. You will need them if support is required in the future.

Redirection of smartcards

A smartcard will be redirected into a session.

PIE application launcher for Citrix

Enables the grid theme for organizing Citrix apps.

The following setting is active if **Enable component's logging** is enabled.

Component's logging verbosity: Specifies the level of detail for the log files.

Possible options:

- "debug": Detailed information on the flow through the system.
- "info": Runtime events (startup/shutdown).
- "warning": Events that may lead to unexpected behavior.
- "error": Other errors or unexpected conditions.
- "critical": Events that may break the workflow.

Path to certificate: Absolute path to the certificate your Imprivata Appliance or Certification Authority issued. (Default: `/wfs/ca-certs/ssoCA.cer`)

⚠️ IMPORTANT NOTE

If you rename the certificate or decide to store it in a different place, you have to adjust the path accordingly under **Sessions > Appliance Mode > Imprivata > Path to Certificate**.

Best practice is to change it directly through the profile which also issued the firmware update.

Fast User Switching

FUS user: The username for the preconfigured session.

Possible options:

- Hostname: The hostname of the endpoint device will be used as a username.
- MAC address: The MAC address of the device will be used as a username.

²⁵ <https://www.imprivata.com/>



- Serial of the board: The serial number of the device will be used as a username.
- Free text entry

FUS user's domain: The domain the user belongs to.

FUS user's password: The password of the user running the preconfigured session.

Citrix Store URL: URL of the StoreFront website or of XenApp Services.

FUS resource: The resource, like the Desktop or Application, that is assigned to the username.

Single Application Kiosk: The Imprivata PIE agent will be signaled that the FUS resource is an application.

(i) More on FUS at: <https://www.imprivata.com/resources/datasheets/fast-user-switching-imprivata-onesign>

Enable on-screen keyboard

If a touchscreen is used, the on-screen keyboard is enabled.

The following settings are active if **Enable on-screen keyboard** is activated.

x coordinate of on-screen keyboard: Specifies the X position of the on-screen keyboard in pixels. (Default: 2)

y coordinate of on-screen keyboard: Specifies the Y position of the on-screen keyboard in pixels. (Default: 2)

Width of on-screen keyboard in pixels: It is recommended that you specify either the width or the height. (Default: 900)

Height of on-screen keyboard in pixels: It is recommended that you specify either the width or the height. (Default: 0)

The screenshot shows the 'Appliance mode' configuration for sessions. The 'Enable on-screen keyboard' checkbox is checked. Other settings shown include Hostname (lx.test), FUS users's domain (lx.test), FUS users's password (*****), Citrix Store URL (https://citimp-srv.lx.test/citrix/storeweb), and FUS resource (FUS).

(✓) If you need to modify and adjust the sessions, see [Imprivata: Session Customization](#).



- ✓ Imprivata automatically creates a data partition, i.e. storage location for internal data. If you are asked by your support to delete the data partition or you want to delete it for other reasons, see [Imprivata: Clear the Imprivata Data Partition](#).

ⓘ **Useful Registry Keys**

- If you need to set a default AD domain for PIE agent, go to **System > Registry > imprivata.default_domain** and specify the NetBIOS name of your AD domain.
- If you need to ignore the VMware protocol selected by the Imprivata appliance, activate **System > Registry > imprivata.ignore_horizon_protocol**. In this case, the local selection under **Horizon Client > Horizon Client Global > Server Options > Preferred desktop protocol** will be used.
- To avoid focus theft from other windows, activate **System > Registry > imprivata.avoid_focus_ownership**.



RDP MultiPoint Server

Menu path: **Sessions > Appliance Mode > RDP MultiPoint Server**

Connect to server as soon as it is found: If you always have to connect to the same server, you can preset the connection here by giving the DNS name of your RDP MultiPoint Server. Otherwise, the device will find one or more RDP MultiPoint Servers automatically as soon as you launch the session. For this to be possible, the servers must be in the same network as the device and obtain their IP address from the same DHCP server as the device.



XDMCP for This Display

Menu path: **Sessions > Appliance Mode > XDMCP for this display**

If this session type is selected, the device acts as an XDMCP client.

Connection type: The type of the connection.

Possible values:

- "Indirect via localhost- "Indirect": At startup, a list of XDMCP hosts is displayed. This list is generated by the server specified under **Name or IP of the server**. The user can select a host.
- "Direct": The login mask of the host specified under **Name or IP of the server** is displayed.
- "Broadcast": The device starts a broadcast request. The login mask of that XDMCP host is displayed which is the first to respond to the broadcast request.

Name or IP of server: The name or IP of the XDMCP server.

Enable hotkeys for XDMCP Display: Defines whether hotkeys are managed by the device or the host.

Hotkeys are managed by the device. When the user enters a shortcut key that is defined as a hotkey on the device, it starts the appropriate action. The input is not forwarded to the server. (Default)

Hotkeys are not managed by the device. Almost all keyboard shortcuts are forwarded to the server. The hotkey [Ctrl + Alt + s] for opening the IGEL Setup can still be used, provided that this hotkey is activated under **Accessories > Setup**.



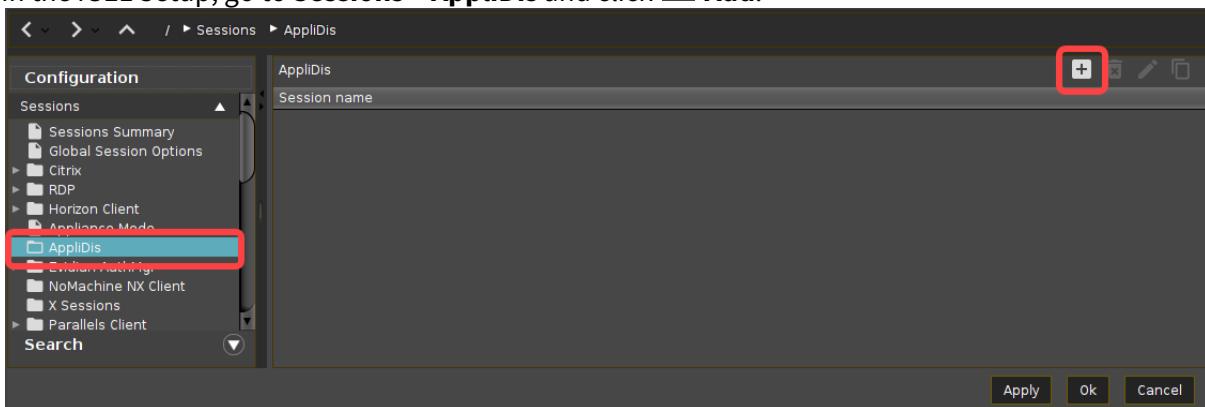
AppliDis

In IGEL OS, you can use the AppliDis client. AppliDis Fusion is a virtualization solution which combines the virtualization of desktops and applications in a single console. For more information, see <https://www.systancia.com/en/systancia-workplace/>.

Menu path: **Sessions > AppliDis**

To create an AppliDis session, proceed as follows:

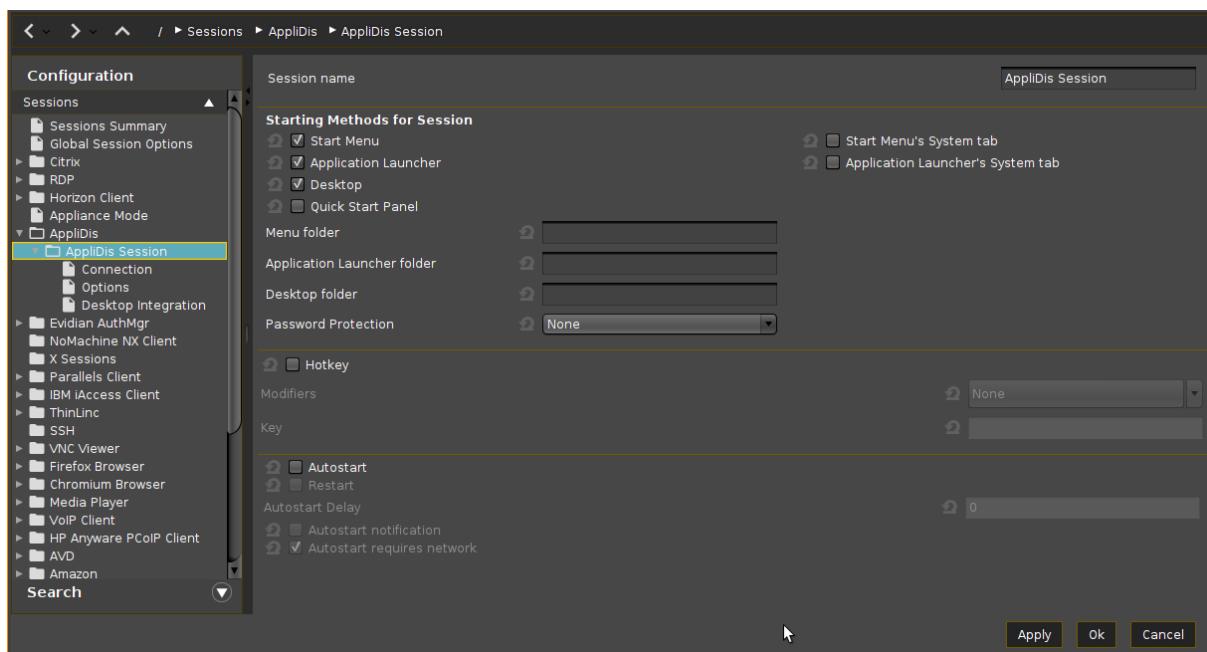
1. In the IGEL Setup, go to **Sessions > AppliDis** and click **Add**.



For the added session, you can perform the following actions:

- Click on to remove the selected entry.
- Click on to edit the selected entry.
- Click on to copy the selected entry.

2. In the following area or under **Desktop Integration**, configure the **session name** and **starting methods** for this session.



3. Configure other settings according to your needs.

4. Click **Apply** or **Ok** to save the settings.

- Connection Settings for the AppliDis Client in IGEL OS(see page 226)
- Options for the AppliDis Client in IGEL OS(see page 227)
- Desktop Integration(see page 230)



Connection Settings for the AppliDis Client in IGEL OS

In IGEL OS, you can add an AppliDis session; for how to add a session, see [AppliDis\(see page 224\)](#). In the **Connection** area, you can provide details of the **server URL** and **connect type** for logging in. If you use AppliDis SLB Linux in the connector mode, the name of the application that uses the connector can be specified here.

Menu path: **Sessions > AppliDis > Connection**

Server URL

Address of the AppliDis server or the administration server

HTTP/HTTPS service port

Protocol for communication with the AppliDis server

Possible options:

- http
- https

Connect type

Possible options:

- Last option used
- TS desktop
- Virtual desktop
- Session maker
- VDI desktop

Forces the VDI desktop

Name of the desktop to be started, e.g. `Win10Test`, `TD-RD Desktop`. This feature is active if "VDI desktop" is selected under **Connect type**.

AppliDis SLB connector mode

Name of the application which the connector uses if AppliDis SLB Linux is to be used in the connector mode.



Options for the AppliDis Client in IGEL OS

In IGEL OS, you can add an AppliDis session; for how to add a session, see [AppliDis\(see page 224\)](#). In the **Options** area, you can define the language, credentials, access path, and further settings for the AppliDis client.

Menu path: **Sessions > AppliDis > Options**

Language

Language for the AppliDis client

Possible options:

- English (Default)
- French

How the password is sent to the RDP Client

The method for sending the password configured below to the RDP Client

Possible options:

- cmdline (Default)
- prompt

Working directory

Complete path of the work directory for the application on the server

User name

User name when logging in to the server

Password

Password when logging in to the server

⚠ Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

Domain

Domain when logging in to the server



Full path to cert

Path to the certificate with file name

Timeout

Maximum time in minutes that the system waits for a response from the server. (Default: 30)

AppliDisXML access path

Path for XML communication with the AppliDis administration server. (Example: `/AppliDisXML/AppliDisServer.asp`)

Lock connection type

- The connection type is locked. (Default)
- The connection type is not locked.

Hide “Close” tab

- The “Close” tab is hidden. (Default)
- The “Close” tab is not hidden.

Close AppliDis client at end of session

- The client is closed when the session ends. (Default)
- The client is not closed.

Force insecure mode

- Insecure mode is forced.
- Insecure mode is not forced. (Default)

Enable debug mode

- Debug mode is enabled.
- Debug mode is disabled. (Default)

Activate SSL mode

- SSL mode is enabled.
- SSL mode is disabled. (Default)



Remember user

- AppliDis remembers the user name. (Default)
- AppliDis does not remember the user name.

Discard credentials

- The credentials are not saved. (Default)
- The credentials are saved.

Hide “Filter” tab

- The “Filter” tab is not shown.
- The “Filter” tab is shown. (Default)

Hide “Service” tab

- The “Service” tab is not shown.
- The “Service” tab is shown. (Default)

Hide “Server” tab

- The “Server” tab is not shown.
- The “Server” tab is shown. (Default)

SLB graphic mode disabled?

- A window for selecting the desktop is not shown. (Default)
- A window is shown where the user can choose which desktop he wants to be connected to.



Desktop Integration

In IGEL OS, you can add an AppliDis session; for how to add a session, see [AppliDis\(see page 224\)](#). In the **Desktop Integration** area, you can define the session name and how the session should be started.

Menu path: **Sessions > AppliDis > Desktop Integration**

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.



Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network



- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.



Evidian AuthMgr

Menu path: **Sessions > Evidian AuthMgr**

The procedure for configuring your Evidian AuthMgr session is described below.

- [Evidian AuthMgr Global](#)(see page 234)
- [Evidian AuthMgr Session](#)(see page 238)



Evidian AuthMgr Global

Menu path: **Setup > Sessions > Evidian AuthMgr > Evidian AuthMgr Global**

Here, you can configure the global settings for Evidian AuthMgr sessions.

- [Restart](#)(see page 235)
- [Options](#)(see page 237)



Restart

Menu path: **Setup > Sessions > Evidian AuthMgr > Evidian AuthMgr Global > Restart**

Here, you can define the desktop integration for restarting Evidian AuthMgr.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.



- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`



Options

Menu path: **Setup > Sessions > Evidian AuthMgr > Evidian AuthMgr Global > Options**

Options

Language selection: Language selection of catalog messages.

Possible values:

- Global setting
- English (UK)
- English (US)
- German
- French
- Danish
- Custom

Custom catalog of messages: Choose here the file for the custom catalog of messages. (Default: `/services/evidian/share/locale/en/rsUserAuth.cat`)

Data Partition

Evidian AuthMgr Data Partition

The data partition is activated so that additional data can be stored persistently.

The data partition is deactivated. (Default)

Size: Size of the Evidian AuthMgr data partition in MB. (Default: 10)



Evidian AuthMgr Session

Menu path: **Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions**

Here, you can set up your own Evidian AuthMgr session.

- [Connection](#)(see page 239)
- [Options](#)(see page 240)
- [Desktop Integration](#)(see page 242)



Connection

Menu path: **Setup > Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions > [Session name] > Connection**

In this area, you can specify the settings for the connection between Evidian AuthMgr and the server.

Protocol: Protocol that is used for user access.

Possible values:

- "HTTP"
- "HTTPS"

Server: IP address or DNS name that is used for user access.

Port: Port that is used for user access.

Possible values:

- "9764 (HTTP)"
- "9765 (HTTPS)"
- "Custom"

Custom port: If you selected "Custom" above, you can enter a port of your own here.

Path to service: Service path that is used for user access. (Default: /soap)

CA certificate: Path to the CA certificate with file name. The certificate is needed for HTTPS connections. (Example: /wfs/ca-certs/ca.crt)



- Download the Certificate for Evidain from the EAM in **base64 encoded x509 CER** format,
- Convert it to crt by the following command: **openssl x509 -inform PEM -in YOUR_CERT.cer -out YOUR_CRT.crt**
- Eventually **move YOUR_CRT.crt** to the endpoint

Roaming session secret: Password for the roaming session.

Fallback User Access Services

Click on the logo to specify up to four alternative connections. These will be used if the primary authentication server is not available. The alternative servers will be queried in sequence.



Options

Menu path: **Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions > [Session name] > Options**

Specify further options for your Evidian AuthMgr session.

Session type

Possible values:

- Citrix ICA
- RDP
- VMware Horizon
- RDWEB
- Custom

If you have selected the user-defined session type, you can enter your own start and stop commands here:

Custom start command: Command that is executed when the card is inserted. (Example: `/wfs/start.bash`)

Custom stop command: Command that is executed when the card is removed. (Example: `/wfs/stopp.bash`)

Language selection: Language selection of catalog messages.

Possible values:

- Automatic
- English (UK)
- English (US)
- German
- French
- Custom

Custom catalog of messages: Choose here the file for the custom catalog of messages. (Default: `/services/evidian/share/locale/en/rsUserAuth.cat`)

Availability message

A message is shown when the authentication tool is available.

A message is not shown when the authentication tool is available.

Tapping mode

The operating mode can be changed by briefly tapping the card on the reader. Each tap triggers an action.

The operating mode cannot be changed by tapping the card on the reader.

Delay for dynamic tapping: Tapping delay in seconds.

Allow password authentication

Password is required for the authentication.

Password is not required for the authentication.

Allow password forgotten

Resetting the password is allowed.

Resetting the password is not allowed.



Default domain name for password authentication: Domain name used by default for password authentication.

Debug mode

Debug mode is activated, and all outputs are switched to the default error output.

Debug mode is deactivated.

Level for trace: Specifies the trace level. The level of detail of the log messages decreases as you move down through the selection list.

Possible values:

- none
- low
- medium
- high
- details

Use configuration file

Instead of the preconfigured session, a custom configuration file is used. All other session settings are ignored.

A custom configuration file is not used.

Path: Path to the configuration file with file name. (Example: `/etc/rsUserAuth/rsUserAuth.ini`)

UPN format

The UPN (User Principal Name) format for credentials is allowed.

The UPN format cannot be used.

No trivial PIN code

A trivial PIN, i.e. consisting of three or more consecutive numbers or identical digits, is not allowed.

A PIN can consist of three or more consecutive numbers or identical digits. (Example: `2345`, `1111`)

4-eye authentication

4-eye authentication is enabled. For details, see <https://www.evidian.com/products/enterprise-sso/4eyes-authentication/>.

4-eye authentication is disabled.

Ignore smartcard removal on this reader: You can ignore the removal of the smartcard/RFID badge on the reader which you specify here via the reader's name or its product ID. The use of wildcards is possible. Example: `*3x21*`



Desktop Integration

Menu path: **Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions > [Session name] > Desktop Integration**

Session name: Name for the session.

The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey



The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

Sessions



- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.



NoMachine NX Client

Menu path: **Sessions > NoMachine NX Client > [Session Name]**

You can configure one or more NoMachine NX sessions.

Further information regarding configuration can be found in the original documentation provided by NoMachine: <http://www.nomachine.com/documents>.

The settings for launching the session are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

- [Server\(see page 248\)](#)
- [Unix Desktop\(see page 249\)](#)
- [Unix Display\(see page 251\)](#)
- [Windows Desktop\(see page 252\)](#)
- [Windows Display\(see page 253\)](#)
- [VNC Desktop\(see page 255\)](#)
- [VNC Display\(see page 256\)](#)
- [Shadow Display\(see page 257\)](#)
- [Logon\(see page 259\)](#)
- [Advanced\(see page 260\)](#)
- [Services\(see page 262\)](#)
- [Desktop Integration\(see page 263\)](#)



Server

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Server**

Here, you can specify the connection data for the *NoMachine NX session*.

- **Host:** Host name or IP address of the *NoMachine NX* server.
- **Port:** Port for connecting with the *NoMachine NX* server (default: 22).
- **Connection service:** Protocol for connecting to the *NoMachine NX* server.
Possible values:
 - SSH
 - NX
- **Session:** Session type
Possible values:
 - Unix: The session will run under Unix/Linux on the server side. X11 serves as the transmission protocol.
 - Windows: The session will run under Windows on the server side. RDP serves as the transmission protocol.
 - VNC: The session will be transmitted with VNC (Virtual Network Computing) via RFP (Remote Framebuffer Protocol). On the server side, the session can run on any operating system. A VNC server is required on the server.
 - Shadow: Protocol version for older VNC servers
- **Use following DSA key:** DSA key which is to be used instead of the default key when logging on to the server. If no key is entered here, i.e. the field is empty, the thin client's default key will be used. The default key is saved under `/wfs/nxkeys/server.id_dsa.key`.



Unix Desktop

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Unix Desktop**

Here, you can specify which window manager or display manager is to be launched on the server when the user logs on with the *NoMachine NX* client. The window manager must be available on the server.

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Session** is set to "Unix".

- **Desktop**

Possible values:

- KDE: KDE will be launched.
- Gnome: Gnome will be launched.
- CDE: CDE will be launched.
- XDM: The display manager XDM will be launched.
- Custom: A custom window manager will be used.

Settings options if "Desktop" is set to "XDM":

- **Login**: These options are available if **Desktop** is set to "XDM".
 - **Let the NX server decide**: The configuration of the *NoMachine NX* server will be used for logon purposes.
 - **Query an X desktop manager**: The *NoMachine NX* client will connect to the X desktop manager of the computer defined under **Host**. The set **Port** will be used for this connection (default: 177).
 - **Broadcast XDM request**: The *NoMachine NX* client will send a request for available XDM servers in the subnet via the set **Port** (default: 177). The *NoMachine NX* client will use the first XDM server that responds to the request.
 - **Get a list of available X desktop managers**: The *NoMachine NX* client will send a request to the computer defined under **Host** via the set **Port** (default: 177). This computer will reply with a list of available XDM servers. This option is relevant to older versions of the *NoMachine NX* server.

Settings options if "Desktop" is set to "Custom":

Application

- **Run console**: The terminal set by default will be launched. Example: Xfce terminal
- **Run default X client script on server**: The script for the default desktop environment set by default will be launched. Example: `/home/user/startxfce.sh`
- **Run the following command**: Start command for the desired application or the desired window manager. Example: `startxfce`



Options

- **Floating window:** The session will be shown in a separate window. This option makes particularly efficient use of bandwidth.
- **Use X agent encoding**
 - The data traffic will be decoded by the NX agent rather than in the X protocol. (default)
 - The data traffic will remain in the X protocol and will be tunneled and compressed by the NX proxy.
- **Use taint of X replies**
 - Trivial sources of X roundtrips will be suppressed by generating the response on the side of the X client. This option is relevant to older versions of the *NoMachine NX* server. (default)
- **New virtual desktop:** The session will take place on a new virtual desktop on the server side.



Unix Display

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Unix Display**

Here, you can define the properties for image transmission from the NoMachine NX server to the NoMachine NX client.

- i** The image transmission properties can also be defined on the server side. If a server-side setting competes with a client-side setting, the server-side setting will be effective.

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Server > Session** is set to "Unix".

Display: Size of the display area that is used for the session.

Possible values:

- "640x480"
- "800x600"
- "1024x768"
- "Available area": The entire display area is used for the session. The taskbar is not visible.
- "Fullscreen- "Custom": The **Width** and **Height** can be freely defined.
- "Multimonitor fullscreen": The session will be shown in full-screen mode on all available monitors, i.e. stretched across the entire screen of each monitor.

Width: Width of the display area for the session. (Default: 800)

Height: Height of the display area for the session. (Default: 600)

Use custom settings

The image transmission properties can be changed on the client side.

The image transmission properties are specified on the server side only. (Default)

Use both JPEG and RGB compression: JPEG compression (results in losses) as well as RGB compression (loss-free) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.

Use JPEG and RGB compression, and use custom JPEG quality: JPEG compression (results in losses) as well as RGB compression (loss-free) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.

Only use JPEG compression: Only JPEG compression (results in losses) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.

Use JPEG compression and custom JPEG quality: Only JPEG compression (results in losses) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.

Only use RGB compression: Only RGB compression (loss-free) will be used.

Use plain X bitmaps: The images will be transmitted as bitmaps without compression.

JPEG quality: If **Use JPEG and RGB compression, and use custom JPEG quality** or **Use JPEG compression and cusom JPEG quality** is enabled, the quality of images in JPEG format can be defined. (Default: 6)



Windows Desktop

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Windows Desktop**

Here, you can specify which *Windows* terminal server (or remote desktop service) is used, how the user logs on and whether the entire desktop or an individual application is launched.

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Session** is set to "Windows".

- **Windows terminal server:** Host name or IP address of the *Windows* server on which the desktop or the application runs
- **Windows terminal server domain:** Domain in which the *Windows* terminal server is located
- **Use the NX user's credentials:** When the session starts, the logon information under **Setup > NoMachine NX Client Sessions > [Session Name] > Logon** will be used. (default)
- **Use following credentials:** When the session starts, the logon information under **Username** and **Password** will be used.
 - **Username:** User name for starting the session
 - **Password:** Password for starting the session
- **Start Windows login screen:** When starting the session, the user must enter their logon information.
- **Run desktop:** When starting the session, the *Windows* desktop is shown (default)
- **Run application:** When starting the session, the *Windows* application given in the text field is launched.



Windows Display

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Windows Display**

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Session** is set to "Windows".

- **Display:** Size of the display area that is used for the session

Possible values:

- 640x480
- 800x600
- 1024x768
- Available area:
 - **Full screen:** The session will be shown in full-screen mode, i. e. stretched across the entire screen.
 - Custom: The **width** and **height** can be freely defined.
 - Multi-monitor full screen:

- **Width:** Width of the display area for the session (default: 800)

- **Height:** Height of the display area for the session (default: 600)

- **Colors**

Possible values:

- 256
- 32K
- 64K
- 16M

- **Use custom settings**

The image transmission properties can be changed on the client side.

The image transmission properties are specified on the server side only. (default)

- **Use JPEG and RGB compression:** JPEG compression (results in losses) as well as RGB compression (loss-free) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.
- **Use JPEG and RGB compression, and define JPEG quality:** JPEG compression (results in losses) as well as RGB compression (loss-free) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.
- **Only use JPEG compression:** Only JPEG compression (results in losses) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.
- **Use JPEG compression and custom JPEG quality:** Only JPEG compression (results in losses) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.
- **Only use RGB compression:** Only RGB compression (loss-free) will be used.
- **Use plain X bitmaps:** The images will be transmitted as bitmaps without compression.
- **JPEG quality:** If **Use JPEG and RGB compression and define JPEG quality** or **Use JPEG compression and define JPEG quality** is enabled, the quality of images in JPEG format can be defined (default: 6).

- **Enable RDP image cache**



- The cache is enabled. This increases the amount of memory needed. However, the speed of the session may be increased. (default)



VNC Desktop

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > VNC Desktop**

Here, you can specify the VNC server as well as the password for the VNC session.

- i** These settings are only relevant up to NoMachine NX Server Version 3.5.

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Session** is set to "VNC".

- **VNC server:** Name or IP address of the server
- **:** Number of the display.
- **Password:** Password for the VNC session



VNC Display

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > VNC Display**

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Session** is set to "VNC".

i These settings are only relevant up to NoMachine NX Server Version 3.5.

- **Display:** Size of the display area that is used for the session

Possible values:

- 640x480
- 800x600
- 1024x768
- Available area
- Fullscreen: The session will be shown in full-screen mode, i. e. stretched across the entire screen.
- Custom: The **width** and **height** can be freely defined.
- Multimonitor Fullscreen

- **Width:** Width of the display area for the session (default: 800)

- **Height:** Height of the display area for the session (default: 600)

- **Use custom settings**

The image transmission properties can be changed on the client side.

The image transmission properties are specified on the server side only. (default)

- **Use both JPEG and RGB compression**: JPEG compression (results in losses) as well as RGB compression (loss-free) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.

- **Use JPEG and RGB compression, and use custom JPEG quality**: JPEG compression (results in losses) as well as RGB compression (loss-free) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.

- **Only use JPEG compression**: Only JPEG compression (results in losses) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.

- **Use JPEG compression and custom JPEG quality**: Only JPEG compression (results in losses) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.

- **Only use RGB compression**: Only RGB compression (loss-free) will be used.

- **Use plain X bitmaps**: The images will be transmitted as bitmaps without compression.

- **JPEG quality**: If **Use JPEG and RGB compression and define JPEG quality** or **Use JPEG compression and define JPEG quality** is enabled, the quality of images in JPEG format can be defined (default: 6).



Shadow Display

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Shadow Display**

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Session** is set to "Shadow".

i These settings are only relevant up to NoMachine NX Version 3.5.

- **Display:** Size of the display area that is used for the session

Possible values:

- 640x480
- 800x600
- 1024x768
- Available area:
 - **Fullscreen:** The session will be shown in fullscreen mode, i. e. stretched across the entire screen.
 - Custom: The **width** and **height** can be freely defined.
 - Multi-monitor full screen:

- **Width:** Width of the display area for the session (default: 800)

- **Height:** Height of the display area for the session (default: 600)

- **Enable custom settings**

The image transmission properties can be changed on the client side.

The image transmission properties are specified on the server side only. (default)

- **Use both JPEG and RGB compression:** JPEG compression (lossy) as well as RGB compression (lossless) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.
- **Use JPEG and RGB compression, and use custom JPEG quality:** JPEG compression (lossy) as well as RGB compression (lossless) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.
- **Only use JPEG compression:** Only JPEG compression (lossy) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.
- **Use JPEG compression and custom JPEG quality:** Only JPEG compression (lossy) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.
- **Only use RGB compression:** Only RGB compression (lossless) will be used.
- **Use plain X images:** The images will be transmitted as bitmaps without compression.
- **JPEG quality:** If **Use JPEG and RGB compression and use custom JPEG quality** or **Use JPEG compression and custom JPEG quality** is enabled, the quality of images in JPEG format can be defined (default: 6).

- **Enable render extension**

The "Render" or "XRender" protocol extension is enabled. This allows a transparency effect where windows overlap on the screen. (default)

- **Disable the backing store**

The cache is disabled. This reduces the amount of memory needed. However, the speed of the session may be reduced.

The cache is enabled. (default)



- **Disable the composite extension**

The "Composite" protocol extension is disabled. Transparency effects where windows overlap on the screen are not possible.

The "Composite" protocol extension is enabled. (default)

- **Disable the shared memory extension**

The shared memory extension is disabled.

The shared memory extension is enabled. (default)

- **Disable emulation of shared pixmaps**

The emulation of shared images (shared pixmaps) is disabled.

The emulation of shared images (shared pixmaps) is enabled. (default)



Logon

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Logon**

Here, you can specify the logon information for starting the session.

- **Login method**

Possible values:

- **Password**: The user logs on with a logon and password.
- Private key: The logon takes place with a private key.

- **Login**: User name when logging on to the server

- **Password**: Password when logging on to the server

⚠ Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.



Advanced

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Advanced**

Here, you can change advanced settings.

- **Link speed**

Possible values:

- Modem
- ISDN
- ADSL
- WAN
- LAN

- **Disable ZLIB stream compression**

Possible values:

- The data traffic between the client and server will not be compressed.

i Switching off compression can be helpful if the data traffic is compressed on another level, e.g. by VPN software.

- The data traffic between the client and server will be compressed. (default)

- **Enable SSL encryption on all traffic**

- Connections with NX, SSH and UDP will be encrypted. (default)

- Connections with NX and SSH will be encrypted, connections with UDP will remain unencrypted.

- **Connect through a HTTP proxy**

- The connection between the client and server will be routed via an HTTP proxy.

- The connection between the client and server will be direct. (default)

- **Host:** Host name or IP address of the HTTP proxy

- **Port:** Port of the HTTP proxy (default: 8080)

- **Username:** User name when logging on to the HTTP proxy

i This setting is only relevant up to NoMachine NX Server Version 3.5.

- **Password:** Password when logging on to the HTTP proxy

i This setting is only relevant up to NoMachine NX Server Version 3.5.

- **Remember my password**

i This setting is only relevant up to NoMachine NX Server Version 3.5.

- The password will be saved.

- The password will not be saved and must therefore be entered again for each session. (default)

- **Disable deferred screen updates:** Delayed screen refreshing ("lazy encoding") compensates for bottlenecks in data transmission. If a bottleneck occurs, refresh procedures requiring large amounts of bandwidth are delayed in favor of interactivity. There are two levels of delayed screen



refreshing. With Level 1, refresh actions which are not displayed directly ("offscreen") are dismissed. With Level 2, refresh actions which are displayed directly ("onscreen") are dismissed.

- i This setting is only relevant up to NoMachine NX Server Version 3.5.

Bottlenecks in data transmission are not compensated for through delayed screen refreshing.
 If the connection speed is set to "WAN", Level 1 delayed screen refreshing will be used. If the connection speed is set to "MODEM", "ISDN" or "ADSL", Level 2 delayed screen refreshing will be used. (default)

- **Disk cache:** Size of the persistent memory for caching images (default: 64 MB)

- i This setting is only relevant up to NoMachine NX Server Version 3.5.

- **Memory cache:** Size of the volatile memory for caching images (default: 16 MB)

- i This setting is only relevant up to NoMachine NX Server Version 3.5.



Services

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Services**

Here, you can enable or disable services for printers and audio playback on your thin client.

- **Enable multimedia support**

You will find further information regarding audio playback on the *NoMachine NX* client in the [NoMachine Knowledge Base](#)²⁶.

- Audio output is forwarded to the media player via esound.
 A dedicated channel is used for audio output. (default)

- **Enable CUPS printing**

- Printing via the thin client is enabled. (default)
 Printing via the thin client is disabled.

- **Port:** Port via which CUPS can be configured with a browser (default: [631](#))

- **Public printer**

- The printer connected to the thin client is shared via the network. A server-side configuration is required for this purpose.
 The printer is not shared. (default)

²⁶ <https://www.nomachine.com/?q=AR03D00355>



Desktop Integration

Menu path: **Sessions > NoMachine NX Client > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the NoMachine NX session.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.



X Sessions

Menu path: **Sessions > X Sessions > [Session Name]**

You can configure one or more X sessions.

The settings for launching the session are described below.

Session name: Name for the session.

! The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.



- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.



No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.

-
- [Server](#)(see page 269)
 - [Desktop Integration](#)(see page 271)



Server

Menu path: **Setup > Sessions > X Sessions > [session name] > Server**

Connection type: Connection type for the XDMCP session

Possible options:

- Indirect via localhost: At startup, the thin client generates a list of found XDMCP hosts. The user can select a host.
- Indirect: At startup, a list of XDMCP hosts is displayed. This list is generated by the server specified under **Name or IP of server**. The user can select a host.
- Direct: The login mask of the host specified under **Name or IP of server** is displayed
- Broadcast: The thin client starts a broadcast request. The login mask of that XDMCP host is displayed which responds first.
- Local display: The command specified under **Command to be displayed** is run.

Name or IP of server: Hostname or IP address of the XDMCP server

Command to be displayed: Command to be executed. The display is set in the DISPLAY environment variable.

Access control

Access to this display from other computers will be controlled.

Terminate after one session

The session is terminated when the user has logged out from the remote server.

Use quit hotkey

The session can be terminated with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`. Here, you will find the available modifiers and the associated key symbols:

- (No modifier) = `None`
-  = `Shift`
-  = `Ctrl`
-  = `Super_L`
-  = `Alt`

Key combinations are formed as follows with `|`:

`Ctrl + Windows` = `Ctrl|Super_L`

Quit hotkey: Key for the hotkey

-  To enter a key that does not have a visible character, e. g. the `[Tab]` key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Use fullscreen



- The XDCMP session is displayed in fullscreen mode.

Use fullscreen restricted to workarea

- The thin client's local taskbar is visible.

Window size: Window size for the XDMCP session. Default: 640x480

Color depth: Color depth for the XDMCP session.

Possible options:

- Same as display: The system settings for the thin client is used.
- 256 colors
- 65535 colors
- True Color (24)
- True Color (32)

Color allocation policy

Possible options:

- Default
- Mono
- Gray
- Color

Start monitor: Selects the monitor on which the XDMCP session is displayed.

Possible options:

- No configuration: The monitor is selected according to already existing windows and to the current position the mouse pointer.
- 1st monitor
- 2nd monitor
- Fullscreen on all monitors



Desktop Integration

Menu path: **Sessions > X Sessions > [Session Name] > Desktop Integration**

You can configure one or more X sessions.

The settings for launching the session are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.



- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.



Autostart requires network

- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.



Parallels Client Global

Menu path: **Sessions > Parallels Client > Parallels Client Global**

In this area, you can configure global settings for all Parallels Client sessions.

- [Keyboard](#)(see page 275)
- [USB Redirection](#)(see page 276)



Keyboard

Menu path: **Setup > Sessions > Parallels Client > Parallels Client Global > Keyboard**

In this area, you can select the keyboard layout for Parallels Client sessions.

Keyboard layout

Possible values:

- System presets as well as all available input schemes.



USB Redirection

Menu path: **Setup > Sessions > Parallels Client > Parallels Client Global > USB Redirection**

In this area, you can configure USB Redirection for Parallels Client sessions.

USB Redirection

USB redirection is enabled.

USB redirection is disabled. (Default)

Automatically redirect all USB devices: Defines whether the **Device Rules** will be ignored and all USB devices redirected.

All USB devices will be redirected.

USB devices will be redirected according to the **Device Rules**. (Default)

Device Rules

In this area, you can define device rules for USB redirection.

Defining new rules:

Click to get to the **Add** dialog.

In the **Add** dialog, you can define the following settings:

Rule

Possible values:

- "Deny"
- "Allow"

Vendor ID: Hexadecimal manufacturer number.

Product ID: Hexadecimal device number.

Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see [Using “System Information” Function\(see page 592\)](#).

System Information example:



Devices - USB Devices - System Information

Information View Help

Refresh Generate Report Copy to Clipboard Synchronize

Computer

- Summary
- Operating System
- Security
- Kernel Modules
- Boots
- Languages
- Memory Usage
- Filesystems
- Display
- Environment Variables

Devices

- System DMI
- Processor
- Graphics Processors
- Monitors
- Memory Devices
- PCI Devices
- USB Devices**

Network

Interfaces

Done.

Device Information

Product [0x0002] 2.0 root hub
Vendor [0x1d6b] Linux Foundation
Linux
Device EHCI Host Controller
Manufacturer Linux 5.12.19 ehci_hcd
Linux
Max Current 0 mA
USB Version 2.0
Speed 480 Mb/s

The device **002:004 logitech 960 Headset** is highlighted with a red box.

Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:

Local Terminal

```
File Edit View Terminal Tabs Help
root@ITC005056930CAD:~# lsusb | grep -i logitech
Bus 002 Device 004: ID 046d:0a45 Logitech, Inc. 960 Headset
root@ITC005056930CAD:~#
```

Name: Free text entry.

PTP/MTP redirection

PTP/MTP redirection is enabled.

PTP/MTP redirection is disabled. (Default)

Automatically redirect all PTP/MTP devices: Defines whether the **Device Rules** will be ignored and all PTP/MTP devices redirected.

All PTP/MTP devices will be redirected.

PTP/MTP devices will be redirected according to the **Device Rules**. (Default)



Device Rules

In this area, you can define device rules for PTP/MTP redirection.

Defining new rules:

Click to get to the **Add** dialog.

In the **Add** dialog, you can define the following settings:

Rule

Possible values:

- "Deny"
- "Allow"

Vendor ID: Hexadecimal manufacturer number.

Product ID: Hexadecimal device number.

Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see [Using “System Information” Function\(see page 592\)](#).

System Information example:



Devices - USB Devices - System Information

Information View Help

Refresh Generate Report Copy to Clipboard Synchronize

Computer

- Summary
- Operating System
- Security
- Kernel Modules
- Boots
- Languages
- Memory Usage
- Filesystems
- Display
- Environment Variables

Devices

- System DMI
- Processor
- Graphics Processors
- Monitors
- Memory Devices
- PCI Devices
- USB Devices**
- Network
- Interfaces

Done.

001:001 Linux 2.0 root hub
 002:001 Linux 1.1 root hub
 002:002 VMware Virtual Mouse
 002:003 VMware Virtual USB Hub
 002:004 **logitech** 960 Headset

Device Information

Product [0x0002] 2.0 root hub
 Vendor [0x1d6b] Linux Foundation
Linux
 Device EHCI Host Controller
 Manufacturer Linux 5.12.19 ehci_hcd
Linux
 Max Current 0 mA
 USB Version 2.00
 Speed 480 Mb/s

Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb` :

Local Terminal

File Edit View Terminal Tabs Help

```
root@ITC005056930CAD:~# lsusb | grep -i logitech
Bus 002 Device 004: ID 046d:0a45 Logitech, Inc. 960 Headset
root@ITC005056930CAD:~#
```

Name: Free text entry.



Parallels Client Session

Menu path: **Sessions > Parallels Client > Parallels Client Sessions > [Session Name]**

You can configure one or more Parallels Client sessions.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.



Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

ⓘ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with | :

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

- ⓘ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.



The session is started automatically, even when no network is available.

- [Connection](#)(see page 283)
- [Display](#)(see page 285)
- [Local Resources](#)(see page 286)
- [Experience](#)(see page 287)
- [Network](#)(see page 288)
- [Advanced](#)(see page 289)
- [Desktop Integration](#)(see page 290)



Connection

Menu path: **Setup > Sessions > Parallels Client > Parallels Client Sessions > [Session Name] > Connection**

In this area, you can specify the settings for the connection between the Parallels Client and the server.

Application Server

Primary Server: Name or IP address of the primary application server.

Secondary Server: Name or IP address of the secondary application server. The secondary application server is used if the primary application server cannot be contacted.

Connection Mode

Possible values:

- "Gateway Mode": This mode is suitable if the Parallels Client does not have access to a physical server and no special demands as regards security apply. The Parallels Client establishes a connection to the Parallels SecureClientGateway via port 80. The RDP sessions runs in a tunnel within this connection.
- "Direct Mode": This mode is suitable if the Parallels Client has direct access to a physical server. The Parallels Client establishes a connection to the Parallels SecureClientGateway via port 80 in order to negotiate connection data for the RDP session with the application server. The Parallels Client then terminates the connection to the gateway and establishes the session with the application server. This mode is the most efficient because the connection to the gateway is temporary and the data traffic is correspondingly low.
- "Gateway SSL Mode": This mode is suitable if the Parallels Client does not have access to a physical server and there are high demands as regards security. The Parallels Client establishes a connection to the Parallels SecureClientGateway via port 443. The RDP sessions runs in a tunnel within this connection.
- "Direct SSL Mode": This mode is suitable if the Parallels Client has direct access to a physical server and there are high demands as regards security. The Parallels Client establishes a connection to the Parallels SecureClientGateway via port 443 in order to negotiate connection data for the RDP session with the application server. The Parallels Client then terminates the connection to the gateway and establishes the session with the application server.

Port: Port for communication with the application server. (Default: 80)

Logon

Use system credentials

The system-wide logon data will be used for logging on to the application server (single sign-on). This option can be used if the local device logon takes place via Kerberos. The logon data saved temporarily when logging on to the device will be used for the user name and password.

The logon data given under **User name**, **Password**, and **Domain** will be used when logging on to the application server. (Default)

User: User name when logging on to the application server.



Password: Password when logging on to the application server.

- ⚠** Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

Domain: Domain when logging on to the application server.

Enable support for FIPS 140-2 compliance

- The support for FIPS 140-2 standard is enabled.
 The support for FIPS 140-2 standard is disabled. (Default)



Display

Display color depth: Number of colors displayed

Possible values:

- 8 bit
- 15 bit
- 16 bit
- 24 bit
- 32 bit

Graphics acceleration: Type of graphics acceleration. Higher graphics acceleration means better graphics quality, but requires more CPU power.

Possible options:

- "None": No acceleration
- "Basic": Basic acceleration
- "RemoteFX": Microsoft RemoteFX will be used.
- "RemoteFX Adaptive": RemoteFX Adaptive and H.264 codecs will be used.
- "AVC Adaptive": H.264/AVC will be used.

Info: If "RemoteFX" or "RemoteFX Adaptive" is enabled, the color depth will automatically be set internally to 32 bit, regardless of the value set under **Display color depth**.

Use all monitors for desktop session (if applicable)

All monitors will be used for the desktop session.

The primary monitor will be used for the desktop session. (Default)

Use only primary monitor for published applications

Published applications run on the server, the input and output data is exchanged between the client and the application server.

Published applications will only be shown on the primary monitor.

Published applications will only be shown on all available monitors. (Default)

Span desktop across all monitors

The desktop will be shown across all available monitors.

The desktop will only be shown on the primary monitor. (Default)



Local Resources

Menu path: **Setup > Parallels Client > Parallels Client Sessions > [Session Name] > Local Resources**

Remote audio playback

Possible values:

- "Bring to this computer- "Do not play": The device does not play back the audio data supplied by the application server.
- "Leave at remote computer": The audio data will be played back on the application server.

Remote audio recording

Possible values:

- "Record from this computer": The audio input (microphone) is redirected to the application server.
- "Do not record": The audio input (microphone) is not redirected to the application server.

Apply Windows key combinations for desktops only

Possible values:

- "On the local computer": Windows-specific hotkeys are used for the local desktop only.
- "On the remote computer": Windows-specific hotkeys are used for the application server only.
- "In full-screen mode only": Windows-specific hotkeys are used for remote applications in full-screen mode only.

Local devices

Connect local serial ports

- The device's serial interfaces can be used in the Parallels Client session.
 The serial interfaces cannot be used in the Parallels Client session. (Default)

Connect local smartcards

- The device's card reader can be used in the Parallels Client session.
 The card reader cannot be used in the Parallels Client session. (Default)

Connect local drives

- The drives connected to the device can be used in the Parallels Client session.
 The drives cannot be used in the Parallels Client session. (Default)

Connect local printers

- The printer connected to the device can be used in the Parallels Client session.
 The printer cannot be used in the Parallels Client session. (Default)

Connect clipboard

- The clipboard of the Parallels Client session can be used. (Default)
 The clipboard of the Parallels Client session cannot be used.



Experience

Menu path: **Setup > Parallels Client > Parallels Client Sessions > Parallels Client Session > Experience**

You can enable or disable the features for the graphical display according to the bandwidth of the network connection. The features can also be activated or deactivated individually.

Connection speed: Activates the features for the graphical display depending on the bandwidth of the network connection to provide the optimal performance.

Possible options:

- "Modem 56 Kbps": The features **Themes** and **Bitmap caching** will be enabled.
- "Low speed broadband (256 Kbps-2 Mbps)": The features **Themes** and **Bitmap caching** will be enabled.
- "Satellite (2 Mbps-16 Mbps with high latency)": The features **Menu and window animation**, **Desktop composition**, **Themes**, and **Bitmap caching** will be enabled.
- "High speed broadband (2 Mbps-16 Mbps)": The features **Menu and window animation**, **Desktop composition**, **Themes**, and **Bitmap caching** will be enabled.
- "WAN (10 Mbps or higher with high latency)": All features below will be enabled.
- "LAN (10 Mbps or higher)- "Detect connection quality automatically": The automatically detected quality of the network connection determines which of the features below should be used for the optimal user experience. The individual feature selection is not possible.

Desktop background

The desktop background image for the session will be shown.

Font smoothing

Edges will be smoothed when text is displayed.

Menu and window animation

Transitions for menus and windows will be animated.

Desktop composition

Visual effects can be used for the desktop. For details on desktop composition, see e.g. <https://docs.microsoft.com/en-us/windows/win32/dwm/dwm-overview>.

Show contents of window while dragging

The window content will be shown when a window is moved.

Themes

The design of the desktop can be modified.

Bitmap caching

Bitmap resources, e.g. icons or images, are cached locally. This allows reducing the amount of data sent, and, thus improves the performance.



Network

Menu path: **Setup > Parallels Client > Parallels Client Sessions > [Session Name] > Network**

Here, you can configure a proxy for communication between the Parallels Client and application server.

Use proxy server

- A proxy is used for communication between the Parallels Client and the application server.
 A direct network connection is used for communication between the Parallels Client and the application server.
(default)

Proxy type: Type or protocol of the proxy used

Possible values:

- SOCKS 4
- SOCKS 4A
- SOCKS 5
- HTTP 1.1

Proxy host: URL of the proxy

Proxy port: Port of the proxy (default: 8080)

Use proxy credentials: If a proxy demands a logon, this option must be enabled and the logon data must be entered under **Proxy user** and **Proxy password**.

- The logon data in **Proxy user** and **Proxy password** will be sent to the proxy.

Proxy user: User name when logging on to the proxy

Proxy password: Password when logging on to the proxy. The password is relevant if either the “SOCKS 5” or “HTTP 1.1” protocol is selected as the proxy type.



Advanced

Menu path: **Setup > Sessions > Parallels Client > Parallels Client Sessions > [Session Name] > Advanced**

Redirect URLs to client

- URLs will be opened on the client.
 URLs will be opened on the application server. (Default)

Redirect MAIL to client

- E-mails will be opened on the client.
 E-mails will be opened on the application server. (Default)

Compression

- The data flow between the Parallels Client and the application server will be compressed. (Default)

 Compression reduces network traffic but requires more CPU power.

- The data flow between the Parallels Client and the application server will not be compressed.

Use pre-windows 2000 login format

- Legacy login format (pre-Windows 2000) can be used. (Default)
 Legacy login format (pre-Windows 2000) cannot be used.

Network level authentication

- Network level authentication (NLA) is activated for the Parallels Client session. The client has to authenticate before connecting to the server. (Default)

For more information about NLA, see <https://technet.microsoft.com/en-us/magazine/hh750380.aspx>.

- Network level authentication is disabled.

Override computer name: The name entered here will override the name of the application server shown at the top of the session window.



Desktop Integration

Menu path: **Sessions > Parallels Client > Parallels Client Sessions > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the Parallels Client session.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.



Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

ⓘ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with | :

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

- ⓘ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

Sessions



- The session is started automatically, even when no network is available.



PowerTerm Selection in IGEL OS

IGEL OS integrates the Ericom PowerTerm terminal emulator solution, which allows you to easily access your legacy applications.

For more information on Ericom PowerTerm, see e.g. <https://www.ericom.com/powerterm/embedded-thin-clients/>.

Under **PowerTerm Selection**, you can choose the required version of the PowerTerm terminal emulator in order to ensure the best possible compatibility with your terminal applications.

Menu path: **Sessions > PowerTerm Terminal Emulation > PowerTerm Selection**

i Licensed Feature

This feature requires an add-on license; see Add-On Licenses. Please contact your IGEL sales representative.

PowerTerm version

Selects the version of the PowerTerm terminal emulator.

For the included PowerTerm versions, see the "Component Versions" section in the IGEL OS release notes.

⚠ When using UMS profiles for configuration, make sure the firmware version the profile is **based on** matches the firmware actually installed on the device (see Creating Profiles). If they do not match and the client version selected via the profile is not included in the firmware, the client version will fall back to default.



PowerTerm Session

Menu path: **Sessions > PowerTerm Terminal Emulation > PowerTerm Session**

You can configure one or more sessions for PowerTerm terminal emulation.

To edit the list, proceed as follows:

- Click on to create a new entry.
- Click on to remove the selected entry.
- Click on to edit the selected entry.
- Click on to copy the selected entry.

The configuration dialogs were designed to look as similar as possible to the setup pages described in the original documentation from ERICOM Software Ltd.

You will find detailed information on configuring the PowerTerm software in the [PowerTerm Interconnect Manual](#) on the Ericom website²⁷.

²⁷ <http://www.ericom.com/help.asp?cat=support>



Desktop Integration

Menu path: **Sessions > PowerTerm Terminal Emulation > PowerTerm Sessions > [Session Name] > Desktop Integration**

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.



Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network



- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.



IBM iAccess Client

Menu path: **Sessions > IBM iAccess Client**

IBM iAccess Client is an emulation of the IBM-5250 terminal in Java and supports numerous encodings.

- ▶ Add a session in order to be able to use the IBM iAccess Client.
- ▶ Under the **Connection** point under **Destination address**, give at least the DNS name or the IP address of a server. The client can also retrieve further logon information interactively.
- ▶ Under **Help > Information Center** in the IBM iAccess Client menu, you can read the help provided by the manufacturer in your browser.

- i** IBM iAccess certificates for server authentication and encryption can be distributed as files using the Universal Management Suite (UMS).

- [iAccess Global](#)(see page 299)
- [IBM iAccess Session](#)(see page 302)



iAccess Global

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Global**

Here you can define global settings for the emulation.

- [Tab Setup](#)(see page 300)
- [Font](#)(see page 301)



Tab Setup

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Global > Tab Setup**

Open new sessions in a new tab

- The new session will be opened in a new tab. (Default)
 A new session will be opened in a new window.

Always display the tab bar

- The tab bar will always be displayed.
 The tab bar will not be displayed. (Default)

Switch to new tab when created

- Switches to new tab. (Default)
 Remains in current tab.

Send a warning when closing multiple tabs

- Sends warning. (Default)
 Multiple tabs are closed without warning.

Do not start tabbed sessions until the tab is selected

- Applies.
 Does not apply. (Default)

New Tab Action

- Disable and hide
- Run the same
- Run other...

Tab Placement

- Top
- Bottom
- Left
- Right



Font

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Global > Font**

Font File or Directory: Enter the path to your font file or font directory.



IBM iAccess Session

Menu path: **Sessions > IBM iAccess Client > iAccess Sessions > [Session Name]**

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combo or your own key symbol/combo. A key symbol is a defined chain of characters, e.g. `Ctrl`.



- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with :

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

- To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.



- **Connection**(see page 305)
- **Screen**(see page 308)
- **Preferences**(see page 313)



Connection

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Connection**

Destination Address: Name or IP of the server

Destination Port: Server port (Default value: "default")

- i** If you leave **Destination Address** set to the string value "default" (default value) while **Use TLS/SSL** is enabled, port 229 is used. Without **Use TLS/SSL** enabled, port 23 is used. However, you are free to enter a custom port number.

Use TLS/SSL

- TLS/SSL is used.
 TLS/SSL is not used. (Standard)

Server Authentication: Defines if the client validates the authenticity of the server when connecting.

- i** To perform server authentication, the endpoint device must have the CA certificate that is associated with the server certificate. For instructions on how to deploy the certificate on the device, see Deploying Trusted Root Certificates in IGEL OS.

- The client requires the server to authenticate itself. (Default)
 The client connects to the server without server authentication.

Workstation ID: Name of the client that is presented to the server. This name must be unique. For more information, go to **Help > Information Center** in your iAccess client.

Screen Size

Possible values:

- 24x80
- 27x132

Host Code Page

Possible values:

- 1140 United States Euro
- 1141 Germany Euro
- 1141 Austria Euro
- 1142 Denmark Euro
- ...

Enable Unicode Data Stream

- Unicode Data Stream is enabled.
 Unicode Data Stream is disabled. (Default)

Enable DBCS in Unicode Fields

- DBCS is enabled in unicode fields.



DBCS is disabled in unicode fields. (Default)

Auto-Connect

Automatically connect to the server on client startup. (Default)

Auto-Reconnect

Automatically make a reconnect attempt if the server connection is lost. (Default)

-
- Advanced(see page 307)



Advanced

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Connection > Advanced**

Connection Timeout (seconds) (Default: 0)

Inactivity Timeout (minutes) (Default: 0)

Keep-Alive

- Keep-Alive is enabled.
- Keep-Alive is disabled. (Default)

Enable ENPTUI

- ENPTUI is enabled. (Default)

Password Prompting

Possible values:

- Use default user name to prompt once for each system: The credentials preconfigured in the fields **User ID** and **Password (optional)** are used.
- [Prompt for user name and password every time](#)
- Use Kerberos authentication: The credentials from the Active Directory login are used; only available if the user has logged in to the thin client via Active Directory. For more information, see [Active Directory/Kerberos](#)(see page 807).

User ID: The user ID to be used when **Password Prompting** is set to "Use default user name to prompt once for each system".

Password (optional): The password to be used when **Password Prompting** is set to "Use default user name to prompt once for each system".

⚠ Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

Bypass sign-on:

- The logon to the system is bypassed. (Default)



Screen

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Screen**

Cursor Shape

Possible Values:

- [Underline](#)
 - Block
-

- [Font\(see page 309\)](#)
- [Cursor\(see page 310\)](#)
- [Rule Line\(see page 311\)](#)
- [Color\(see page 312\)](#)



Font

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Screen > Font**

Fixed Font

- Use a fixed font.
- Use no fixed font. (Default)

Fixed Font Size

Possible values:

- 8
- 10
- 12
- 14
- ...
- 58

Font Scaling

- Font is scaled. (Default)

Antialiasing

- Antialiasing is activated.
- Antialiasing is disabled. (Default)

Font Name

Possible values:

- IBM3270
- Monospaced
- Courier 10 Pitch
- DejaVu Sans Mono
- Liberation Mono
- Lucida Sans Typewriter
- Numbus Mono L
- PComm Session
- Ubuntu Mono

Font Style

Possible values:

- Plain
- Bold
- Italic



Cursor

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Screen > Cursor**

Cursor Shape

Possible values:

- Underline
- Block

Cursor Pointer

Possible values

- Default
- Crosshair

Allow blinking cursor

- Blinking cursor is allowed.
 Blinking cursor is disabled. (Default)

Show blinking text with

Possible values:

- Blinking Text
- Host Color
- Mapped color

Blink Color: Select a color in which the cursor should blink.

Blink Color Background: Select a background color.



Rule Line

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Screen > Rule Line**

Rule Line

Rule line is activated.

Rule line is disabled. (Default)

Follow Cursor

The follow cursor effect is enabled.

The follow cursor effect is disabled. (Default)

Style

Possible values:

- [Crosshair](#)
- Vertical
- Horizontal



Color

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Screen > Color**

Field Color: Choose respective colors.

OIA Color: Select a suitable color for the respective indicators.

- Status Indicators
- Information Indicators
- Attention Indicators
- Error Indicators
- OIA Background

Other

- **Screen Background:** Choose a color.

This color overrides all Field Color Background colors which are set to black.

- **Highlight active field**

- Active field is highlighted.
- Active field is not highlighted. (Default)
- **Active field:** Choose a color
 - **Active Field Background:** Choose a color
 - **Crosshair Ruler Color:** Choose a color
 - **Column Separator:** Choose a color



Preferences

Menüpfad: **Sessions > IBM iAccess Client > iAccess Sessions > [session name] > Preferences**

Start window maximized

- The windows starts in maximal size.
- The windows does not start in maximal size. (Default)

Automatic Resize

- Automatic window resizing is enabled. (Default)
- Automatic window resizing is disabled.

Show Border

- The session screen is framed by a border.
- No additional border is added. (Default)

Graphical OIA

- The Graphical OIA (Graphical Operator Information Area) is displayed. (Default)
- The Graphical OIA (Graphical Operator Information Area) is hidden.

Textual OIA

- The Textual OIA (Textual Operator Information Area) is displayed.
- The Textual OIA (Textual Operator Information Area) is hidden. (Default)

Keypad

- The Keypad is displayed.
- The Keypad is hidden. (Default)

Toolbar

- The toolbar is displayed. (Default)
- The toolbar is hidden.

Toolbar Text

- Textual items are added to the toolbar icons.
- No textual items are added to the toolbar icons. (Default)

Status Bar

- The status bar is displayed. (Default)
- The status bar is hidden.

Macro Manager

- The Macro Manager toolbar is displayed.
- The Macro Manager toolbar is hidden. (Default)

Right Mouse Button Popup Keypad



- Right-clicking will bring up the the Popup Keypad.
- Right-clicking will bring up the default menu. (Default)

Scratch Pad

- The Scratch Pad (integrated basic text editor) is displayed.
- The Scratch Pad (integrated basic text editor) is hidden. (Default)

'Save' in Scratch Pad

- The **Save** button in the Scratch Pad is active.
- The **Save** button in the Scratch Pad is inactive. (Default)

Quick Connect

- The Quick Connect toolbar is displayed.
- The Quick Connect toolbar is hidden. (Default)

Search Text

- The Search Text area is displayed.
- The Search Text area is hidden. (Default)

Screen History

- The Screen History area is displayed.
- The Screen History area is hidden. (Default)

History Screen Type Simple (Text)

- The History Screen will be displayed black and white.
- The History Screen will have the default terminal (green screen) look and feel. (Default)

Menu Bar

- The main menu bar is displayed. (Default)
 - The main menu bar is hidden.
-

- [Window](#)(see page 315)
- [Start Options](#)(see page 316)
- [Language](#)(see page 317)
- [Keyboard](#)(see page 318)
- [Popup Keypad](#)(see page 319)
- [Toolbar](#)(see page 320)



Window

Menu path: **Sessions > IBM iAccess Client > [session name] > Preferences > Window**

Here you can define how the iAccess client application window is positioned and sized by default on start. If you leave the fields empty, the window will be positioned and sized automatically.

Width: Width of the window

Height: Height of the window

Horizontal offset: Horizontal offset of the window

Vertical offset: Vertical offset of the window



Start Options

Menu path: **Sessions > IBM iAccess Client > iAccess Sessions > [session name] > Preferences > Start Options**

Session ID

Possible values:

- Automatic
- [Various alphabetic values]



Language

Menu path: **Sessions > IBM iAccess Client > iAccess Sessions > [session name] > Preferences > Language**

Emulation Language

Possible values:

- Default: The language of the IGEL User Interface (**User Interface > Language**) will be used.
- [Various languages]



Keyboard

Menu path: **Sessions > IBM iAccess Client > iAccess Sessions > [session name] > Preferences > Keyboard**

Keyboard Remapping File: Enter the file name (Default: IBMi.kmp)

i The directory `/userhome/IBM/iAccessClient/Emulator` is used by default.



Popup Keypad

Menu path: **Sessions > IBM iAccess Client > iAccess Sessions > [session name] > Preferences > Popup Keyboard**

Popup Keypad File: Enter the file name.

- ⓘ The directory `/userhome/IBM/iAccessClient/Emulator` is used by default.



Toolbar

Menu path: Sessions > IBM iAccess Client > iAccess Sessions > [session name] > Preferences > Toolbar

Toolbar File: Enter the file name.

- i** The directory `/userhome/IBM/iAccessClient/Emulator` is used by default.



ThinLinc Global

Menu path: **Sessions > ThinLinc > ThinLinc Global**

In this area, you can change the global settings for ThinLinc sessions.

- [Server](#)(see page 322)
- [Window](#)(see page 323)
- [Options](#)(see page 324)
- [Optimization](#)(see page 326)
- [VNC Optimization](#)(see page 327)



Server

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > Server**

You can specify the port for communication between the client and server and allow remote monitoring of the client through shadowing.

- **SSH port**

Possible values:

- Default SSH (22): Port 22 is used.
- HTTP (80): Port 80 is used.
- Custom: Under **Custom port number**, you can enter an alternative port number.

- **Custom port number**: Alternative port number

- **Allow shadowing**

The session can be remote monitored by shadowing via VNC.

The session cannot be remote monitored by shadowing. (default)



Window

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > Window**

In this area, you can define the window settings for ThinLinc sessions.

Screen size

Possible values:

- "800x600"
- "1024x768"
- "1280x1024"
- "1600x1200"
- "Current monitor- "All monitors": The display area of all monitors is used for the ThinLinc session.
- "Work area (maximized)": The display area of the current monitor minus the height of the taskbar is used for the ThinLinc session.
- "Custom size": The display area specified with **Custom screen width** and **Custom screen height** is used for the ThinLinc session.

Custom screen width: Width of the display area for the session in pixels.

Custom screen height: Height of the display area for the session in pixels.

Full-screen mode

The entire display area is used for the ThinLinc session. (Default)

Full-screen all monitor

The entire display area of all monitors is used for the ThinLinc session. (Default)

Control bar for ThinLinc sessions

If the ThinLinc session takes place in full-screen mode, an in-session control bar will be shown. You can minimize or close the session with the control bar. Further information can be found under [In-Session Control Bar](#)(see page 661).

The in-session control bar will not be shown. (Default)



Options

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > Options**

You can change various settings and enable local directories.

Enable sound

Audio output will be forwarded from the server to the device. The audio data can then be played back via the built-in loudspeaker or the headset.

Audio output will not be forwarded to the device. (Default)

Redirect serial port

The serial port data will be forwarded from the device to the server. The serial port can be used in the ThinLinc session.

The serial port data will not be forwarded to the server. (Default)

Enable printer

The local printer can be used in the ThinLinc session. (Default)

The local printer cannot be used in the ThinLinc session.

Enable smartcard readers

The server has access to the device's local smartcard reader.

The server does not have access to the local smartcard reader. (Default)

Enable drive access

The server has access to local directories. These directories can be selected in the **Exported Paths and Permissions** area.

The server does not have access to local directories. (Default)

Exported Paths and Permissions

To edit the list, proceed as follows:

- Click on to create a new entry.
- Click on to remove the selected entry.
- Click on to edit the selected entry.
- Click on to copy the selected entry.

To select a local directory for server-side access, proceed as follows:

1. Click on .
2. In the **Path** field, enter the local directory path. Example: `/userhome`
3. Select the **Permission** that the server is to have for the directory.
 - Read only: The server has read rights for the directory but no write rights.
 - Read/write: The server has read and write rights for the directory.
 - Disabled: The server has no read rights and no write rights for the directory.



- ⓘ If you set a directory to “Disabled”, ensure that it is not a sub-directory of a directory for which the server has read or write rights.

4. Click on **Ok**.



Optimization

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization**

You can select a suitable compression procedure in order to optimize the transmission speed between the client and server.

- **Enable custom compression level**

- You can specify how much the data transmitted between the client and server are compressed.
 The default value will be used for the compression level. (default)

- **Compression level:** Allows you to select the compression level; 9 is the highest compression (default: 8)

- **Enable JPEG compression:** If this option is enabled, graphical data will be compressed using the JPEG procedure.

- i A higher JPEG compression level saves bandwidth but reduces the image quality.

- Graphical data will be compressed in accordance with the JPEG procedure. (default)

- **JPEG quality:** Allows you to select the image quality. 1 means the highest compression and the lowest image quality, 9 means the lowest compression and the highest image quality. (default: 7)

- **SSH compression**

- The data will be compressed using SSH compression.

- The data will not be compressed using SSH compression. (default)



VNC Optimization

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > VNC Optimization**

You can change VNC protocol settings in order to optimize transmission.

VNC autoselect

The preferred coding and color depth will be specified automatically. (Default)

The **Preferred coding** and **Color depth** can be specified by the user.

Preferred encoding: Specifies how the data to be transmitted are to be coded. The coding is negotiated between the client and server.

Possible values:

- "Tight- "ZRLE": Compatible with RealVNC.
- "Hextile": Recommended for fast networks.
- "Raw": No compression.

Color depth: Allows you to select the color resolution.

Possible values:

- "Full (all colors)- "Medium (256 colors)"
- "Low (64 colors)"
- "Very low (8 colors)"



ThinLinc Session

Menu path: **Sessions > ThinLinc > ThinLinc Sessions > [Session Name]**

- ▶ Click on **Add** to create a ThinLinc session.

In this area, you can configure desktop integration for the ThinLinc session.

Session name: Name for the session.

The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.



- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.



No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.

-
- [Server](#)(see page 331)
 - [Login](#)(see page 332)
 - [Window](#)(see page 334)
 - [Options](#)(see page 335)
 - [Optimization](#)(see page 336)
 - [VNC Optimization](#)(see page 337)
 - [User Interface](#)(see page 338)
 - [Desktop Integration](#)(see page 339)



Server

Menu path: **Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Server**

Server: Name or IP address of the ThinLinc server

User: User name for the connection to the ThinLinc server

Password: Password for the connection to the ThinLinc server

⚠ Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

Use global SSH port settings

The port set under **Sessions > ThinLinc > ThinLinc Global > Server** will be used. (Default)

The port set in **SSH port** or **Custom port number** will be used.

SSH port

Possible values:

- **Default SSH (22):** Port 22 is used.
- **HTTP (80):** Port 80 is used.
- **Custom:** Under **Custom port number**, you can enter an alternative port number.

Custom port number: Alternative port number



Login

Menu path: **Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Login**

Method of authentication: A method used for the authentication.

Possible values:

- "Password"
- "Public key"
- "Smartcard"
- "Kerberos"

User: The user credentials are taken from **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Server > User**.

Password: A password specified under **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Server > Password** is used for the authentication. (Available if **Password** is selected as **Method of authentication**).

- i** If modified here (under **Login**), **User** and **Password** will automatically be changed under **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Server**.

The following settings can be configured if **Smartcard** is used as a **Method of authentication**.

Smartcard only

Use certificate subject as name for login

- The certificate subject will be used as login name. (Default)
- The user credentials from **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Server > User** will be used as login name.

Connect the client automatically if a smartcard is found

- The client will be connected automatically if a smartcard is detected (available if **Use subject of smartcard as name for login** is enabled). (Default)
- The client will not be connected automatically by the smartcard detection.

Disconnect the client automatically when the smartcard is removed

- The client will be disconnected automatically if the smartcard is removed. (Default)
- The client will not be disconnected at the smartcard removal.

Allow transmission of the smartcard's passphrase for logging in

- The transmission of the smartcard's passphrase for logging in is allowed.
- The transmission of the smartcard's passphrase for logging in is not allowed. (Default)

- ⚠** The transmission of the smartcard's passphrase is not recommended by Cendio.

Smartcard filter: The smartcard filter must be specified in the format described under "SMARTCARD_FILTER_n" in <https://www.cendio.com/resources/docs/tag/clientconf.html>.





Window

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Window**

In this area, you can define the window settings for the specific ThinLinc session.

- i** You can enable the in-session control bar for ThinLinc sessions only in the global settings, see [Window\(see page 323\)](#).

Use global screen settings

The settings under **Setup > Sessions > ThinLinc > ThinLinc Global > Window** will be used. (Default)

The settings for this session are defined here.

Screen size

Possible values:

- "800x600"
- "1024x768"
- "1280x1024"
- "1600x1200"
- "Current monitor- "All monitors": The display area of all monitors is used for the ThinLinc session.
- "Work area (maximized)": The display area of the current monitor minus the height of the taskbar is used for the ThinLinc session.
- "Custom size": The display area specified with **Custom screen width** and **Custom screen height** is used for the ThinLinc session.

Custom screen width: Width of the display area for the session in pixels.

Custom screen height: Height of the display area for the session in pixels.

Full-screen mode

The entire display area is used for the ThinLinc session. (Default)

Full-screen all monitor

The entire display area of all monitors is used for the ThinLinc session. (Default)



Options

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Options**

You can change various settings and enable local directories.

Use global shadowing settings

- The option **Setup > Sessions > ThinLinc > ThinLinc Global > Server > Enable Shadowing** will be used.
 The global setting **Enable shadowing** will not be used for this session.

Enable shadowing

- The session can be monitored remotely by shadowing via VNC.
 The session cannot be remotely monitored by shadowing. (Default)

Use global resource settings

- The settings under **Setup > Sessions > ThinLinc > ThinLinc Global > Options** will be used. (Default)
 The settings for this session are defined here.

Enable sound

- Audio output will be forwarded from the server to the device. The audio data can then be played back via the built-in loudspeaker or the headset.
 Audio output will not be forwarded to the device. (Default)

Enable serial port

- The serial port data will be forwarded from the device to the server. The serial port can be used in the ThinLinc session.
 The serial port data will not be forwarded to the server. (Default)

Enable printer

- The local printer can be used in the ThinLinc session. (Default)
 The local printer cannot be used in the ThinLinc session.

Enable smartcard readers

- The server has access to the device's local smartcard reader.
 The server does not have access to the local smartcard reader. (Default)

Enable drive access

- The server has access to local directories. These directories can be selected in the **Exported Paths and Permissions** area.
 The server does not have access to local directories. (Default)

Options popup key: Key to be used for opening the options menu during the session. (Default: F8)



Optimization

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Optimization**

You can select a suitable compression procedure in order to optimize the transmission speed between the client and server.

- **Use global compression level**

- The global settings under **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization > Use custom compression level** option and **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization > Compression level** selection will be used. (default)
 The specific settings for this session will be used.

- **Enable custom compression level**

- You can specify how much the data transmitted between the client and server are compressed.
 The default value will be used for the compression level. (default)

- **Compression level:** Allows you to select the compression level; 9 is the highest compression (default: 8)

- **Use global JPEG quality settings**

- The global settings under **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization > Use JPEG compression** option and **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization > JPEG Quality** selection will be used. (default)
 The specific settings for this session are defined here.

- **Enable JPEG compression**

A higher JPEG compression level saves bandwidth but reduces the image quality.

- Graphical data will be compressed in accordance with the JPEG procedure. (default)

- **JPEG quality:** Allows you to select the image quality. 1 means the highest compression and the lowest image quality, 9 means the lowest compression and the highest image quality. (default: 7)

- **Use global SSH connection settings**

- The global settings under **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization > SSH Compression** option will be used. (default)
 The specific setting for this session will be used.

- **SSH compression**

- The data will be compressed using SSH compression.
 The data will not be compressed using SSH compression. (default)



VNC Optimization

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > VNC Optimization**

You can change VNC protocol settings in order to optimize transmission.

Use global VNC settings

The global settings under **Setup > Sessions > ThinLinc > ThinLinc Global > VNC optimization** will be used. (Default)

The specific settings for this session are defined here.

VNC auto select

The **Preferred encoding** and **Color level** will be specified automatically. (Default)

The **Preferred encoding** and **Color level** can be specified by the user.

Preferred encoding: Specifies how the data to be transmitted are to be coded. The coding is negotiated between the client and server.

Possible values:

- "Tight- "ZRLE": Compatible with RealVNC.
- "Hextile": Recommended for fast networks.
- "Raw": No compression.

Color level: Allows you to select the color resolution.

Possible values:

- "Full (all colors)- "Medium (256 colors)"
- "Low (64 colors)"
- "Very low (8 colors)"



User Interface

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > User Interface**

You can change the fields and settings options of the logon window as well as the **ThinLinc Client Options** dialog.

- **Lock server name**
 The server name given under **Setup > Sessions > ThinLinc Sessions > Server** will be used and it will not be possible to change it in the logon window. (default)
- **Hide options button**
 The **Options** button will not appear in the logon window. The **ThinLinc Client Options** dialog therefore cannot be opened. (default)
- **Advanced mode**
 The fields that can be opened under **Advanced** will appear when starting the session.
 The fields that can be opened under **Advanced** will not appear when starting the session. (default)
- **Lock ThinLinc options tab**
 The settings in the **Options** tab of the **ThinLinc Client Options** dialog cannot be changed. (default)
- **Lock Local Devices options tab**
 The settings in the **Local Devices** tab of the **ThinLinc Client Options** dialog cannot be changed. (default)
- **Lock ThinLinc Screen tab**
 The settings in the **Screen** tab of the **ThinLinc Client Options** dialog cannot be changed. (default)
- **Lock ThinLinc Optimization tab**
 The settings in the **Optimization** tab of the **ThinLinc Client Options** dialog cannot be changed. (default)
- **Lock Security tab**
 The settings in the **Security** tab of the **ThinLinc Client Options** dialog cannot be changed. (default)
- **Debug level:** Specifies how detailed the debugging information is to be. 1 is the lowest level (default), 5 is the highest.



Desktop Integration

Menu path: **Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the ThinLinc session.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.



SSH Session

Menu path: **Sessions > SSH > [Session Name]**

You can launch applications on a remote computer via SSH (Secure Shell). The display is usually on the terminal; X11 connections too can be routed via SSH.

- ▶ Click on **Add** to create an SSH session.

In the following area, you can configure desktop integration for the SSH session.

Session name: Name for the session.

The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

-
- [Command](#)(see page 345)
 - [Options](#)(see page 346)
 - [Desktop Integration](#)(see page 347)



Command

Menu path: **Sessions > SSH > [Session Name] > Command**

Remote user name: User name under which the application runs on the remote computer If you do not give a name, you will be asked when the session starts.

Remote host: Host name or IP address of the remote computer.

Command line: Command which is to be executed on the remote computer immediately after logging in.



Options

Menu path: **Sessions > SSH > [Session Name] > Options**

 As of IGEL OS 11.04.100, SSHv1 is no longer supported. Migrate to SSHv2 if you have not yet done so.

Here, you can change the following settings:

Enable X11 connection forwarding

X11 applications on the remote computer that are launched via the SSH session will be shown on your device. (Default)

No X11 programs can be launched on the remote computer via the SSH session.

Enable compression

The data will be compressed for transmission.

Port: SSH port. (Default: 22)



Desktop Integration

Menu path: **Sessions > SSH > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the SSH session.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.



VNC Viewer Sessions

Menu path: **Sessions > VNC Viewer > VNC Viewer Sessions > [Session Name]**

With the VNC viewer, you can access the graphical user interface of a remote computer.

- ▶ Click on to create a VNC viewer session.

The settings for starting the session are described below.

Session name: Name for the session.

The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.



- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

- [Connection](#)(see page 353)
- [Compression](#)(see page 354)
- [Input](#)(see page 355)
- [Misc](#)(see page 356)
- [Desktop Integration](#)(see page 357)



Connection

Menu path: **Setup > Sessions > VNC Viewer > VNC Viewer Sessions > [Session Name] > Connection**

- **Name or IP address of VNC server:** Host name or IP address of the VNC server
- **Password:** User password for logging on to the VNC server, if necessary

⚠ Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.



Compression

Menu path: **Setup > Sessions > VNC Viewer > VNC Viewer Sessions > [Session Name] > Compression**

- **Compression level (default = 2):** Allows you to select the compression level; 9 is the highest compression (default: 2)
- **JPEG quality level:** Allows you to select the image quality. 1 means the highest compression and the lowest image quality, 9 means the lowest compression and the highest image quality. (default: 8)



Input

Menu path: **Setup > Sessions > VNC Viewer > VNC Viewer Sessions > [Session Name] > Input**

Here, you can change the settings for keyboard input for the VNC session.

- **View only**

- Mouse and keyboard inputs are not forwarded to the remote computer. You can only observe the remote computer.
- Mouse and keyboard inputs are forwarded to the remote computer. You can remote control the remote computer. (default)

- **Pass system keys directly to the server (full-screen)**

- You can use system key combinations in the VNC session, e.g. [Alt] + [Tab]. (default)
- System key combinations cannot be used in the VNC session.

- **Menu key:** Key which brings up the menu.

Possible options (default: F8):

- [F2] ... [F12]
- [Pause]
- [Print]
- [Scroll lock]
- [Esc]
- [Ins]
- [Del]
- [Home]
- [Page up] ▲
- [Page down] ▼



Misc

Menu path: **Setup > Sessions > VNC Viewer > VNC Viewer Sessions > [Session Name] > Misc**

- **Shared mode**

- When starting a session, other users' sessions with the same server are not terminated. The sessions run alongside each other with equal status.
- If another user has a VNC session with the same server, the other user's session will be terminated when the session is started. (default)

- **Fullscreen mode**

- The session will be shown in full-screen mode. The taskbar is not visible.
- The taskbar is visible. (default)

- **Color level:** Number of possible colors

Possible values:

- Default: The highest available color depth will be used.
- Very low (8 colors)
- Low (64 colors)
- Medium (256 colors)



Desktop Integration

Menu path: **Sessions > VNC Viewer > VNC Viewer Sessions > [Session Name] > Desktop Integration**

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.



Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

Sessions



- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.



Firefox Browser Global

Menu path: **Sessions > Firefox Browser > Firefox Browser Global**

In this area, you can define the start page, display resolution, and font size for the browser.

You can change the following settings:

When browser starts: Specifies what pages are shown when the browser is launched.

- Start with a blank page
- Show my start page (default)
- Resume previous session: All tabs from the last session are reopened.

Start page: Specifies the URL of the start page. You can specify the number of start pages by separating the URLs of the start pages with a vertical dash "|".

Default web browser: Defines which browser will be chosen by the system, e.g. for opening Citrix Storefront.

Possible options:

- "Firefox Browser"
- "Chromium Browser"

Display resolution: Specifies the display resolution for the browser in DPI. Typical values are **72** for medium screens and **96** for large screens.

Possible values:

- System setting
- (Various discreet values)

Minimum font size: Specifies the minimum size of the fonts displayed on websites. The formats of the websites are overwritten in the process.

Possible values:

- None: The fonts can be as small as you like. (default)
- (Various discreet values)

Show browser splash screen

While the browser is starting, a Firefox logo will be shown in the middle of the screen. (default)

No Firefox logo will be shown.

For information on the kiosk mode, see Use the Firefox Browser in Kiosk Mode.

i Please note: With an enabled **Browser content redirection** under **Sessions > Citrix > Citrix Global > HDX Multimedia**, any H.264 multimedia content within Firefox (incl. video playback) is not functional anymore. These two features cannot be used simultaneously. See [HDX Multimedia Settings for an IGEL OS Citrix Session](#)(see page 80).

- [Tabs](#)(see page 362)
- [Content](#)(see page 363)
- [Print](#)(see page 365)



- [Proxy](#)(see page 366)
- [Privacy](#)(see page 369)
- [Security](#)(see page 371)
- [Advanced](#)(see page 372)
- [Encryption](#)(see page 375)
- [Certificates](#)(see page 376)
- [Smartcard Middleware for Firefox Browser in IGEL OS](#)(see page 377)
- [Restart](#)(see page 380)
- [Window](#)(see page 381)
- [Menus & Toolbars](#)(see page 382)
- [Hotkeys](#)(see page 385)
- [Context](#)(see page 386)
- [Commands](#)(see page 387)



Tabs

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Tabs**

In this area, you can define settings for the browser tabs.

New pages should be opened in: Specifies how links to new pages are to be opened.

Possible values:

- Current window: The page will open in the current window, even if the link defines a new window as the target.
- New window: If the link does not define a target, the page will open in the current window. If the link defines a new window as the target, the page will open in a new window. (default)
- New tab: If the link does not define a target, the page will open in the current window. If the link defines a new window as the target, the page will open in a new tab.

Warn me when closing multiple tabs

A warning will be shown as soon as you attempt to close a browser window with a number of tabs.

No warning will be shown if you close a number of browser windows. (default)

Warn me when opening multiple tabs might slow down the browser

A warning will be shown if a very large number of tabs are loaded simultaneously. (default)

No warning will be shown if a very large number of tabs are loaded simultaneously.

When a link is opened in a new tab, switch to it immediately

When a new tab is opened via a link, the focus will switch to the new tab.

When a new tab is opened via a link, the focus will not change. (default)



Content

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Content**

In this area, you can change settings regarding popups, JavaScript, downloads and the browser display.

Block pop-up windows

The automatic opening of popup windows by websites will be blocked. With **Exceptions...**, you can allow popups to be opened automatically for specific websites.

The automatic opening of popup windows will not be blocked. (default)

To add an exception for the automatic opening of popups, proceed as follows:

1. Click on **Exceptions....**
2. Click on .
3. In the **Website** field, give the URL of the website for which the exception is to apply.
4. Click on **Ok**.

Load images automatically

Websites will be loaded fully including all images. (default)

Images in websites will not be loaded; placeholders will be shown instead of the images. As a result of this, websites can be loaded more quickly, but the layout is impaired. With **Exceptions...** you can allow or prevent automatic loading for specific websites.

To add an exception for the automatic loading of images, proceed as follows:

1. Click on **Exceptions....**
2. Click on .
3. In the **Website** field, give the URL of the website for which the exception is to apply.
4. Using the **Status** drop-down menu, specify whether the automatic loading of images is to be allowed or prevented for the given website.
5. Click on **Ok**.

Type of download directory: Specifies the directory in which a downloaded file is saved.

- User directory: The file is saved locally on the thin client desktop.
- Custom path: You can specify whether the downloaded file is to be opened with an application or saved locally. (default)

Download path: Local directory in which the downloaded file is saved if **Type of download directory** is set to **Custom path**. (default: `/tmp`)

Enable JavaScript

JavaScript code will be executed on websites. (default)

JavaScript code will not be executed.

Raise or lower windows

A website can place windows in the background or foreground via JavaScript. (default)

Websites cannot place windows in the background or foreground via JavaScript.



Move or resize existing windows

- A website can move windows or change the window size via JavaScript.
- Websites cannot move windows or change the window size via JavaScript. (default)

Disable or replace context menus

- A website can define a custom context menu via JavaScript; the browser's own context menu will be suppressed in the process.
- Websites cannot define a custom context menu.

Languages for web pages: One or more preferred languages for multilingual websites, given in the form of language abbreviations separated by commas. The languages should be given in the order of preference. Example: With `de, en, fr, it`, the website will be shown in German, if available, otherwise in English, etc.



Print

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Print**

In this area, you can set the default paper size for the printer.

Use system settings for default paper size

The globally set paper size will be used when printing websites. (Default)

You can set the paper size via **Default paper size**.

Default paper size: Preset paper size when printing websites.

Possible values:

- Letter
- Legal
- Executive
- A5
- A4
- A3



Proxy

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Proxy**

In this area, you can change the proxy configuration.

To change the proxy configuration, proceed as follows:

1. In the **Proxy Configuration** pull-down menu, select the type of proxy configuration.
The following proxy configurations are available:
 - [Direct connection to the Internet](#)
 - Manual proxy configuration
 - Automatic proxy configuration
 - System-wide proxy configuration
 - Auto-detect proxy settings for this network
2. Enter the necessary configuration data for the selected proxy configuration.

Direct Connection to the Internet

With this proxy configuration, no proxy is used.

Manual Proxy Configuration

The configuration data must be specified in the following fields.

FTP proxy: URL of the proxy for FTP

Port: Port of the proxy for FTP

HTTP proxy: URL of the proxy for HTTP

Port: Port of the proxy for HTTP

SSL proxy: URL of the proxy for SSL

Port: Port of the proxy for SSL

SOCKS host: URL of the proxy for SOCKS

Port: Port of the proxy for SOCKS

SOCKS protocol version: Version of the SOCKS protocol used (default: [SOCKS v5](#))

No proxy for: List of URLs for which no proxy is to be used (default: `localhost, 127.0.0.1`)

Proxy realm: Area in which the browser authenticates itself for the proxy. Together with the user name and password, this information is necessary for authentication.

- i** The **Proxy realm** field is internally pre-populated with the value `moz-proxy://[HTTP Proxy]:[Port]`. If the field is empty, this value will be used when authenticating the browser. If the proxy expects another unknown value for the proxy realm, you can determine this as follows: Leave the **User name** and **Password** fields empty and launch the browser. The dialog window which appears will contain the correct value for the **Proxy realm** field:



Authentication Required

The proxy `moz-proxy://172.30.178.10:8080` is requesting a username and password. The site says: `"moz-proxy://172.30.178.10:8080"`

User Name:

Password:

In the example above, the value for the **Proxy realm** field is as follows: `moz-proxy://172.30.178.10:8080`

Use passthrough authentication: This option can be used if the local thin client logon takes place via Kerberos.

The logon information saved temporarily when logging on to the thin client will be carried over when logging on to the proxy.

User name: User name with which the browser authenticates itself for the proxy.

Password: Password with which the browser authenticates itself for the proxy.

Do not prompt for proxy authentication if credentials are saved

If logon data are already saved in the browser, the user will not be asked for a user name and password. (default)

 This option should not be enabled in multiuser environments. If this option is enabled in a multiuser environment, a user can use the logon data of a previous user.

Automatic Proxy Configuration

With this proxy configuration, the PAC file (Proxy Auto Config) available under **URL** will be used.

URL: URL of the proxy configuration file

Do not prompt for proxy authentication if credentials are saved

If logon data are already saved in the browser, the user will not be asked for a user name and password. (default)

 This option should not be enabled in multiuser environments. If this option is enabled in a multiuser environment, a user can use the logon data of a previous user.

System-Wide Proxy Configuration

With this proxy configuration, the proxy configured under **Setup > Network > Proxy** will be used.

Do not prompt for proxy authentication if credentials are saved



If logon data are already saved in the browser, the user will not be asked for a user name and password.
(default)

! This option should not be enabled in multiuser environments. If this option is enabled in a multiuser environment, a user can use the logon data of a previous user.

Auto-Detect Proxy Settings for This Network

With this proxy configuration, WPAD (Web Proxy Autodiscovery Protocol) will be used. The browser will determine the URL of the WPAD file `wpad.dat` automatically with the help of DNS.

Do not prompt for proxy authentication if credentials are saved

If logon data are already saved in the browser, the user will not be asked for a user name and password.
(default)

! This option should not be enabled in multiuser environments. If this option is enabled in a multiuser environment, a user can use the logon data of a previous user.



Privacy

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Privacy**

In this area, you can configure settings relevant to data protection.

Save browsing history (in days): Specifies how long your browsing history will be stored. If you select **Do not store history**, all browsing history data will be lost when the browser restarts. (default: 9)

-  All browsing history data stored before the period specified here will be lost.

Save information entered in forms and the search bar

- Entries in forms and search bars will be retained after the browser restarts.
 Entries in forms and search bars will be retained only for the duration of the session. (default)

Remember passwords

- Passwords entered will be retained after the browser restarts.
 Passwords entered will be retained only for the duration of the session. (default)

Clear private data when closing browser

- Data entered will be deleted when the browser is closed. What data are deleted is specified in the following options.
 Data entered will not be deleted when the browser is closed. (default)

Select the Items to Be Cleared

The options in this area are effective if **Clear private data when closing browser** is enabled.

Browsing & download history

- Addresses (URLs) of visited websites and the list of downloads will be deleted when the browser is closed. (default)

Form & search history

- Entries in the search window and in website forms will be deleted when the browser is closed. (default)

Saved passwords

- Passwords entered will be deleted when the browser is closed.
 Passwords entered will be retained after the browser restarts. (default)

Cookies

- Cookies will be deleted when the browser is closed. (default)

Cache

- The cache for temporarily saving websites will be emptied when the browser is closed. (default)

Active logins



Ongoing sessions on websites will be terminated when the browser is closed and will need to be restarted after the browser restarts. (default)

Ongoing sessions on websites will be retained after the browser restarts.

Allow private browsing feature

You can open one or more private windows in the browser. All data from private windows will be deleted after the browser is closed.

Private windows cannot be opened. (default)

Always start in private browsing mode

The browser will start in private mode. All data will be deleted after the browser is closed.

The browser will start in default mode. (default)

Enable "Do Not Track" feature

The browser will inform the website you are visiting that you do not wish to be tracked, i.e. you do not want your surfing history to be recorded. (default)

- i** The browser will use the DNT ("Do Not Track") field in the HTTP header for this purpose. Observing this setting is voluntary; from a technical point of view, websites can still record the surfing history even when DNT is set to 1.

Enable built-in tracking protection

The browser will block specific domains and websites that use tracking. The browser has an internal list for selecting the domains and websites to be blocked. (default)

- i** If tracking protection is enabled, a shield symbol will be shown at the left-hand edge of the address bar.

Suggest visited sites in URL bar

Suggestions will be shown while an address is being typed in the address bar. The suggestions will be based on previously visited websites which are stored in the history. (default)

Suggest only typed visited sites

The suggestions will be based only on the websites that were typed directly into the address bar. Websites that were visited via bookmarks or links in other websites will not be used for the suggestions.

Websites that were visited via bookmarks or links in other websites will also be used for the suggestions. (default)

Suggest bookmarked sites in URL bar

Suggestions will be shown while an address is being typed in the address bar. The suggestions will be based on bookmarks. (default)

Suggest open tabs in URL bar

Suggestions will be shown while an address is being typed in the address bar. The suggestions will be based on previously opened tabs. (default)



Security

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Security**

In this area, you can define settings for preventing phishing and malware.

Safe browsing

The browser will check each address entered as to whether it can be found in the black list of fraudulent websites which use phishing. If this is the case, you will be given a warning.

The browser will not check whether an address is on the black list of fraudulent websites.

Malware protection

The browser will check before a file is downloaded whether the relevant website can be found in the black list of fraudulent websites which provide malware for downloading. If this is the case, you will be given a warning.

The browser will not check whether an address is on the black list of fraudulent websites which provide malware for downloading.

Hide local filesystem

The local file system will not be shown in the dialogs for saving data. The user cannot change the location for saving files.

The local file system will be shown in the dialogs for saving data.



Advanced

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Advanced**

In this area, you can change various settings as well as add or change custom configuration parameters.

You can change the following settings:

Use old search bar

- The logo of the search engine currently set will be shown in the search window.
- The search engine currently set will not be shown in the search window, and search suggestions will be shown in the drop-down menu. (default)

Caret browsing on browser start

- Caret browsing is enabled when the browser starts. If caret browsing is enabled, you can navigate with the keyboard in websites without using the mouse. With the insertion mark, you can copy text to the clipboard.

i You can enable or disable caret browsing at any time by pressing [F7]. To prevent caret browsing being disabled, you will also need to enable the **Sessions > Firefox Browser > Firefox Browser Global > Hotkeys > Disable hotkeys for caret browsing** option.

- Caret browsing is not enabled when the browser starts. (default)

Find as you type

- Search suggestions that match the characters typed will be shown while you type.
- No search suggestions will be shown while you type. (default)

Warn me when websites try to redirect or reload the page

- A message window will be shown as soon as a website tries to get the browser to load another website or reload the current page.
- No message window will be shown if a website tries to load another website or reload the current page. (default)

Check my spelling as I type

Possible options:

- "Off": Your spelling will not be checked while you type.
- "On for text fields": Your spelling will be checked if you are typing in text fields with multiple lines. (default)
- "On for text fields and lines": Your spelling will be checked if you are typing in text fields with one line or multiple lines.

Use autoscrolling

- You can launch automatic page scrolling by clicking on the middle mouse button to place a scroll symbol in the text and then positioning the mouse pointer above or below the anchor.
- Autoscrolling is disabled. (default)

Use smooth scrolling

- You can browse through a page using the [Page Up/Down] keys smoothly as with scrolling.



When you press the [Page Up/Down] keys, the display will jump immediately. (default)

Disable GStreamer in Browser

GStreamer will not be used to play back videos. This may be a good idea if you experience problems when playing back videos.

- ⓘ We recommend that you disable this option if there is no multimedia codec pack installed on your thin client and you wish to view videos on HTML5 websites.

GStreamer will be used to play back videos.

Disable OpenGL acceleration

Hardware acceleration with OpenGL will not be used. This may be a good idea if you experience problems with OpenGL applications.

To add a custom preference, proceed as follows:

- ⚠ Changes to the advanced Firefox browser settings can impair its stability, security and speed. IGEL Support is not responsible for problems caused by changing the browser configuration, even if the browser configuration was changed in the IGEL setup.

- ⓘ Custom preferences can also be changed in the browser via `about:config`. To do this, the **Firefox Browser > Firefox Browser Global > Window > Hide configuration page of the browser** option must be disabled.

Custom Preferences

In this area, you can add custom preferences.

► Click  to get to the **Add** dialogue.

In the **Add** dialogue, you can define the following settings:

Active: Defines whether the preference is active.

The preference is active. (Default)

The preference is not active.

Mode: The mode of the preference.

Possible values:

- "`pref`": You can change the value in the browser via `about:config`. When the browser restarts, this change will be lost and the value set here will be used.
- "`defaultPref`": You can change the value in the browser via `about:config`. When the browser restarts, this change will remain.
- "`lockPref`": You cannot change the value in the browser via `about:config`.
- "`clearPref`": You cannot change the value in the browser via `about:config` and the value will not be shown via `about:config`.

Custom preference: The name of the custom preference. Example: `ui.textSelectBackground`



Type: The type of the custom preference.

Possible values:

- "String": The value is a string of characters.
- "Integer": The value is a whole number.
- "Booleantrue or `false`.

Value: The value of the custom preference. The possible entries depend on the **Type** selected.

► Click **Ok** to add the custom preference.

The custom preference will take effect the next time that the browser is launched.

You will find information regarding custom preferences in Firefox in the MozillaZine Knowledge Base under [Firefox About:config entries](#)²⁸.

²⁸ http://kb.mozilla.org/About:config_entries



Encryption

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Encryption**

In this area, you can define the settings for encryption methods.

Minimum required encryption protocol: This protocol will be used to establish a secure connection if no higher protocol is available. Higher protocols are preferred.

Possible options:

- SSL3
- TLS 1.0
- TLS 1.1
- TLS 1.2

Maximum supported encryption protocol: This protocol is requested when negotiating the connection. If this protocol is not available, the next lowest protocol will be requested.

Possible options:

- SSL3
- TLS 1.0
- TLS 1.1
- TLS 1.2



Certificates

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Certificates**

In this area, you can define the settings for certificate validation.

When a website requests a certificate: Specifies how the browser behaves if a website requests a security certificate.

Possible values:

- Select one automatically: The browser selects a certificate automatically. (default)
- Ask me every time: A dialog window requesting the certificate will be displayed.

View certificates: If you click on this button, the certificates saved in the browser's **Certificate Manager** will be displayed.

Certificate validation: Specifies the validation of certificates using OCSP (Online Certificate Status Protocol).

- Do not use OCSP for certificate validation: The certificate will not be validated using OCSP.
- Validate a certificate if it specifies an OCSP server: The certificate will be validated with the OCSP server specified in the certificate. If no OCSP server is specified, no certificate validation will take place. (default)
- Validate all certificates with the following OCSP server: All certificates will be validated with the OCSP server specified under the **Service URL**, irrespective of which OCSP server is specified in the certificate.

Response signer: Signer of the response from the OCSP server

Service URL: URL of the OCSP server

When an OCSP server connection fails, treat the certificate as invalid:

If, owing to a failed connection to the OCSP server, no validation can take place, the certificate will be treated as invalid. In this case, the browser will show the “This connection is not trusted” error message.

The certificate will not be deemed invalid if no check can take place because there is no connection to the OSCP server. (default)

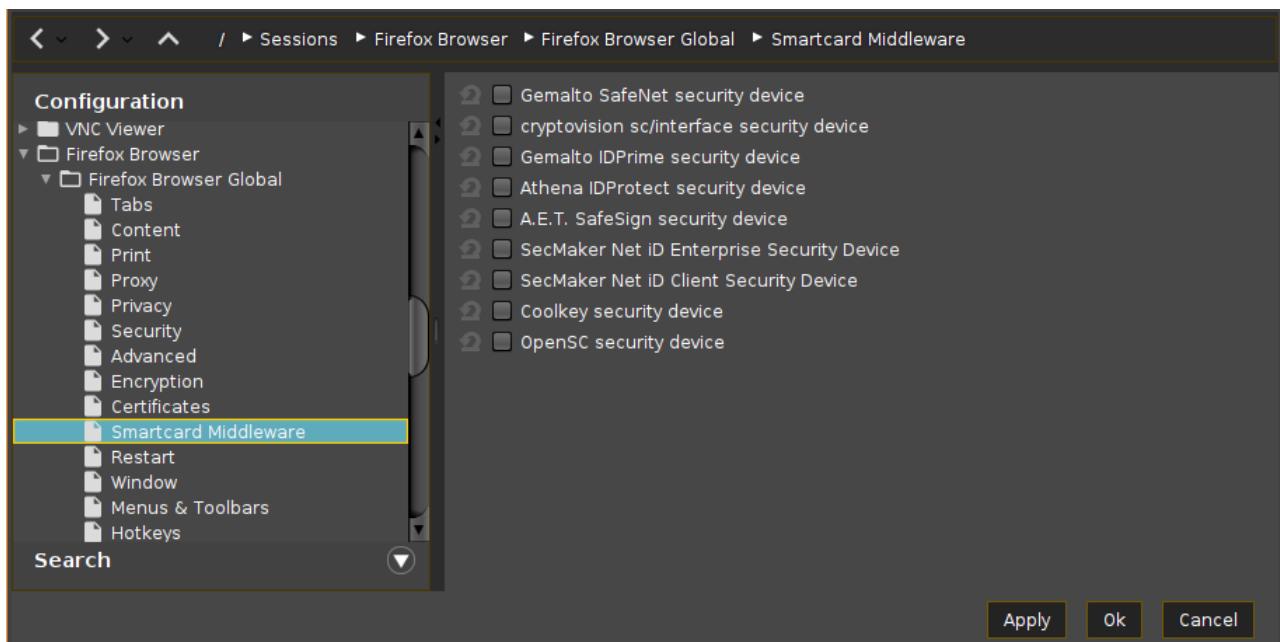


Smartcard Middleware for Firefox Browser in IGEL OS

In this area of the IGEL Setup, you can activate or deactivate smartcard middleware (PKCS#11 module) that is to be used for encryption. If you want to use your own PKCS#11 library with the Firefox browser, see Using a Custom PKCS#11 Library.

For more information on smartcard authentication in IGEL OS, see the how-to Smartcard Authentication in IGEL OS.

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Smartcard Middleware**



Gemalto SafeNet security device

- Gemalto/SafeNet eToken will be used for encryption.
- Gemalto/SafeNet eToken will not be used for encryption.*

cryptovision sc/interface security device

- cryptovision sc/interface will be used for encryption.
- cryptovision sc/interface will not be used for encryption.*

Gemalto IDPrime security device

- Gemalto IDPrime will be used for encryption. Enable this Gemalto middleware when you want to operate Gemalto Common Criteria devices in unlinked mode.



Gemalto IDPrime will not be used for encryption.*

Athena IDProtect security device

Athena IDProtect will be used for encryption.

Athena IDProtect will not be used for encryption.*

A.E.T. SafeSign security device

A.E.T. SafeSign will be used for encryption.

A.E.T. SafeSign will not be used for encryption.*

SecMaker Net iD Enterprise security device

SecMaker Net iD Enterprise, formerly known as "SecMaker Net iD", will be used for encryption.

SecMaker Net iD Enterprise will not be used for encryption.*

SecMaker Net iD Client security device

SecMaker Net iD Client will be used for encryption. SecMaker Net iD Client is the next generation of Net iD Enterprise, see <http://docs.secmaker.com/net-id-client/latest/index.html>.

SecMaker Net iD Client will not be used for encryption.*

Coolkey security device

Coolkey will be used for encryption.

Coolkey will be not used for encryption.*

OpenSC security device

OpenSC will be used for encryption.

OpenSC will not be used for encryption.*

90meter security device

Licensed Feature

This feature requires an add-on license; see Add-On Licenses. Please contact your IGEL sales representative.

90meter will be used for encryption.

90meter will not be used for encryption.*



* IGEL OS system default



Restart

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Restart**

In this area, you can specify whether the browser automatically starts and whether it is automatically restarted after being closed and after what delay time.

Restart

- The browser automatically restarts if it was closed.
 The browser does not automatically restart if it was closed. (default)

Restart after idle time

- If no action on the part of the user has occurred after the idle time has elapsed, the browser will automatically be restarted.
 There will be no automatic restart after a specific idle time has elapsed. (default)

Idle time after which a restart occurs: Time interval after which the browser is automatically restarted if in the meantime no action on the part of the user has occurred. (default: 5)
The time unit can be selected under **Unit**.

Unit: Time interval for the idling time

Possible options:

- Minutes
- Seconds



Window

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Window**

In this area, you can define the window settings for a browser session.

Start in full-screen mode

- The browser will start in fullscreen mode.
 The browser will start in a standard window. (default)

Firefox translation: Language of the user interface

Possible values:

- System setting: The language set under **User Interface > Language > Language** will be used for the browser. (default)
- English
- German
- French
- Dutch
- Spanish
- Italian

Hide configuration page of the browser

- The browser configuration page (`about:config`) is locked. As a result, the user cannot change the configuration. (default)
 The browser configuration page (`about:config`) can be used.



Menus & Toolbars

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Menus & Toolbars**

In this area, you can change the browser's menus and toolbars.

Hide app menu/menu bar

- The button for opening the browser menu will not be shown.
- The button for opening the browser menu will be shown. (default)

Use old menu bar

- The browser menu will be shown in the menu bar as in earlier browser versions.
- The browser menu can be opened via a button. (default)

Hide the Following Items in App Menu/Menu Bar

Hide bookmarks menu

- The bookmarks menu will not be shown in the menu bar.
- The bookmarks menu will be shown in the menu bar. (default)

Hide tools menu

- The “Tools” menu will not be shown.
- The “Tools” menu will be shown. (default)

Hide history entry

- The button for showing the browser history will not be shown.
- The button for showing the browser history will be shown. (default)

Hide tabs toolbar

- The tabs will not be shown in the menu bar. The user cannot switch between a number of tabs.
- The tabs will be shown in the menu bar. (default)

Hide bookmarks toolbar

- The bookmarks toolbar will not be shown. (default)
- The bookmarks toolbar will be shown.

Hide sidebar

- The sidebar will not be shown.
- The sidebar will be shown. The bookmarks can be shown in the sidebar. (default)

Hide navigation toolbar

- The navigation bar will not be shown.
- The navigation bar will be shown. (default)

Hide the toolbar for searching the page



- The search bar will not be shown.
- The search bar will be shown. (default)

Toolbar Items

Hide URL input

- Only search terms can be entered in the entry field; URLs cannot be entered manually.
- Both search terms and URLs can be entered in the entry field. (default)

Hide "Print" button

- The button for printing websites will not be shown.
- The button for printing websites will be shown. (default)

Hide "Home" button

- The Home button will not be shown.
- The Home button will be shown. (default)

Hide "Search" input

- The search field will not be shown.
- The search field will be shown. (default)

Hide "Bookmarks" and "RSS Feed" button

- The button for displaying bookmarks and RSS feeds will not be shown.
- The button for displaying bookmarks and RSS feeds will be shown. (default)

Toolbarconfig

User customization of toolbars

- The user can customize the toolbars. (default)
- The user cannot customize the toolbars.

Navigation toolbar: Specifies which symbols are shown in the navigation toolbar. The symbols are given as follows; multiple symbols should be separated by commas ",":

loop-button	
zoom-controls	- 100% +
edit-controls	Ausschn... Kopieren Einfügen
history-panelmenu	

privatebrowsing-button	
save-page-button	
find-button	
open-file-button	
developer-button	
sidebar-button	
feed-button	
print-button	
characterencoding-button	
social-share-button	
panic-button	
web-apps-button	
new-window-button	
fullscreen-button	
tabview-button	
downloads-button	

Application menu: Specifies which symbols are shown in the application menu. Multiple symbols should be separated by commas „,“.



Hotkeys

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Hotkeys**

In this area, you can disable Firefox hotkeys.

Disable hotkey Quit/Close

- The hotkey for terminating/closing the browser is disabled.
 The hotkey for terminating/closing the browser is enabled. (default)

Disable hotkey for print dialog

- The hotkey for opening the print dialog is disabled.
 The hotkey for opening the print dialog is enabled. (default)

Disable hotkey for save page

- The hotkey for saving a website is disabled.
 The hotkey for saving a website is enabled. (default)

Disable hotkeys for opening new window/tab

- The hotkey for opening a new window or tab is disabled.
 The hotkey for opening a new window or tab is enabled. (default)

Disable hotkeys for opening a new webpage/location and download window

- The hotkey for opening a new website/location and the download window is disabled.
 The hotkey for opening a new website/location and the download window is enabled. (default)

Disable hotkeys to show history and page info

- The hotkey for showing the history and page information is disabled.
 The hotkey for showing the history and page information is enabled. (default)

Disable hotkeys for creating bookmarks

- The hotkey for creating a bookmark is disabled.
 The hotkey for creating a bookmark is enabled. (default)

Disable hotkeys for opening help pages

- The hotkey for displaying help is disabled.
 The hotkey for displaying help is enabled. (default)

Disable hotkeys for caret browsing

- The hotkey for starting caret browsing is disabled.
 The hotkey for starting caret browsing is enabled. (default)



Context

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Context**

In this area, you can disable various items in the browser context menu.

Disable navigation elements in context menu

- The navigation elements will not be shown in the context menu.
- The navigation elements will be shown in the context menu. (default)

Disable button for save page

- The button for saving a page will not be shown in the context menu.
- The button for saving a page will be shown in the context menu. (default)

Disable button for open new window/tab

- The button for opening a new window/tab will not be shown in the context menu.
- The button for opening a new window/tab will be shown in the context menu. (default)

Disable button for show info/source

- The button for showing page information/page source text will not be shown in the context menu.
- The button for showing page information/page source text will be shown in the context menu. (default)

Disable button for creating and editing bookmarks

- The button for creating and editing bookmarks will not be shown in the context menu.
- The button for creating and editing bookmarks will be shown in the context menu. (default)

Disable button for searching the web

- The button for searching the web will not be shown in the context menu.
- The button for searching the web will be shown in the context menu. (default)

Hide the browser's context menu

- The context menu will not be shown.
- The context menu will be shown. (default)



Commands

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Commands**

In this area, you can define start options for browser commands.

The following commands are available:

Restart Browser

To open the dialogue for defining start options, proceed as follows:

1. Select the command. Example: **Restart Browser**
2. Click **Modify...**

The following start options are available:

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`



Firefox Browser Session

Menu path: **Sessions > Firefox Browser > Firefox Browser Sessions > [Session Name]**

In this area, you can configure desktop integration for the browser session.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.



Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.



- The session is started automatically, even when no network is available.
-

- [Settings](#)(see page 392)
- [Desktop Integration](#)(see page 393)
- [Plugins](#)(see page 395)



Settings

Menu path: **Sessions > Firefox Browser > Firefox Browser Sessions > [Session Name] > Settings**

In this area, you can change the following settings:

When browser starts: Specifies what pages are shown when the browser is launched.

Possible options:

- "Global setting"
- "Start with a blank page"
- "Show my home page"
- "Resume previous session": All tabs from the last session are reopened.

Start page: Specifies the URL of the start page. You can specify a number of start pages by separating the URLs of the start pages with a vertical dash "|". This setting is active only when "Show my home page" is chosen under **When browser starts**.

Start monitor: Specifies the monitor on which the browser is launched. (Default: 1st monitor)

Autostart

The browser is automatically launched when the system starts.



Desktop Integration

Menu path: **Sessions > Firefox Browser > Firefox Browser Sessions > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the Firefox browser session.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.



Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

ⓘ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with | :

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

- ⓘ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.



Plugins

Menu path: **Sessions > Firefox Browser > Plugins**

To obtain an overview of the plugins available in the browser, proceed as follows:

- ▶ Click on the **About:Plugins** button.

The browser will start with the `about:plugins` page. The plugins available in the browser will be shown.



Chromium Browser Global Session in IGEL OS

IGEL OS has a built-in Chromium browser. On this Setup page, you can set the default browser for IGEL OS, enable or disable hardware video acceleration and change the startup behavior of the Chromium browser.

The settings will be valid for all Chromium browser sessions.

Menu path: **Sessions > Chromium Browser > Chromium Browser Global**

Use IGEL Setup for configuration

- The settings made in the IGEL Setup or the UMS configuration dialog will be effective.
- The settings made in the IGEL Setup or the UMS configuration dialog will not have any effect on the behavior of Chromium.

Default web browser

Defines which browser will be chosen by the system, e.g. for opening Citrix Storefront.
Possible options:

- **Firefox Browser***
- **Chromium Browser**

Hardware Video Acceleration

- Hardware video acceleration is enabled for the Chromium browser.*
Please see How Can I Use H.264 Hardware Acceleration for Chromium or Firefox Browsers on IGEL OS Endpoint Devices?
- Hardware video acceleration is disabled for the Chromium browser.

Automatic browser restart on exit

- Chromium is restarted when the user closes it.
- Chromium is not restarted on exit.*

Show browser splash screen

- The Chromium splash screen is shown at the start.
- Chromium starts without a splash screen.*

-
- [General\(see page 398\)](#)
 - [Content\(see page 399\)](#)



- [Proxy](#)(see page 400)
- [Privacy](#)(see page 402)
- [Security](#)(see page 404)
- [Encryption Settings for the Chromium Browser in IGEL OS](#)(see page 405)
- [Menus & Toolbars](#)(see page 406)
- [Window](#)(see page 407)
- [Custom Setup](#)(see page 408)
- [Smartcard Middleware for Chromium Browser in IGEL OS](#)(see page 412)

*IGEL OS system default



General

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > General**

In this area, you can change the following settings:

On startup: Specifies what pages are shown when Chromium is launched.

Possible options:

- "Open the new tab page"
- "Open a specific page or set of pages": The page or set of pages specified under **Startup page** are opened.
- "Continue where you left off": All tabs from the last session are reopened.

Startup page: Specifies the URL of the start page. You can specify a set of start pages by separating the URLs of the start pages with a vertical dash "|". This setting is active only when "Open a specific page or set of pages" is chosen under **On startup**.

New tab page setting: Specifies the page that is shown when a new tab is opened.

Possible options:

- "Open a blank page"
- "Open a specific page": The page defined under **New tab page location** is shown.

New tab page location: Specifies the page that is shown when the user opens a new tab. This is effective only if **New tab page setting** is set to "Open a specific page".

Font size: Specifies the font size for web content.

Possible options:

- "Very small"
- "Small"
- "Medium (recommended)"
- "Large"
- "Very large"



Content

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Content**

Block pop-ups and redirects

Pop-up windows and redirects are blocked.

Exceptions...: Add websites on which pop-up windows and redirects are not blocked.

Load images automatically

Images from websites are loaded automatically.

Exceptions...: Add websites on which images are not loaded automatically.

Type of download directory

Possible options:

- "Custom location": The user will be prompted for a location to download a file.
- "userhome": Files will be downloaded to `/userhome/Downloads`.

Location: Defines the path files are downloaded to. Only effective when **Type of download directory** is set to "Custom location".

JavaScript

JavaScript is enabled.

Languages: One or more preferred languages for multilingual websites, given in the form of language abbreviations separated by commas. The languages should be given in the order of preference. Example: With "de, en, fr, it", the website will be shown in German, if available, otherwise in English and so on.

Integrated translation service of Chromium

When a web page has a language that differs from your system language, Chromium will offer to translate the page.

Autoplay

Embedded audio and video content on a web page is played automatically when the page is loaded.

Audio and video content is not played automatically.



Proxy

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Proxy**

In this area, you can change the proxy configuration.

To change the proxy configuration, proceed as follows:

1. In the **Proxy Configuration** menu, select the type of proxy configuration.
The following proxy configurations are available:
 - "Never use a proxy"
 - "Use fixed proxy servers"
 - "Use a .pac proxy script"
 - "Use system proxy settings"
 - "Auto detect proxy settings"
2. Enter the necessary configuration data for the selected proxy configuration.

"Never use a proxy"

With this proxy configuration, no proxy is used.

"Use fixed proxy servers"

The configuration data must be specified in the following fields.

- **FTP proxy:** URL of the proxy for FTP
- **Port:** Port of the proxy for FTP
- **HTTP proxy:** URL of the proxy for HTTP
- **Port:** Port of the proxy for HTTP
- **SSL proxy:** URL of the proxy for SSL
- **Port:** Port of the proxy for SSL
- **SOCKS host:** URL of the proxy for SOCKS
- **Port:** Port of the proxy for SOCKS
- **SOCKS protocol version:** Version of the SOCKS protocol used (default: SOCKS v5)
- **No proxy for:** List of URLs for which no proxy is to be used (default: `localhost, 127.0.0.1`)

"Use a .pac proxy script"

With this proxy configuration, the PAC file (Proxy Auto Config) available under **URL** will be used.

- **URL:** URL of the proxy configuration file

"Use system proxy settings"

With this proxy configuration, the proxy configured under **Network > Proxy** will be used.



"Auto detect proxy settings"

With this proxy configuration, WPAD (Web Proxy Autodiscovery Protocol) will be used. The browser will determine the URL of the WPAD file `wpad.dat` automatically with the help of DNS.



Privacy

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Privacy**

Autofill addresses and more

- Entries in forms and search bars will be retained after Chromium restarts.
 Entries in forms and search bars will be retained only for the duration of the session.

Autofill payments

- Entries in payment forms will be retained after Chromium restarts.
 Entries in payment forms will be retained only for the duration of the session.

Autofill passwords

- Passwords entered will be retained after Chromium restarts.
 Passwords entered will be retained only for the duration of the session.

Clear browsing data

- Data entered will be deleted when Chromium is closed. What data are deleted is specified in the following options.
 Data entered will not be deleted when the browser is closed.

Browsing & download history

- Addresses (URLs) of visited websites and the list of downloads will be deleted when Chromium is closed.

Saved passwords

- Passwords entered will be deleted when Chromium is closed.

Cookies

- Cookies will be deleted when Chromium is closed.

Cache

- The cache for temporarily saving web pages will be emptied when Chromium is closed.

Allow incognito mode: When the incognito mode is active, all data from private windows will be deleted after Chromium is closed.

Possible options:

- "Enabled": The user can open browser windows in incognito mode.
- "Disabled": The user cannot open browser windows in incognito mode.
- "Forced": All browser windows started by the user are in incognito mode.

Enable "Do Not Track" feature

- Chromium will inform the website you are visiting that you do not wish to be tracked, i.e. you do not want your surfing history to be recorded.



- ⓘ The browser will use the `DNT` ("Do Not Track") field in the HTTP header for this purpose. Observing this setting is voluntary; from a technical point of view, websites can still record the surfing history even when `DNT` is set to 1.

Enable search suggestions

Suggestions will be shown while an address is being typed in the address bar. The suggestions will be based on previously visited websites which are stored in the history.



Security

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Security**

On this page, you can define settings for safe browsing and for the handling of files.

Safe browsing

Chromium will check all web content, including e.g. images and scripts, against a continuously updated list of known phishing and malware websites. If Chromium finds suspicious content, you will be given a warning.

Chromium will not check web content.

File access

Chromium can access local files on the endpoint device. Downloads and uploads are allowed. Before a file is downloaded, a confirmation dialog is shown.

Local files cannot be accessed by Chromium. Neither downloads nor uploads are allowed. When the user tries to download a file, a message informs the user that downloads are blocked.

Download allowlist: The MIME types listed here are not blocked even when **File access** is deactivated. The storage location is defined under **Sessions > Chromium Browser > Chromium Browser Global > Content**, parameter **Location**. If the file suffix matches with one of the entries in **Open file types automatically after downloading**, the file is opened immediately after download. The list entries are separated by semicolons ";".

Open file types automatically after downloading: Any file whose suffix is listed here will be opened immediately after download. The list entries are separated by semicolons ";".



Encryption Settings for the Chromium Browser in IGEL OS

Here, you can select the minimum and maximum SSL/TLS version for the Chromium Browser that is built into IGEL OS.

Note that it is always better to upgrade to a higher TLS version on the server than to downgrade to a lower version on the client.

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Encryption**

Minimum SSL/TLS version

This protocol will be used to establish a secure connection if no higher protocol is available. Higher protocols are preferred.

Possible options:

- TLS 1.2*
- TLS 1.3

Maximum SSL/TLS version

This protocol is requested when negotiating the connection. If this protocol is not available, the next lowest protocol will be requested.

Possible options:

- TLS 1.2
- TLS 1.3*

*IGEL OS system default



Menus & Toolbars

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Menus & Toolbars**

In this area, you can change the browser's menus and toolbars.

Hide home button

- The home button will not be shown.
- The home button will be shown.

Hide bookmarks toolbar

- The bookmarks menu will not be shown in the menu bar.
- The bookmarks menu will be shown in the menu bar.



Window

Menu path: **Sessions > Chromium Browser > Chromium Global > Window**

In this area, you can define the window settings for a Chromium session.

Enable kiosk mode

- Chromium starts in kiosk mode.
- Chromium starts in normal mode.

Start maximized

- Chromium starts in a maximized window.
- Chromium starts in a window with default size.

Chromium translation: Changes the default language when Chromium offers to translate a web page.

Block Chromium settings

- The settings menu of Chromium can not be accessed by the user.
- The user can access the settings menu.



Custom Setup

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Custom Setup**

- [Chromium Policies for IGEL OS](#)(see page 409)
- [Custom Command-Line Options](#)(see page 411)



Chromium Policies for IGEL OS

Here, you can add, edit, and remove policies for the Chromium sessions on your IGEL OS device. Please note that the custom settings always win over the IGEL Setup, i.e. if a policy is defined both here and in the Setup, but with different values, the value defined here is effective.

For a complete list of available policies, see <https://chromeenterprise.google/policies/>.

- ⓘ Please note that the enterprise policy URL pattern format that is defined by Chrome is not fully supported by the IGEL Setup.

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Custom Setup > Policies**

- Click on **Add** to create a policy.

Policy name

Name of the policy as described in <https://chromeenterprise.google/policies/>.

Policy value

Value of the policy. The data format is described in <https://chromeenterprise.google/policies/>. Please note the following:

- Use the correct data type (see the right column of the relevant policy description, e.g. <https://chromeenterprise.google/policies/#URLBlocklist>)
- Use the Linux examples
- Make sure to separate the policy name from the policy value; some of the examples in the Chrome documentation include the policy name accidentally, e.g. <https://chromeenterprise.google/policies/#PrintingPaperSizeDefault>.

URL Blocklist Example

If you want to block the websites `badsite.com` and `malware.com`, define your policy as follows (see also <https://chromeenterprise.google/policies/#URLBlocklist>):

- **Policy name:** `URLBlocklist`
- **Policy value:** `["badsite.com", "malware.com"]`

A screenshot of a dark-themed dialog box titled "Add". It has two input fields: "Policy name" with the value "URLBlocklist" and "Policy value" with the value "[\"badsite.com\", \"malware.com\"]". At the bottom are "Ok" and "Cancel" buttons.

Policy name	URLBlocklist
Policy value	["badsite.com", "malware.com"]

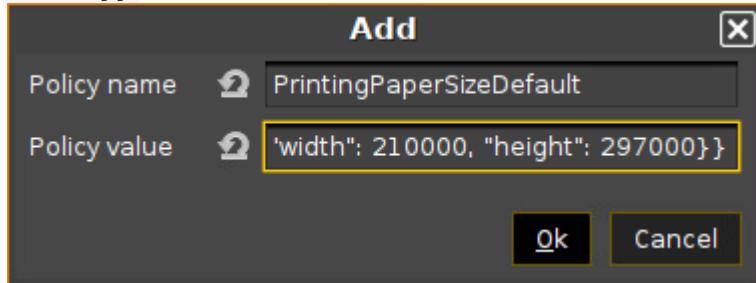
Ok Cancel



Printing Paper Size Example

If you want to define a paper size for printing, define your policy as follows (see <https://chromeenterprise.google/policies/#PrintingPaperSizeDefault>):

- **Policy name:** PrintingPaperSizeDefault
- **Policy value:** {"name": "custom", "custom_size": {"width": 210000, "height": 297000}}





Custom Command-Line Options

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Custom Setup > Custom Command-Line Options**

Here, you can define command-line parameters that are passed to Chromium on startup. The syntax is exactly the same as if Chromium would be started from a terminal.

Custom command-line parameters: One or more command-line parameters. Multiple parameters are separated by whitespace.

Example:

```
--proxy-server="socks://localhost:8080" --incognito
```



Smartcard Middleware for Chromium Browser in IGEL OS

In this area of the IGEL Setup, you can activate or deactivate smartcard middleware (PKCS#11 module) that is to be used for encryption. Alternatively, you can specify here your own PKCS#11 module that you want to use with the Chromium browser.

For more information on smartcard authentication in IGEL OS, see the how-to Smartcard Authentication in IGEL OS.

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Smartcard Middleware**

A screenshot of the IGEL Setup software interface. The title bar shows the path: Sessions > Chromium Browser > Chromium Browser Global > Smartcard Middleware. The left sidebar has a tree view with Configuration, VNC Viewer, Firefox Browser, Chromium Browser (selected), Chromium Browser Global (selected), and Smartcard Middleware (highlighted with a yellow selection bar). The main pane lists various security device options with checkboxes: Gemalto SafeNet security device, cryptovision sc/interface security device, Gemalto IDPrime security device, Athena IDProtect security device, A.E.T. SafeSign security device, SecMaker Net iD Enterprise security device, SecMaker Net iD Client security device, Coolkey security device, OpenSC security device, and Use a custom security device. Below these are fields for Name of the security device and Path to the library, each with a browse button. At the bottom are Apply, Ok, and Cancel buttons.

Security Device	Status
Gemalto SafeNet security device	<input checked="" type="checkbox"/>
cryptovision sc/interface security device	<input checked="" type="checkbox"/>
Gemalto IDPrime security device	<input type="checkbox"/>
Athena IDProtect security device	<input type="checkbox"/>
A.E.T. SafeSign security device	<input type="checkbox"/>
SecMaker Net iD Enterprise security device	<input type="checkbox"/>
SecMaker Net iD Client security device	<input type="checkbox"/>
Coolkey security device	<input type="checkbox"/>
OpenSC security device	<input type="checkbox"/>
Use a custom security device	<input type="checkbox"/>

Gemalto SafeNet security device

- Gemalto/SafeNet eToken will be used for encryption.
 Gemalto/SafeNet eToken will not be used for encryption.*

cryptovision sc/interface security device

- cryptovision sc/interface will be used for encryption.
 cryptovision sc/interface will not be used for encryption.*



Gemalto IDPrime security device

- Gemalto IDPrime will be used for encryption. Enable this Gemalto middleware when you want to operate Gemalto Common Criteria devices in unlinked mode.
- Gemalto IDPrime will not be used for encryption.*

Athena IDProtect security device

- Athena IDProtect will be used for encryption.
- Athena IDProtect will not be used for encryption.*

A.E.T. SafeSign security device

- A.E.T. SafeSign will be used for encryption.
- A.E.T. SafeSign will not be used for encryption.*

SecMaker Net iD Enterprise security device

- SecMaker Net iD Enterprise, formerly known as "SecMaker Net iD", will be used for encryption.
- SecMaker Net iD Enterprise will not be used for encryption.*

SecMaker Net iD Client security device

- SecMaker Net iD Client will be used for encryption. SecMaker Net iD Client is the next generation of Net iD Enterprise, see <http://docs.secmaker.com/net-id-client/latest/index.html>.
- SecMaker Net iD Client will not be used for encryption.*

Coolkey security device

- Coolkey will be used for encryption.
- Coolkey will not be used for encryption.*

OpenSC security device

- OpenSC will be used for encryption.
- OpenSC will not be used for encryption.*

90meter security device

Licensed Feature



This feature requires an add-on license; see Add-On Licenses. Please contact your IGEL sales representative.

- 90meter will be used for encryption.
 90meter will not be used for encryption.*

Use a custom security device

- The PKCS#11 module stored under the **Path to the library** is used. See also Using a Custom PKCS#11 Library.
 The custom security device will not be used for encryption.*

⚠ In case of the installation of a custom PKCS#11 library, the file(s) must be placed on the endpoint device either via UMS file transfer or Custom Partition.
The use of the `/wfs` folder is NOT recommended because of its space limit.

Name of the security device

Name of the custom security device that uses the library specified under **Path to the library**

Path to the library

Path to the custom PKCS#11 module

* IGEL OS system default



Chromium Sessions

Menu path: **Sessions > Chromium Browser > Chromium Sessions > [Session Name]**

In this area, you can configure desktop integration for the Chromium session.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. **Ctrl**.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
-  = `Shift`
- `[Ctrl]` = `Ctrl`
-  = `Mod4`

 When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

-  To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

- [Settings](#)(see page 417)
- [Desktop Integration](#)(see page 418)



Settings

Menu path: **Sessions > Chromium Browser > Chromium Sessions > [Session Name] > Settings**

In this area, you can change the following settings:

On startup: Specifies what pages are shown when Chromium is launched.

Possible options:

- "Global setting"
- "Open the new tab page"
- "Open a specific page or set of pages": The page or set of pages specified under **Startup page** are opened.
- "Continue where you left off": All tabs from the last session are reopened.

Startup page: Specifies the URL of the start page. You can specify a number of start pages by separating the URLs of the start pages with a vertical dash "|". This setting is active only when "Show my home page" is chosen under **On startup**.



Desktop Integration

Menu path: **Sessions > Chromium Browser > Chromium Sessions > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the Chromium session.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
-  = `Shift`
- `[Ctrl]` = `Ctrl`
-  = `Mod4`

 When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows key` = `Ctrl|Super_L`

Key: Key for the hotkey

-  To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.



Media Player Global

Menu path: **Sessions > Media Player > Media Player Global**

Here, you can change the global settings for the device's media player:

- [Window](#)(see page 421)
- [Playback](#)(see page 422)
- [Video](#)(see page 423)
- [Options](#)(see page 424)



Window

Menu path: **Setup > Sessions > Media Player > Media Player Global > Window**

Aspect ratio: Aspect ratio for video playback

Possible values:

- Auto: The aspect ratio of the playback window will adapt to the video being played.
- Square
- 4:3 (TV)
- 16:9 (widescreen)
- 2.11:1 (DVB)

Fullscreen

- The media player will be shown in full-screen mode.
 The media player will be shown in a standard window. (Default)

Automatically resize the player window when a new video is loaded

- The window size will adapt to the video being played.
 The window size will not change. (Default)

Main window should stay on top

- The media player window will always remain in the foreground. Other windows cannot be placed on top of the media player window.
 The media player window will behave like a standard window. Other windows can be placed on top of the media player window. (Default)

Show controls

- The media player operating components will be shown. (Default)
 The media player operating components will not be shown; only the playback window is visible.



Playback

Menu path: **Sessions > Media Player > Media Player Global > Playback**

Repeat mode

- The playlist will be repeated until the user stops playback.
 The playlist will be played back once only. (default)

Shuffle mode

- The playlist will be played back in a random order.
 The playlist will be played back in the set order. (default)

Show visual effects when an audio file is played

- Visual effects will be shown when playing back audio data.
 No visual effects will be shown. (default)

Type of visualization: The type of visual effects when playing back audio data

Possible values:

- Monoscope
- Goom!

Visualization size: The size of the visual effects shown

- i** This parameter is effective only if gstreamer 0.10 is selected as the multimedia framework, which results in Totem being selected as the media player. With the default setting for IGEL OS 10.05 and higher (gstreamer 1.x in combination with Parole) the parameter is not effective.
The multimedia framework and media player can be changed in the Registry under **System > Registry > multimedia > gstreamer > version** (registry key: `multimedia.gstreamer.version`).

Possible values:

- Small
- Normal
- Large
- Extra large



Video

Menu path: **Setup > Sessions > Media Player > Media Player Global > Video**

- **Video output:** Specifies the video output method.

Possible options:

- **Auto:** The video output method will be set depending on availability. The following options will be queried in this order. Examples: If available, hardware acceleration will be used. If hardware acceleration is not available but the X video extension is, the X video extension will be used.
- **Hardware accelerated:** Hardware acceleration will be used.
- **X video extension:** The images will be written to the graphics card memory using *shared memory*. Hardware acceleration will be used.
- **X Window System:** Video will be output via the X11 protocol. Hardware acceleration will not be used.



Options

Menu path: **Setup > Sessions > Media Player > Media Player Global > Options**

- **Disable screensaver when playing audio**

- The screensaver will not be started during audio playback. (default)
- The screensaver will start after the set idling time, even if audio is being played back.

- **Network connection speed**

Possible values:

- 56 kBps modem/ISDN
- 112 kBps dual ISDN/DSL
- 256 kBps DSL/cache
- 384 kBps DSL/cache
- 512 kBps DSL/cache
- 1.5 MBps T1/Intranet/LAN
- Intranet/LAN

- **Buffer size:** The buffer compensates for fluctuations in the network speed. (default: 3)

- **Autoload subtitle**

- Subtitles contained in the video will be shown automatically. (default)
- Subtitles contained in the video will only be shown if the user has enabled them via **View > Subtitles**.

- **Subtitle encoding:** Character coding for the subtitles. The value is set to UTF-8.

- **Font name:** Font that is used for the subtitles

Possible values:

- Sans
- Sans Bold
- Serif
- Serif Bold

- **Font size:** Size of the font that is used for the subtitles (default: 20)



Media Player Session

Menu path: **Sessions > Media Player > Media Player Sessions > [Session Name]**

In this area, you can configure desktop integration for the media player.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

- [Playback](#)(see page 428)
- [Options](#)(see page 429)
- [Desktop Integration](#)(see page 430)



Playback

Menu path: **Setup > Sessions > Media Player > Media Player Sessions > [Session Name] > Playback**

In this area, you can specify which audio data or video data are played back with which window settings when the media player session starts.

- **Medium / filename:** Path to the audio data or video data that are to be played back when the media player session starts. This can be a local path or a URL.
- **Use default fullscreen mode configuration**
 - The setting under **Setup > Sessions > Media Player > Media Player Global > Window** will be used. (default)
 - The setting will be set on a session-specific basis with **Play video in fullscreen**.
- **Play video in fullscreen**
 - The media player will be shown in fullscreen mode.
 - The media player will be shown in a standard window. (default)
- **Use image aspect ratio setting**
 - The setting under **Setup > Sessions > Media Player > Media Player Global > Window** will be used. (default)
 - The setting will be set on a session-specific basis with **Aspect ratio**.
- **Aspect ratio:** Aspect ratio for video playback
 - Possible values:
 - Auto: The aspect ratio of the playback window will adapt to the video being played.
 - Square
 - 4:3 (TV)
 - 16:9 (widescreen)
 - 2.11:1 (DVB)



Options

Menu path: **Setup > Sessions > Media Player > Media Player Sessions > [Session Name] > Options**

- **Use default controls configuration**

- The setting under **Setup > Sessions > Media Player > Media Player Global > Window** will be used. (default)
- The setting will be set on a session-specific basis with **Show controls**.

- **Show controls**

- The media player operating components will be shown. (default)
- The media player operating components will not be shown; only the playback window is visible.



Desktop Integration

Menu path: **Sessions > Media Player > Media Player Sessions > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the media player.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.



VoIP Client

Menu path: **Sessions > VoIP Client**

Ekiga Voice over IP client allows you to use the SIP (Session Initiation Protocol) and H.323; see <http://ekiga.org>²⁹.

You will find a detailed description of all Ekiga options under <http://wiki.ekiga.org/index.php/Manual>.

In this area, you can configure desktop integration for the VoIP session.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

²⁹ <http://ekiga.org/>



Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows key` = `Ctrl|Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.



Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

- [Account](#)(see page 436)
- [Audio](#)(see page 438)
- [SIP](#)(see page 439)
- [H.323](#)(see page 440)
- [Call Options](#)(see page 441)
- [Phone Book](#)(see page 442)
- [Preferences](#)(see page 443)
- [Desktop Integration](#)(see page 444)



Account

Menu path: **Setup > Sessions > VoIP Client > User Account**

You can set up or change one or more user accounts as well as specify the name displayed.

- **Full Name:** Name of the user; this name will be shown to the other person. Example: John Doe

To set up an SIP user account, proceed as follows:

- ⓘ Ensure that the VoIP client was terminated before you start setting up or changing a user account. Changes will only be saved if the client is not running.

1. Click **[+]**.
2. If the user account is to be active once set up, enable the **Enable Account** option.
3. Enter the following data:
 - **Protocol:** Select **SIP**.
 - **Name:** Name for this user account.

- ⓘ Choose a name which allows a distinction to be made easily between a number of user accounts.

- **Registrar:** URI with which the VoIP client registers. This can be a DNS name or an IP address.
- **User name:** Numerical or alphanumerical value. The user name is part of the SIP address.
Example: `john.doe` in `john.doe@example.com`
- **Login Name:** Numerical or alphanumerical value. Name with which the VoIP client registers on the registrar. This name can differ from the name given under **user name**.
- **Password:** Password with which the VoIP client registers on the registrar
- **Registration Update Timeout:** Timeout after which the registration should be updated (default: 3600)

4. Click **Ok**.
The user account has been set up.

To set up an H.323 user account, proceed as follows:

- ⓘ Ensure that the VoIP client was terminated before you start setting up or changing a user account. Changes will only be saved if the client is not running.

1. Click **[+]**.
2. If the user account is to be active once set up, enable the **Enable Account** option.
3. Enter the following data:
 - **Protokoll:** Wählen Sie **H323**.
 - **Name:** Name für dieses Benutzerkonto.



- ⓘ Choose a name which allows a distinction to be made easily between a number of user accounts.

- **Gatekeeper:** URI with which the VoIP client registers. This can be a DNS name or an IP address.
- **User name:** Numerical or alphanumerical value. Example: `john.doe` in `john.doe@example.com`
- **Passwort:** Password with which the VoIP client logs on to the registrar
- **Registration Update Timeout:** Timeout after which the registration should be updated (default: 3600)

4. Click **Ok**.

The user account has been set up.



Audio

Menu path: **Setup > Sessions > VoIP Client > Audio**

You can change the audio settings of the VoIP client.

- ⓘ Recommendation: Configure the settings **Device for ringtone**, **Device for audio playback** and **Device for audio recording** in the VoIP client. All available audio devices of the thin client are shown in the VoIP client.

To configure the audio devices in the VoIP client, proceed as follows:

1. In the *IGEL* setup, ensure that the option **Save configuration changes made in the application** is enabled under **Sessions > VoIP Client > Preferences**.
2. Start the VoIP client.
3. Configure your desired settings in the VoIP client under **Edit > Preferences > Audio > Devices**.
4. To save your settings, close the VoIP client window, right-click on in the system tray and select **Close**.

The changes will be saved in the *IGEL* setup once the VoIP client is terminated.

Settings in the setup:

- **Sound event output device:** Specifies which audio device is used for the ringtone.
 - ⓘ It is recommended that you select the audio device that is connected to the thin client's built-in loudspeaker.
- **Audio output device:** Specifies which audio device is used for playback. Example: the audio device that is connected to the loudspeakers of the headset.
- **Audio input device:** Specifies which audio device is used for recording. Example: the audio device that is connected to the microphone of the headset.
- **Enable silence detection:** If this option is enabled, audio transmission will be suppressed in the absence of voice activity. This helps to save bandwidth.
 - ⓘ Voice activity detection can reduce the voice quality.
- **Enable echo cancellation:** If this option is enabled, the VoIP client will suppress echoes of your own voice.
- **Maximum jitter buffer (in milliseconds):** The jitter buffer improves voice quality by compensating for delay variations when transmitting voice packets. The VoIP client continuously measures delay variations and automatically adjusts the buffer size. The bigger the delay variations are, the bigger the jitter buffer will be set. (Default: 500)
 - ⓘ A bigger jitter buffer results in greater latency.



SIP

Menu path: **Setup > Sessions > VoIP Client > SIP**

You can change SIP-specific settings for the proxy, forwarding and the multi-frequency dialing process (DTMF).

- **Outbound Proxy:** URI of the SIP proxy that handles outbound calls.
- **Forward URI:** SIP URI to which inbound calls are forwarded if forwarding is enabled. You will find further information on forwarding under [Call Options](#)(see page 441).
- **Send DTMF as:** Specifies how key sequences are transmitted while a connection is in place.
Possible values:
 - INFO: The key sequence is transmitted as SIP INFO.
 - RFC 2833: The key sequence is transmitted using RTP (Real-time Transport Protocol).



H.323

Menu path: **Setup > Sessions > VoIP Client > H.323**

You can change H.323-specific settings for forwarding, H.245, quick start and for the multi-frequency dialing process (DTMF).

- **Forward URI:** H.323 URI to which inbound calls are forwarded if forwarding is enabled. You will find further information on forwarding under [Call Options](#)(see page 441).
- **Enable H.245 tunneling**
 H.245 messages will be packaged in H.225 messages. In this way, no additional TCP connection must be established. (Default)

For H.245 tunneling, port 1720 is required.

A separate TCP connection is established for H.245.

- **Enable early H.245**
 H.245 will be launched at an earlier point in the connection process. The voice connection can be established more quickly as a result. (Standard)

- **Enable Fast Start procedure**

The voice connection will be established in quick start mode (fast connect, part of H.323 v2). (Standard)

- **DTMF senden als:** Specifies how key sequences are transmitted while a connection is in place.

Mögliche Werte:

- **String:** The key sequence is transmitted using H.245 User Input Indication.
- **Tone:** The key sequence is transmitted as a tone sequence in the audio data flow.
- **RFC 2833:** The key sequence is transmitted using RTP (Real-time Transport Protocol).
- **Q.931:** The key sequence is transmitted via the signaling channel.



Call Options

Menu path: **Setup > Sessions > VoIP Client > Call Options**

You can change settings for inbound calls.

- **Always forward calls to the given address:** If this option is enabled, inbound calls will immediately be forwarded to the address defined in **Setup > Sessions > VoIP Client > SIP > Forward URI** (see [SIP\(see page 439\)](#)) or **Setup > Sessions > VoIP Client > H.323> Forward URI** (see [H.323\(see page 440\)](#)).
- **Forward calls to the given address if no answer:** If this option is enabled, inbound calls will be forwarded to the address defined in **Setup > Sessions > VoIP Client > SIP > URI for Forwarding** (see [SIP\(see page 439\)](#)) or **Setup > Sessions > VoIP Client > H.323> URI for Forwarding** (see [H.323\(see page 440\)](#)) after the time specified under **Time limit for calls not taken**. If this option is disabled, inbound calls will be rejected after the time specified under **Time limit for calls not taken**.
- **Forward calls to the given address if busy:** If this option is enabled, inbound calls during a call will be forwarded to the address defined in **Setup > Sessions > VoIP Client > SIP > URI for Forwarding** (see [SIP\(see page 439\)](#)) or **Setup > Sessions > VoIP Client > H.323> URI for Forwarding** (see [H.323\(see page 440\)](#)).
- **No Answer Timeout:** Time in seconds after which calls not taken are rejected or forwarded.



Phone Book

Menu path: **Setup > Sessions > VoIP Client > Telephone Book**

You can add one or more LDAP address books or local contacts.

To add an LDAP address book, proceed as follows:

1. In the **List of LDAP address books** area, click on .
2. Enter the following data:
 - **Name:** Name with which the LDAP address book will be displayed in the VoIP client
 - **Server Name:** Host name of the LDAP server
 - **Port:** Port for the connection to the LDAP server (Default: 389)
 - **Base DN:** Basis for the search in the LDAP tree
 - **Scope:** Area for the LDAP search
 - Possible options:
 - Single level
 - Subtree
 - **Display name attribute:** LDAP attribute that is displayed as the name of the contact in the VoIP client. (Default: cn)
 - **Call Attribute:** LDAP attribute that contains the telephone number (Standard: telephoneNumber)
 - **Filter Template:** Filter for the LDAP search (Default: (cn=\$))
 - **Bind ID:** Identifier for the LDAP search. This identifier is sent to the LDAP server in a BIND request.
 - **Password:** Password for the user account for the LDAP search
3. Click **Ok**.

To add a contact to the local contact list, proceed as follows:

1. In the **List of Contacts** area, click on .
2. Enter the following data:
 - **Name:** Name of the SIP or H.323 address displayed
 - **Address:** SIP or H.323 address. Example: `sip:500@example.com`
 - **Group:** Optional group name in order to group contacts
3. Click **Ok**.



Preferences

Menu path: **Setup > Sessions > VoIP Client > Settings**

You can change VoIP client settings.

- **Save configuration changes made in the application**

changes made in the VoIP client will be saved in the *IGEL* setup when the VoIP client is terminated. This applies to all settings available in the *IGEL* setup, with the exception of settings for the LDAP address book. (Default)



Desktop Integration

Menu path: **Sessions > VoIP Client > Desktop Integration**

In this area, you can configure desktop integration for the VoIP client session.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.



PCoIP Sessions with the HP Anyware Client in IGEL OS

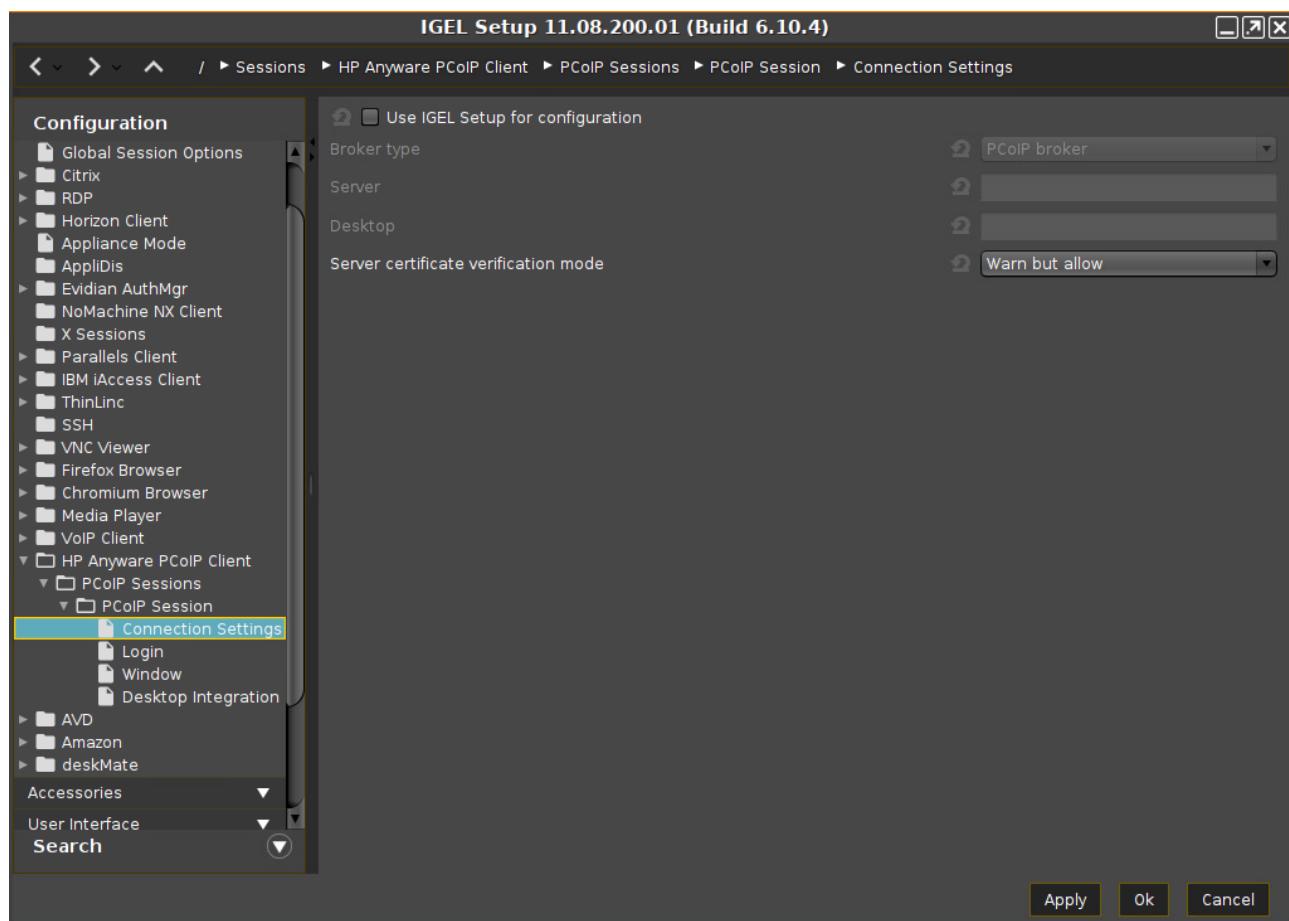
You can configure one or more HP Anyware PCoIP sessions on your IGEL OS device. If you want to use Amazon WorkSpaces via HP Anyware PCoIP, see Using Amazon WorkSpaces via the HP Anyware PCoIP Client.

Menu path: **Sessions > HP Anyware PCoIP Client > PCoIP Sessions**

- i If you are using Amazon WorkSpace, note that Linux connectivity is usually disabled by default, see [Amazon WorkSpaces Linux Client Application³⁰](#). You will have to enable this before connecting.

Connection Settings

Menu path: **Sessions > HP Anyware PCoIP Client > PCoIP Sessions > PCoIP Session > Connection Settings**



³⁰ <https://docs.aws.amazon.com/workspaces/latest/userguide/amazon-workspaces-linux-client.html>



Use IGEL Setup for configuration

- The connection settings are configured via IGEL Setup.
 IGEL Setup does not control the connection settings. (Default)

Broker type

Possible options:

- **PCoIP broker** (Default)
- **Direct hardhost**

Server

Host name or IP address of the PCoIP server

Desktop

Name of the virtual desktop. This parameter is only relevant if the user is assigned to more than one virtual desktop on the server, e. g. Amazon Web Services (AWS). If the user has several desktops and the field **Desktop** is empty, a selection of all available desktops is displayed after login. If the field **Desktop** contains the name of an available desktop, the session is started with this desktop.

Server certificate verification mode

Possible options:

- **Not required**
- **Warn but allow** (Default)
- **Full verification**: For secure operation, this verification mode is recommended.

Login

Menu path: **Sessions > HP Anyware PCoIP Client > PCoIP Sessions > PCoIP Session > Login**

A screenshot of the IGEL Setup software interface. The title bar reads "IGEL Setup 11.08.200.rc6.01 (Build 6.10.4)". The menu path is "Sessions > HP Anyware PCoIP Client > PCoIP Sessions > PCoIP Session > Login".

The left sidebar shows a tree view of configuration options:

- Configuration
 - AppliDis
 - Evidian AuthMgr
 - NoMachine NX Client
 - X Sessions
 - Parallels Client
 - IBM iAccess Client
 - ThinLinc
 - SSH
 - VNC Viewer
 - Firefox Browser
 - Chromium Browser
 - Media Player
 - VoIP Client
 - HP Anyware PCoIP Client
 - PCoIP Sessions
 - PCoIP Session
 - Connection Settings
 - Login
 - Window
 - Desktop Integration
 - AVD
 - deskMate
 - Unified Communications
- Accessories
- User Interface
- Network
- Devices
- Security
- Search

Authentication type

Password authentication

Smartcard PIN

Authentication type

Possible options:

- **Password authentication** (default)
- **Smartcard authentication**

Smartcard PIN

PIN required for smartcard authentication; only valid if **Authentication type** is set to **Smartcard authentication**.

Window

Menu path: **Sessions > HP Anyware PCoIP Client > PCoIP Sessions > PCoIP Session > Window**



IGEL Setup 11.08.200.rc6.01 (Build 6.10.4)

Window mode: Fullscreen one monitor

User interface translation: System setting

Configuration

- AppliDis
- Evidian AuthMgr
- NoMachine NX Client
- X Sessions
- Parallels Client
- IBM iAccess Client
- ThinLinc
- SSH
- VNC Viewer
- Firefox Browser
- Chromium Browser
- Media Player
- VoIP Client
- HP Anyware PCoIP Client
- PCoIP Sessions
- PCoIP Session
- Connection Settings
- Login
- Window** (selected)
- Desktop Integration
- AVD
- deskMate
- Unified Communications

Accessories

User Interface

Network

Devices

Security

Search

Apply Ok Cancel

Window mode

Possible options:

- **User defined:** The user can change the window mode via the PCoIP client. The window mode that has been used last is stored. (Default)
- **Fullscreen one monitor**
- **Fullscreen all monitors**
- **Window**

User interface translation

Possible options:

- **System setting** (default)
- **English**
- **German**
- **French**
- **Spanish**
- **Portuguese (EU)**



- **Portuguese (Brazil)**
- **Italian**
- **Japanese**
- **Chinese (Simplified)**
- **Chinese (Traditional)**

Desktop Integration

Menu path: **Sessions > HP Anyware PCoIP Client > PCoIP Sessions > PCoIP Session > Desktop Integration**

The screenshot shows the 'Session name' field set to 'PCoIP Session'. Under 'Starting Methods for Session', several checkboxes are checked: 'Start Menu', 'Application Launcher', and 'Desktop'. Other options like 'Quick Start Panel', 'Start Menu's System tab', 'Application Launcher's System tab', and 'Desktop Context Menu' are available but unchecked. The 'Modifiers' section shows 'None' selected. In the 'Autostart' section, 'Autostart' and 'Restart' are unchecked, while 'Autostart notification' and 'Autostart requires network' are checked. A note at the bottom states: 'The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()'.

Session name: Name for the session.

! The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu



The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
-  = `Shift`



- [Ctrl] = Ctrl
- = Mod4

i When this keyboard key is used as a modifier, it is represented as Mod4 ; when it is used as a key, it is represented as Super_L .

- [Alt] = Alt

Key combinations are formed as follows with | :

- Ctrl + = Ctrl | Super_L

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard . Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.



AVD Global

Menu path: **Sessions > AVD > AVD Global**

- [Plugins](#)(see page 455)



Plugins

Menu path: **Sessions > AVD > AVD Global > Plugins**

- [Fabulatech](#)(see page 456)



Fabulatech

Menu path: **Sessions > AVD > AVD Global > Plugins > Fabulatech**

The Fabulatech redirection of webcams and scanners as well as the common Fabulatech USB redirection can be enabled or disabled. The Fabulatech USB redirection can be controlled based on class rules and device rules.

For the Fabulatech USB redirection, a server-side component is required. We recommend the USB for Remote Desktop IGEL Edition; see <http://www.usb-over-network.com/partners/igel/>.

- ⚠ Enable either native USB redirection or Fabulatech USB redirection – not both together. Disable USB redirection if you use DriveLock.
- ⚠ Ensure that no other hotplug storage device (USB stick) is connected if a session is started with Fabulatech USB redirection. Otherwise, the hotplug storage device will not be securely removed when the session starts, and this could lead to data loss.
- ✓ You can enable or disable all Fabulatech redirections for each individual session; go to **Sessions > AVD > AVD Sessions > [Session name] > Plugins** and set **Fabulatech Webcam/Scanner/USB Redirection** accordingly (see [Plugins](#)(see page 472)).

Fabulatech Webcam Redirection

Fabulatech webcam redirection is enabled.

Fabulatech Scanner Redirection

Fabulatech scanner redirection is enabled.

Fabulatech USB Redirection

Fabulatech USB redirection is enabled.

Default rule: This rule will apply if no special rule was configured for a class or a device.

- Deny
- Allow

✓ Tip

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

Class Rules

Class rules apply to USB device classes and sub-classes.

Managing rules:

Create a new entry

Remove the selected entry



Edit the selected entry

Copy the selected entry

Class rule properties:

Rule:

- Allow: Devices that have the properties defined here are redirected by the Fabulatech USB Redirection.
- Deny: Devices that have the properties defined here are not redirected.

Class ID: Device class

Subclass ID: Subclass relating to the specified device class

Name: Free text entry

Override serial: Serial number that will appear in the session

Override name: Device name that will appear in the session

Postpone

The USB device is only removed from the system (endpoint device) when the session starts.

The USB device is no longer shown immediately after the system is booted.

i This setting is only effective if the **Takeaway** parameter is enabled.

Takeaway

The USB device may be removed from the system (endpoint device).

The USB device may not be removed. (Default)

No Reset

The device will not be automatically reset after the connection with the session has been terminated.

The device will be reset after the connection with the session has been terminated.

Device Rules

A device rule applies to a specific device that is identified by its serial number.

Device rule settings:

Rule:

- Allow
- Deny

Vendor ID: Hexadecimal manufacturer number

Product ID: Hexadecimal device number

i **Getting USB Device Information**



To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see [Using “System Information” Function\(see page 592\)](#).

System Information example:

The screenshot shows the 'Devices - USB Devices - System Information' window. The left sidebar has a tree view with 'Computer' expanded, showing 'Summary', 'Operating System', 'Security', 'Kernel Modules', 'Boots', 'Languages', 'Memory Usage', 'Filesystems', 'Display', 'Environment Variables', 'Devices' (expanded), 'System DMI', 'Processor', 'Graphics Processors', 'Monitors', 'Memory Devices', 'PCI Devices' (highlighted with a red box), 'USB Devices' (highlighted with a red box), 'Network', and 'Interfaces'. The main pane lists USB devices with their details:

Address	Driver	Product	Vendor
001:001	Linux	2.0 root hub	
002:001	Linux	1.1 root hub	
002:002	VMware	Virtual Mouse	
002:003	VMware	Virtual USB Hub	
002:004	logitech	960 Headset	

Device Information

- Product [0x0002] 2.0 root hub
- Vendor [0x1d6b] Linux Foundation
- Linux**
- Device EHCI Host Controller
- Manufacturer Linux 5.12.19 ehci_hcd
- Linux**
- Max Current 0 mA
- USB Version 2.00
- Speed 480 Mb/s

Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:

```
Local Terminal
File Edit View Terminal Tabs Help
root@ITC005056930CAD:~# lsusb | grep -i logitech
Bus 002 Device 004: ID 046d:0a45 Logitech, Inc. 960 Headset
root@ITC005056930CAD:~#
```

Name: Free text entry

Override serial: Serial number that will appear in the session.

Override name: Device name that will appear in the session.

Postpone

The USB device is only removed from the system (endpoint device) when the session starts.



- The USB device is no longer shown immediately after the system is booted.

i This setting is only effective if the **Takeaway** parameter is enabled.

Takeaway

- The USB device may be removed from the system (endpoint device).
- The USB device may not be removed.

No Reset

- The device will not be automatically reset after the connection with the session has been terminated.
- The device will be reset after the connection with the session has been terminated.



AVD Session

Menu path: **Sessions > AVD > AVD Sessions > [Session Name]**

In this area, you can configure desktop integration for the AVD session.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

- [Logon](#)(see page 463)
- [Options](#)(see page 465)
- [Proxy Settings for IGEL OS AVD Sessions](#)(see page 466)
- [Display](#)(see page 468)
- [Printing](#)(see page 469)
- [Plugins](#)(see page 472)
- [Desktop Integration](#)(see page 473)



Logon

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Logon**

Username@domain or @domain: A user name or a preset domain name used for the [automatic connection](#)(see [page 463](#)) to the AVD session. The string after "@" is taken as a preset domain name.

Example:

`avd@your.domain.com` : To log in, the user does not need to enter the username and the domain name.

`@your.domain.com` : To log in, the user only needs to enter the username, e.g. `a vd`. The preset domain – `your.domain.com` – will automatically be appended.

i Overwriting the Preset Domain Name

Use the following registry key to specify whether the user should be able to overwrite the preset domain, e.g. with `username@other-domain.com` :

Path	System > Registry
Registry	<code>sessions.wvd%.options.allow-preset-domain-overwrite</code>
Value	<u>enabled / disabled</u>
Note	If enabled: the domain entered by the user is accepted. If disabled: the domain entered by the user is replaced with the preset domain.

Password: Password used for the [automatic connection](#)(see [page 463](#)) to the AVD session.

i If the Login Credentials Should Not Be Applied Automatically

You can use the following registry key to always prompt for a user name and password or only for a password when connecting to an AVD session:

Path	System > Registry
Parameter	Always prompt for username and password upon session host connection
Registry	<code>sessions.wvd%.options.always-prompt-for-session-username-and-password</code>
Value	<u>enabled / disabled</u>
Path	System > Registry
Parameter	Always prompt for password upon session host connection
Registry	<code>sessions.wvd%.options.always-prompt-for-session-password</code>
Value	<u>enabled / disabled</u>



Note

On the server side, you can enable the RDP group policy "Always prompt for password upon connection" to achieve the same result.

Workspace resource to automatically start when connected: Name of the resource that is to be started automatically.

For an example, see How to Connect IGEL OS to Azure Virtual Desktop.



Options

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Options**

See also the list of implemented features: Feature Matrix: AVD (RDP3) for IGEL OS 11.

Clipboard redirection

Text and images from the clipboard are shared between the AVD session and the local client.

Drive redirection

Redirection is bound to the `/media` folder, so that locally mounted storage devices, including USB sticks, are forwarded to the AVD session. (Default)

Smartcard redirection

Smartcards are forwarded to the AVD session.

Exit on last session closed

When the last session window is closed, the entire IGEL AVD Client automatically closes. (Default)

In-session toolbar

The in-session toolbar is enabled. (Default)

Audio output redirection

The audio output is redirected between the AVD session and the local client. (Default)

AAC Codec

The AAC (Advanced Audio Coding) codec used for support of audio output redirection is enabled. (Default)

Audio input redirection

The audio input (microphone) is redirected between the local client and the AVD session. (Default)



Proxy Settings for IGEL OS AVD Sessions

In the following area, you can configure proxy settings for your AVD sessions in IGEL OS.

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Proxy**

The screenshot shows the IGEL OS configuration interface. The left sidebar has a tree view with categories like ThinLinc, SSH, VNC Viewer, Firefox Browser, Chromium Browser, Media Player, VoIP Client, Teradici PCoIP Client, and AVD. Under AVD, there are sub-categories: AVD Global, AVD Sessions, and AVD Session. The 'Proxy' option under AVD Session is selected and highlighted with a blue bar at the bottom of the list. The main panel on the right is titled 'Configuration' and contains sections for 'Proxy mode', 'Proxy host', and 'Proxy port'. A dropdown menu labeled 'Session specific proxy' is open, showing three options: 'Session specific proxy' (selected and highlighted with a yellow border), 'Global proxy setting', and 'Automatic proxy configuration'. Below the dropdown are two input fields for 'Proxy host' and 'Proxy port'.

i **Proxy Configuration via a PAC File**

If you want to use a PAC file, set **Proxy mode** to "Global proxy setting" and specify the **URL** of the PAC file under **Network > Proxy > Automatic proxy configuration**.

Proxy mode

Specifies if a proxy should be used.

Possible options:

- **Off***: A proxy is disabled. The direct connection to the Internet is used.
- **Global proxy setting**: The proxy configured under **Network > Proxy** is used, see [Proxy](#)(see page 752).
- **Session specific proxy**: The proxy configuration specified under **Proxy host** and **Proxy port** is used.

The following fields are active if **Proxy mode** is set to "Session specific proxy":

Proxy host

Hostname or IP address of the proxy server

Sessions



Proxy port

Port on which the proxy service is available

*IGEL OS system default



Display

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Display**

Window size: Specifies the width and height of the window.

Possible options:

- "Full-screen- "Work area": The session is shown on the full screen, minus the area needed by the device's taskbar.
- Numeric details: The session is shown in the selected resolution or on the selected percentage of the screen area.

Start monitor: Specifies the monitor on which the session is displayed.

Possible options:

- "No configuration- "1st monitor"
- "2nd monitor"

Multimonitor full-screen mode: This setting is relevant if more than one monitor is connected to the terminal.

Possible options:

- "Global setting": Currently the same as "Multiple monitors".
- "Single monitor": Restricts the full-screen session to one monitor.
- "Multiple monitors- "Expand to all monitors": Expands the full-screen session across all monitors.

Scale factor: Specifies the desktop scaling in percent.

Possible values:

- "Automatic scaleUser Interface > Display > Options > Monitor-DPI is used for the session.
- Numeric details: The display is magnified by the factor given here.



Printing

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Printing**

- CUPS Printer Redirection(see page 470)
- ezeep by ThinPrint in IGEL OS(see page 471)



CUPS Printer Redirection

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Printing > CUPS Printer Redirection**

CUPS Printer Redirection

CUPS printers configured under **Devices > Printer > CUPS > Printers** are redirected to the AVD session from the local endpoint. To disable/enable a CUPS printer for the AVD session, go to **Devices > Printer > CUPS > Printers > [printer name] > Mapping in sessions > Map printer in AVD sessions**, see [Printers - Configure CUPS Printers in IGEL OS](#)(see page 756).

- ▶ Set the printer driver name under **System > Registry > print.cups.printer%.wvd_printer_driver**:
 - The default Windows driver name is "Microsoft PS Class Driver"; it is usually installed by default and works generically.
 - In the case of a custom printer driver, make sure the driver is installed on the AVD side and enter the exact name of the driver.



ezeep by ThinPrint in IGEL OS

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Printing > ezeep by ThinPrint**

Printing with ezeep

ezeep cloud printing is enabled for the AVD session. To add and enable/disable ezeep printers, go to **Devices > Printer > CUPS > Printer**, see [Printers - Configure CUPS Printers in IGEL OS](#)(see page 756).

Required Custom Commands

You have to add some custom commands and disable workspace-1 option for the AVD session, or ezeep won't work.

Custom Command

(required for Versions 11.06.100 - 11.06.119)

1. Go to **System > Firmware Customization > Base > Initialization**.
2. Add the following custom command:

```
sed -i "s/wvd/avd/g" /usr/share/polkit-1/actions/
com.igel.avd_ezeep_* /services/avd/bin/avd_ezeep_*
systemctl try-restart polkit.service
```
3. Restart your IGEL OS.

Disable Workspace-1 option

(required in all 11.06.xxx Versions)

1. Go to **System > Registry > Sessions > WVD0 > Options > Workspace-1 > enabled**.
2. remove the checkbox



Plugins

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Plugins**

Fabulatech Webcam/Scanner/USB Redirection

The Fabulatech plugin is active for this session. Please note that the individual redirections enabled by the plugin, i.e. webcam redirection, scanner redirection, and USB redirection are configured system-wide under **Sessions > AVD > AVD Global > Plugins > Fabulatech**; see [Fabulatech](#)(see page 456).

The Fabulatech plugin is not active for this session.

Zoom VDI Media Plugin

The audio and video streams for Zoom are redirected between the endpoint devices resp. between the endpoint devices and the Zoom server. Audio and video data is not processed by the AVD server.

The audio and video streams for Zoom are not redirected.



Desktop Integration

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the AVD session.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.



Amazon WorkSpaces

Menu path: **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces > [Session Name]**

Amazon WorkSpaces is a cloud-native desktop virtualization, which is built on the AWS Cloud and used to provide Windows or Linux desktops. For more information, see <https://aws.amazon.com/workspaces/>.

With the integrated Amazon WorkSpaces Client, you can easily configure Amazon WorkSpaces sessions on IGEL OS.

In this area, you can configure desktop integration for the Amazon WorkSpaces session.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

- [Connection Settings](#)(see page 479)
- [Local Settings](#)(see page 480)
- [Network Settings](#)(see page 481)
- [Window](#)(see page 482)
- [Desktop Integration](#)(see page 483)



Connection Settings

Menu path: **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces > [Session Name] > Connection Settings**

Registration code: The WorkSpaces registration code which you got from Amazon

WorkSpace name: Name of the WorkSpace, e.g. `AWS_TechDOC_RD`

Keep me logged in

Login credentials will be saved.



Local Settings

Menu path: **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces > [Session Name] > Local Settings**

Log level

Possible options:

- "Normal logging": Standard logging, which includes info-level details such as runtime events, authorization requests, etc. and is used for informative purposes.
- "Advanced logging": Detailed logging, which includes debug-level details and is used for diagnostic or troubleshooting purposes.
- "Verbose logging": The most detailed logging, which includes trace-level details and is used for very extended diagnostics.

Logs can be found under `/var/tmp/awsc#/Amazon Web Services/Amazon WorkSpaces/logs`.



Network Settings

Menu path: **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces > [Session Name] > Network Settings**

Use proxy

A proxy will be used.

Proxy address: Hostname or IP address of the proxy server

Proxy port: Port on which the proxy service is available



Window

Menu path: **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces > [Session Name] > Window**

Window size

Possible options:

- "Window mode": The session is shown in a standard window.
- "Full-screen mode": The entire display area is used for the session.

High DPI streaming mode

The support for high pixel density (high DPI) displays is activated, and the screen resolution of the WorkSpace matches the high DPI resolution of the monitor. Note that this setting may affect the performance. For more information on high DPI mode, see [WorkSpaces high DPI display support³¹](#).

³¹ https://docs.aws.amazon.com/workspaces/latest/userguide/high_dpi_support.html



Desktop Integration

Menu path: **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces > [Session Name] > Desktop Integration**

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.



Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

Sessions



- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.



deskMate Session

Menu path: **Sessions > deskMate > deskMate Sessions > [Session Name]**

In this area, you can configure desktop integration for the deskMate session.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

- [Provider](#)(see page 489)
- [Options](#)(see page 490)
- [Network](#)(see page 491)
- [Desktop Integration](#)(see page 492)



Provider

Menu path: **Sessions > deskMate > deskMate Sessions > [Session Name] > Provider**

Provider URL: URL to the deskMate portal, issued by your deskMate provider. Example: `https://example.tocario.com`

Login email address: Email address used for logging in to the deskMate session.



Options

Menu path: **Sessions > deskMate > deskMate Sessions > [Session Name] > Options**

Full-screen

The entire display area will be used for the deskMate session.

Clipboard redirection

Clipboard data can be shared between a session and the local computer. (Default)

Display scaling

Local display of the deskMate session can be resized.

Adaptive resolution

The remote desktop resolution will automatically be adjusted in accordance with the local resolution. (Default)

Enable logging

Debug logs will be created.

LogFile destination: Path to the debug logs generated if **Enable logging** is activated. (Default: /userhome/deskmate.log)



Network

Menu path: **Sessions > deskMate > deskMate Sessions > [Session Name] > Network**

Use a proxy server

An HTTP proxy will be used.

Proxy host address: Hostname or IP address of the proxy server

Proxy host port: Port on which the proxy service is available



Desktop Integration

Menu path: **Sessions > deskMate > deskMate Sessions > [Session Name] > Desktop Integration**

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.



Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network



- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.



Unified Communications

Menu path: **Sessions > Unified Communications**

- [Zoom Client Selection in IGEL OS\(see page 496\)](#)
- [Cisco Webex Meetings VDI Selection in IGEL OS\(see page 498\)](#)



Zoom Client Selection in IGEL OS

If you use Zoom optimization, you have to select the required version of the Zoom VDI Media Plugin.

- ⓘ The **Zoom VDI Media Plugin** version must be equal to or less than the version of the server-side Zoom VDI application; a plugin with a higher version is not supported. Zoom recommends updating the Zoom plugin after updating the Zoom VDI application since new features can require an updated plugin. For more information, see the Zoom article [VDI backwards compatibility](#)³².

In addition, you can enable or disable the Smart Virtual Background feature of Zoom.

- ⓘ The Smart Virtual Background feature has a high consumption of CPU power. On weakly equipped endpoint devices, performance issues can occur.

Menu path: **Sessions > Unified Communications > Zoom Client Configuration**

Zoom client version

Selects the Zoom client version to be used for the Zoom VDI Media Plugin. For the included Zoom client versions, see the "Component Versions" section in the IGEL OS release notes.

The Zoom client for the relevant sessions can be activated as follows:

- **Sessions > Citrix > Citrix Global > Unified Communications > VDI Solutions**(see page 85), parameter **Zoom VDI Media Plugin**
- **Sessions > Horizon Client > Horizon Client Global > Unified Communications > VDI Solutions**(see page 194), parameter **Zoom VDI Media Plugin**
- **Sessions > AVD > AVD Sessions > [session name] > Plugins**(see page 472), parameter **Zoom VDI Media Plugin**

- ⚠ When using UMS profiles for configuration, make sure the firmware version the profile is **based on** matches the firmware actually installed on the device (see Creating Profiles). If they do not match and the client version selected via the profile is not included in the firmware, the client version will fall back to default.

Smart Virtual Background Support

Controls whether the Smart Virtual Background feature can be activated by the user.

Possible Options:

- **Off**: Smart Virtual Background cannot be activated.
- **Auto** (default): The system checks whether the hardware supports Smart Virtual Background feature. If this is the case, the feature can be activated.

³² <https://support.zoom.us/hc/en-us/articles/360041602711-VDI-backwards-compatibility>



- **Always:** Smart Virtual Background can be activated irrespective of the hardware.



Cisco Webex Meetings VDI Selection in IGEL OS

When configuring Cisco Webex Meetings, you can select the required version of the Cisco Webex Meetings VDI plugin.

- ⓘ The Cisco Webex Meetings VDI plugin and your server-side application should have the same version. For details on backward compatibility, see [Webex Meetings VDI Release Notes](#)³³.

Menu path: **Sessions > Unified Communications > Cisco Webex Meetings VDI Selection**

Cisco Webex Meetings client version

Selects the version to be used for the Cisco Webex Meetings VDI client. For the included client versions, see the "Component Versions" section in the IGEL OS release notes.

The Cisco Webex Meetings VDI client for the relevant sessions can be activated as follows:

- **Sessions > Citrix > Citrix Global > Unified Communications > Cisco**(see page 85), parameter **Cisco Webex Meetings VDI**
- **Sessions > Horizon Client > Horizon Client Global > Unified Communications > Cisco**(see page 194), parameter **Cisco Webex Meetings VDI**

- ⚠ When using UMS profiles for configuration, make sure the firmware version the profile is **based on** matches the firmware actually installed on the device (see [Creating Profiles](#)). If they do not match and the client version selected via the profile is not included in the firmware, the client version will fall back to default.

³³ https://help.webex.com/en-us/article/glj57y/Release-Notes-for-Cisco-Webex-Meetings-Virtual-Desktop-Software-Release-42.x#Cisco_Reference.dita_fcb4e1d7-dbef-4bab-8842-9b1a8f84a9e5



Accessories

- [ICA Connection Center](#)(see page 500)
- [Terminals](#)(see page 504)
- [Change Smartcard Password](#)(see page 508)
- [Change Password](#)(see page 511)
- [Setup](#)(see page 514)
- [Quick Settings](#)(see page 521)
- [Display Switch](#)(see page 524)
- [Application Launcher](#)(see page 535)
- [Sound Preferences](#)(see page 539)
- [System Log Viewer](#)(see page 545)
- [UMS Registration](#)(see page 550)
- [Touchscreen Calibration](#)(see page 553)
- [Task Manager](#)(see page 557)
- [Screenshot Tool](#)(see page 564)
- [On-Screen Keyboard](#)(see page 568)
- [Monitor Calibration](#)(see page 573)
- [Commands](#)(see page 576)
- [Network Tools](#)(see page 578)
- [Bluetooth Tool](#)(see page 583)
- [System Information](#)(see page 589)
- [Disk Utility](#)(see page 593)
- [Disk Removal](#)(see page 597)
- [Mobile Device Access](#)(see page 599)
- [Firmware Update](#)(see page 602)
- [Smartcard Personalization](#)(see page 606)
- [Identify Monitors](#)(see page 610)
- [Webcam Information](#)(see page 614)
- [ICG Agent Setup](#)(see page 618)
- [Licensing](#)(see page 622)
- [Login Enterprise](#)(see page 625)
- [Connector ID Key Software](#)(see page 626)
- [OS 11 Upgrade](#)(see page 627)
- [Conky System Monitor](#)(see page 630)



ICA Connection Center

Menu path: **Accessories > ICA Connection Center**

With the *Citrix ICA Connection Center*, you are given an overview of the existing connections to *Citrix* servers as well as information regarding connection properties. You can also terminate server connections and log off from *Citrix* servers. For details of how to use the **ICA Connection Center**, see [Using ICA Connection Center](#)(see page 503).

The settings for starting the function are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode\(see page 213\)](#).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode [XDMCP for this Display](#))
- **Desktop Context Menu** (not in appliance mode [XDMCP for this Display](#))
- **Application Launcher** (includes [Application Launcher's system tab](#); not in appliance mode [XDMCP for this Display](#))
- **Hotkey**
- **Autostart** (not in appliance mode [XDMCP for this Display](#))

The session cannot be started in appliance mode.

-
- [Using ICA Connection Center\(see page 503\)](#)



Using ICA Connection Center

To obtain an overview of the existing connections to Citrix servers, proceed as follows:

- ▶ Start the ICA Connection Center. The start options are described under [ICA Connection Center](#)(see page 500). All applications are shown in a tree structure with the associated *Citrix* servers.

- ⓘ With the help of the tree structure, you can see which applications run on which servers. If a number of applications run on the same server, this will make the exchanging of data between these applications easier.

To view the properties of a connection to a *Citrix* server, proceed as follows:

1. Start the ICA Connection Center. The start options are described under [ICA Connection Center](#)(see page 500).
2. Click on the server whose connection properties you want to view.
3. Click on the **Properties** button.
The connection properties as well as constantly updated information regarding the number of incoming and outgoing bytes and frames will be shown.
4. If you would like to reset the counter for incoming and outgoing bytes to 0, click on **Reset**.

To terminate a server connection, proceed as follows:

1. Start the ICA Connection Center. The start options are described under [ICA Connection Center](#)(see page 500).
2. Click on the server whose connection you want to terminate.
3. Click on **Terminate**.
The connection to the server is terminated. The *Citrix* session will be interrupted. The applications will not be terminated on the server. As a result, the application status will be retained until the session is resumed.

To log off from the Citrix server, proceed as follows:

1. Start the ICA Connection Center. The start options are described under [ICA Connection Center](#)(see page 500).
2. Click on the server from which you want to log off.
3. Click on **Log off**.
The connection to the server is terminated. The *Citrix* session will end. The applications on the server will be terminated.



Terminals

Menu path: **Accessories > Terminals > Local Terminal**

With the local terminal, you can execute local commands on your device. For details of how to use the local terminal, see [Using Local Terminal](#)(see page 507).

- ⓘ It is also possible to access a local shell without a terminal session: Alternatively, you can switch to the virtual terminals `tty11` and `tty12` by pressing [Ctrl]+[Alt]+[F11] or [Ctrl]+[Alt]+[F12]. Pressing [Ctrl]+[Alt]+[F1] takes you back to the user interface.

The settings for starting the function are described below.

Session name: Name for the session.

- ❗ The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.



Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.



No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

-
- [Using Local Terminal](#)(see page 507)



Using Local Terminal

To use the local terminal, proceed as follows:

1. Start the local terminal. The start options are described under [Terminals](#)(see page 504).
2. Log in as `user` or `root`.

- ❗ If under **Setup > Security > Password**, in the **Administrator** area, the option **Use password** is enabled, you will need to enter the administrator password to access a local terminal as `root`. If an administrator password is set, accessing a local terminal as `user` is only possible if the following two conditions are met:
- Access to local terminals has been activated for `user`. This is possible with the registry key `system.security.usershell`. The default setting of the registry key forbids terminal access for `user`.
 - Under **Setup > Security > Password**, in the **User** area, the option **Use password** is enabled.
- For accessing a local terminal as `user`, the user password will have to be entered.

You can enter the shell commands supported by IGEL OS.



Change Smartcard Password

Menu path: **Accessories > Change Smartcard Password**

With this function, you can change the password for your IGEL smartcard. For details of how to use the function, see [Using "Change smartcard password" Function\(see page 510\)](#).

Further information regarding the IGEL smartcard can be found under Authentication with IGEL Smartcard.

The settings for starting the function are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

- Using Change Smartcard Password Function(see page 510)



Using Change Smartcard Password Function

With this function, you can change the password for your IGEL smartcard. In order to do this, the **Logon with IGEL smartcard** option must be enabled under **Security > Logon > IGEL Smartcard**.

To change the password for your IGEL smartcard, proceed as follows:

1. Start the **Change Smartcard Password** function. The start options are described under [Change Smartcard Password](#)(see page 508).
2. Enter the following data in the dialog:
 - **Old smartcard password:** Previous password
 - **New smartcard password:** Chosen password
 - **Reenter new smartcard password:** Chosen password (entered again)

The password for your IGEL smartcard will be changed.



Change Password

Menu path: **Accessories > Change Password**

With this function, the user can change the password or PIN for the login method he used for his current session, provided one of the following login methods was used:

- Active Directory with username and password
- Active Directory with third-party smartcard
- IGEL smartcard
- Local user password

i The **Change Password** function starts when the user clicks the password change button in the dialog informing him that a change of password is required. This dialog is presented after login.

For details of how to use the **Change Password** function, see [Using "Change password" function\(see page 513\)](#).

The settings for starting the function are described below.

Session name: Name for the session.

! The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.



Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

ⓘ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows key` = `Ctrl|Super_L`

Key: Key for the hotkey

ⓘ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

- [Using Change Password Function](#)(see page 513)



Using Change Password Function

To change your password for your current login method (Active Directory with user and password, Active Directory with third-party smartcard, IGEL smartcard, or local user with screenlock password), proceed as follows

1. Start the **Change password** function. The start options are described under [Change password\(see page 511\)](#).
2. Enter the changed password or PIN in the dialog. The dialog differs according to the login method that is currently used.
3. Click **OK**.
The password is changed.



Setup

Menu path: **Accessories > Setup**

With the IGEL Setup, you can configure your endpoint device. For details of how to allow the user access to the individual areas of the Setup, see [Setup User Permissions - Define Access to IGEL Setup Areas](#)(see page 516). For details of how to change the setup options, see [Options](#)(see page 520).

The settings for starting the function are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.



Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

ⓘ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows key` = `Ctrl|Super_L`

Key: Key for the hotkey

- ⓘ** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

- [Setup User Permissions - Define Access to IGEL Setup Areas](#)(see page 516)
- [Setup Administrator Permissions - Define Access to IGEL Setup Areas](#)(see page 518)
- [Options](#)(see page 520)

Setup User Permissions - Define Access to IGEL Setup Areas

In the IGEL OS, you can define passwords for different authorization levels (e.g. administrator, setup administrator, setup user, etc.) to protect the system against unauthorized changes, see [Password - Restrict Access to IGEL OS Components](#)(see page 799). If a password was set up for the administrator, the IGEL Setup can only be opened with administrator rights, i.e. after entering the administrator password. However, it can sometimes be necessary to provide access to individual areas of the IGEL Setup for the user. This is usually required to allow the user to change settings like the system language, right/left-handed mouse, keyboard layout, timezone, etc. if they are not preconfigured via a profile.

The following article explains how to specify which options in the IGEL Setup should be visible and/or configurable for the setup user. For details on configuring permissions for the setup administrator, see [Setup Administrator Permissions - Define Access to IGEL Setup Areas](#)(see page 518).

Menu path: **Accessories > Setup > Setup User Permissions**

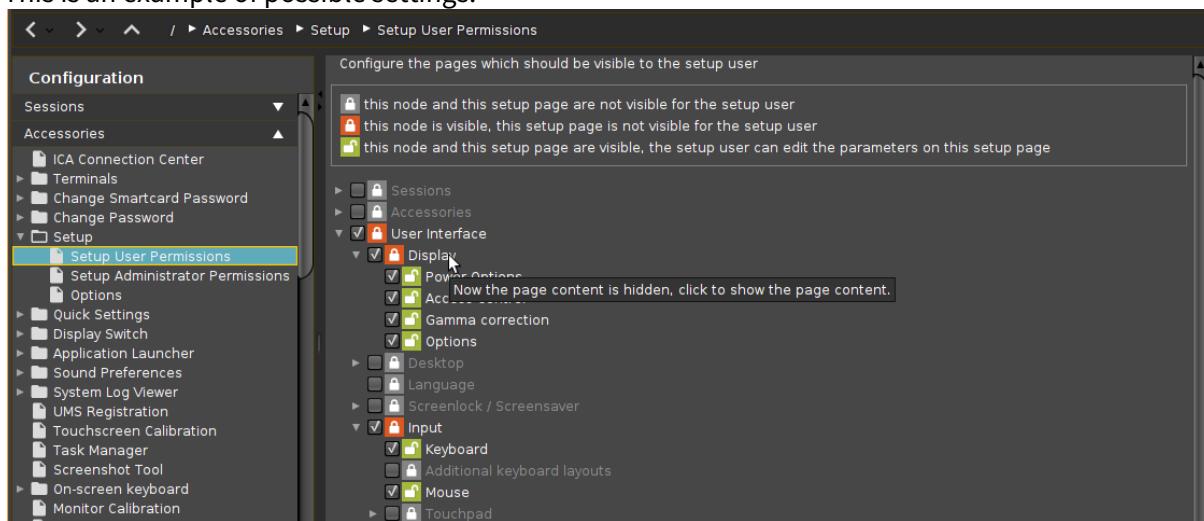
To enable setup pages for the user, proceed as follows:

1. In the Setup, go to **Accessories > Setup > Setup User Permissions** and enable those areas to which the user is to have access.

Possible settings:

	Node	Setup Page
	not visible	not visible
	visible	not visible
	visible	configurable

This is an example of possible settings:





- ⓘ If you enable a setup page on the lower levels, the node points required for access will automatically be marked as visible (but blocked for editing purposes).
 Example: If you activate all sub-nodes under **Display** (see the screenshot above), the higher-level **Display** node will still be marked as , and, therefore, settings on the **Display** page itself will be invisible for the setup user. This means you have to actively mark the higher-level node as if editing has to be enabled.

2. If not already done: Under **Security > Password**(see page 799), enable the password for the **administrator** and the **setup user**.

- ⓘ If users are to be allowed to edit parts of the Setup even without a password, create a **quick setup**(see page 45) session, the password for the **setup user** will not be enabled in this case.



Setup Administrator Permissions - Define Access to IGEL Setup Areas

In the IGEL OS, you can define passwords for different authorization levels (e.g. administrator, setup administrator, setup user, etc.) to protect the system against unauthorized changes, see [Password - Restrict Access to IGEL OS Components](#)(see page 799). If a password was set up for the administrator, the IGEL Setup can only be opened with administrator rights, i.e. after entering the administrator password. However, it can be necessary to provide access to individual areas of the IGEL Setup for administrators performing minor administrative tasks, so that they can change local settings if they are not configured by a profile. This may be required, for example, to allow modifying printer settings or custom commands, adding a new local session like a Chromium browser, etc.

The following article explains how to specify which options in the IGEL Setup should be visible and/or configurable for the setup administrator. For details on configuring permissions for the setup user, see [Setup User Permissions - Define Access to IGEL Setup Areas](#)(see page 516).

Menu path: **Accessories > Setup > Setup Administrator Permissions**

To enable setup pages for the setup administrator, proceed as follows:

1. In the Setup, go to **Accessories > Setup > Setup Administrator Permissions** and enable those areas to which the setup administrator is to have access.

Possible settings:

	Node	Setup Page
	not visible	not visible
	visible	not visible
	visible	configurable

This is an example of possible settings:



- i** If you enable a setup page on the lower levels, the node points required for access will automatically be marked as visible (but blocked for editing purposes).
Example: If you activate all sub-nodes under **Display** (see the screenshot above), the higher-level **Display** node will still be marked as , and, therefore, settings on the **Display** page itself will be invisible for the setup administrator. This means you have to actively mark the higher-level node as if editing has to be enabled.

2. If not already done: Under **Security > Password**(see page 799), enable the password for the **administrator** and the **setup administrator**.

- i** If administrators are to be allowed to edit parts of the setup even without a password, create a [quick setup](#)(see page 45) session, the password for the **setup administrator** will not be enabled in this case.



Options

Menu path: **Accessories > Setup > Options**

You can configure the display of tooltips in the setup.

Enable Tooltips

- When the mouse pointer is placed over a parameter, the associated tooltip will be shown after the set **delay**.
- No tooltip will be shown.

Tooltip Delay: Time interval in tenths of a second during which the mouse pointer must be placed over a parameter for the tooltip to be shown.



Quick Settings

Menu path: **Accessories > Quick Settings**

With the IGEL Setup, you can allow the user access to individual areas of the Setup. Instructions can be found under [Setup User Permissions - Define Access to IGEL Setup Areas](#)(see page 516).

The settings for starting the function are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.



Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

ⓘ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with | :

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

- ⓘ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

-
- [Setup User Permissions](#)(see page 523)



Setup User Permissions

Menu path: **Accessories > Quick Settings > Setup User Permissions**

Define which setup pages are visible to users.

You will find instructions for this function under [Setup User Permissions - Define Access to IGEL Setup Areas\(see page 516\)](#).



Display Switch

Menu path: **Accessories > Display Switch**

With this function, you can configure the display on several screens. For details of how to set the function, see [Options](#)(see page 527). For details of how to use the function, see [Using "Display Switch" Function](#)(see page 532).

The settings for starting the function are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.



- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode [XDMCP for this Display](#))
- **Desktop Context Menu** (not in appliance mode [XDMCP for this Display](#))
- **Application Launcher** (includes [Application Launcher's system tab](#); not in appliance mode [XDMCP for this Display](#))
- **Hotkey**
- **Autostart** (not in appliance mode [XDMCP for this Display](#))

The session cannot be started in appliance mode.

-
- [Options](#)(see page 527)
 - [Minimal Dialog](#)(see page 529)
 - [Advanced Dialog](#)(see page 531)
 - [Using Display Switch](#)(see page 532)



Options

Menu path: **Accessories > Display Switch > Options**

You can change the way the **Display Switch** function behaves.

Dialog type

Possible values:

- Minimal dialog: The **Display Switch** function starts with the simple dialog.
- Advanced dialog: The **Display Switch** function starts with the advanced dialog.

Smart display configuration

Every configuration of your monitors will be saved.

Monitor configurations will not be saved.

Preserve settings over reboot

The settings for the **Display Switch** function will be preserved over a reboot.

The settings for the **Display Switch** function will be reset to the default settings in the event of a reboot. (Default)

Configure new displays when connected

The **Display Switch** function starts as soon as new screens are connected. You can then configure the new screens.

The **Display Switch** function does not start automatically when new screens are connected. (Default)

Options in Minimal Dialog

Mirror displays

The **Mirror screens** option is shown in the minimal dialog. (Default)

The option is not shown in the minimal dialog.

Extend to the left

The **Extend to the left** option is shown in the minimal dialog. (Default)

The option is not shown in the minimal dialog.

Extend to the right

The **Extend to the right** option is shown in the minimal dialog. (Default)

The option is not shown in the minimal dialog.

Rotate displays (Page orientation)

The **Rotate displays (Page orientation)** option is shown in the minimal dialog.

The option is not shown in the minimal dialog. (Default)

Mouse options

The **Left-handed mouse, Pointer speed** and **Double click interval** settings are shown.

The mouse settings are not shown. (Default)



Advanced

- The **Advanced** button is shown. With **Advanced**, you can switch to the advanced dialog. (Default)
 The **Advanced** button is not shown.

Reset

- The **Reset** button is shown. With **Reset**, you can restore the default settings. (Default)
 The **Reset** button is not shown.

Timeout for confirmation dialog: Specifies how long a dialog for confirming the configuration should be shown. (Default: 10 seconds)

For more information, see the manual chapters

- [Minimal Dialog](#)(see page 529)
- [Advanced Dialog](#)(see page 531)
- [Using Display Switch](#)(see page 532)

or the how-to [Display Switch](#).

Minimal Dialog

Selection	Function
	Uses only display 1.
	Shows the same content on all screens, i.e. clone mode or mirroring.
	Extends the display area to the screen on the right.
	Extends the display area to the screen on the left
	Uses only display 2.
	Rotates the selected display to the left or to the right.

Identify Displays: Starts the monitor detection.

Advanced: Switches to **Advanced** mode of display configuration.

Reset: Restores the default settings.

Close: Closes the **IGEL Display Switch** window.

Mouse options

- **Lefthand Mode**

Lefthand mode is active.

Righthand mode is active. (Default)



- **Pointer speed:** Value for the mouse speed in percentage between 1 (slow) and 100 (fast). (Default: 50)
- **Double click:** Maximum interval in milliseconds between two mouse clicks to still be recognized as a double-click. (Default: 300)

For more information, see [Using Display Switch](#)(see page 532) and [Display Switch](#).



Advanced Dialog

You can access the advanced settings by clicking **Advanced** in the minimal dialog.

Advanced settings (pan/scale/resolution) can be configured in a collapsible area on the right. To enlarge the **Advanced** modes window, click the arrow on the right side of the window.

The following parameters must be activated for the **Display Switch** function to be able to save the settings:

- **Display Switch > Options > Preserve settings over reboot**
- **Display Switch > Options > Smart display configuration**

In the collapsible area:

- **Use this display**
 Enables the selected display.
 Disables the selected display.

- **Index:** Give the selected display an order number.

- **Rotation:** Rotation of selected display

Possible values:

- None
- Left
- Inverted
- Right

- **Resolution:** Select the resolution of the selected display. (Default: Automatic)

- **Refresh rate:** Depends on the resolution (Default: Automatic)

- **Panning:** Set up a virtual screen that is larger than your physical screen. It will look like an enlarged screen. By moving the mouse to the edge of the screen, hidden parts become visible. (Default: None)

- **Reflection:** Transforms the display as if being reflected by a mirror.

Possible values:

- None
- Horizontal
- Vertical
- Horizontal and Vertical

- **Scale from:** A software variant of the resolution. This can be useful if you need a resolution that is not available on the hardware. (Default: None)

For more information, see the articles [Using Display Switch](#)(see page 532) and [Display Switch](#).



Using Display Switch

The function **Display Switch** has been extended with IGEL OS 11.01.100. It is now possible to use several different profiles, which are automatically selected at runtime depending on the currently connected monitors.

A profile is created when the current monitor layout, or the current resolution, is configured via **Display Switch**. The profile is automatically assigned to the currently connected monitors and recognizes the manufacturer, model by plug and, if available, the status of the laptop cover. When the screen configuration changes (by hot (un)plugging), the system will automatically switch to the profile.

The **Display Switch** function has been redesigned in IGEL OS 11.01.100 with a new graphical user interface. All basic functions can be configured by drag-and-drop.

- ▶ Start the **Display Switch** function. The start options are described under [Display Switch](#)(see page 524).

Identify Displays

- ▶ To start screen detection, click on **Identify Displays**

The names and properties of the screens will be detected. The connection, the assigned number (**1** = main screen) and the name will be shown on each screen. Example: **1: DVI-D(II): Samsung 24"**

Defining Main Screen

1. If necessary, switch to the advanced dialog with **Advanced**.
2. Select the screen that you wish to define as the main screen.
3. Set the **Index** to 1.
The display is now marked as the main screen.

Split Display over Several Screens

You have various options for using several screens. In the dialog, the connection, the assigned number (**1** = main screen) and the name is shown for each screen. Example: **1: DVI-D(II): Samsung 24"**

The procedure with the minimal dialog is described below. To switch from the advanced to the minimal dialog, click on **Simple**.

- ▶ To show the same content on all screens (Shadow screens), click on .
- ▶ If you would like to expand the display to all screens and the other screens are to the left of the main screen, click on .
- ▶ If you would like to expand the display to all screens and the other screens are to the right of the main screen, click on .

From IGEL OS 11.01.100, a drag-and-drop interface is available for individual customization. Click **Advanced** to show the drag-and-drop interface:

- ▶ Use drag-and-drop to move the displays to the desired configuration. They will snap together when they touch each other at the edge.



- ▶ If you no longer need a monitor, in **Advanced** mode you can simply drag it to the upper right corner to the **Disabled** area to disable it.
- ▶ To display the same content on multiple displays, drag them one on top the other. **Mirror \<other>** will be displayed. The mirroring monitor is displayed in the lower right corner.
- ▶ Click **Apply** to set the current status. Click **Yes** in the **Keep Configuration** window to save the configuration permanently and associate it with the profile.

Rotate Displays (Page Orientation)

The procedure with the minimal dialog is described below; **Setup > Accessories > Display Switch > Options > Rotate displays (Page orientation)** must be enabled. To switch from the advanced to the minimal dialog, click on **Basic**.

- ▶ To rotate the display counterclockwise, click on .
- ▶ To rotate the display clockwise, click on .

Change Mouse Settings

The procedure with the minimal dialog is described below; **Setup > Accessories > Display Switch > Options > Mouse Options** must be enabled. To switch from the advanced to the minimal dialog, click on **Simple**.

- ▶ To adjust the mouse for left-handed users, enable the **Lefthanded Mode**.
- ▶ To adjust the speed of the mouse pointer, change the value under **Pointer speed**. The higher the value, the further the mouse pointer will move when the mouse is moved.
- ▶ To change the time interval within which two consecutive mouse clicks are recognized as a double-click, change the number of milliseconds under **Double click interval**.

Zoom Display (Screen Magnifying Glass)

You can magnify the screen content. The effect is the same as with the screen magnifying glass in Microsoft Windows: All text and graphics are magnified by the same factor; this results in a virtual display area which is bigger than the monitor's available display area. The user therefore sees a magnified section of the entire screen; the section can be moved by moving the mouse to the edge of the screen.

1. If necessary, switch to the advanced dialog with **Advanced**.
2. Under **Panning**, set the desired value. Example: 3860x2160
3. Under **Resolution**, set a low value. This value simulates the actual resolution of the screen.
Example: **1280x800**
4. Click on **Apply**.
The screen content will be magnified. The magnification factor results from the ratio of the virtual resolution and the simulated actual resolution.



- i** If the same content is displayed on a number of screens (Shadow screens), all screens will show the same section. However, you can set a different magnification level for each of the screens.

Change Refresh Rate

- i** This is only possible if a resolution has been selected. The respective resolutions can be different. A refresh rate of 60 Hz is usually suitable for standard screens.
1. If necessary, switch to the advanced dialog with **Advanced**.
 2. Under **Refresh rate**, set the desired value.

Restore Default Settings

- Click on **Reset** to restore the default settings.

For more information, see the article [Display Switch](#).



Application Launcher

Menu path: **Accessories > Application Launcher**

With the Application Launcher, you can launch predefined sessions and device functions/tools. You are also given information regarding the device and the licenses used.

Further information can be found under [Application Launcher\(see page 35\)](#).

The settings for starting the function are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode [XDMCP for this Display](#))
- **Desktop Context Menu** (not in appliance mode [XDMCP for this Display](#))
- **Application Launcher** (includes [Application Launcher's system tab](#); not in appliance mode [XDMCP for this Display](#))
- **Hotkey**
- **Autostart** (not in appliance mode [XDMCP for this Display](#))

The session cannot be started in appliance mode.

-
- [Application Launcher Configuration](#)(see page 538)



Application Launcher Configuration

Menu path: **Setup > Accessories > Application Launcher > Application Launcher Configuration**

You can hide individual areas and elements of the Application Launcher.

- **Hide system page**

- The button for displaying the system tools (accessories) will not be shown.
- The button for displaying the system tools (accessories) will be shown. (default)

- **Hide reboot button**

- The button for restarting the thin client will not be shown.
- The button for restarting the thin client will be shown. (default)

- **Hide shut down button**

- The button for shutting down the thin client will not be shown.
- The button for shutting down the thin client will be shown. (default)

- **Show current user name in about, application launcher and startmenu**

- The current user will be shown at the top edge of the relevant window.
- The current user will not be shown.

In order for user names to be recognized and passed on, you must configure two settings beforehand:

- Enable Active Directory/Kerberos: **Security > Active Directory/Kerberos**
- Enable local logon: **Security > Logon > Active Directory/Kerberos**

- **Single click mode:**

- Sessions are started with a single-click. This option was set up specially for users of touchscreen monitors.
- Sessions are started with a double-click. (default)



Sound Preferences

Menu path: **Accessories > Sound Preferences**

With this function, you can configure your device's audio system. For details of how to change the presets for the audio system, see [Options\(see page 542\)](#). For details of how to use the function, see [Using "Sound Preferences" Function\(see page 544\)](#).

The settings for starting the function are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode [XDMCP for this Display](#))
- **Desktop Context Menu** (not in appliance mode [XDMCP for this Display](#))
- **Application Launcher** (includes [Application Launcher's system tab](#); not in appliance mode [XDMCP for this Display](#))
- **Hotkey**
- **Autostart** (not in appliance mode [XDMCP for this Display](#))

The session cannot be started in appliance mode.

-
- [Options](#)(see page 542)
 - [Using Sound Preferences Function](#)(see page 544)



Options

Menu path: **Accessories > Sound Preferences > Options**

With this function, you can change presets for the audio system. The settings can be changed at any time via the "Sound Preferences" function; see [Using "Sound Preferences" function\(see page 544\)](#).

Show volume control in taskbar

- The button is shown in the taskbar. When the user clicks on this button, the volume control will be shown. (Default)
- The button will not be shown. The user must start the Audio Settings function to change the volume. Further information can be found under [Using "Sound preferences" function\(see page 539\)](#).

Remote volume settings

- The settings for the parameters **Mute**, **PCM volume**, **Input mute**, and **Input volume** are restored after each system restart.
- The last settings set by the user will remain after the next system start. (Default)

Mute

- Audio playback is off.
- Audio playback is on. (Default)

PCM volume: Preset volume in percent (default: 50)

Input mute

- The audio input is muted. Sounds from a microphone that are recorded are not transferred via the thin client.
- The audio input is switched on. Sounds from a microphone that are recorded can be transferred via the thin client. (Default)

Input volume: Volume in percent at which sounds at the audio input are recorded, for example from a microphone. (Default: 100)

Default Sound Output

Port name

Possible options:

- Automatic: The audio output is automatically assigned to a device. The following order applies here:
 1. USB devices
 2. PCI devices; this also includes the HDMI interface.
 3. Internal speakerNot connected ports will be ignored.
- HDMI / DisplayPort
- Speaker
- Headset



Device name: Select the device for audio output from a list of available devices. If the device is not present at the moment, you can type its name in. Examples: "Built-in Audio Analog Stereo", "Microsoft LifeChat LX-3000".

Default Sound Input

Port name

Possible options:

- Automatic: The audio input is automatically assigned to a device. The following order applies here:
 1. USB devices
 2. PCI devicesNot connected ports will be ignored.
- Microphone
- Headset microphone

Device name: Select the device for audio input from a list of available devices. If the device is not present at the moment, you can type its name in. Example: "Microsoft LifeChat LX-3000".



Using Sound Preferences Function

- ▶ Start the **Sound Preferences** function. The start options are described under [Sound Preferences\(see page 539\)](#).

To change the playback volume, proceed as follows:

- ▶ Move the playback volume slider to the right to increase the volume or to the left to reduce the volume.

To select and configure the device for playback, proceed as follows:

1. Click on the **Output** tab.
2. Under **Play sound through**, select the device which is to be used for playback.
3. If necessary, adjust the **Balance**, **Fade** and **Subwoofer** settings.

To select and configure the device for recording, proceed as follows:

1. Click on the **Input** tab.
2. Under **Record sound from**, select the device which is to be used for recording.
3. Adjust the **Input volume** if necessary.

To change the playback volume for specific applications, proceed as follows:

1. Click on the **Applications** tab.
2. Adjust the volume control for the relevant application.



System Log Viewer

Menu path: **Accessories > System Log Viewer**

With this function, you can view your device's system logs. For details of how to add additional logs to the logs shown by default, see [Options\(see page 548\)](#). For details of how to use the function, see [Using “System Log Viewer” function\(see page 549\)](#).

The settings for starting the function are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.



Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

ⓘ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with | :

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

- ⓘ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).



The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

- [Options\(see page 548\)](#)
- [Using System Log Viewer Function\(see page 549\)](#)



Options

Menu path: **Setup > Accessories > System Log Viewer > Options**

Here, you can add additional files to the files shown by default. The **System Log Viewer** function shows the following files by default:

- /config/Xserver/card0
- /config/Xserver/xorg.conf-0
- /config/sound/card0
- /config/sound/card1
- /config/sound/default_card_name
- /var/log/Xorg.0.log

To add a further file to the display, proceed as follows:

1. Click on **[+]**.
2. In the **Add** dialog, enter the path and the file name of the desired file. Example: `/var/log/igfmount.log`

(i) If you want to add several files, you can also use the asterisk *. Example: `/var/log/ *.log` or `/var/log/ *.txt`
3. Click **OK**.
When the **System Log Viewer** function is started, the file that you have added will be shown.



Using System Log Viewer Function

1. Start the **System Log Viewer** function. The start options are described under [System Log Viewer](#)(see page 545).
2. In the left-hand column, select the file that you want to view.
The selected file will be shown in the right-hand column.



UMS Registration

Menu path: **Accessories > UMS Registration**

With this function, you can register your endpoint device in the *UMS (IGEL Universal Management Suite)* locally. For details of how to use the function, see [Using "UMS Registration" Function](#)(see page 552).

The settings for starting the function are described below.

Session name: Name for the session.

The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.



- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in `(keysym 0xff09, Tab)`

- Using UMS Registration Function (see page 552)



Using UMS Registration Function

Menu path: **Accessories > UMS Registration**

1. Start the **UMS Registration** function. The start options are described under [UMS Registration\(see page 550\)](#).
2. Enter the following data:
 - **Server address:** IP address or host name and port number of the UMS Server if it is not the default port. Example: `IP address:30002`
 - **Login:** User name for logging in to the UMS Console.
 - **Password:** Password for logging in to the UMS Console.

i Any UMS user with sufficient rights can be specified under **Login** and **Password**.
Example:
If a device has to be registered in the root folder "Devices", "scan for devices" permission will suffice.
If a device has to be registered in a particular folder, the user must also have the "move" permission for this folder.

- **Structure Tag:** Character string for assigning the device to a specific UMS directory.
 - **New host name:** Name under which the device is registered in the UMS. This name will also be displayed under **Network > LAN Interfaces > Terminal name**.
3. If you want to assign a specific UMS directory to the device, click on **Select** under **Directory** and select the desired directory from the list.
 4. Click on **Register**.



Touchscreen Calibration

Menu path: **Accessories > Touchscreen Calibration**

With this function, you can calibrate the touchscreen connected to your endpoint device. For details of how to use the function, see [Using “Touchscreen Calibration” function](#)(see page 556).

The settings for starting the function are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.



- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode [XDMCP for this Display](#))
- **Desktop Context Menu** (not in appliance mode [XDMCP for this Display](#))
- **Application Launcher** (includes [Application Launcher's system tab](#); not in appliance mode [XDMCP for this Display](#))
- **Hotkey**
- **Autostart** (not in appliance mode [XDMCP for this Display](#))

The session cannot be started in appliance mode.

-
- [Using Touchscreen Calibration](#)(see page 556)



Using Touchscreen Calibration

- ▶ Ensure that **Enable touchscreen** is enabled under **User Interface > Input > Touchscreen**.

You will find a description of the touchscreen calibration procedure in the Touchscreen Calibration how-to.



Task Manager

Menu path: **Accessories > Task Manager**

This function provides an overview of the applications and other processes running on the device. You can also pause or end processes and change the priority of processes. For details of how to use the Task Manager, see [Using Task Manager](#)(see page 560).

The settings for starting the function are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode [XDMCP for this Display](#))
- **Desktop Context Menu** (not in appliance mode [XDMCP for this Display](#))
- **Application Launcher** (includes [Application Launcher's system tab](#); not in appliance mode [XDMCP for this Display](#))
- **Hotkey**
- **Autostart** (not in appliance mode [XDMCP for this Display](#))

The session cannot be started in appliance mode.

-
- [Using Task Manager](#)(see page 560)



Using Task Manager

With the Task Manager, you can observe and influence applications and processes in the following ways:

- Determining thin client processor usage
- Determining thin client memory usage
- Determining processor usage by a specific application
- Determining memory usage by a specific application
- Pausing and continuing an application
- Closing an application
- Force closing an application
- Changing the priority of an application

- Launch the **Task Manager** function. The launch options are described under [Task Manager](#)(see page 557).

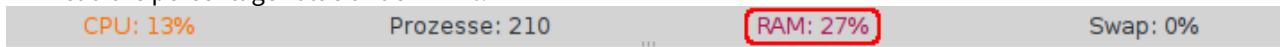
To determine the thin client's total processor usage, proceed as follows:

- Read the percentage value under **CPU**:



To determine the thin client's total memory usage, proceed as follows:

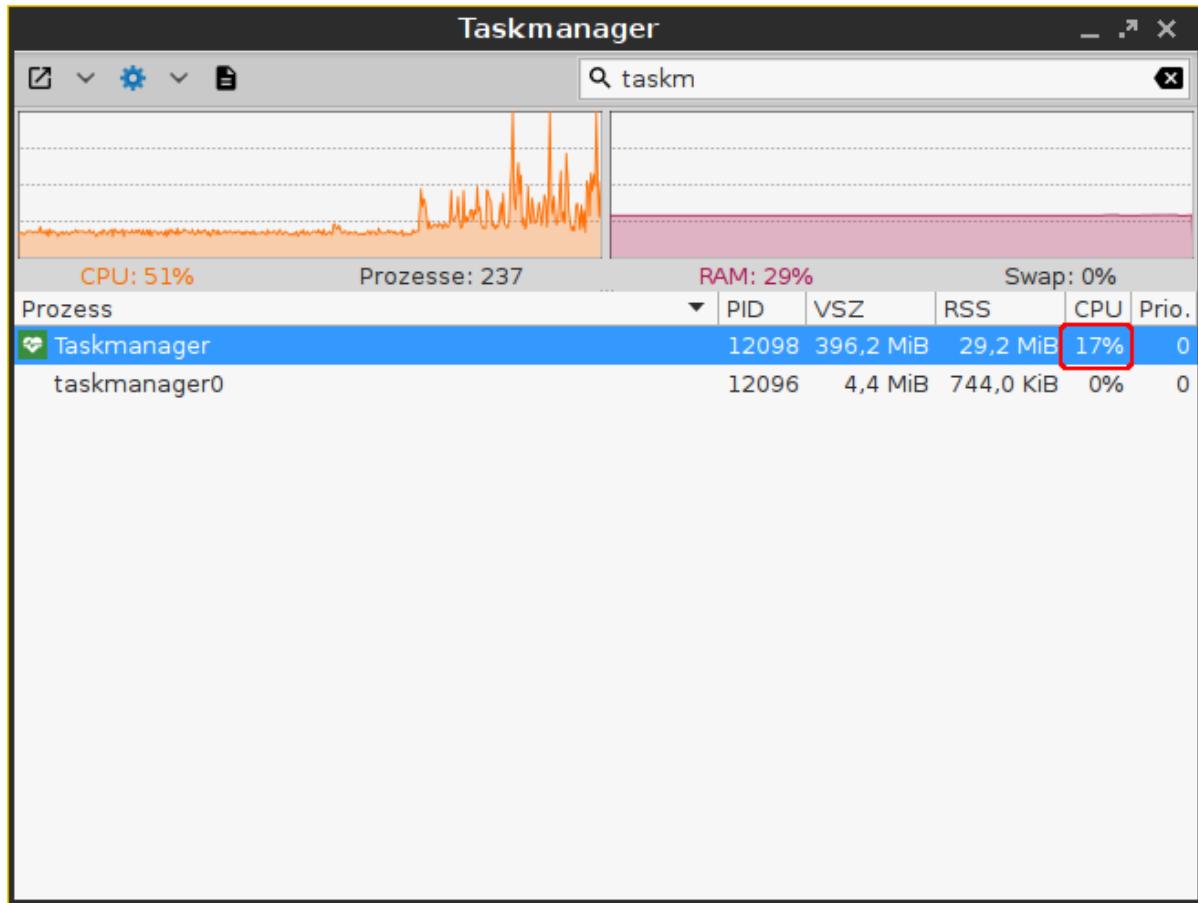
- Read the percentage value under **RAM**:



- To calculate the value in bytes, click on and enable the option **Show memory usage in bytes**.

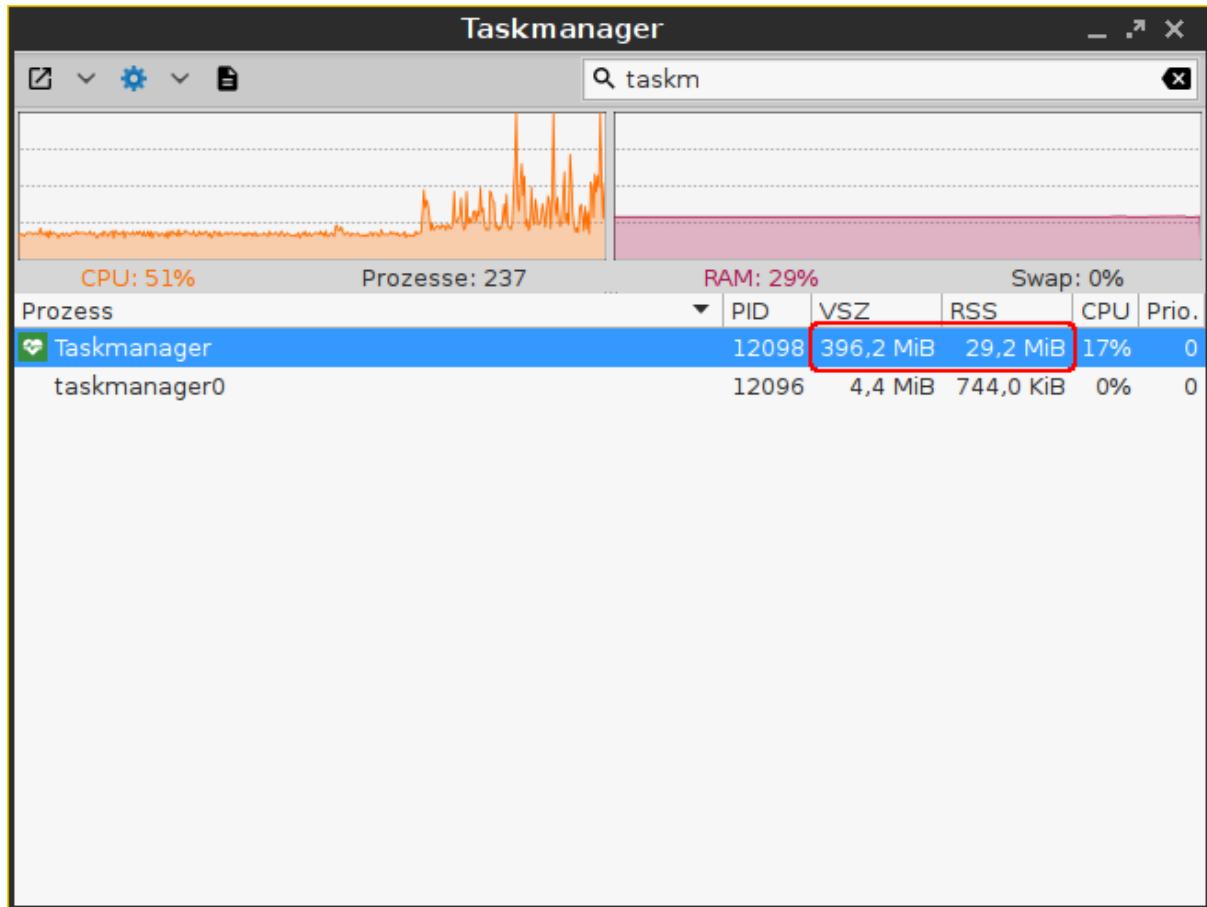
To determine the extent to which a specific application contributes to processor usage, proceed as follows:

1. In the search window, enter the name of the application or part of the name.
The Task Manager will now show only the relevant applications and processes.
2. Read the percentage value for the relevant application in the **CPU** column.



To determine the extent to which a specific application contributes to memory usage, proceed as follows:

1. Click next to on and ensure that **Virtual Bytes** and **Private Bytes** are enabled.
2. In the search window, enter the name of the application or part of the name.
The Task Manager will now show only the relevant applications and processes.
3. Read the values in the **VSZ** and **RSS** columns.
The **VSZ** column shows how much memory is available for the application. The **RSS** column shows how much memory the application is currently using.



To pause an application, proceed as follows:

1. Highlight the application.
2. Open the application's context menu by right-clicking on it and select **Pause**.
The application will be paused (Signal SIGSTOP). You can then continue the application.

To continue an application, proceed as follows:

1. Highlight the application.
2. Open the application's context menu by right-clicking on it and select **Continue**.
The application will continue (Signal SIGCONT).

To close an application, proceed as follows:

1. Highlight the application.
2. Open the application's context menu by right-clicking on it and select **Close**.
The application will close (Signal SIGTERM).

- ⓘ In this case, the application is instructed to close by the operating system. If the application does not react to this instruction, you can force it to close with the **Kill** command.

To force an application to close, proceed as follows:

1. Highlight the application.
2. Open the application's context menu by right-clicking on it and select **Kill**.
The application will be forced to close (Signal SIGKILL).

To change the priority of an application, proceed as follows:

1. Highlight the application.
2. Open the application's context menu by right-clicking on it and select **Priority**.
3. Select one of the following values for the priority:

- ⓘ As a normal user, you can only change the priority from a higher value to a lower value.
Example: If you have changed the priority from "Normal" to "Low", you can only then change it to "Very low" – you can no longer change it back to "Normal". The administrator can increase the priority.
- ⓘ The priority corresponds to the nice value. High values result in a low priority, while low values result in a high priority.

- **Very low** (nice value: 15)
- **Low** (nice value: 5)
- **Normal** (nice value: 0)
- **High** (nice value: -5). This value can only be set by the administrator.
- **Very high** (nice value: -15) This value can only be set by the administrator.



Screenshot Tool

Menu path: **Accessories > Screenshot Tool**

With this function, you can take a screenshot. For details of how to use the function, see [Using “Screenshot Tool”](#)(see page 567).

The settings for starting the function are described below.

Session name: Name for the session.

The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.



- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

Special Hotkeys

With the hotkeys defined under **User Interface > Hotkeys > Commands**, you can use the function as follows:

- **Screenshot of the active window:** This hotkey takes a screenshot of the window currently active.
 - **Screenshot of the entire screen:** This hotkey takes a screenshot of the entire screen.
-
- [Using Screenshot Tool](#)(see page 567)



Using Screenshot Tool

1. Launch the **Screenshot Tool** function. The launch options are described under [Screenshot Tool](#)(see page 564).
2. Select the **area** you would like to photograph. You have the following options:

i If you start the function via **User Interface > Hotkeys > Commands > Screenshot of active window** or **User Interface > Hotkeys > Commands > Screenshot of entire screen**, no options will be shown.

- **Entire screen**
 The entire screen content will be photographed.
- **Active window**
 The window that is currently active will be photographed.
- **Select a region**
 You can select a section of the screen using the mouse.
- **Capture mouse pointer**
 The mouse pointer is visible on the screenshot.

3. Specify the **Delay before capturing** in seconds. The minimum value is 1.
4. Click on **OK**.

If you have enabled **Entire screen** or **Active window**, the screenshot will be taken after the **Delay before capturing** has elapsed.

If you have enabled **Select a region**, you can select the desired part of the screen using the mouse. To do this, press and hold the left mouse button while dragging the mouse across the screen.

5. Specify how the screenshot is to be used. You have the following options:

- **Save:** If this option is enabled, the screenshot will be saved in PNG format via your thin client. You can save the screenshot locally, on a network drive or on a USB mass storage device.
- **Copy to the clipboard:** If this option is enabled, the screenshot will be available in the thin client's local cache. You can access the local cache from an RDP session and open the image in an RDP session application.
- **Open with:** If this option is enabled, the screenshot will be opened in your thin client's image viewer as soon as it is taken.



On-Screen Keyboard

Menu path: **Accessories > On-Screen Keyboard**

This function shows an on-screen keyboard on the desktop.

The settings for starting the function are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.



- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode\(see page 213\)](#).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

-
- [Appearance\(see page 570\)](#)
 - [Application Integration\(see page 571\)](#)



Apearance

Menu path: **Accessories > On-Screen Keyboard > Appearance**

- **Show Function Keys**

The on-screen keyboard features the function keys [F1] ... [F12]. (default)

- **Show Navigation Keys**

The on-screen keyboard features the arrow keys for navigating on the screen. (default)

- **Show Numpad**

The on-screen keyboard features the number block.

The on-screen keyboard does not feature the number block. (default)

- **Enable switching to alternative layout**

This option is available from IGEL Linux version 10.04.100 onwards.

The on-screen keyboard has an additional key by which the user can toggle between the normal layout and a reduced layout. The reduced layout resembles the numpad, with the following differences:

- Additional backspace key [\leftarrow]

- Additional tab key [$\overleftarrow{\overrightarrow{t}}$]

- Additional space key []

- Additional escape key [Esc]

- Return key [\square] instead of [Enter] key

Switching to the reduced layout is not possible. (default)



Application Integration

Taskbar settings for the login dialog

These settings are relevant if a login is necessary in order to use the device. This applies to all logon methods that are possible with the device.

Show on-screen keyboard button

- A button for launching the on-screen keyboard will be shown during the login dialog.
- The on-screen keyboard cannot be launched during the login dialog. (Default)

Start on-screen keyboard automatically

- The on-screen keyboard is shown during the login dialog. The on-screen keyboard can be used for input in the logon dialog.
- The on-screen keyboard is not shown during the login dialog. However, it can be launched via a button if **Show on-screen keyboard button** is enabled. (Default)

Taskbar settings when the screenlock is active

Show on-screen keyboard button

- If the screen is locked, a button for launching the on-screen keyboard will be shown.
- If the screen is locked, the on-screen keyboard cannot be launched. (Default)

Start on-screen keyboard automatically

- If the screen is locked, the on-screen keyboard will be shown.
- If the screen is locked, the on-screen keyboard will not be shown. However, it can be launched via a button if **Show on-screen keyboard button** is enabled. (Default)

On-Screen Keyboard Toggle Button

Show button

- A button for switching the on-screen keyboard on and off will be shown on the desktop.
- The button will not be shown. (Default)

Touch and hold delay: Time in milliseconds, after which the button reacts to movement. (Default: 1000 ms)

Button size: A size between 40 and 80 pixels can be chosen. (Default: 60px)

Automatically show on-screen keyboard when text field is selected

- The on-screen keyboard is shown automatically when an input field gets the focus.
- The on-screen keyboard is not shown automatically.



For further information, see Configuring the Automatic Appearance of on-screen software keyboard.



Monitor Calibration

Menu path: **Accessories > Monitor Calibration**

With this function, you can calibrate the monitor connected to your endpoint device.

A test image which you can modify using the arrow keys will appear. Using this test image, you can automatically or manually recalibrate your screen. This applies to old, analog monitors in particular. New monitors calibrate themselves.

The settings for starting the function are described below.

Session name: Name for the session.

! The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.



Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.



Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.



Commands

Menu path: **Accessories > Commands**

The following system commands can be made accessible to the user:

- **Logoff:** Logs the user off from the device.
- **Reboot Terminal:** Restarts the device.
- **Restart windowmanager:** Restarts the device's user interface.
- **Shutdown terminal:** Shuts down the device.
- **Sort icons:** Sorts the symbols on the desktop so that they form a block.

► To edit a user command, double click the relevant entry in the list.

If you have made changes to the hotkey, you can check these by clicking the relevant entry in the **Key** column.

You can change the following starting methods:

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.



Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.



Network Tools

Menu path: **Accessories > Network Tools**

This function provides the following tools for network analysis:

- **Devices**
- **Ping**
- **Netstat**
- **Traceroute**
- **Lookup**

For how to use the network tools, see [Using “Network Tools” function - Devices](#)(see page 581).

The settings for starting the function are described below.

Session name: Name for the session.

The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.



Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

ⓘ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows key` = `Ctrl|Super_L`

Key: Key for the hotkey

ⓘ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.



Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

-
- [Using Network Tools Function](#)(see page 581)



Using Network Tools Function

- ▶ Start the **Network Tools** function. The start options are described under [Network Tools](#)(see page 578).

To obtain information regarding a network device available on your thin client, proceed as follows:

1. Click on the **Devices** tab.
2. Under **Network device**, select the network device for which you would like to obtain information.
The information regarding the selected network device will be shown.

To send a ping query to a device in your network, proceed as follows:

1. Click on the **Ping** tab.
2. Under **Network address**, enter the IP address or the host name of the device to which you would like to send a ping query.
3. If necessary, add the number of ping queries under **Send**.
4. Click on the **Ping** button.
The set number of ping queries will be sent. The results will then be shown.

To obtain information regarding the network status of your thin client, proceed as follows:

1. Click on the **Netstat** tab.
2. Select the desired information under Display:
 - **Routing Table Information**
 - **Active Network Services**
 - **Multicast Information**
3. Click on the **Netstat** button.
The desired information will be shown.

To identify the router via which an IP data packet from your thin client reaches a specific target computer, proceed as follows:

1. Click on the **Traceroute** tab.
2. Under **Network address**, give the IP address of the target computer.
3. Click on the **Trace** button.
The thin client will send IP packets to the target computer at short intervals, each with a TTL (Time To Live, i.e. maximum number of hops) increased by 1.
When the packet reaches the target computer, "reached" will be shown in the last line and no further packet will be sent.
If no computer replies, "no reply" will be shown.

With the **Lookup** function, you can request DNS information regarding any address on the Internet from your thin client.

Further information regarding the DNS (Domain Name System) can be found on Wikipedia under [Domain Name System](#)³⁴.

Detailed descriptions of the Domain Name concept can be found in [RFC 1034](#)³⁵ and in related RFCs.

To obtain DNS information regarding an address on the Internet, proceed as follows:

³⁴ https://en.wikipedia.org/wiki/Domain_Name_System

³⁵ <https://tools.ietf.org/html/rfc1034>



1. Click on the **Lookup** tab.
2. Under **Network address**, give the IP address or the host name.
3. Under **Information type**, select which information is to be shown. The following information types are available:
 - Default information
 - Internet address
 - Canonical name
 - Processor type/operating system
 - Mailbox exchange
 - Mailbox information
 - Name server
 - Computer name for address
 - Text information
 - Generally known services
 - Any / all information
4. Click on **Lookup**.
The desired information will be shown.



Bluetooth Tool

Menu path: **Accessories > Bluetooth Tool**

With the **Bluetooth Tool**, you can connect Bluetooth devices, e.g. a keyboard, a mouse, or a headset, to your thin client. For details of how to use the function, see [Using Bluetooth Tool](#)(see page 586).

- ⓘ In order to be able to use Bluetooth, it must be enabled under **Devices > Bluetooth**.

The settings for starting the function are described below.

Session name: Name for the session.

- ⚠ The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

- The session can be launched from the start menu.

Application Launcher

- The session can be launched with the Application Launcher.

Desktop

- The session can be launched with a program launcher on the desktop.

Quick start panel

- The session can be launched with the quick start panel.

Start menu's system tab

- The session can be launched with the start menu's system tab.

Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

Desktop context menu

- The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.



Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.



Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

-
- [Using Bluetooth Tool](#)(see page 586)

Using Bluetooth Tool

Menu path: **Accessories > Bluetooth Tool**

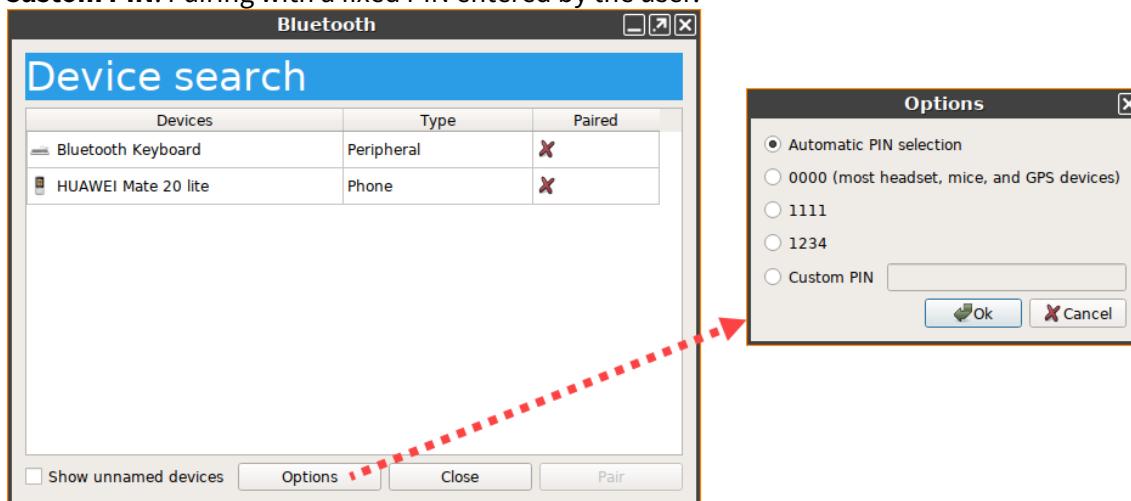
Overview

With the **Bluetooth Tool**, you can connect Bluetooth devices, e.g. a keyboard, a mouse, or a headset, to your endpoint device.

- (i) If your endpoint device (e.g. UD2 D220) does not support Bluetooth, it is necessary to connect a Bluetooth USB adapter to it.

The **Bluetooth Tool** supports the following coupling methods, i.e. the mutual authentication of the Bluetooth device and endpoint device:

- **Automatic PIN selection:** Pairing with automatic PIN allocation
- **0000, 1111, 1234:** Pairing with a fixed PIN (for most headsets, mice, or GPS devices)
- **Custom PIN:** Pairing with a fixed PIN entered by the user.



In addition, also Bluetooth devices that do not require pairing are supported.

Connecting a Bluetooth Device with Automatic PIN Selection

1. Ensure that the coupling mode is enabled on the Bluetooth device.
2. Start the **Bluetooth Tool**. The start options are described under [Bluetooth Tool](#)(see page 583). The **Device search** dialog will be shown.
3. Enable **Show unnamed devices** if you want to include unnamed Bluetooth devices in the search list.
After a few seconds, the Bluetooth devices found by the endpoint device will be displayed.
4. Highlight the desired Bluetooth device.
5. Under **Options**, enable **Automatic PIN selection**.
6. Click on **Pair**.



7. A PIN will be shown in the dialog on your endpoint device.
 - If the PIN is identical to the PIN shown on your Bluetooth device, confirm the coupling.
 - If a Bluetooth device requires the manual entering of a PIN (e.g. keyboard), type in the PIN shown in the dialog.In a few seconds, the status of the connection will be shown.
8. On successful connection, close the dialog.

For an example on how to connect a Bluetooth device, see [Bluetooth Tool](#).

Connecting a Bluetooth Device with a Fixed PIN

1. Ensure that the coupling mode is enabled on the Bluetooth device.
2. Start the **Bluetooth Tool**. The start options are described under [Bluetooth Tool](#)(see page 583).
The **Device search** dialog will be shown.
3. Enable **Show unnamed devices** if you want to include unnamed Bluetooth devices in the search list.
After a few seconds, the Bluetooth devices found by the endpoint device will be displayed.
4. Highlight the desired Bluetooth device.
5. Under **Options**, select one of the specified PINs or enable **Custom PIN** and enter the PIN for the Bluetooth device. You will find this PIN in the documentation for your Bluetooth device.
6. Click on **Pair**.
In a few seconds, the status of the connection will be shown.
7. On successful connection, close the dialog.

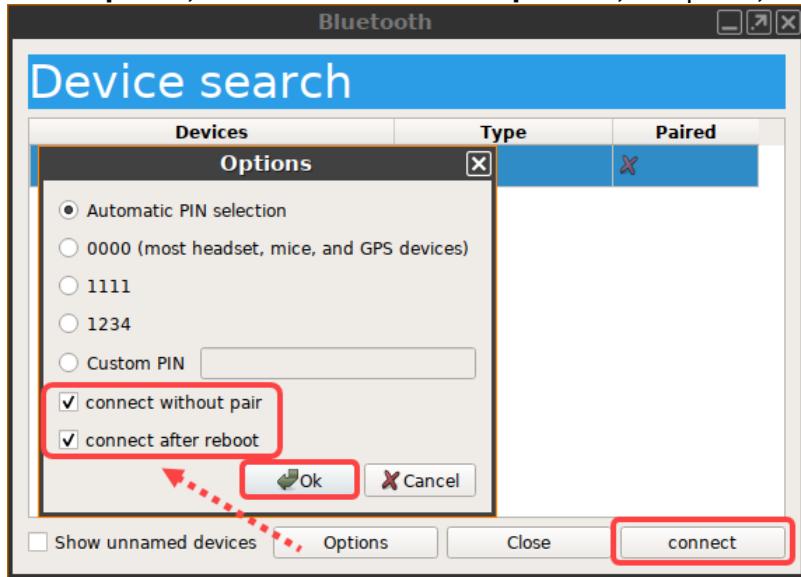
Cancelling Coupling to a Bluetooth Device

1. Start the **Bluetooth Tool**. The start options are described under [Bluetooth Tool](#)(see page 583).
The connected Bluetooth device will be shown in the **Device search** dialog.
2. Highlight the connected Bluetooth device and click on **Unpair**.
The status of the connection will be shown.
3. Close the dialog.

Enabling Support for Devices That Do Not Require Coupling

1. Open the Setup (or the configuration dialog of the UMS), go to **System > Registry > devices > bluetooth > connect_only** and activate **Connect devices without pairing** (registry key: `devices.bluetooth.connect_only`).
2. Click **Apply** or **Ok** to confirm the changes.
3. Start the **Bluetooth Tool**. The start options are described under [Bluetooth Tool](#)(see page 583).
The **Device search** dialog will be shown.
4. Highlight the desired Bluetooth device.

5. Under **Options**, enable **Connect without pair** and, if required, **Connect after reboot**.



6. Click on **Connect**.

i Some devices do not connect automatically after the reboot. To fix that, you can use the following command in a script:
`bluetoothctl connect <device-ID>`
The return value tells you if the device is connected (0) or not (1).



System Information

Menu path: **Accessories > System Information**

With this function, you can obtain information regarding the operating system of your device and the installed system components, internal and connected hardware and the network. You can also measure the performance of your device using various benchmarks.

The information shown can be copied to the clipboard in order to send it to the IGEL Support department for example.

For details of how to use the function, see [Using “System Information” Function\(see page 592\)](#).

The settings for starting the function are described below.

Session name: Name for the session.

The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.



Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

ⓘ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows key` = `Ctrl|Super_L`

Key: Key for the hotkey

ⓘ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.



Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

-
- [Using System Information Function](#)(see page 592)

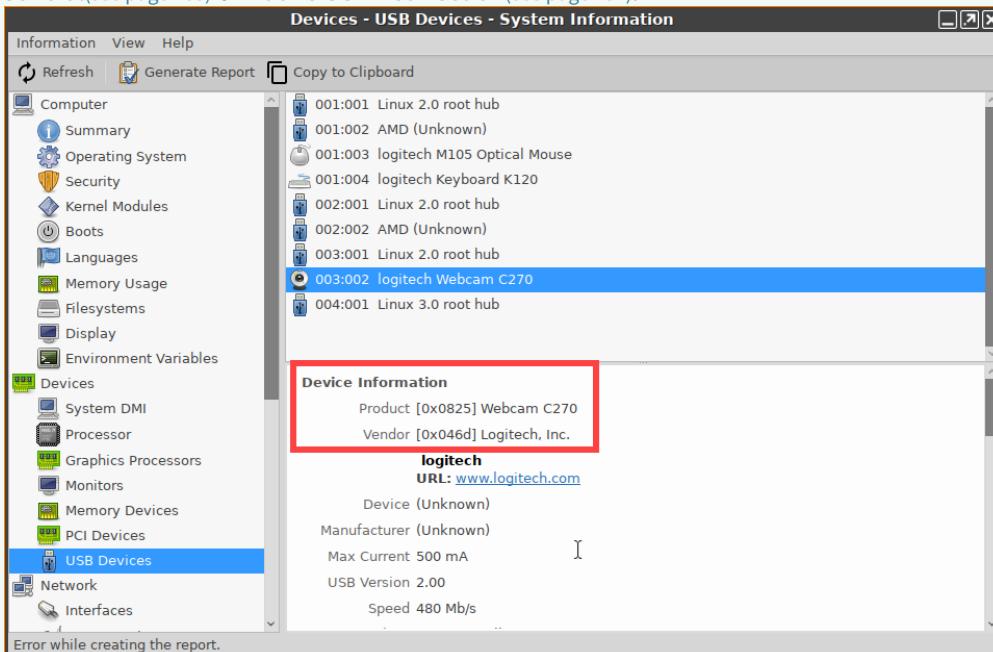
Using System Information Function

Menu path: **Accessories > System Information**

To obtain system information regarding a specific component of your device, proceed as follows:

1. Start the **System Information** function. The start options are described under [System Information](#)(see page 589).
2. Click on the desired area, e.g. **Computer > Operating System**.
The information regarding the desired area will be shown.
3. To send the information shown, e.g. to the IGEL Support department, click on the **Copy to Clipboard** button.
The information is on your clipboard. With **Paste** or [Ctrl] + [V], you can paste the information into an e-mail or a web form.

- ✓ You can use the **System Information** function to find out the **Vendor ID** and **Product ID** of your connected hardware. They are required, for example, if you want to configure **Device Rules**, see e.g. [USB Access Control](#)(see page 785) or [Native USB Redirection](#)(see page 131).



See also [Issues with USB IDs in USB Devices Rules](#).



Disk Utility

Menu path: **Accessories > Disk Utility**

With this function, you can obtain information regarding the hotplug storage devices connected to your thin client. You can also remove hotplug storage devices safely, i.e. without the risk of losing data.

- ⓘ The **Disk Utility** function can only be started if the automatic mounting of hotplug storage devices is enabled. The automatic mounting of hotplug storage devices is enabled if the option "**Dynamic**" is selected under **Setup > Devices > Storage Devices > Storage Hotplug > Client drive mapping** or the number in **Setup > Devices > Storage Devices > Storage Hotplug > Number of drives** is greater than "0".

For details of how to use the function, see [Using “Disk Utility”](#)(see page 596).

The settings for starting the function are described below.

Session name: Name for the session.

- ❗ The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.



Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

ⓘ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows key` = `Ctrl|Super_L`

Key: Key for the hotkey

ⓘ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.



Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode [XDMCP for this Display](#))
- **Desktop Context Menu** (not in appliance mode [XDMCP for this Display](#))
- **Application Launcher** (includes [Application Launcher's system tab](#); not in appliance mode [XDMCP for this Display](#))
- **Hotkey**
- **Autostart** (not in appliance mode [XDMCP for this Display](#))

The session cannot be started in appliance mode.

-
- [Using Disk Utility](#)(see page 596)



Using Disk Utility

To obtain information regarding a hotplug storage device connected to your thin client, proceed as follows:

1. Start the **Disk Utility** function. The start options are described under [Disk Utility](#)(see page 593).
2. Click on the desired hotplug storage device in the left-hand column.
The information regarding the hotplug storage device is shown in the right-hand column.

To remove a hotplug storage device safely, proceed as follows:

1. Start the **Disk Utility** function. The start options are described under [Disk Utility](#)(see page 593).
2. Click on the **Safely Remove Hardware** button in the right-hand column.
The hotplug storage device is disconnected from the thin client. Once it has been disconnected, the storage device can be removed from the thin client.

i If **Setup > Devices > Storage Devices > Storage Hotplug > Hotplug beep** is enabled, a signal tone will signal that the device has been disconnected successfully. If **Setup > Devices > Storage Devices > Storage Hotplug > Hotplug message** is enabled, a message window will signal that the device has been disconnected successfully. Further information can be found under [Storage Hotplug](#)(see page 779).



Disk Removal

Menu path: **Accessories > Disk Removal**

With this function, you can remove a hotplug storage device connected to your endpoint device safely without the risk of losing data.

The settings for starting the function are described below:

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.



Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

ⓘ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with | :

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

- ⓘ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#) (see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

Disk utility in eject menu:

Allows to start the disk utility from the eject menu.

See also [Using “Disk Utility”](#) (see page 596).



Mobile Device Access

Menu path: **Accessories > Mobile Device Access**

ⓘ Feature Not Available on IZ Devices

This feature is not available on IGEL IZ devices (IGEL Zero HDX, IGEL Zero RFX, or IGEL Zero Horizon).

With this function, you can access the directories and files of a mobile device. Mobile device access is available from IGEL OS 10.04.100 onwards.

⚠ Feature with limited support! The mobile device access feature comes with limited support and without any warranty. Any support for this feature is provided on a non-binding, “best effort” basis.

The following device types can be used:

- Smartphones with Android (via MTP / PTP) or iOS
- Tablets with Android via MTP / PTP) or iOS
- Digital cameras

ⓘ The functionality may differ according to the specific device and operating system version.

To use the mobile device access feature, you must first activate the function. For information about the activation and use, see Using Mobile Device Access.

The settings for starting the function are described below.

Session name: Name for the session.

⚠ The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab



- The session can be launched with the start menu's system tab.

Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

Desktop context menu

- The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
-  = `Shift`
-  = `Ctrl`
-  = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`



Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.



Firmware Update

Menu path: **Accessories > Firmware Update**

With this function, you can update your endpoint device's firmware. For details of how to use the function, see [Using "Firmware Update"](#) (see page 605).

The settings for starting the function are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.



- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode [XDMCP for this Display](#))
- **Desktop Context Menu** (not in appliance mode [XDMCP for this Display](#))
- **Application Launcher** (includes [Application Launcher's system tab](#); not in appliance mode [XDMCP for this Display](#))
- **Hotkey**
- **Autostart** (not in appliance mode [XDMCP for this Display](#))

The session cannot be started in appliance mode.

-
- [Using Firmware Update Function](#)(see page 605)



Using Firmware Update Function

To launch the firmware update for your endpoint device, proceed as follows:

1. Ensure that the settings under **System > Update > Firmware Update** are correct. Further information can be found under [Firmware Update\(see page 826\)](#).
2. Start the **Firmware Update** function. The start options are described under [Firmware Update\(see page 602\)](#).
3. Confirm this by clicking **Yes**.
The latest firmware will be loaded onto your endpoint device. The device will restart in the process.



Smartcard Personalization

Menu path: **Accessories > Smartcard Personalization**

With this function, you can change the password for your IGEL smartcard. For details of how to use the function, see [Using “Smartcard Personalization” function \(see page 609\)](#).

Further information regarding the IGEL smartcard can be found in the Authentication with IGEL Smartcard how-to.

The settings for starting the function are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

-
- [Using Smartcard Personalization Function](#)(see page 609)



Using Smartcard Personalization Function

With this function, you can change your user name, the associated password and sessions on your IGEL smartcard.

To personalize an IGEL smartcard, proceed as follows:

1. Start the **Smartcard Personalization** function. The start options are described under [Smartcard Personalization](#)(see page 606).
2. Specify the access data on your IGEL smartcard:
 - **First name:** First name of the user
 - **Last name:** Surname of the user
 - **Require password**
 - A password must be entered when logging on with this IGEL smartcard.
 - No password must be entered when logging on.
 - **Password:** Password for logging on with this IGEL smartcard.
3. Select the sessions and functions that are to be available on this IGEL smartcard.
4. Specify the start behavior for the sessions and functions on this IGEL smartcard:
 - **Autostart**
 - The session/function will automatically start after you log on. The application launchers configured in the desktop integration are available.
 - The session will not automatically start. The application launchers configured in the desktop integration are available.
 - **Restart**
 - The session/function will automatically restart after being closed.
 - The session/function will not automatically restart.
5. Click on **Write smartcard**.

 Do not remove the IGEL smartcard before the writing operation is complete.

A confirmation dialog will appear when the writing operation is complete.
You can now remove the IGEL smartcard.



Identify Monitors

Menu path: **Accessories > Identify Monitors**

With this function, you can identify the monitors connected to your thin client. For details of how to use the function, see [Using “Identify Monitors” function](#)(see page 613).

The settings for starting the function are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.



- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).



The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

-
- [Using Identify Monitors Function](#)(see page 613)



Using Identify Monitors Function

To identify the monitors connected to your thin client, proceed as follows:

- ▶ Start the **Identify Monitors** function. The start options are described under [Identify Monitors](#)(see page 610).
The following data are shown for each monitor:

- Socket to which the monitor is connected
- Type of monitor
- Resolution currently used
- Maximum resolution of the monitor if the resolution currently used is a different one



Webcam Information

Menu path: **Accessories > Webcam Information**

With this function, you can change and check the settings for a connected webcam. For details of how to use the **Webcam Information** function, see [Using Webcam Information](#)(see page 617).

The settings for starting the function are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.



- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode [XDMCP for this Display](#))
- **Desktop Context Menu** (not in appliance mode [XDMCP for this Display](#))
- **Application Launcher** (includes [Application Launcher's system tab](#); not in appliance mode [XDMCP for this Display](#))
- **Hotkey**
- **Autostart** (not in appliance mode [XDMCP for this Display](#))

The session cannot be started in appliance mode.

-
- [Using Webcam Information](#)(see page 617)



Using Webcam Information

You can determine and change the width, height and frame rate for the webcam connected.

- ⓘ Alternatively, you can determine the values supported by the webcam in the local terminal with the command `webcam-info -l`.

To determine and change the values for width, height and frame rate, proceed as follows:

1. Start the **Webcam Information** function.
The following values will be shown:
 - **Width:** Width of the image in pixels
 - **Height:** Height of the image in pixels
 - **Rate:** Frame rate in fps (frames per second: individual images per second). Example: **1/30** means 30 individual images per second.
2. Click on one of the fields to change the value. The supported values will be shown in the process.
3. Click on **Test**.
The video image generated by the webcam with the current settings will be shown.
In order to check whether the webcam is functioning in a session (e.g. redirected via Citrix HDX Webcam Redirection), open <https://www.onlinemictest.com/webcam-test/> in your browser within the session.



ICG Agent Setup

Menu path: **Accessories > ICG Agent Setup**

This tool helps you configure the connection to IGEL Cloud Gateway (ICG). To learn how to use it, please refer to [Using ICG Agent Setup](#)(see page 621).

Session name: Name for the session.

The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.



- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.



-
- Using ICG Agent Setup(see page 621)



Using ICG Agent Setup

This assistant helps you configure the connection to IGEL Cloud Gateway (ICG):

- ▶ Start **ICG Agent Setup**. Start options are described in [ICG Agent Setup \(see page 618\)](#).
 - **Address:** IP address or DNS name of the server running ICG. You can specify a TCP port by appending a colon and the port number.
- ▶ After entering the server address, click **Connect**.
 - If you are using an ICG certificate signed by an unknown CA:
Root certificate fingerprint: Fingerprint identifying the root certificate - three of four fields are prefilled.
Supply the missing fingerprint field from the credentials you received from your system administrator.
 - **ICG One-Time Password:** The one-time-password you received from your system administrator.
 - Click this icon in order to make the one-time password readable.
 - Click this icon in order to change the keyboard layout for entering the password.
 - **Login:** Click this button to connect the thin client to ICG.
 - **Finish:** Click this button for instant connection to ICG. Otherwise, it will be started automatically on the next boot.



This cloud icon in the system tray indicates that the thin client is connected to ICG.

- ✓ If you are switching between home office and company office often, it may be feasible to configure your IGEL OS so that it prefers the local UMS over the ICG. This prevents your device from connecting to the ICG instead of the local UMS although the device is located in the company network.

To make the device prefer the local UMS, make the following settings:

- a. Go to **IGEL Setup > System > Registry > system > remotemanager > icg_try_ums_connect** (Search parameter: **system.remotemanager.icg_try_ums_connect**).
- b. Enable **Prefer UMS over ICG**.
- c. Confirm your setting with **Ok**.



Licensing

Menu path: **Accessories > Licensing**

With this function, you can acquire a license from IGEL. An internet connection is required. The following license types are supported:

- Enterprise Management Pack (EMP)
- Software Maintenance

For information on how to use the license browser, see [Activate Your IGEL OS - Manual License Deployment](#)(see page 622).

The settings for starting the function are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.



For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.



Login Enterprise

Menu path: **Setup > Accessories > Login Enterprise**

Login Enterprise Launcher

This accessory can be enabled to act as a remote endpoint that can launch test sessions for the purpose of evaluating the performance and availability of the resources it connects to. To use this feature, there must already be a Login Enterprise Virtual Appliance to which this Launcher can connect.

To learn more about using Login Enterprise with IGEL, see <https://www.loginvsi.com/igel/>. See also the how-to Login Enterprise Configuration.

Server URL: URL of the Login Enterprise server

Secret: See Getting the Secret for Login Enterprise Launcher.



Connector ID Key Software

Menu path: **Accessories > Connector ID Key Software**

Stratusphere UX is used to assess or inventory the current environment as the basis for designing the target environment.

The Stratusphere IGEL agent will detect RDP/RFX, ICA/HDX, PCoIP and Blast protocols to precisely measure the user experience and validate that the new desktops meet performance and security demands.

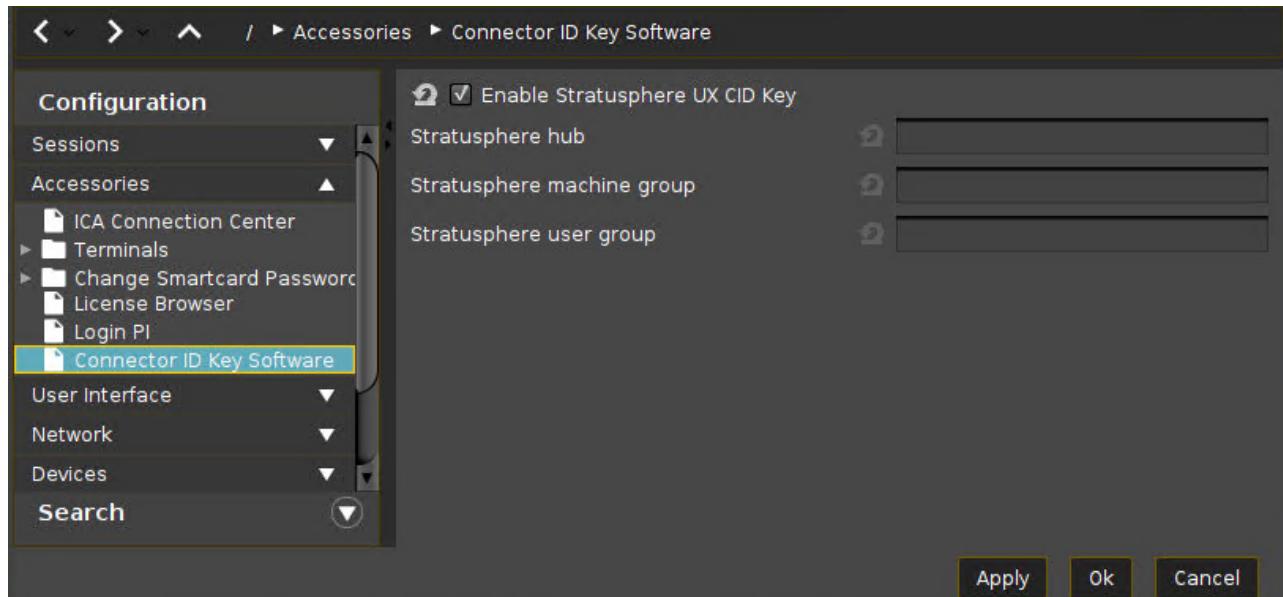
Enable Stratusphere UX CID Key

Stratusphere UX CID Key is enabled.

Stratusphere hub: The hub (IP-address or DNS) of the Stratusphere.

Stratusphere machine group: Machine group of the Stratusphere.

Stratusphere user group: User group of the Stratusphere.





OS 11 Upgrade

Menu path: **Accessories > OS 11 Upgrade**

With this tool, you can upgrade a device from IGEL OS 10 to IGEL OS 11. For more information about this tool, see Testing the Upgrade; for instructions on how to upgrade, see Upgrading IGEL Devices from IGEL OS 10 to IGEL OS 11.

The settings for starting the function are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.



- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)



- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

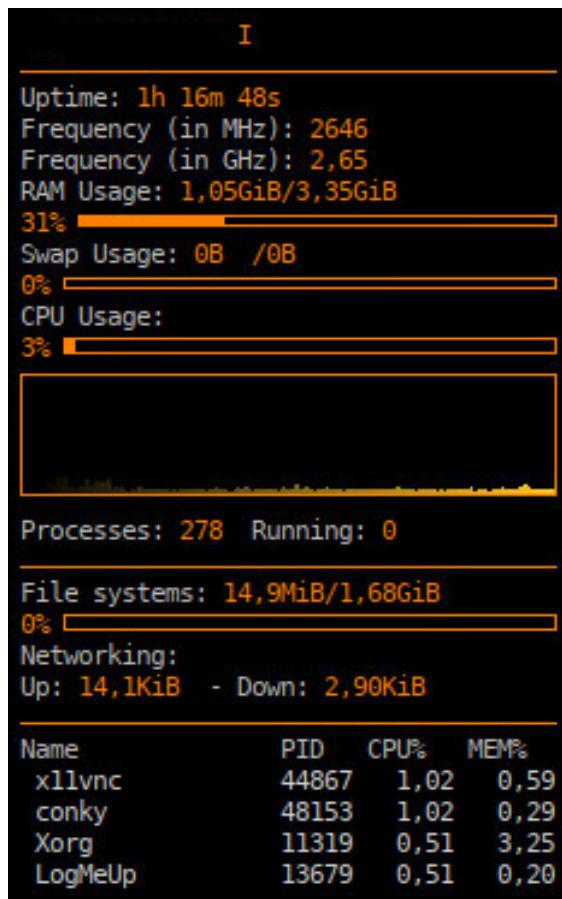
The session cannot be started in appliance mode.



Conky System Monitor

Menu path: **Accessories > Conky System Monitor**

The Conky system monitor displays current system data such as uptime, CPU frequency, RAM usage, and process-specific data. For details of how to configure the Conky system monitor, see [Options\(see page 633\)](#) and [Custom Setup\(see page 634\)](#).



The settings for starting Conky are described below. The start icons also function as stop icons.

Session name: Name for the session.

! The session name must not contain any of these characters: \ / : * ? " < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.



Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- `↑` = `Shift`
- `[Ctrl]` = `Ctrl`



- = Mod4

i When this keyboard key is used as a modifier, it is represented as Mod4 ; when it is used as a key, it is represented as Super_L .

- [Alt] = Alt

Key combinations are formed as follows with | :

- Ctrl + = Ctrl|Super_L

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard . Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the Key field. Example: Tab in (keysym 0xff09 , Tab)

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

- [Options](#)(see page 633)
- [Custom Setup](#)(see page 634)



Options

Menu path: **Accessories > Conky System Monitor > Options**

Use IGEL Setup for configuration

The settings on this Setup page are effective.

- i** The configuration under **Accessories > Conky System Monitor > Custom Setup** (see [Custom Setup\(see page 634\)](#)) is always effective, regardless of whether **Use IGEL Setup for configuration** is activated or not.

Monitor: Monitor on which the Conky system monitor is to be displayed.

Window type

Possible options:

- "Normal": The window layout and behavior can be further specified by the following parameters:
 - **Layer**
 - **Decorations**
 - **Show in the taskbar**
 - **Opacity**
 - **Borders**
- "Desktop": No window decorations; always visible on the desktop; no appearance in the pager or taskbar; sticky across all workspaces. The parameters **Decorations** and **Show in taskbar** are not effective.
 - **Layer**
 - **Opacity**
 - **Borders**
- "Dock": Behavior as documented under <https://linux.die.net/man/1/conky>
- "Panel": The window reserves space along a desktop edge, just like panels and taskbars, preventing maximized windows from overlapping them.
- "Override": The window is not under the control of the window manager.

Alignment: Defines where the window is placed on the screen.

Layer: Defines whether the Conky window is displayed above or below other application windows.

Possible options:

- "Below": The Conky window is always below other application windows.
- "Above": The Conky window is always above other application windows.
- "None": The Conky window is above or below other application windows, depending on the focus.

Font type: Defines the font type for Conky.

Font size: Defines the font size for Conky.

Opacity: Defines the opacity for Conky. If the value is set to 0, the window is completely transparent; if the value is set to 255, there is no transparency.

Offset horizontal: Defines the horizontal offset from the position that is defined by **Alignment**.

Offset vertical: Defines the vertical offset from the position that is defined by **Alignment**.



Custom Setup

Menu path: **Accessories > Conky System Monitor > Custom Setup**

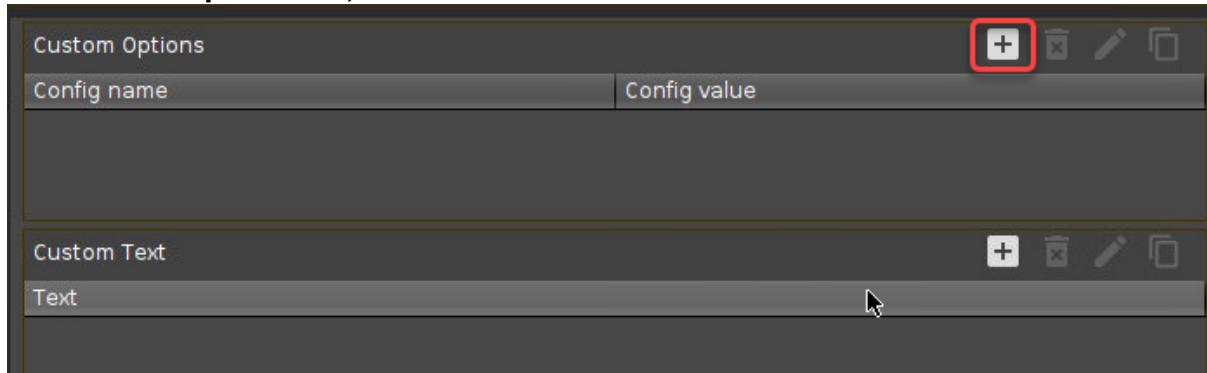
On this Setup page, you can customize Conky in full. For details, see <https://linux.die.net/man/1/conky>.

Custom Options

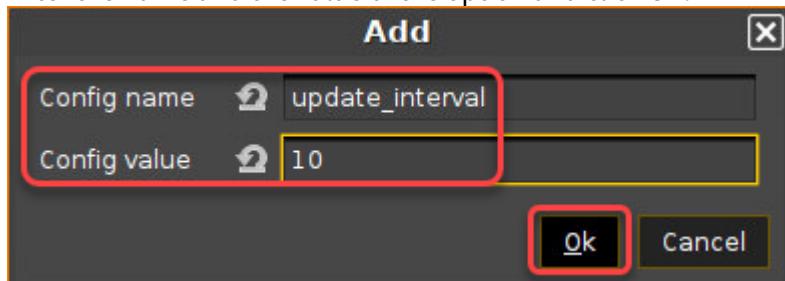
You can find the configuration options of Conky under <https://linux.die.net/man/1/conky>, section "Configuration Settings".

To add a custom option:

1. In the **Custom Options** area, click .



2. Enter the name and the value of the option and click **Ok**.



3. In the main window, click **Apply** or **Ok**.

If Conky is already running, you can see the effect immediately.

Custom Text

In this area, you can define the complete text body of Conky. You can find the relevant details under <https://linux.die.net/man/1/conky>, section "OBJECTS/VARIABLES". The configuration is stored at `/etc/conky/conky.conf`

To add or edit the custom text:



1. In the **Custom Text** area, enter your configuration text.

A screenshot of a software interface showing a "Custom text" input field. The field contains the following text:

```
Custom text
${scroll 40 $nodename - $sysname $kernel on $machine | }
$hr
${addr ens192}
$hr
${color grey}Uptime:${color $uptime}
```

The text starting with "\${scroll" is highlighted with a red rounded rectangle.

2. In the main window, click **Apply** or **Ok**.

If Conky is already running, you can see the effect immediately.



User Interface

- [Display Settings in IGEL OS\(see page 637\)](#)
- [Desktop\(see page 646\)](#)
- [Language Settings for IGEL OS 11\(see page 662\)](#)
- [Screenlock / Screensaver\(see page 663\)](#)
- [Input\(see page 671\)](#)
- [Hotkeys\(see page 681\)](#)
- [Font Services\(see page 685\)](#)



Display Settings in IGEL OS

The following article describes the **Display** settings in IGEL OS, which you will require when configuring your monitors. Take notice that a successful and correct display configuration depends, however, on many factors. For example, cables, current driver / firmware versions, BIOS settings, etc. can influence your screen configuration and, thus, have to be considered when setting up the monitor environment.

For a quick display configuration, you can use also the [Display Switch](#)(see page 524) function.

If you work in an environment with multiple monitors, see also the how-to article [Multimonitor](#).

If you use the Shared Workplace (SWP) feature with user-specific display resolutions, see [Display Configuration for Shared Workplace \(SWP\)](#).

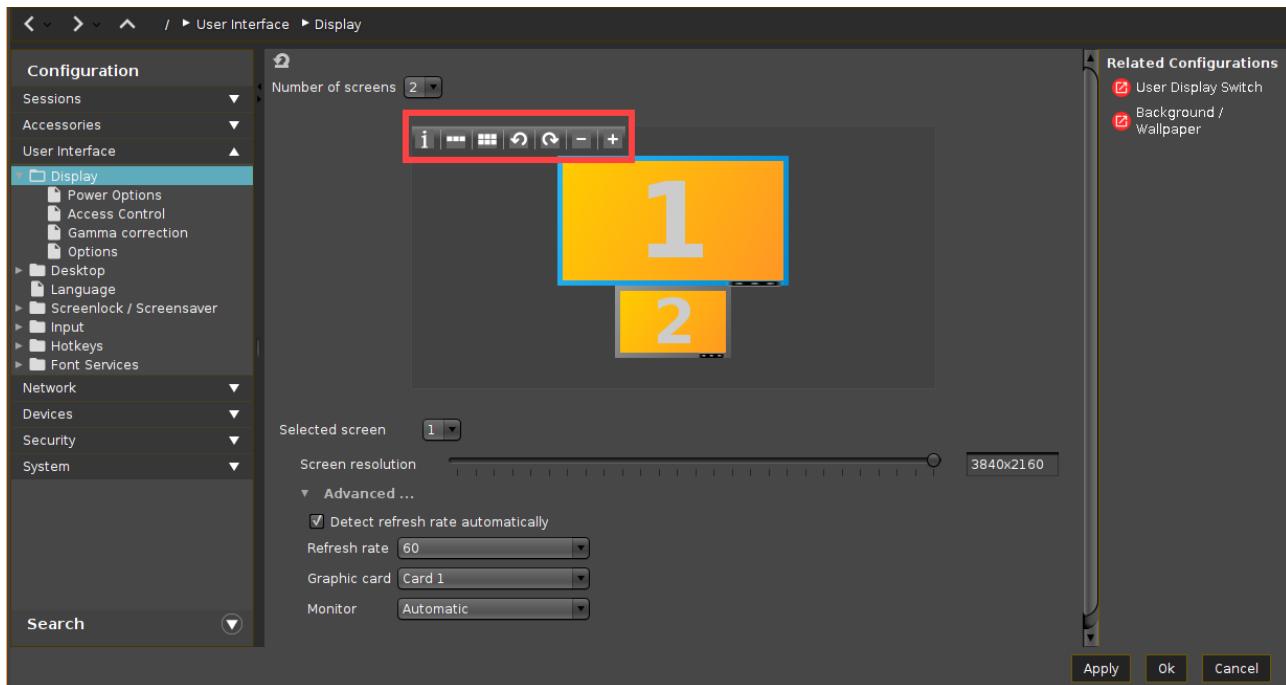
Menu path: **User Interface > Display**

Screen Configuration

- ⚠** Always try the configuration locally before applying it to multiple devices via a profile: A faulty display configuration can cause your GUI to become unstable and lead to a black screen.
If you face a black screen problem because of the wrong display configuration, select one of the following recovery options:
- In the UMS: Edit the display configuration via **Devices > [device name] > [device's context menu] > Edit Configuration** or via a new profile.
OR
 - On the endpoint device: Restart the device and select **Emergency boot (setup only)** during the boot procedure, see [Boot Menu](#)(see page 23) and [Emergency Boot](#)(see page 26). In the Setup, you can then change the display configuration.

Every screen connected to the endpoint device can be configured independently. The position of the individual screens can be determined in relation to Screen 1.

- Click on **i** to show the screen identifier on each device. **i** appears only locally on the device, not in the UMS.



Number of screens

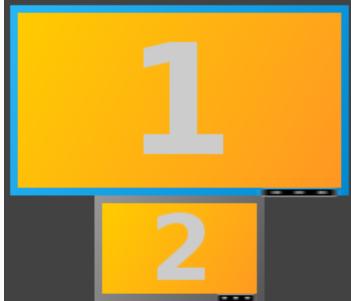
Select how many monitors you would like to use.

	Identifies each screen connected and shows the connection and display resolution for each screen. This function is available only locally on the device. It is not accessible from the UMS.
	Arranges the screens in a single row.
	Arranges the screens in two rows.
	Rotates the selected screen anti-clockwise.
	Rotates the selected screen clockwise.
	Removes the screen which was last added.
	Adds a screen.

The selected screen is highlighted with a blue frame. The black bar at the bottom edge of the screen represents the physical orientation of the monitor.



- ⓘ Configuring a vertically centered display layout, which may be required, for example, in the case of a primary monitor (top) and a touchscreen panel (bottom), is not possible if **Screen resolution** is set to "**Autodetect**". In this case, **Screen resolution** must be specified manually.



Selected screen

Selects a screen using this selection box to configure the following settings.

Screen resolution

Move the slider to the resolution which the selected screen is to have. The resolution is shown in the right-hand box.

- ⓘ You have the option of defining your own resolutions via the registry key `x.xserver0.custom_resolution`. In order for the values set there to take effect, the resolution must be set to "**Autodetect**" (slider at the far left). The following parameters apply to the entry in the registry:
- `WxH` : W = width, H = height (example: 1920x1080)
 - `WxH@R` : W = width, H = height, R = refresh rate (example: 1920x1080@60 or 1920x1200@59.8)

⚠ Be careful when changing resolutions manually. Excessively high resolutions can cause a black screen.



- ⓘ For details of the display resolution supported by your IGEL device, please see the relevant datasheet on igel.com³⁶ or in the datasheet archive for legacy IGEL devices.
Detailed instructions on MST configuration for UD3 and UD7, see:
 - UD3 Model M350C: Multistream Transport
 - UD7 Model H860C: Multistream Transport (MST) / Monitor Daisy Chaining

Advanced...

Detect refresh rate automatically

- A refresh rate for the monitor is identified automatically.*
 A refresh rate for the monitor is to be set manually.

Refresh rate

Number of individual images per second.

Possible values:

- 30 ... 100. (Default: 60)

- ⚠ Be careful when changing the refresh rate manually since the faulty configuration can cause a black screen.

Graphic card

Graphics card assigned to the selected screen. A graphics card can have more outputs than are actually used. In order to ensure transparency, you may need to assign the graphics cards manually.

- ⓘ If **Automatic** is set for the **Monitor** and no configurable monitor is found for the selected graphics card, the next available monitor will be used by another graphics card.

Monitor

Assigns the screen selected under **Selected screen** to a monitor connection. Example: **HDMI(II)**. (Default: Automatic)

- [Power Options](#)(see page 642)
- [Access Control](#)(see page 643)
- [Gamma Correction](#)(see page 644)
- [Options](#)(see page 645)

³⁶ <https://www.igel.com/igel-solution-family/igel-endpoint-hardware/>



*IGEL OS system default



Power Options

Menu path: **Setup > User Interface > Screen > Power Options**

In this area, you can handle display power management.

Please note: Your screen must support *Display power management signaling (DPMS)*.

- **Handle Display Power Management**

The DPMS energy saving functions are enabled.

- ▶ Specify separately for battery and mains operation the number of minutes before the screen switches to a specific energy-saving mode:

Three different modes are offered:

- **Standby Time** (standby mode)
- **Suspend Time** (sleep mode)
- **Off Time** (Off)

If a device is switched on but not used for some time, energy can also be saved by **Brightness Reduction**.

- ▶ Specify by how many percent the brightness of the screen is to be reduced and how long the period of inactivity before brightness reduction should be. Values between 10 seconds and two minutes are available to choose from.

i Naturally, all stages are gone through only if the X-Server does not receive any new entries during this period.



Access Control

Menu path: **Setup > User Interface > Screen > Access Control**

In this area, you can control access to the screen. Thin client access control is enabled by default.

Disable console switching

Access to your terminal screen is possible from any UNIX host. You can no longer access the console using [Ctrl] + [Alt] + [F11] or [Ctrl] + [Alt] + [F12].

You can access the console using [Ctrl] + [Alt] + [F11] or [Ctrl] + [Alt] + [F12]. (default)

Access Control

Access to this display from other computers will be controlled. This access control is enabled by default. (default)

Disable TCP connections

All TCP connections to the display are prohibited. Only local applications are displayed. The xhost mechanism no longer functions.

This parameter is ignored if XDMCP is configured.

Fixed X-Key

You can grant specific users permanent remote access to the thin client:

1. Click on **Calculate**.
A 32-digit key will appear in the **X-Key** field.
2. Enter this key in the Xauthority file on the user's computer.

List of trusted X hosts

Here, you can approve specific computers for console access:

1. Click on the **Add** button to open the entry mask.
2. Give the name of the remote host (not the IP address) you would like to add.
3. Confirm this by clicking **OK**.
The computer will be entered in the list.



Gamma Correction

Menu path: **Setup > User Interface > Screen > Gamma Correction**

In this area, you can increase or decrease the various brightness ranges in order to adjust the display on your screen to your preferences.

- **Selected screen:** Select the screen whose brightness you would like to adjust (default: First Screen).

You can then change the gamma values for red, green and blue. The scale ranges from 0.10 (dark) to 10 (light) and is set to 1.00 by default.

- **Gamma value Red:** Changes the brightness curve for the red color portion.
- **Gamma value Green:** Changes the brightness curve for the green color portion.
- **Gamma value Blue:** Changes the brightness curve for the blue color portion.
- **Link Sliders**
 - All sliders are moved equally in order to change the brightness harmoniously. (default)
 - Each slider can be moved individually. This way, you can also change the color ratio.



Options

Menu path: **Setup > User Interface > Screen > Options**

Configure the options for the display here:

- **Monitor probing (DDC)**

You can share information between the system and the screen via the Display Data Channel. DDC is enabled by default and the native resolution supported by the screen is determined automatically. (default)

Screen properties are not automatically detected.

- **Monitor DPI detection:** Defines how the DPI value should be determined.

Possible options:

- Off: The DPI value is defined by **Monitor DPI**. There is no automatic detection.
- Smart: The DPI value is defined automatically. With this setting, the user interface is readable also on monitors with very high resolutions, e.g. 4k monitors. The DPI value is set to either 96, 125, 150, 175, 200, 225, 250, 275 or 300, depending on which value is closest to the value calculated based on the monitor resolution.
- Pixel-Precise: The DPI value is defined automatically. With this setting, the user interface is readable also on monitors with very high resolutions, e.g. 4k monitors. Unlike the "Smart" option, the value calculated based on the monitor resolution is used directly.

- **Monitor DPI:** Enter the DPI resolution (dots per inch) for your monitor (default: 96). This parameter is only available if **Monitor DPI detection** is set to "Off".

- **Color Depth:** Selects the desktop color depth.

The following options are available:

- True Color (24)
- True Color (32)

Make sure that all screens connected to the thin client support the color setting.



Desktop

Menu path: **Setup > User Interface > Desktop**

On this page, you can configure general settings for the appearance of the desktop:

Local window manager for this display: Here, you can disable the window manager if you only work in full-screen sessions and do not require this service.

User interface theme: The colors of windows such as the Application Launcher, the start menu, the local terminal, the taskbar and messages can be varied. You can either select one of our predefined color schemes or define a color scheme of your own.

- IGEL Dark: The frame color is dark gray, IGEL logos are yellow.
- IGEL Light: The frame color is light gray, IGEL logos are dark gray.
- Custom Colors: Define your own color combinations below.

Desktop icon size: Specify the size in which you would like the icons to be displayed on the desktop.

Desktop icon font color: Specify the font color for the labels associated with the desktop icons. Click **Choose color** to open the color picker.

Monitor for desktop icons: If you use several monitors, select the one which is to display desktop icons.

- All monitors
- As taskbar
- 1st monitor
- 2nd monitor
- (other monitors if connected)

Single click mode:

Open programs with a single click. This option was set up especially for users of touchscreen monitors.

Desktop fonts

Default font: Choose between serif and sans-serif text and between standard and bold. The following are available to choose from:

- Sans
- Sans bold
- Serif
- Serif Bold

Default font size: Specify your desired font size in pt (points) here.

Desktop icon font size: Specify your desired font size for desktop icons in pt (points) here.

Titlebarfont: Choose between serif and sans-serif text and between standard and bold. The following are available to choose from:

- Sans
- Sans bold
- Serif



- **Serif Bold**

Titlebar font size: Specify your desired font size in pt (points) here.

- [Background](#)(see page 648)
- [Taskbar](#)(see page 651)
- [Taskbar Background](#)(see page 653)
- [Taskbar Items](#)(see page 654)
- [Pager - Virtual Workspaces for Organizing the IGEL OS Desktop](#)(see page 655)
- [Start Menu](#)(see page 660)
- [In-Session Control Bar](#)(see page 661)



Background

Menu path: **Setup > User Interface > Desktop > Background**

In this area, you can configure the desktop background with predefined *IGEL* backgrounds, a fill color or a color gradient.

You can also use a background image of your own.

- ⓘ You can set up a separate background image for each monitor that is connected to the thin client.
- ⓘ **Wallpaper** selection options beginning with "Desktop Color" are transparent so that the background colors will shine through.

- **Wallpaper:** Provides a selection of predefined *IGEL* backgrounds:
 - Neutral
 - Off
 - Black
 - Blue
 - Gray
 - Orange
 - Green
 - Yellow
 - Desktop Color Light
 - Desktop Color Dark
 - Desktop Color Light Neutral
 - Desktop Color Dark Neutral
- **Wallpaper Style:** Provides various design versions:
 - Auto
 - Centered
 - Tiled
 - Stretched
 - Scaled
 - Zoomed
- **Color Style:** Sets a fill color or a color gradient.
 - Solid color
 - Horizontal gradient
 - Vertical gradient
- **Desktop Color:** Select a background color if you have not selected an image.
- **2nd Desktop Color:** Select a second background color if you have not selected an image.
- **Custom Wallpaper Download:**
 You can provide a user-specific background image on a download server.
- **Custom Wallpaper file:** Give a name for the background image file.
Specify the download server under **Desktop > Background > Custom Wallpaper Server**.



- ⓘ If you have already defined a server for the system update files, you can use the same server setting for downloading the background image.

The user-specific background image will be downloaded from the specified server if the function was enabled and if requested manually (Update Background Image). The download can also be launched from the *IGEL Universal Management Suite* via **Update desktop changes**.

- ⓘ A user-specific boot image can be provided on a download server. The file types BMP, JPG, GIF, TIF, PNG and SVG are supported for an **own background image** and **bootsplash**. A total storage area of 25 MB is available for all user-specific images.



Custom Wallpaper Server

Menu path: **Setup > User Interface > Desktop > Background > Custom Wallpaper Server**

In this area, you can configure the download server for your own background images.

- **Use firmware update server location**
 - The same server and path configuration is used as for the firmware update.
 - An own server location is used. (default)
- **Protocol:** Determines the protocol that is to be used. The following are available to choose from:
 - HTTP
 - HTTPS
 - FTP
 - SecureFTP
 - FTPS
 - File
- **Server Name:** Name or IP address of the server used.
- **Server Path:** Directory in which you saved the background image.
- **Port:** Port used (default: 80)
- **User name:** Name of the user account on the server
- **Password:** Password for this account
- **Wallpaper update:** Refreshes the background image.



Taskbar

Menu path: **Setup > User Interface > Desktop > Taskbar**

In this area, you can enable and configure the taskbar.

You can change the following settings:

- **Use Taskbar:**

The taskbar is displayed and the following taskbar settings options are available.

- **Taskbar Position:** Specifies the position in which the taskbar is displayed.

Possible values:

- Bottom
- Top
- Left
- Right

- **Vertical Taskbar Mode:** Specifies how items are shown in the taskbar. This parameter is available if **Taskbar Position** is set to **Left** or **Right**.

Possible values:

- Vertical: The session texts are rotated by 90°.
- Deskbar: The session texts are not shown.

- **Taskbar Height/Width:** Specifies the height of the taskbar in pixels (default 40).

i If **Maximum number of rows/columns in window button list** is set to **Automatic**, the window buttons as well as the icons in the Quick Start Panel will be shown in a number of rows depending on the height of the taskbar. The number of rows increases in increments of 55 pixels:

- 1 - 55 pixels: One row
- 56 - 110 pixels: Two rows
- 111 - 165 pixels: Three rows
- 166 - 220 pixels: Four rows
- 221 - 275 pixels: Five rows
- 276 or more pixels: Six rows

The **Maximum number of rows/columns in window button list** parameter is described under Taskbar Items.

- **Number of rows/columns in taskbar:** Specifies the number of rows for the Quick Start Panel. The following taskbar items can be broken down into a number of rows and columns: Icons in the Quick Start Panel, window buttons. Possible values:
 - Automatic: The number of rows for the Quick Start Panel depends on the height and width of the taskbar.
 - Numeric value: The chosen value specifies the number of rows for the Quick Start Panel.
- **Multi Monitor Taskbar Size:** Specifies whether the taskbar is expanded across a number of monitors or restricted to one monitor. Possible values:
 - Restrict taskbar to one monitor
 - Extend taskbar to all monitors



- **Monitor:** Specifies the screen on which the taskbar is shown. This parameter is available if **Taskbar size in Multi Monitor** is set to **Restrict taskbar to one monitor** (default: 1st monitor).
- **Taskbar on top of all windows:**
 The taskbar is accessible on all screens, even in sessions with a full-screen window.
- **Taskbar Auto Hide:**
 The taskbar is hidden and will only be shown if the mouse pointer is moved to the position of the taskbar at the edge of the screen.
- **Auto Hide Behavior:** Specifies when the taskbar is automatically hidden.
Possible values:
 - Intelligent: The taskbar is shown as standard. The taskbar will be hidden if the space is needed by a window, e. g. a window in full-screen mode.
 - Continuous: The taskbar is hidden as standard. The taskbar will be shown if the mouse pointer is moved to the edge of the screen.
- **Taskbar Show Delay:** Time interval in milliseconds before the taskbar is shown. The mouse pointer must be at the edge of the screen constantly during this time interval. This setting is only effective if **Taskbar Auto Hide** is enabled (default: 600).
 - ⓘ With the show delay, you can prevent the taskbar for a full-screen session being covered by the thin client's taskbar. A show delay is necessary if the taskbar for the full-screen session is set to be shown automatically and both taskbars are positioned at the same screen edge. If no show delay is set and the user brings up the taskbar for the full-screen session, this will immediately be covered by the thin client's taskbar. During the show delay time interval, the user has time to move the mouse pointer away from the edge of the screen.
- **Taskbar Hide Delay:** Time interval in milliseconds before the taskbar is hidden. This setting is only effective if **Automatically hide taskbar** is enabled (default: 400).
Further settings options can be found under Screensaver and Screenlock.



Taskbar Background

Menu path: **Setup > User Interface > Desktop > Taskbar Background**

You can specify the background style for the taskbar here.

- **Background Style:**

Possible values:

- System preset
- Solid color
- Color gradient
- Background image

Depending of the above selection you can define following features:

- **Taskbar Color:** Choose the color for the taskbar.
- **2nd Taskbar Color:** Choose the 2nd color for the taskbar if you want to create gradient colors.
- **Reverse Gradient**
 - The color gradient is reverse.
 - The color gradient is normal. (default)
- **Background Image Path:** Path of your background image



Taskbar Items

Menu path: **Setup > User Interface > Desktop > Taskbar Items**

- **Taskbar clock:**

- A clock is shown in the taskbar.

- **Sorting order in window button bar:** Specifies the criteria according to which the window buttons are sorted.

Possible values:

- Time stamp: The window buttons are sorted in the chronological order in which the windows were opened.
- Group and time stamp: The window buttons are grouped according to the type of application. If for example a number of setup applications are open, all associated window buttons will be arranged next to each other. Within the group, the window buttons are sorted chronologically.
- Window title: The window buttons are sorted alphabetically.
- Group and window title: The window buttons are grouped according to type. If for example a number of setup applications are open, all associated window buttons will be arranged next to each other. Within the group, the window buttons are sorted alphabetically.
- Drag and drop: You can order the buttons as you wish using drag and drop. You must drag a button over at least half of the button to be skipped.

- **Maximum number of rows/columns in window button bar:** Specifies the maximum number of rows available for window buttons.

Possible values:

- Automatic: The number of rows depends on the **Taskbar height/width** and **Number of rows/columns in taskbar** parameters, see Taskbar.
- Numeric values: This value specifies the maximum number of rows.

- **Show labels in window button bar:**

- The names of the ongoing sessions are displayed in the associated window buttons. (default)
- Only the icons are displayed.

- **Taskbar system tray:**

- The system tray is shown in the taskbar. (default)

- **Size of icons in system tray:** Specifies the size of system tray icons (volume, network connection etc.).

You can choose a pre-defined value or enter a numeric value between 1 and 64.

Predefined values:

- Automatic: The size is adjusted to the height and width of the taskbar.
- Small: 20 pixels
- Medium: 40 pixels
- Large: 60 pixels

Further settings options can be found under On-screen Keyboard, Keyboard and Additional Keyboard Layouts and Screensaver and Screenlock.



Pager - Virtual Workspaces for Organizing the IGEL OS Desktop

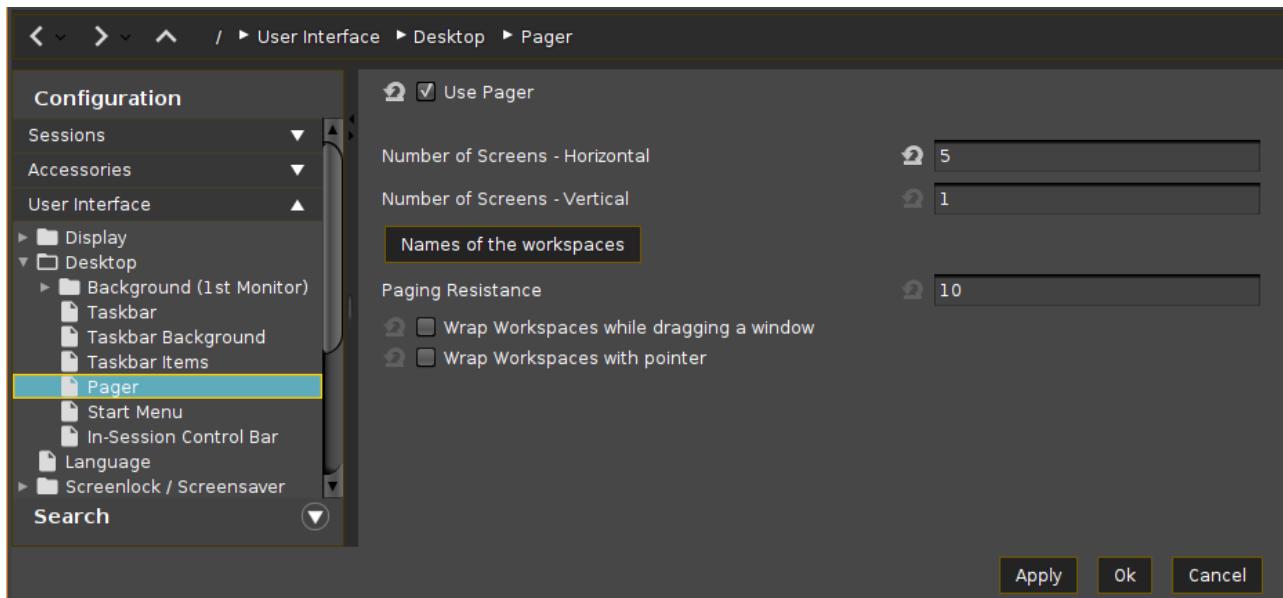
In IGEL OS, you can use the **Pager** tool to enable the use of multiple virtual desktops. The Pager allows you to divide one desktop into several virtual workspaces and, thus, to better organize your desktop: for example, you can open a certain type of applications in one workspace and another type of applications in the second workspace.

The Pager makes switching between multiple open applications easier – you can switch between full-screen applications at the click of a mouse. Instead of minimizing / maximizing sessions or switching between them using key combinations, you simply click on the desired workspace using the mouse. When you switch back, the virtual desktop is displayed exactly as before (unless you restarted the system or changed the language in the IGEL Setup).

⚠ Make sure you have enabled **User Interface > Desktop > Taskbar**(see page 651) > **Taskbar on top of all windows**.

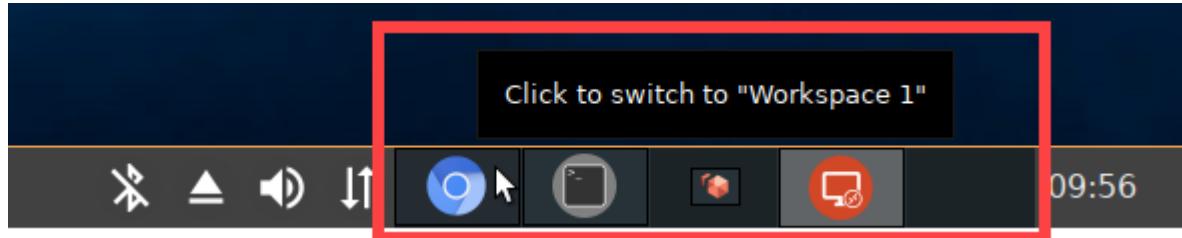
ⓘ The Pager can be used only in non-appliance mode.

Menu path: **User Interface > Desktop > Pager**



Use Pager

The Pager is enabled. You can configure up to 25 virtual desktops. The Pager will be displayed on the right of the taskbar:



For details on how to use the pager, see the below section "[Example for how to Use the Pager\(see page 656\)](#)".

- The Pager is disabled.*

Number of Screens - Horizontal

Specifies how many workspaces will be shown next to each other. (Default: 2)

Number of Screens - Vertical

Specifies how many workspaces will be shown above each other. (Default: 1)

Names of the workspaces

Specify names for the individual desktops.

Paging Resistance

Specifies how many pixels the cursor needs to be moved over the edge of the screen before it triggers a switch of the desktop. (Default: 10)

You only need to make this setting if you enable at least one of the following options – **Wrap workspaces while dragging a window** or **Wrap workspaces with pointer**.

Wrap workspaces while dragging a window

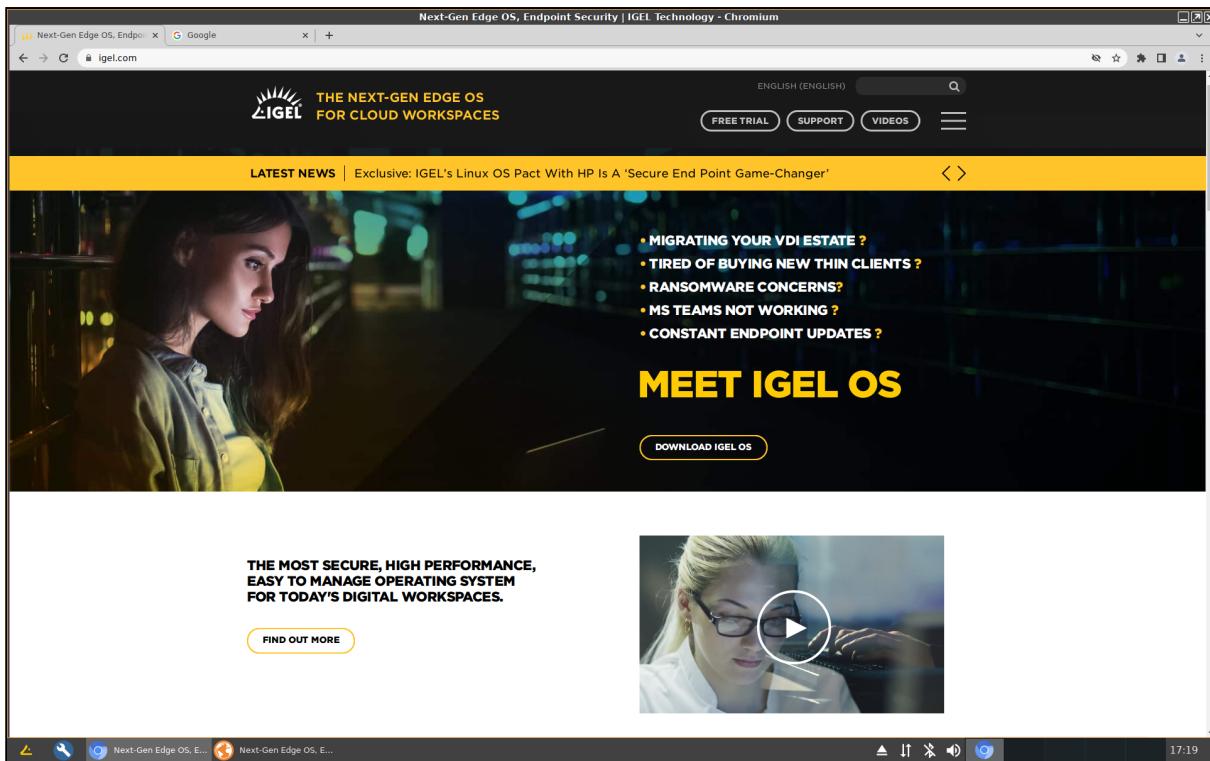
- The desktop is switched as soon as a window is dragged out of view.
 The desktop is not switched when a window is dragged out of view.*

Wrap workspaces with pointer

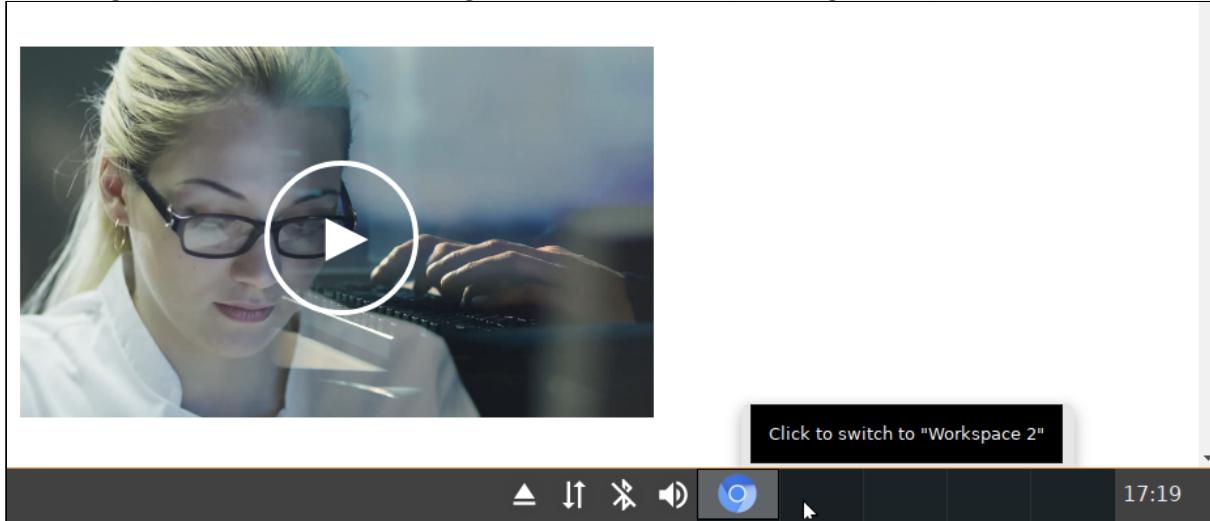
- The desktop is switched as soon as the mouse reaches the edge of the screen.
 The desktop is not switched when the mouse reaches the edge of the screen.*

Example for how to Use the Pager

1. Start your endpoint device and launch the desired sessions / applications, e.g. Firefox and Chromium browsers.

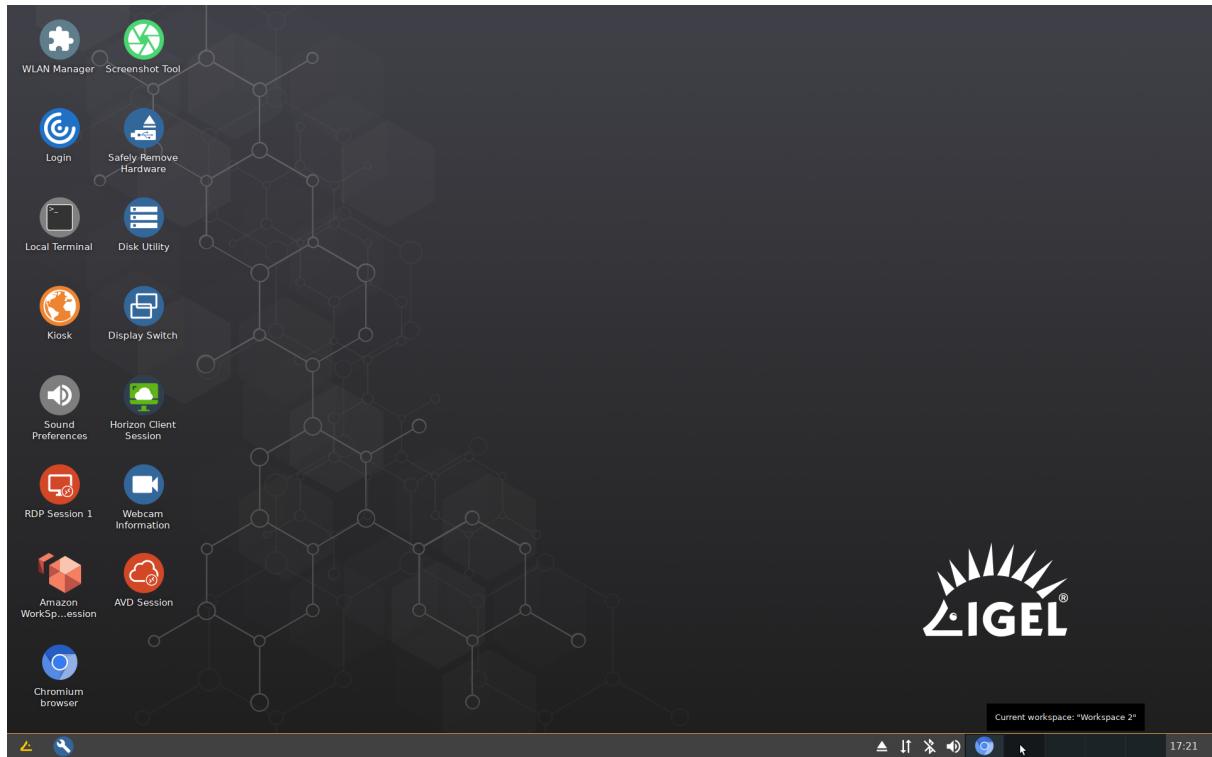


2. In the Pager panel in the taskbar, navigate to another workspace, e.g. Workspace 2, and click it.

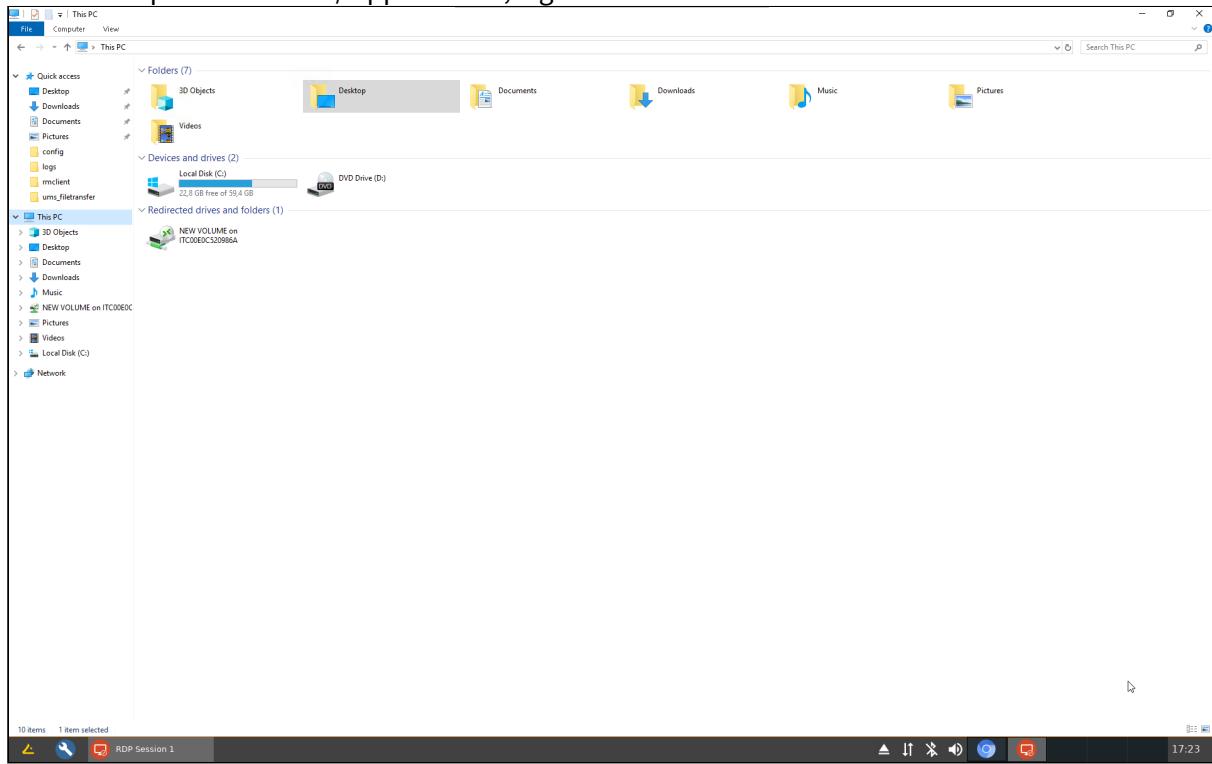


You will see the "empty" desktop, i.e. without opened sessions / applications.

User Interface



3. Start the required sessions / applications, e.g. an RDP session.





4. When you need to switch back to the Firefox and Chromium browsers, simply select the corresponding workspace (in this example, Workspace 1) in the Pager panel in the taskbar. Your desktop will be displayed exactly as before the switch to Workspace 2. Thus, you switch between your browser sessions and an RDP session without minimizing the latter.

 **Tip**

You can use drag & drop to rearrange the sessions / applications between the workspaces: in the respective virtual desktop, click on the required application / session symbol on the left of the taskbar and drag it to the desired workspace.

*IGEL OS system default



Start Menu

Menu path: **Setup > User Interface > Desktop > Start Menu**

In this area, you can configure the desktop start menu:

- **Start menu type:**

- **Auto:** A default setting that automatically selects the advanced or legacy type of the start menu depending on the processor.
- **Advanced:** An expanded start menu featuring a search function and a more attractive design. It requires more resources, which is particularly noticeable on slow devices.
- **Legacy:** A start menu resembles the one from Windows 95 – a list of available sessions and options.

Options in Start Menu

Select which options are to be shown in the start menu:

- **Screenlock**
- **Logout**
- **Reboot**
- **Shutdown**
- **System tab**
- **About**
- **Show current user name in About, Application Launcher and start menu**
 - The current user will be shown at the top edge of the relevant window.
 - The current user will not be shown.

i In order for user names to be recognized and passed on, you must configure two settings beforehand:

- Enable Active Directory/Kerberos: **Security > Active Directory/Kerberos**
- Enable local logon: **Security > Logon > Active Directory/Kerberos**



In-Session Control Bar

Menu path: **Setup > User Interface > Desktop > In-Session Control Bar**

In a full-screen session, the in-session control bar allows you

- to eject a USB drive,
- to start the wireless manager (only available in Appliance Mode),
- to start the Mobile Device Access USB tool (only available if the Mobile Device Access USB feature is enabled),
- to minimize the session view (not available in Appliance Mode),
- to end the session.

Use in-session control bar in all supported sessions

The in-session control bar is shown. Depending on the configuration, the in-session control bar will be permanently visible or will be shown as soon as you move the cursor to the top edge of the screen.

In-session control bar is not used. (default)

The in-session control bar is available for the following session types:

- **RDP** - see [RDP Global](#)(see page 111)
- **Citrix** - see [Citrix Global](#)(see page 52)
- **ThinLinc** - see [ThinLinc](#)(see page 321)
- **NX** - see [NX](#)(see page 245)
- **Parallel 2X Client** - see [Parallel 2X Client](#)(see page 274)

To use the in-session control bar, proceed as follows:

- ▶ To eject a USB device, click .
- ▶ To start the wireless manager, click  (only available in Appliance Mode).
- ▶ To start the Mobile Device Access USB tool, click  (only available if the Mobile Device Access USB feature is enabled).
- ▶ To minimize the session view, click .
- ▶ To end the session, click .
- ▶ To make the in-session control bar permanently visible, click .



Language Settings for IGEL OS 11

In this area, you can configure the country-specific language settings.

Menu path: **Setup > User Interface > Language**

Language

The language of the user interface.

Keyboard layout

When the language is changed for the first time, the keyboard layout is automatically set to the same language.

Show indicator in taskbar

- Shows a country abbreviation for the keyboard layout in the taskbar.
- No indicator is shown. (System default)

Input language

The keyboard layout is used by default.

Standards and formats

Specifies how country-specific formats for the time and currency are displayed, for example. The default setting is geared to the input language selected.



Screenlock / Screensaver

Menu path: **User Interface > Desktop > Screen Lock/Saver**

You can set up the screen saver so that it is activated automatically after a time limit expires, via a button or in response to a key combination (hotkey). You can also select a password option. The look of the taskbar can be configured separately for the logon dialog and the locked screen.

The screen can be locked via icons in the Quick Start Panel and on the desktop or via the hotkey [Ctrl-Shift-L].

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:



- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.



No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode\(see page 213\)](#).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.

- [Options\(see page 666\)](#)
- [Taskbar\(see page 668\)](#)
- [Screensaver\(see page 669\)](#)



Options

Menu path: **Setup > User Interface > Screenlock / Screensaver > Options**

Start automatically

The screenlock or screensaver starts automatically if there is no activity on the endpoint device within this time limit. The screen can be unlocked by the user or, if the **Allow administrator password** is not disabled, the administrator with the relevant password (see: [Password - Restrict Access to IGEL OS Components\(see page 799\)](#)). (Default)

Timeout: Period of time in minutes before the screenlock or the screensaver starts. (Default: 5)

Screenlock Password

- **None:** No password is set. A screenlock cannot be set up.
- **User password:** A user password is deployed to unlock the screen, see [Password - Restrict Access to IGEL OS Components\(see page 799\)](#). If the user is [logged in via Active Directory \(AD\)](#)(see page 807), the AD credentials are used instead of the user password to unlock the screen.
- **Local user password:** A separate password specified under **Set** is deployed to unlock the screen. This password is also used for **Security > Logon > Local User > Login with local user password**, see [Local User\(see page 812\)](#). If the user is [logged in via Active Directory \(AD\)](#)(see page 807), the AD credentials are used instead of the local user password to unlock the screen.

Different screenlock timeout

You can specify a time limit of your own for the screenlock. (Default)

The same time limit will be used for the screenlock as for the screensaver. This means that after the set time the screen will be locked and then the screensaver will appear.

Screenlock timeout: Period of time in minutes before the screenlock starts. (Default: 5)

Allow administrator password

Access is allowed for the user and the administrator, see [Password - Restrict Access to IGEL OS Components\(see page 799\)](#). (Default)

Access is allowed for the user only.

Countdown duration in seconds: Countdown time with which the screenlock is initiated. If the value is 0, the screen is locked without a countdown. (Default: 0)

- i** The appearance of the digits for the countdown is specified together with the settings for the clock display under **Setup > User Interface > Screenlock / Screensaver > Screensaver**; see [Screensaver\(see page 669\)](#). The following parameters are relevant for the countdown:
- **Clock display monitor**
 - **Show seconds**
 - **Horizontal clock position**
 - **Vertical clock position**
 - **Clock background color**



- **Clock foreground color**

Countdown visual effect: While the countdown is running, a current screenshot is displayed in the background. This parameter determines the visual effect that the screenshot will be displayed with.

Possible options:

- Dark screenshot
- Gray screenshot

Countdown background image: Path and file name of an image file, which is displayed in the background while the countdown is running. This background image is displayed instead of the screenshot, if the path and file name are valid; if the field is empty, the screenshot is displayed. Supported file formats: JPEG, PNG, GIF. Example: `/images/image.jpg`



Taskbar

Menu path: **Setup > User Interface > Desktop > Screenlock / Screensaver > Taskbar**

Taskbar settings for the login dialog

- Show taskbar in login screen. (Default)
- Show clock. (Default)
- Show keyboard layout switcher. (Default)
- Show on-screen keyboard button.
- Start on-screen keyboard automatically.
- Show reboot button.
- Show shutdown button. (Default)

Taskbar settings when the screenlock is active

- Show taskbar in screenlock. (Default)
- Show clock. (Default)
- Show keyboard layout switcher. (Default)
- Show on-screen keyboard button.
- Start on-screen keyboard automatically.
- Show reboot button.
- Show shutdown button.
- Show logoff button.

i There is no separate option for enabling/disabling network connection icons in the login dialog and/or on the locked screen. With **Show taskbar in login screen** and **Show taskbar in screenlock** enabled, they appear automatically if the option **Enable tray icon** is activated under **Setup > Network > LAN Interfaces > Interface 1 (or Interface 2, Wireless)** and/or under **Setup > Network > Mobile Broadband** (and/or **VPN**).

i The network connection icons in the login dialog and on the locked screen, with the exception of the Wi-Fi icon, serve for information purposes only and thus are inactive on clicking. The Wi-Fi icon invokes a [dialog for turning Wi-Fi on/off](#)(see page 701) or the [Wireless Manager](#)(see page 699) in case it is activated under **Setup > Network > LAN Interfaces > Wireless**.



Screensaver

Menu path: **Setup > User Interface > Desktop > Screen Lock/Saver > Screensaver**

- **Screen background color:** Color palette for determining the background color of the screen.
- **Enable image display**
 - An image will be shown as the screensaver. (default)
- **File for screen saver logo:** Complete path for an individual image file or directory that contains an unlimited number of images. If no path is given, the IGEL logo will be used.
 - Info:** If you enter a folder instead of a single image file as the source, all images in the folder will be displayed as a slide show, the **display time** for the images can be configured.
- **One image per monitor**
 - If a number of monitors are used, a different image will be shown on each one. (default)
 - Images will be distributed over the monitors.
- **Image duration:** Time in seconds until the image is changed. (default: 10)
- **Image display mode:** Type of display. The following are available to choose from:
 - Small-sized hopping - Small images are shown in changing positions.
 - Medium-sized hopping - Larger images are shown in changing positions.
 - Full-screen center cut-out - The images are shown in full-screen size. However, they may be clipped.
 - Full-screen letterbox - The images are shown as large as possible in relation to the screen size.
- **Clock display monitor:** Selects the monitor on which the clock is to be shown. The following are available to choose from:
 - None
 - All
 - A specific monitor
- **Show seconds:** Shows the seconds too in digital format.
- **Clock display size:** The following sizes are available to choose from:
 - Tiny
 - Small
 - Medium
 - Large
 - Huge
- **Horizontal clock position**
 - Left
 - Center
 - Right
- **Vertical clock position**
 - Top
 - Center
 - Bottom
- **Clock background color:** Color palette for determining the background color of the clock.
- **Clock background opacity percentage:** 75% is preset.



- **Clock foreground color:** Color palette for determining the foreground color of the clock.



Input

Menu path: **Setup > User Interface > Input**

These setup pages allow you to set the keyboard layout and other input options.

The following input devices can be set up:

- [Keyboard](#)(see page 672)
- [Additional Keyboard Layouts](#)(see page 673)
- [Mouse](#)(see page 674)
- [Touchpad](#)(see page 675)
- [Touchscreen](#)(see page 678)
- [Signature Pad](#)(see page 680)



Keyboard

Menu path: **User Interface > Input > Keyboard**

In this area, you can configure the keyboard.

Keyboard layout: Specify the keyboard layout. The selected layout applies to all parts of the system including emulations, window sessions and X applications.

Enable dead keys

Dead keys can be used to enter special characters.

Keyboard type: Specifies the keyboard type.

Possible values:

- **Default:** Automatically selects the keyboard type according to the computer type (Macbook, Chromebook or PC105 for all others).
- Standard PC keyboard (105 keys)
- IBM keyboard (122 keys)
- Trimodal keyboard
- Sun Type 6 keyboard
- Chromebook
- Macbook
- Macbook international
- Thinkpad

Show indicator in taskbar

Shows the language code for the keyboard in the taskbar.

Character Repeat

Repeat delay: Determines the delay (in milliseconds) before automatic repetition begins.

Repeat rate: Determines the number of times a character repeats per second.

Start with NumLock on

NumLock will be enabled automatically during the boot process.

Secure keyboard input with Cherry SECURE BOARD

A secure keyboard input mode will be enabled for the connected Cherry SECURE BOARD. In this mode, keyboard traffic between the keyboard and the endpoint is transmitted over a TLS 1.3 encrypted connection. The standard keyboard channel will be locked, which means that keyboard input devices without the secure mode will be blocked; see <https://www.cherry-world.com/cherry-secure-board-1-0.html>.



Additional Keyboard Layouts

Menu path: **Setup > User Interface > Input > Additional Keyboard Layouts**

In this area, you can define additional keyboard layouts which can be selected by the user.

- **Enable this layout**
 Keyboard layout is enabled and can be defined.
- **Keyboard layout:** Selects the language for the keyboard layout.
- **Enable dead keys:** Enable this function if the keyboard used supports dead keys for special characters.
- **Hotkey**
 A hotkey allowing you to switch to this keyboard can be defined.
- **Key:** Select a key for the key combination.
- **Modifier:** If necessary, select an additional modifier.

Hotkey for default keyboard layout

- **Enable hotkey to switch to the default keyboard layout**
 A hotkey which takes you back to the default keyboard layout can be defined. This is useful when a number of keyboard layouts are configured.

Hotkey for next keyboard layout

- **Enable hotkey to switch between a number of keyboard layouts**
 A hotkey which switches to the next keyboard layout can be defined. This is useful when a number of keyboard layouts are configured.
Further settings can be configured under On-screen Keyboard.



Mouse

Menu path: **Setup > User Interface > Input > Mouse**

In this area, you can configure the mouse.

- **Lefthand mode**
 The mouse is switched to left-handed mode.
- **Emulation 3 Button Mouse**: Enables/disables emulation of the third (middle) mouse button for mice with only two physical buttons. This third button is emulated by pressing both buttons at the same time. If 3-button emulation was enabled, the emulation time limit determines how long (in milliseconds) the driver waits before deciding whether two buttons were pressed at the same time.
- **Hide Cursor**: The mouse pointer will be hidden after the defined time limit.
- **Pointer Speed**: Determines the mouse resolution in counts per inch.
- **Double Click Interval**: Changes the maximum interval in milliseconds between two consecutive mouse clicks which are to be recognized as a double-click.
- **Double Click Distance**: Changes the maximum distance in pixels between two clicks which are to be recognized as a double-click. The object under the second click is double-clicked.



Touchpad

Menu path: **Setup > User Interface > Input > Touchpad**

Here, you can configure touchpad settings.

- ⓘ The actual settings depend on the hardware supported by the particular touchpad.

- **Enable Touchpad** Enable the touchpad
- **Hotkey** Each time you press the hotkey, you toggle the touchpad on or off.
 - **Modifiers:** Modifiers for the hotkey
 - **Key:** Key for the hotkey
- **Custom configuration**
 - Using the following options, adapt the touchpad to your needs.
 - No custom configuration (default)
- **Operation Mode:** Allows various touchpad modes.
Possible values:
 - Enable touchpad
 - Switch off touchpad
 - Turn off tapping and scrolling only
- **Min speed:** Minimum speed of the pointer in seconds (default: 1.00)
- **Max speed:** Maximum speed of the pointer in seconds (default: 1.75)
- **Acceleration:** Acceleration from the minimum to the maximum speed in seconds (default: 0.01)

The following settings apply by default:

- **Top Left Action:** No action
- **Bottom Left Action:** No action
- **Top Right Action:** Middle mouse button
- **Bottom Right Action:** Right mouse button

With some touchpads, you can assign functions to the four corners. Specify which mouse button is clicked by tapping in the relevant corner:

- No action
- Left mouse button
- Middle mouse button
- Right mouse button



Touchpad Scrolling

Define the properties for vertical and horizontal scrolling here.

Vertical

- **Vertical scrolling:**
 The right edge of the touchpad will be used as a vertical scrollbar. The vertical scroll speed can be set.
 The right edge is not enabled as a scrollbar. (default)
- **Vertical scroll speed:** Specifies from what distance scrolling is recognized when moving in a vertical direction. (default: 25.00)
- **Scroll vertically with two fingers:**
 Two-finger scrolling is enabled for vertical scrolling.
 Two-finger scrolling is disabled.

Horizontal

- **Horizontal scrolling:**
 The bottom edge of the touchpad will be used as a horizontal scrollbar. The horizontal scroll speed can be set.
 The bottom edge is not enabled as a scrollbar. (default)
- **Horizontal scroll speed:** Specifies from what distance scrolling is recognized when moving in a horizontal direction. (default: 25.00)
- **Scroll horizontally with two fingers:**
 Two-finger scrolling is enabled for horizontal scrolling.
 Two-finger scrolling is disabled.



Touchpad Advanced

Further settings are possible here:

- **Corner coasting**

- You can continue scrolling if your finger reaches the corner when scrolling vertically or horizontally along the touchpad edges.

- **Circular scrolling**

- You can scroll in a circle. In the selection menu, specify where circular scrolling is to begin.

- **Circular scrolling enabled at**

- [All Edges](#)

- Top Edge

- Top Right Corner

- Right Edge

- Bottom Right Corner

- Bottom Edge

- Bottom Left Corner

- Left Edge

- Top Left Corner

- **Tap and drag gesture**

- You can move items by tapping and dragging them.

- **Locked drags**

- The tap and drag gesture ends only after an additional tap; it will otherwise end when you let go.

- **Palm detect**

- Avoids triggering a function accidentally with the palm of your hand. The function must be supported by the device.

- **ClickPad**

- ClickPads are permitted. These are touchpads with so-called integrated soft buttons on which physical clicks are possible.



Touchscreen

Menu path: **Setup > User Interface > Input > Touchscreen**

Here, you can configure a touchscreen. To ensure that you can open the setup and navigate within it, the initial configuration should take place with a mouse and keyboard connected.

You will find an up-to-date list of the touchscreens supported by IGEL in the [IGEL Third Party Hardware Database³⁷](#).

Enable touchscreen

- The touchscreen is enabled.
- The touchscreen is disabled. (Default)

Touchscreen type: Selects the touchscreen driver which is to be used.

Possible options:

- ["EvTouch \(USB\)"](#)
- "eGalax"
- "Elo Multitouch (USB)"
- "Elo Singletouch (USB)"
- "TSharc"

You will find the complete list of supported devices in the [IGEL Hardware Database³⁸](#).

Touchscreen already calibrated

If you enable the touchscreen function, the touchscreen must be calibrated first.

- Calibration starts automatically after each system boot. (Default)
- Calibration does not start automatically after each system boot.

Swap X and Y values

X values are interpreted as Y values and Y values as X values. Enable this option if the mouse pointer moves vertically when you move your finger in a horizontal direction.

- X and Y values are not swapped. (Default)

Minimal X/Y value: These values are determined by the calibration tool. However, you can also change them manually. (Default: 0)

Maximal X/Y value: These values are determined by the calibration tool. However, you can also change them manually. (Default: 4000)

Untouch delay: The maximum permitted time (in milliseconds) between two instances of contact which are still registered as a single touch. When moving windows by drag & drop, for example, your contact with the screen may inadvertently be interrupted. Increasing this value prevents the thin client from recognizing two individual contacts if you let go in this way. (Default: 3)

Report delay: Determines how long (in milliseconds) the screen needs to be touched in order for the contact to be recognized. (Default: 2)

Emulate right button

³⁷ <https://www.igel.com/linux-3rd-party-hardware-database/>

³⁸ <https://www.igel.com/linux-3rd-party-hardware-database/>



- A right-click is generated by touching the screen for a long time.
- Touching the screen for a long time does not generate a right-click. (Default)

Right button timeout: Time (in milliseconds) after which a right-click is generated. (Default: 1000)

Set driver-specific defaults: Loads the preset for the driver currently selected under **Touchscreen type**. Click on this button once after changing the touchscreen type or to restore the default settings.

Multimonitor

Graphic card: Graphics card assigned to the selected touchscreen. A graphics card can have more outputs than are actually used. In order to ensure transparency, you may need to assign the graphics cards manually.

- i** If “Automatic” is set for the **Touchscreen monitor** and no configurable monitor is found for the selected graphics card, the next available monitor will be used by another graphics card.

Touchscreen monitor: Assigns a monitor connection to the touchscreen. Example: **DisplayPort** (Default: Automatic)

To set up a touchscreen and on-screen keyboard, proceed as follows:

- ▶ Enable the on-screen keyboard for the touchscreen use under **IGEL Setup > Accessories > On-Screen Keyboard**; see [On-Screen Keyboard](#)(see page 568).

- i** The layout for the normal keyboard will also be used for the on-screen keyboard.

- ▶ Calibrate the touchscreen for optimum contact recognition. The **touchscreen calibration** application can be found under **Application Launcher > System**.

In the calibration program, you will see a pattern with calibration points which must be touched one after another.



Signature Pad

Menu path: **Setup > User Interface > Input > Signature Pad**

You can connect signature pads from the following manufacturers here:

- StepOver;
- signotec.

StepOver

- **Enable StepOver TCP Client**

The StepOver TCP Client is enabled and you can use USB signature pads from this manufacturer in sessions.

The StepOver TCP Client is not enabled. (Default)

- **Listening TCP port:** If necessary, you can change the TCP port. (Default: 8888)

signotec

- **Enable signotec VCOM daemon**

The signotec VCOM daemon is enabled and you can use USB signature pads from this manufacturer in sessions.

The signotec VCOM daemon is not enabled. (Default)

See also the tip & trick Connecting Signature Pads.



Hotkeys

Menu path: **Setup > User Interface > Hotkeys > Commands**

In order to make it easier to use your thin client, hotkeys are available for frequent operating routines. A hotkey is a combination of one or more modifiers and an alphanumeric key.

You can enable or disable hotkeys and change the keys used. For more information, see [Commands\(see page 682\)](#).

-
- [Commands\(see page 682\)](#)



Commands

Menu path: **Setup > User Interface > Hotkeys > Commands**

You can activate, deactivate and change the hotkeys that are available to the user.

Settings in the Dialog

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
-  = `Shift`
- `[Ctrl]` = `Ctrl`
-  = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows Key` = `Ctrl|Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Available Hotkeys and their Default Settings

Hide all windows and show desktop

Default:



- activated
- **Modifiers:** `Ctrl|Mod4`
- **Key:** `d`
- **Appliance Mode Access:** deactivated

Mapping Ctrl+Alt+End to Ctrl+Alt+Del for Citrix sessions

Default:

- deactivated
- **Modifiers:** `Ctrl|Alt + End`
- **Key:** `End`
- **Appliance Mode Access:** deactivated

Open start menu

Default:

- deactivated
- **Modifiers:** `Shift + Super`
- **Key:** `Super_L`
- **Appliance Mode Access:** deactivated

Open start menu (alternative):

Default:

- deactivated
- **Modifiers:** `Shift + Super`
- **Key:** `Super_L`
- **Appliance Mode Access:** deactivated

Screenshot of active window

Default:

- deactivated
- **Modifiers:** `Ctrl|Alt`
- **Key:** `Print`
- **Appliance Mode Access:** deactivated

Screenshot of entire screen

Default:

- deactivated
- **Modifiers:** `Ctrl|Shift`
- **Key:** `Print`

Switch between active windows using Task Switcher

Default:

- activated
- **Modifiers:** `Ctrl|Alt`
- **Key:** `Tab`
- **Appliance Mode Access:** deactivated

Switch between active windows using Task Switcher (backwards)

Default:



- activated
- **Modifiers:** `Ctrl|Alt|Shift`
- **Key:** `Tab`
- **Appliance Mode Access:** deactivated

Switch focus to next window

Default:

- activated
- **Modifiers:** `Ctrl`
- **Key:** `Escape`
- **Appliance Mode Access:** deactivated

Switch focus to next window (alternative)

Default:

- activated
- **Modifiers:** `Ctrl|Alt`
- **Key:** `Up`
- **Appliance Mode Access:** deactivated

Switch focus to next window (reverse order)

Default:

- activated
- **Modifiers:** `Ctrl|Alt`
- **Key:** `Down`
- **Appliance Mode Access:** deactivated

Volume down (multimedia key)

Default:

- activated
- **Modifiers:** (none)
- **Key:** `XF86AudioLowerVolume`

Volume mute (multimedia key)

Default:

- activated
- **Modifiers:** (none)
- **Key:** `XF86AudioMute`
- **Appliance Mode Access:** deactivated

Volume up (multimedia key)

Default:

- activated
- **Modifiers:** (none)
- **Key:** `XF86AudioRaiseVolume`
- **Appliance Mode Access:** deactivated



Font Services

Menu path: **Setup > User Interface > Font Services**

You can import further fonts in addition to the ones provided by IGEL:

- XC Font Service(see page 686)
- NFS Font Service(see page 687)



XC Font Service

Menüpfad: **Setup > User Interface > Font Services > XC Font Service**

In this area, you can configure the XC Font Service.

- **Enable XC Font Service**

- The XC Font Service is enabled.
 Der XC Font Service is not enabled. (Default)

Once you have enabled the XC Font Service, you can define the following settings:

- **XC Font Server:** The server on which the XC Font Service is running.
- **Port Number:** The port number on which the XC Font Service is available. (Default: 7100)
- **Prefer Local Fonts**
 - Local fonts are used before a request is sent to the font server.
 - Local fonts are not preferred. (Default)



NFS Font Service

Menu path: **Setup > User Interface > Font Services > NFS Font Service**

Using the NFS font service is another way to import additional fonts. The NFS font service also offers the advantage that the mount point for the fonts can be configured. This is necessary for a number of remote applications that search for your fonts in a specific directory.

To define and enable an NFS font path entry in order to use the NFS font service, proceed as follows.

1. Click on **Add** to open the dialog window:
 - **Local Path:** Defines the local directory for the mount point
 - **NFS Server:** Name or IP address of the server that makes available the font directories via NFS.
 - **Remote Path:** Path on the server under which the fonts are available.
 - **Prefer Local Fonts**
 Local fonts are used before a request is sent to the font server.
2. Click on **OK** to enable the entry.
3. Export the font directory on the server via NFS read-only for the thin client.



Network

In this area, you can configure network connections of the endpoint device.

- [LAN Interfaces](#)(see page 689)
- [Mobile Broadband](#)(see page 707)
- [DHCP Client](#)(see page 709)
- [VPN](#)(see page 712)
- [SCEP Client \(NDES\)](#)(see page 739)
- [Routing](#)(see page 744)
- [Hosts](#)(see page 746)
- [Network Drives](#)(see page 747)
- [Proxy](#)(see page 752)



LAN Interfaces

Menu path: **Setup > Network > LAN Interfaces**

Here, you can configure the LAN interfaces.

(i) Predictable Network Interface Names (PNINs)

As of IGEL OS 11.06, the names of Ethernet and WLAN interfaces are predictable network interface names (PNINs), see [Predictable Network Interface Names](#)³⁹. This ensures the stability of interface names on reboot and generally improves the reliability of associating configurations with interfaces.

- As "eth0", "eth1", and "wlan0" have been replaced by PNINs, configurations or custom scripts that include the old names of Ethernet and WLAN interfaces, e.g. `eth0`, `eth2`, `wlan0`, etc. have to be adjusted.

The following already existing configurations do NOT require manual adjustment since old names `eth0`, `eth1`, etc. will internally be replaced by the correct PNINs automatically:

- Tcpdump
- **Bind interface** under **Security > Smartcard > Services**, see [Services](#)(see page 818)

- To view the PNINs and the order of the configured interfaces, you can use the following commands. The default interface is always listed first, the second interface is listed second, etc.

Ethernet (LAN): `cat /config/net/en-interfaces`

WLAN: `cat /config/net/wl-interfaces`

(Note: Only the first wireless interface (former `wlan0`) is supported. All other wireless interfaces will be ignored.)

- If you need to configure more than two Ethernet interfaces, go to **System > Registry > network.interfaces.ethernet.device%** and add an instance.
To explicitly assign a configuration instance to a certain interface, enter the corresponding PNIN for the registry key **network.interfaces.ethernet.device%.ifname**.

Activate default interface (Ethernet)

The default interface is enabled. (Default)

The Ethernet interface is not enabled.

Get IP from the DHCP server: The IP address of the client will be obtained automatically using DHCP. (Default)

DHCP options can be specified under [DHCP Client](#)(see page 709).

Specify an IP address: The IP address and the network mask are entered manually.

IP address: IP address of the device.

Network mask: Network mask of the device.

Default gateway: IP address of the default gateway.

Enable

Routing via the default gateway is enabled.

³⁹ <https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/>



Routing via the default gateway is not enabled. (Default)

Terminal name: Local name of the device. If the field is empty, the default name combined of ' ITC ' with a MAC address will be generated.

Enable DNS

The manual DNS configuration will be used.

The DNS configuration will be carried out by DHCP or BOOTP. (Default)

Default domain: Usually the name of the local network.

Name server: IP address of the name server to be used.

Name server: IP address of an alternative name server.

Manually overwrite DHCP settings

The default route, the domain name, and the DNS server will be overwritten by manual entries.

Manual entries will not overwrite DHCP settings. (Default)

Dynamic DNS registration:

The terminal name will be registered dynamically via the DNS or DHCP server.

The terminal name will not be registered dynamically. (Default)

Dynamic DNS registration method

- DHCP: Updates the terminal name through DHCP option 81.
- DNS: Sends updates to the DNS server in accordance with RFC 2136.

TSIG key file for additional DNS authentication: Path to the private key if TSIG-based DDNS registration is used.

-
- [Individual Interface](#)(see page 691)
 - [Wireless](#)(see page 696)



Individual Interface

Menu path: **Setup > Network > LAN Interfaces > [Interface]**

i Predictable Network Interface Names (PNINs)

As of IGEL OS 11.06, the names of Ethernet and WLAN interfaces are predictable network interface names (PNINs), see [Predictable Network Interface Names](#)⁴⁰. This ensures the stability of interface names on reboot and generally improves the reliability of associating configurations with interfaces.

- As "eth0", "eth1", and "wlan0" have been replaced by PNINs, configurations or custom scripts that include the old names of Ethernet and WLAN interfaces, e.g. `eth0`, `eth2`, `wlan0`, have to be adjusted.

The following already existing configurations do NOT require manual adjustment since old names `eth0`, `eth1`, etc. will internally be replaced by the correct PNINs automatically:

- Tcpdump
- **Bind interface** under **Security > Smartcard > Services**, see [Services](#)(see page 818)

- To view the PNINs and the order of the configured interfaces, you can use the following commands. The default interface is always listed first, the second interface is listed second, etc.

Ethernet (LAN): `cat /config/net/en-interfaces`

WLAN: `cat /config/net/wl-interfaces`

(Note: Only the first wireless interface (former `wlan0`) is supported. All other wireless interfaces will be ignored.)

- If you need to configure more than two Ethernet interfaces, go to **System > Registry > network.interfaces.ethernet.device%** and add an instance.

To explicitly assign a configuration instance to a certain interface, enter the corresponding PNIN for the registry key **network.interfaces.ethernet.device%.ifname**.

Activate default interface (Ethernet)

The default interface will be enabled. (Default)

The Ethernet interface will not be enabled.

Get IP from DHCP server

The IP address of the client will be obtained automatically using DHCP. (Default)

DHCP options can be specified under [DHCP Client](#)(see page 709).

Specify an IP address: The IP address and the network mask are entered manually.

IP address: IP address of the device.

Network mask: Network mask of the device.

IPv6 Configuration

- Compatibility mode: Behavior of earlier firmware versions.
- Disabled: IPv6 completely disabled.

⁴⁰ <https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/>



- Automatic: IPv6 auto configuration based on router advertisements (can include DHCPv6).
For further information, see [RFC 4861](#).⁴¹
- DHCPv6: IPv6 configuration using DHCPv6 if router advertisements are not available.
This is mentioned in [RFC 4862 Section 5.5.2](#).⁴²

Network link type

- [Auto sense](#)
- 1000 Mb/s full duplex
- 100 Mb/s full duplex
- 100 Mb/s half duplex
- 10 Mb/s full duplex
- 10 Mb/s half duplex

Force auto-negotiation

With this option, problems with half/full duplex for specific switches that expect the auto-negotiation flag for fixed bandwidths can be addressed.

Automatic negotiation will not be forced. (Default)

Enable tray icon

A tray icon for the network interface will be shown. (Default)

Enable context menu

A context menu will be shown when you click on the tray icon. (Default)

Enable network info dialog

A dialog window with information regarding the network connection will be shown when you click on the context menu. (Default)

-
- [Authentication](#)(see page 693)
 - [Wake-on-LAN](#)(see page 695)

⁴¹ <https://tools.ietf.org/html/rfc4861>

⁴² <https://tools.ietf.org/html/rfc4862#section-5.5.2>



Authentication

Menu path: **Setup > Network > LAN Interfaces > [Interface] > Authentication**

Here, you can enable and configure network port authentication.

Enable IEEE-802.1x authentication

- Network port authentication is enabled.
 Network port authentication is not enabled. (Default)

If you enable authentication, further options are available:

EAP type: Here, you can select the authentication procedure:

- PEAP: Protected Extensible Authentication Protocol
- TLS: Transport Layer Security with client certificate
- TTLS: Tunneled Transport Layer Security
- FAST: Flexible Authentication via Secure Tunneling

Anonymous identity: This identity is sent by authentication instead of the actual **Identity**. This prevents the disclosure of the actual identity of the user. The anonymous identity is relevant for any of the above-mentioned **EAP types**, except for "TLS".

Auth method: The following authentication methods are available:

- MSCHAPV2: Microsoft Challenge Handshake Authentication Protocol
- TLS: Transport Layer Security with client certificate
- GTC: Generic Token Card
- MD5: MD5-Challenge
- PAP: Password Authentication Protocol

Validate server certificate

- The server's certificate is checked cryptographically. (Default)

CA Root certificate: The path to the CA root certificate file. This can be in PEM or DER format.

Identity: User name for RADIUS

Password: Password for network access

- i** If you leave the **Identity** and **Password** fields empty, an entry mask for authentication purposes will be shown. However, this does not apply to the methods with a client certificate (TLS and PEAP-TLS) where these details are mandatory.

The following settings are relevant if you have selected "TLS" as **EAP type**:

Manage certificates with SCEP (NDES)

- Client certificates will automatically be managed with [SCEP](#)(see page 739).
 Client certificates will not be managed with [SCEP](#)(see page 739). (Default)

Client certificate: Path to the file with the certificate for client authentication in the PEM (base64) or DER format.



- ⓘ If a private key in the PKCS#12 format is used, leave this field empty.

Private key: Path to the file with the private key for the client certificate. The file can be in the PEM (base64), DER, or PFX format. The **Private key password** may be required for access.

Identity: User name for network access

Private key password: Password for the **Private key** for the client certificate

The following setting is relevant if you have selected "FAST" as **EAP type**:

Automatic PAC provisioning: Specifies how the PAC (Protected Access Credential) is delivered to the client.
Possible options:

- "disabled": PAC files have to be transferred to the device manually, e.g. via UMS file transfer.
- "unauthenticated": An anonymous tunnel will be used for PAC provisioning.
- "authenticated": An authenticated tunnel will be used for PAC provisioning.
- "unrestricted

- ⓘ PAC files are stored in `/wfs/eap_fast_pacs/`.

PAC file names are automatically derived from the **Identity**, but are coded. In the case of the manual PAC provisioning, you can determine the PAC file names with the following script: `/bin/gen_pac_filename.sh`

- ⓘ In tests with `hostapd`, it has been necessary to disable TLS 1.2. To do that, enter the following command for **System > Registry**

`> network.interfaces.ethernet.device%.ieee8021x.phase1_direct: tls_disable_tls1_2=1`



Wake-on-LAN

Menu path: **Setup > Network > LAN Interfaces > [Interface] > Wake-On-LAN**

Select the packets or messages with which the endpoint device can be started via the network.

For further information on the Wake-on-LAN functionality of the UMS, see Wake-on-LAN.

Wake on magic packet

The device can be started with a Wake-on-LAN magic packet. (Default)

Wake on ARP packet

The device can be started with a Wake on ARP packet.

The device cannot be started with a Wake on ARP packet. (Default)

Wake on broadcast message

The device can be started with a Wake on broadcast message.

The device cannot be started with a Wake on broadcast message. (Default)

Wake on multicast message

The device can be started with a Wake on multicast message.

The device cannot be started with a Wake on multicast message. (Default)

Wake on physical activity

The device can be started with a physical activity.

The device cannot be started with a physical activity. (Default)

Wake on unicast message

The device can be started with a Wake on unicast message.

The device cannot be started with a Wake on unicast message. (Default)



Wireless

Menu path: **Setup > Network > LAN Interfaces > Wireless**

In this area, you can configure everything relating to your wireless connections.

- ❖ Configure the [wireless frequency range](#)(see page 706) to ensure that your device meets the local regulations for wireless equipment.

You will find details of compatible wireless hardware in the [IGEL Linux 3rd Party Hardware Database](#)⁴³.

ⓘ Predictable Network Interface Names (PNINs)

As of IGEL OS 11.06, the names of Ethernet and WLAN interfaces are predictable network interface names (PNINs), see [Predictable Network Interface Names](#)⁴⁴. This ensures the stability of interface names on reboot and generally improves the reliability of associating configurations with interfaces.

- As "eth0", "eth1", and "wlan0" have been replaced by PNINs, configurations or custom scripts that include the old names of Ethernet and WLAN interfaces, e.g. `eth0`, `eth2`, `wlan0`, have to be adjusted.

The following already existing configurations do NOT require manual adjustment since old names `eth0`, `eth1`, etc. will internally be replaced by the correct PNINs automatically:

- Tcpdump
- **Bind interface** under **Security > Smartcard > Services**, see [Services](#)(see page 818)

- To view the PNINs and the order of the configured interfaces, you can use the following commands. The default interface is always listed first, the second interface is listed second, etc.

Ethernet (LAN): `cat /config/net/en-interfaces`

WLAN: `cat /config/net/wl-interfaces`

(Note: Only the first wireless interface (former `wlan0`) is supported. All other wireless interfaces will be ignored.)

- If you need to configure more than two Ethernet interfaces, go to **System > Registry > network.interfaces.ethernet.device%** and add an instance.

To explicitly assign a configuration instance to a certain interface, enter the corresponding PNIN for the registry key **network.interfaces.ethernet.device%.ifname**.

Activate wireless interface

The default interface is enabled.

The wireless interface is not enabled. (Default)

Get IP from DHCP server: The IP address of the endpoint device will be obtained automatically using DHCP. (Default)

DHCP options can be specified under [DHCP Client](#)(see page 709).

Specify IP address: The IP address and the network mask are entered manually

⁴³ <https://www.igel.com/linux-3rd-party-hardware-database/>

⁴⁴ <https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/>

IP address: IP address of the endpoint device

Network mask: Network mask of the endpoint device

IPv6 configuration:

- Compatibility mode: Behavior of earlier firmware versions
- Disabled: IPv6 is completely disabled.
- Automatic: IPv6 auto-configuration is based on router advertisements (can include DHCPv6). You will find further information in [RFC 4861](#)⁴⁵.
- DHCPv6: IPv6 configuration using DHCPv6 if router advertisements are not available. You will find further information in [RFC 4862 Section 5.5.2](#)⁴⁶.

Enable tray icon

A tray icon for the wireless interface will be shown. (Default)

Enable context menu

A context menu will be shown when you click on the tray icon. (Default)

Enable network info dialog

A dialog window with information regarding the network connection will be shown when you click on the context menu. (Default)

Enable Wireless Manager

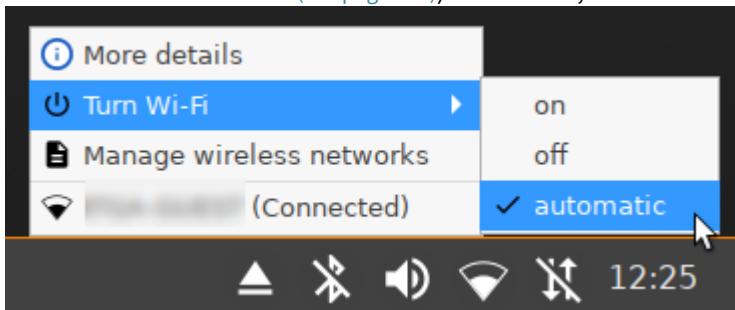
The [Wireless Manager](#)(see page 699) is enabled. This tool allows the user to establish a connection to a wireless network quickly.

The Wireless Manager is disabled. (Default)

Enable Wi-Fi automatic switch

When a device is disconnected from the network cable, Wi-Fi is automatically turned on. When the device is connected again to the network cable, Wi-Fi is automatically turned off.

- If the registry key **System > Registry > network.applet.wireless.enable_wifi_switch** (see [Switch for the Wi-Fi Connection](#)(see page 701)) is enabled, automatic mode is added to the Wi-Fi switch.



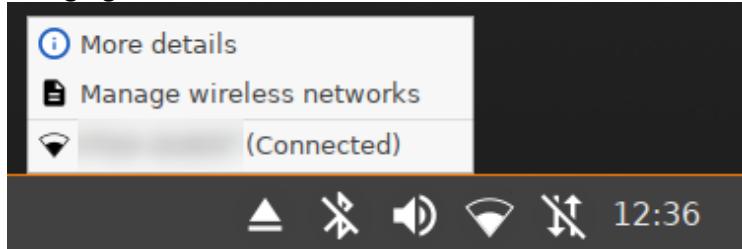
- If the registry key **System > Registry > network.applet.wireless.enable_wifi_switch** is disabled, Wi-Fi automatic switch functionality will work in the background. The option for

⁴⁵ <https://tools.ietf.org/html/rfc4861>

⁴⁶ <https://tools.ietf.org/html/rfc4862#section-5.5.2>



changing the Wi-Fi mode is not shown.



An automatic connection to a wireless network is disabled. (Default)

- i** If you use wireless regularly, it is recommended to enable the following options: **Enable tray icon**, **Enable context menu**, and **Enable Wireless Manager**. Via the **Wireless Manager**, you can use IGEL Café Wireless. If you have to frequently switch between LAN and WLAN networks, it is also useful to activate **Enable Wi-Fi automatic switch**.

- [Wireless Manager](#)(see page 699)
- [Switch for the Wi-Fi Connection](#)(see page 701)
- [Default Wi-Fi Network](#)(see page 702)
- [Additional Wi-Fi Networks](#)(see page 705)
- [Wireless Regulatory Domain](#)(see page 706)

Wireless Manager

The Wireless Manager tool allows the user to connect quickly to available wireless networks.

- ⓘ The Wireless Manager can be enabled under **Network > LAN Interfaces > Wireless**.

You can bring up the Wireless Manager from the tray icon for wireless:



See also How to Launch the Wireless Manager within IGEL OS when the Taskbar Is Hidden.

1. Click on the tray icon for wireless and select **Manage wireless networks** from the context menu.



2. Search for available networks.
 - The list of active networks is sorted according to the quality of their signal strength.
 - Previously configured connections are flagged with a tick in the **Configured** column.
 - The connection currently active is likewise flagged with a symbol under **Connected**.
3. Double-click on a network in the list in order to open the entry mask.
You can either **permanently save** the logon information or enter it each time you establish a connection to this network.



i Click on the key symbol in order to display the key phrase while you are typing.

4. Click on the **Connect network** button in order to establish the previously configured connection:
The tray icon will change to show the connection quality.
Hidden networks appear in the Wireless Manager with the network name empty or can be defined using the **Search for network** button.
In order to connect to a previously unknown hidden network, you must first enter the SSID before the access data are retrieved:

i If you have configured the available connections, you will no longer need the Wireless Manager in order to establish a connection.

In the context menu for the tray icon, all available networks are listed and can be brought up from here.

5. The IGEL Setup shows all connections configured by the local user under **Network > LAN Interfaces > Wireless > Additional Wi-Fi Networks**.

See also Café Wireless (Wi-Fi).

Switch for the Wi-Fi Connection

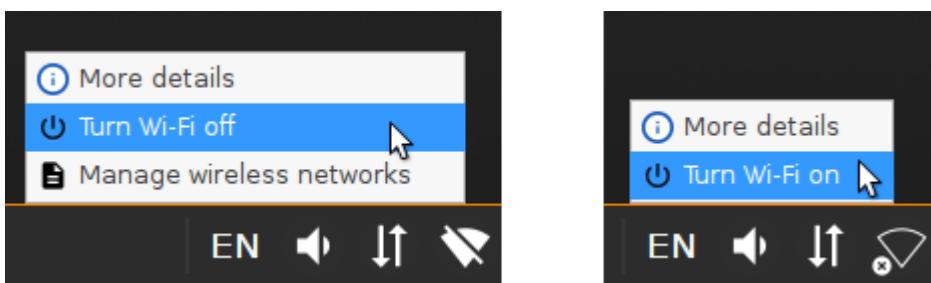
You can turn Wi-Fi off or on.

To use the switch for the Wi-Fi connection, **Enable Wi-Fi switch** under **Setup > System > Registry > Parameter > network > applet > wireless > enable_wifi_switch** must be activated. (Default)

Turning Wi-Fi Off or On

If You Are Logged In

- ▶ Select **Turn Wi-Fi off / Turn Wi-Fi on** from the context menu of the Wi-Fi tray icon.



If the Login Dialog Is Displayed or the Screen Is Locked

- ▶ To turn Wi-Fi off, click the tray icon  and select **OK** in the **Turn Wi-Fi off** dialog. If the [Wireless Manager](#)(see page 699) is activated, you can also use there the button .
- ▶ To turn Wi-Fi on, click  and select **OK** in the **Turn Wi-Fi on** dialog.



Default Wi-Fi Network

Menu path: **Setup > Network > LAN Interfaces > Wireless > Default Wi-Fi network**

Here, you can configure wireless network connections.

Disable Encryption: No encryption will be used. (Default)

Enable WEP Encryption: WEP encryption will be used.

Enable WPA Encryption: WPA encryption will be used.

- ⓘ You will need to give further information depending on the encryption method chosen.

Wireless Network Name (SSID): Name of the wireless network (SSID)

For WEP Encryption

Transmit key ID: Choose from a maximum of four configurable keys. (Default: 1)

Key Format:

- ASCII
- Hexadecimal

Key [1-4]: Enter the key here.

- ⓘ Characters to be entered for WEP keys:
 - For 64-bit encryption, 5 characters (ASCII) or 10 hex digits (hexadecimal)
 - For 128-bit encryption, 13 characters (ASCII) or 26 hex digits (hexadecimal)

For WPA/WPA2/WPA3 Personal Encryption

Network authentication

- WPA Personal: Wi-Fi Protected Access Pre-Shared Key (WPA / IEEE 802.11i/D3.0)
- WPA2 Personal: Wi-Fi Protected Access Pre-Shared Key (WPA2 / IEEE 802.11i/RSN)
- WPA3 Personal: Wi-Fi Protected Access SAE (Simultaneous Authentication of Equals)

Network key: WPA network key/passphrase as set at the dial-in point. This is either an ASCII character string with a length of 8...63 or exactly 64 hexadecimal digits.

Data encryption:

- Default: The default value depends on which network authentication method is selected - TKIP for WPA, AES (CCMP) for WPA2.
- TKIP: Temporal Key Integrity Protocol (IEEE 802.11i/D7.0)
- AES (CCMP): AES in Counter mode with CBC-MAC (RFC 3610, IEEE 802.11i/D7.0)
- AES (CCMP) + TKIP: One of two encryption methods is selected by the access point.
- Automatic: The access point can choose the encryption method freely – nothing is stipulated.

AP Scan mode: Scan mode for access points



- Default
- Broadcast: Alternative for access points which allow the SSID broadcast
- No broadcast: Alternative for access points which refuse the SSID broadcast (hidden access points)

For WPA/WPA2 Enterprise Encryption

Network authentication:

- WPA Enterprise: Wi-Fi Protected Access with 802.1X authentication (WPA / IEEE 802.11i/D3.0)
- WPA2 Enterprise: Wi-Fi Protected Access with 802.1X authentication (WPA2/IEEE 802.11i/RSN)

Data encryption:

- Default: The default value depends on which network authentication method is selected - TKIP for WPA, AES (CCMP) for WPA2.
- TKIP: Temporal Key Integrity Protocol (IEEE 802.11i/D7.0)
- AES (CCMP): AES in Counter mode with CBC-MAC (RFC 3610, IEEE 802.11i/D7.0)
- AES (CCMP) + TKIP: One of two encryption methods is selected by the access point.
- Automatic: The access point can choose the encryption method freely – nothing is stipulated.

AP Scan mode: Scan mode for access points

- Default
- Broadcast: Alternative for access points which allow the SSID broadcast
- No broadcast: Alternative for access points which refuse the SSID broadcast (hidden access points)

EAP Type

- PEAP: Protected Extensible Authentication Protocol
- TLS: Transport Layer Security with client certificate
- TTLS: Tunneled Transport Layer Security
- FAST: Flexible Authentication via Secure Tunneling

Anonymous identity: This identity is sent by authentication instead of the actual **Identity**. This prevents the disclosure of the actual identity of the user. The anonymous identity is relevant for any of the above-mentioned **EAP types**, except for "TLS".

Auth Method: Method for authentication that is available for the selected EAP type
Possible options:

- MSCHAPv2: Microsoft Challenge Handshake Authentication Protocol
- TLS: Transport Layer Security with client certificate
- GTC: Generic Token Card
- MD5: MD5-Challenge
- PAP: Password Authentication Protocol

Validate Server Certificate

- The endpoint device validates the authenticity of the authentication server against the certificate file. This certificate file is stored under the path defined by **CA Root Certificate**.
- The authenticity of the authentication server is not validated.

CA Root Certificate: Path and file name of the file that contains the certificates with which the authentication server authenticates itself.



Identity: User name that is stored at the authentication server

Password: Password relevant to the user name

The following settings are relevant if you have selected "TLS" as **EAP type**:

Manage certificates with SCEP (NDES)

- Client certificates will automatically be managed with [SCEP\(see page 739\)](#).
- Client certificates will not be managed with [SCEP\(see page 739\)](#). (Default)

Client certificate: Path to the file with the certificate for client authentication in the PEM (base64) or DER format.

- i** If a private key in the PKCS#12 format is used, leave this field empty.

Private key: Path to the file with the private key for the client certificate. The file can be in the PEM (base64), DER, or PFX format. The **Private key password** may be required for access.

Identity: User name for network access

Private key password: Password for the **Private key** for the client certificate

Learn more from the how-to Using WPA Enterprise / WPA2 Enterprise with TLS Client Certificates.

The following setting is relevant if you have selected "FAST" as **EAP type**:

Automatic PAC provisioning: Specifies how the PAC (Protected Access Credential) is delivered to the client.
Possible options:

- "disabled": PAC files have to be transferred to the device manually, e.g. via UMS file transfer.
- "unauthenticated": An anonymous tunnel will be used for PAC provisioning.
- "authenticated": An authenticated tunnel will be used for PAC provisioning.
- "unrestricted

- i** PAC files are stored in `/wfs/eap_fast_pacs/`.
PAC file names are automatically derived from the **Identity**, but are coded. In the case of the manual PAC provisioning, you can determine the PAC file names with the following script: `/bin/gen_pac_filename.sh`

- i** In tests with `hostapd`, it has been necessary to disable TLS 1.2. To do that, enter the command `tls_disable_tls1_2=1` for the following registry keys:
 - **System > Registry > network.interfaces.wirelesslan.device0.wpa.phase1_direct**
 - **System > Registry > network.interfaces.wirelesslan.device0.alt_ssid%.wpa.phase1_direct**



Additional Wi-Fi Networks

Menu path: **Setup > Network > LAN Interfaces > Wireless > Additional Wi-Fi Networks**

You can add other wireless networks here. The settings options per wireless network correspond to those for the [Default Wi-Fi Network](#)(see page 702).

To edit the wireless network list, proceed as follows:

- ▶ Click to create a new entry.
- ▶ Click to remove the selected entry.
- ▶ Click to edit the selected entry.
- ▶ Click to copy the selected entry.



Wireless Regulatory Domain

Menu path: **Setup > Network > LAN Interfaces > Wireless > Wireless Regulatory Domain**

This page allows you to set the wireless device in accordance with local regulations.

Wireless regulatory domains: Select the area in which the device is located.

- Not configured
- Africa
- Arctic
- Asia
- Australia
- Europe
- North America
- South America
- World

Location: Select the country in which the device is located.

- Not configured
- Albania
- Armenia
- [...]
- Cyprus
- Austria

The list below sets out the technical requirements for the selected location for your information.



Mobile Broadband

Menu path: **Setup > Network > Mobile Broadband Network**

Here, you can change the settings for a modem or a surf stick. This function is available from **IGEL Linux Version 10.03.100**.

- ❖ Ensure that data traffic is adequately secured. You can do this in the following ways:
 - Use a private APN.
 - Use OpenVPN and block traffic that would circumvent VPN with firewall rules.

If the device is already inserted and has been configured, the network connection will be established after the thin client boots. It can take between a few seconds and around 1 minute to establish a connection. The network connection will remain in place until the surf stick is removed or the thin client is put on standby or shut down.

The status of the network connection is shown in the system tray:

- The network connection is established; the thin client is online This symbol is only shown if "Modem" is selected as the device type. If "Router" is selected as the device type, the symbol for a LAN connection will be shown.
- The network connection was interrupted; the thin client is offline This symbol is only shown if "Modem" is selected as the device type. If "Router" is selected as the device type, the corresponding symbol for a LAN connection will be shown.

You can change the following settings:

- **Enable mobile broadband**

- The mobile broadband network can be used if a supported modem is connected.
- The mobile broadband network cannot be used. (default)

- **Device type**

Possible options:

- **Modem:** The device will be operated as a modem. The access data can be changed with the parameters **number**, **user name**, **password**, **APN**, **network ID** and **PIN**.
- Router: The device will be operated as a router. The device must be configured in advance in such a way that it is ready for use when it is inserted.

- i** Select the "Router" device type if you use a device from Huawei in the HiLink mode; example: Huawei E3372.

- **Number:** Access number for your network connection. If you do not know the access number, ask your mobile communications operator for it.
- **User name:** User name for your network connection. If you do not know the user name, ask your mobile communications operator for it.
- **Password:** Password for your network connection. If you do not know the password, ask your mobile communications operator for it.
- **APN:** APN (Access Point Name) for your network connection. If you do not know the APN, ask your mobile communications operator for it.



- **Network ID:** Network ID for your network connection. If you do not know the network ID, ask your mobile communications operator for it.
- **PIN:** PIN for the SIM card used.
- **Enable tray icon**
 - The current status of the network connection is shown with the symbol or .
 - The current status of the network connection is not shown with a symbol.
- **Enable context menu**
 - If you click on or , a context menu can be opened.
 - No context menu can be opened.
- **Enable network info dialog**
 - Via the context menu, you can bring up detailed information regarding the network connection.
 - No detailed information regarding the network connection can be brought up.
- **Enable mobile broadband configuration dialog**
 - Via the context menu, you can open a configuration dialog in order to change the access data.
 - The configuration dialog cannot be opened.



DHCP Client

Menu path: **Setup > Network > DHCP Client**

Here, you can change the advanced settings for the firmware's built-in DCHP client.

- [Default Options](#)(see page 710)
- [User-Defined Options](#)(see page 711)



Default Options

Menu path: **Setup > Network > DHCP Client > Default Options**

- **User Class:** A freely definable character string which can serve as a criterion for allocating specific settings for the DHCP server.
- **List of standard options:** Options with which the client can request information from the DHCP server.
You will find information regarding the various DHCP options in [RFC 2132 DHCP Options and BOOTP Vendor Extensions⁴⁷](#).

To edit the list, proceed as follows:

- Click on to create a new entry.
- Click on to remove the selected entry.
- Click on to edit the selected entry.
- Click on to copy the selected entry.

⁴⁷ <https://tools.ietf.org/html/rfc2132>



User-Defined Options

Menu path: **Setup > Network > DHCP Client > User-Defined Options**

- To create a new entry, click on in the **List of custom options** area.

- For more information regarding these options, see the manual for your DHCP server or your network components.

- **Enabled**
 The option is enabled. (default)
 The action is not enabled.
- **Option Name:** Add a prefix of your own in order to prevent a conflict with the default DHCP options. Example of the syntax: [YourPrefix]-[OptionName] . English letters, numbers and the special character “-” are allowed.
- **Code:** A number that is used by the DHCP server and DHCP client to reference an option. A number between 80 and 254 can be chosen. (default: 80)
- **Data Type:** Type of option. Possible values:
boolean
integer 8
integer 16
integer 32
signed integer 8
signed integer 16
signed integer 32
unsigned integer 8
unsigned integer 16
unsigned integer 32
ip address
text
string



VPN

Menu path: **Setup > Network > VPN**

Remote users securely access company networks via virtual private network protocols (VPN).

- **Enable tray icon**
 A tray icon for the network interface will be shown. (default)
 - **Enable context menu**
 A context menu will be shown when you click on the tray icon. (default)
 - **Enable network info dialog**
 A dialog window with information regarding the network connection will be shown when you click on the context menu. (default)
-

- [OpenVPN](#)(see page 713)
- [NCP VPN Client](#)(see page 724)
- [OpenConnect VPN](#)(see page 726)
- [genucard](#)(see page 731)



OpenVPN

Menu path: **Setup > Network > VPN > OpenVPN**

The *OpenVPN* client puts in place a virtual private network using TLS encryption and requires *OpenVPN 2.x* as a VPN server.

i IGEL *Linux 10.01.100* does not support the use of *OpenVPN* with smartcards and eTokens.

i If problems with *OpenVPN* occur, read the `/tmp/journal.log` log file with the [System Log Viewer](#)(see [page 549](#)) accessory.

- **Enable Autostart During Boot**

Shows the **Auto** column in the list of *OpenVPN* sessions. Highlight the desired session and click on **Set Auto** to enable this connection to be established during the boot procedure.

Autostart is disabled. (default)

- **Restart connection when disconnected:**

To manage the list of *OpenVPN* session, proceed as follows:

- ▶ Click to create a new entry.
- ▶ Click to remove the selected entry.
- ▶ Click to edit the selected entry.
- ▶ Click to copy the selected entry.

-
- [Session](#)(see page 714)
 - [Options](#)(see page 716)
 - [TLS Options for IGEL OS OpenVPN](#)(see page 717)
 - [Proxy](#)(see page 719)
 - [IPv4](#)(see page 720)
 - [Route](#)(see page 721)
 - [Desktop Integration](#)(see page 722)



Session

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > Session**

- **OpenVPN Server(s)**: Name or public IP address of the OpenVPN server
- **Authentication type**
 - **TLS certificates**: Authentication with user certificate and private key
 - **Name/password**: Authentication with user name and password
 - **Name/password with TLS-certificates**: Combines name/password with user certificate.
 - **Static key**: Authentication with a private key. No PKI infrastructure is needed for this.

TLS Certificates Authentication Type

- ⓘ Persistent storage of files is possible in the folder `/wfs` resp. subfolders of `/wfs` only.
Files stored under other paths will be lost when the thin client is rebooted.

- **Client certificate file**: File with the client certificate. Enter a path relative to `/wfs/OpenVPN` or select using the file selection.
- **CA certificate file**: File with the CA certificate. Enter a path relative to `/wfs/OpenVPN` or select using the file selection.
- **Private key file**: File with the private key. Enter a path relative to `/wfs/OpenVPN` or select using the file selection.
- **Private key password**: Password in case one is set for the private key

- ⓘ If you have a PKCS#12 file which contains the client certificate, CA certificate and private key, always enter its name in the three file fields. The advantage lies in the fact that only a single file needs to be distributed.

For details of how to distribute certificates and keys securely to thin clients, see the [Securely Distributing Keys and Certificates](#)(see page 714) How-To.

Name/Password Authentication Type

- **Username**: User name - if you leave this field empty, the user will be asked for it when establishing a connection.
- **Password required**
 - The user must enter a password. (default)
- **Password**: Password - if you leave this field empty, the user will be asked for it when establishing a connection.
- **CA certificate file**: File with the CA certificate. Enter a path relative to `/wfs/OpenVPN` or select using the file selection.

Name/Password with TLS-Certificates Authentication Type

- **Username**: User name - if you leave this field empty, the user will be asked for it when establishing a connection.



- **Password required**
 The user must enter a password. (default)
- **Password:** Password - if you leave this field empty, the user will be asked for it when establishing a connection.
- **CA certificate file:** File with the CA certificate. Enter a path relative to `/wfs/OpenVPN` or select using the file selection.
- **Clientcertificate file:** File with the user certificate. Enter a path relative to `/wfs/OpenVPN` or select using the file selection.
- **CA certificate file:** File with the CA certificate. Enter a path relative to `/wfs/OpenVPN` or select using the file selection.
- **Private key file:** File with the private key. Enter a path relative to `/wfs/OpenVPN` or select using the file selection.
- **Private key password:** Password in case one is set for the private key

i If you have a PKCS#12 file which contains the user certificate, CA certificate and private key, always enter its name in the three file fields. The advantage lies in the fact that only a single file needs to be distributed.

For details of how to distribute certificates and keys securely to thin clients, see the [Securely Distributing Keys and Certificates](#)(see page 714) how-to.

Static Key Authentication Type

- **Private key file:** File with the static key. Enter a path relative to `/wfs/OpenVPN` or select using the file selection.
- **Key direction:**
 - None: No key direction
 - 0: If the default option is not used, one side of the connection should use Direction 0 and the other Direction 1.
 - 1: If the default option is not used, one side of the connection should use Direction 0 and the other Direction 1.
- **Remote IP address:** The VPN IP address of the server
- **Local IP address:** The VPN IP address of the client



Options

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > Options**

Here, you can configure the options for the OpenVPN client in order to ensure interaction with the server.

Further information regarding the options can be found in the [OpenVPN documentation](#)⁴⁸ which is maintained by the OpenVPN project.

- **Gateway port:** Local gateway port (default: 1194)
- **Custom renegotiation interval:** Renegotiate data channel key after given number of seconds (default: 0)
- **Use LZO data compression**
 - The client will use LZO compression. Necessary if the server uses compression.
 - The client will not use LZO compression. (default)
- **Protocol used for communication to the host**
 - udp: UDP will be used.
 - tcp-client: TCP will be used.

i If you use a proxy, select **tcp-client**.

- **Virtual network type**
 - tun: Routing will be used
 - tap: Bridging will be used.
- **Use custom tunnel maximum transmission unit (MTU):** The MTU of the TUN device will be used as a given value. The MTU of the interface will be derived from it.
- **UDP fragment size:** Allow internal data fragmenting up to this size in bytes. Leave this field empty to keep the default value.
- **Restrict tunnel TCP maximum segment size (MSS)**
 - The TCP segment size (MSS) of the tunnel will be restricted.
 - The TCP segment size (MSS) will not be restricted. (default)
- **Randomize remote hosts**
 - The remote gateways will be ordered randomly as a simple type of load balancing.
 - The remote computers will not be ordered randomly. (default)
- **Cipher:** Encryption algorithm for data packets. (default: BF-CBC - Blowfish in the Cipher Block Chaining mode)
- **HMAC authentication:** Hashing algorithm for packet authentication (default: SHA1)

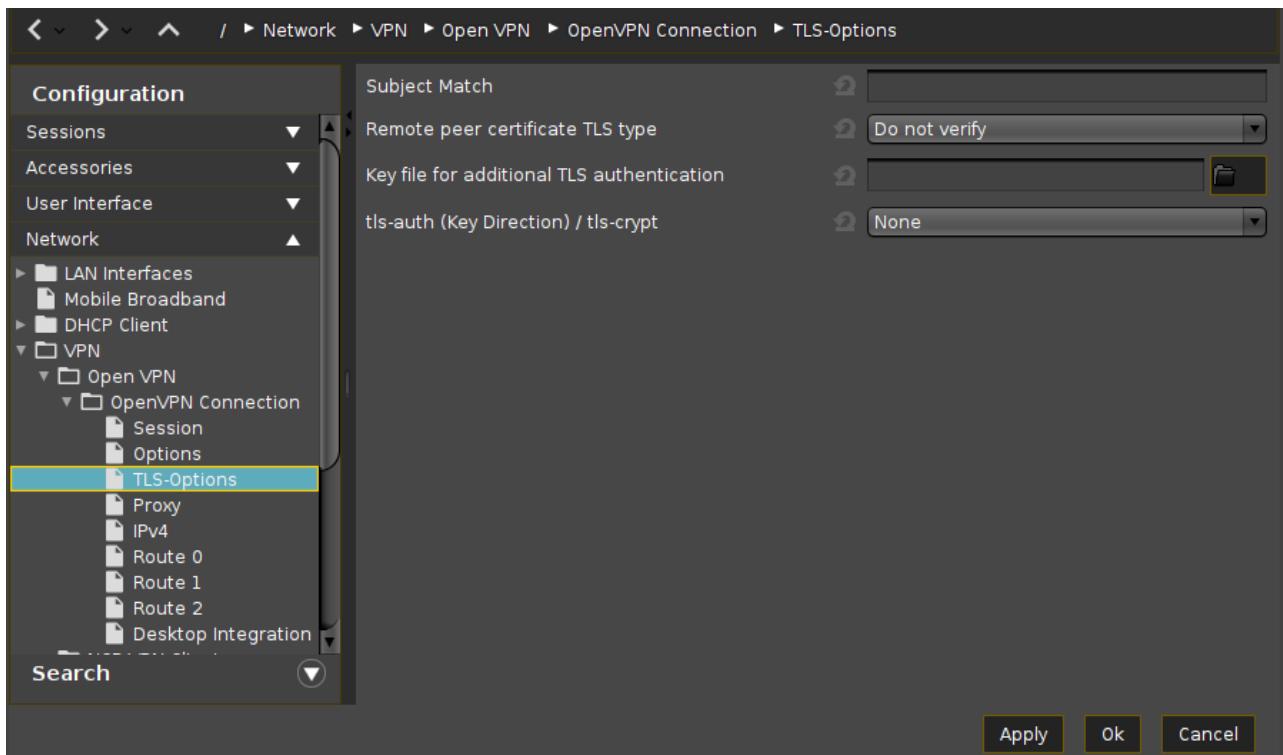
⁴⁸ <https://openvpn.net/index.php/open-source/documentation.html>

TLS Options for IGEL OS OpenVPN

This article shows how to define the TLS options for the OpenVPN client in IGEL OS. Under TLS (Transport Layer Security) Options, you can customize the options for the OpenVPN protocol (tunnel). TLS is the successor to SSL (Secure Sockets Layer). It is a standard consisting of several protocols that can transmit encrypted data between authenticated communication partners over potentially insecure IP networks such as the Internet.

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > TLS Options**

TLS Options for OpenVPN Client in IGEL OS:



Subject match:

The Subject match accept/reject the server connection based on a custom test of the server certificate's embedded X509 subject details. The formatting of these fields changed into a more standardized format. It now looks like: **C=US, L=Somewhere, CN=John Doe, emailAddress=john@example.com**.

See also: <https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/>

Remote peer certificate TLS type:

Require that peer certificate was signed with an explicit key usage and extended key usage based on RFC3280 TLS rules.



This is a useful security option for clients, to ensure that the host they connect to is a designated server. Or the other way around; for a server to verify that only hosts with a client certificate can connect.

- **Do not verify***: no remote certificate check
- **Check for server certificate**: The **--remote-cert-tls server** option is equivalent to **--remote-cert-ku --remote-cert-eku "TLS Web Server Authentication"**
- **Check for client certificate**: The **--remote-cert-tls client** option is equivalent to **--remote-cert-ku --remote-cert-eku "TLS Web Client Authentication"**

- ⓘ This is an important security precaution to protect against a man-in-the-middle attack, where an authorized client attempts to connect to another client by impersonating the server. The attack is easily prevented by having clients verify the server certificate using any one of **--remote-cert-tls**, **--verify-x509-name**, or **--tls-verify**.

Key file for additional TLS authentication:

As the path enter relative to `/wfs/OpenVPN` or select using the file selection. This adds an additional HMAC legitimization level above the TLS control channel in order to prevent DDOS attacks.

tls-auth (Key Direction) / **tls-crypt**:

- **None***: No key direction
- **tls-auth 0**: If the default option is not used, one side of the connection should use Direction 0 and the other Direction 1.
- **tls-auth 1**: If the default option is not used, one side of the connection should use Direction 0 and the other Direction 1.
- **tls-crypt**: In contrast to **tls-auth**, setting a key direction is not required. Use this option if the version of the OpenVPN server is 2.4 or higher. For more information on **tls-crypt**, see e.g., [Reference manual for OpenVPN 2.4⁴⁹](#).

*IGEL OS system defaults

⁴⁹ <https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/>



Proxy

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > Proxy**

Here, you can set up an optional proxy server for the VPN connection.

- ⓘ If you use a proxy, select the value **tcp-client** under **Options > Communication protocol to the host**.

- **Proxy type**

- None: Direct connection to the Internet.
- HTTP: HTTP proxy will be used.
- SOCKS: SOCKS proxy will be used.

Details for HTTP proxy

- **Proxy address**: Name or IP address of the proxy server
- **Proxy port**: Port on which the proxy service is available
- **Retry indefinitely when errors occur**
 - In the event of errors, repeated attempts to establish a connection via proxy will be made.
 - No further attempts to establish a connection will be made (default).

Credentials for HTTP

- **Proxy username**: User name for the proxy server
- **Proxy password**: Password for the proxy server



IPv4

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > IPv4**

By default, OpenVPN uses the server's DNS and routing settings. Here, you can change these settings.

- **Automatic DNS:**
 The name server(s) will be carried over by the OpenVPN server. (default)
 Extra name servers (see below) will be used.
- **Extra name server(s):** One or more name servers, IP addresses separated by commas.
- **Extra search domain(s):** One or more search domains, separated by commas.
- **Automatic routes**
 The routing table will be carried over by the OpenVPN server. (default)
 Extra routes will be configured.
- **VPN is the default route**
 The default route leads to the VPN. (default)
 Extra routes will be configured.



Route

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > Route [0,1,2]**

Here, you can configure extra routes.

- **Enable**
 - This route is enabled.
 - This route is not enabled. (default)
- **Network route / host route:** Type of route
 - Network route: The routing relates to a (sub) network
 - Host route: The routing relates to the address of a computer
- **Network / host IP:** The address of the network (for a network route) or the IP address or the name of the host (for a host route)
- **Network mask:** Mask for the desired IP range, e.g. 255.255.255.0
- **Gateway:** Gateway that routes the packets to the target network
- **Metric:** Here, you can enter a numerical quality assessment for routing decisions, 0 is the best value.



Desktop Integration

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > Desktop Integration**

Session name: Name for the session.

The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey



- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠** Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- i** To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

- The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

- The session cannot be started in appliance mode.



NCP VPN Client

Menu path: **Network > VPN > NCP VPN Client**

- ✓ NCP offers a 30-days trial period for IGEL customers.

The configuration parameters for the NCP Client are configured exclusively via the client program interface itself.

You will find the documentation regarding the NCP Secure Enterprise Client at <https://www.ncp-e.com/en/service-resources/library/>.

- ▶ Click to add an NCP VPN client session and configure the start methods.

Session name: Name for the session.

- ❗ The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

- The session can be launched from the start menu.

Application Launcher

- The session can be launched with the Application Launcher.

Desktop

- The session can be launched with a program launcher on the desktop.

Desktop context menu

- The session can be launched with the desktop context menu.

Hotkey

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. `Ctrl`.

- ⚠ Do not use `[AltGr]` as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure `[AltGr] + [E]` as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`



- [Ctrl] = Ctrl
- = Mod4

i When this keyboard key is used as a modifier, it is represented as Mod4 ; when it is used as a key, it is represented as Super_L .

- [Alt] = Alt

Key combinations are formed as follows with | :

- Ctrl + = Ctrl | Super_L

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard . Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the key symbol for the **Key** field. Example: Tab in (keysym 0xff09, Tab)

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.



OpenConnect VPN

Menu Path: **Setup > Network > VPN > OpenConnect VPN**

i Feature Not Available on IZ Devices

This feature is not available on IGEL IZ devices (IGEL Zero HDX, IGEL Zero RFX, or IGEL Zero Horizon).

The OpenConnect VPN Client puts in place a virtual private network using TLS encryption. This feature is available from *IGEL Linux 10.04.100* onwards.

⚠ Feature with limited support The OpenConnect VPN Client feature comes with limited support and without any warranty. Any support for this feature is provided on a non-binding, “best effort” basis.

- i** The OpenConnect VPN Client feature needs to be enabled manually before you can use it, see [Enabling the OpenConnect VPN Client](#)(see page 730).

• **Enable autostart during boot**

- Autostart is enabled.
 Autostart is disabled. (Default)

• **Restart connection when disconnected**

- Reconnect automatically when a disconnect occurs.
 Do not reconnect automatically when a disconnect occurs. (Default)

To manage the list of *OpenConnect VPN* sessions, proceed as follows:

- ▶ Click to create a new entry.
- ▶ Click to remove the selected entry.
- ▶ Click to edit the selected entry.
- ▶ Click to copy the selected entry.

-
- [Session](#)(see page 727)
 - [Desktop Integration](#)(see page 728)
 - [Enabling the OpenConnect VPN Client](#)(see page 730)



Session

Menu path: **Setup > Network > VPN > OpenConnect VPN > [session name] > Session**

- **Gateway:** IP address, hostname or Fully Qualified Domain Name (FQDN) of the VPN gateway
 - **Connect to Juniper Networks VPN**
 - The protocol of Juniper Networks VPN is used.
 - The protocol of Juniper Networks VPN is not used. (Default)
 - **Name/Password Authentication**
 - User name and password are used for authentication.
 - User name and password are not used for authentication. (Default)
 - **User name:** User name used for authentication
 - **Password:** Password used for authentication
 - **CA Certificate:** Path to the CA certificate
 - **User Certificate:** Path to the user certificate
- i** The certificates should be stored in the directory `/wfs/OpenVPN/` if possible, then they will certainly be found after a reboot.
- **Private Key:** Path to the private key
 - **Private Key password:** Password of the private key



Desktop Integration

Menüpaf: **Setup > Network > VPN > OpenConnect VPN > [session name] > Desktop Integration**

Session Name: Name for the session

! The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start Menu

The session can be started from the start menu. (Default)

Application Launcher

The session can be started with the application launcher. (Default)

Desktop:

The session icon will appear on the desktop. (Default)

Quick Start Panel

The session can be started from the quick start panel.

The session cannot be started from the quick start panel. (Default)

Desktop Context Menu

The session can be started from the desktop context menu.

The session cannot be started from the desktop context menu. (Default)

Application Launcher folder: Path to the application launcher folder

Password Protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup User:** The setup user's password is requested when launching the session.

Hotkey:

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combinations or your own key symbol/combinations. A key symbol is a defined chain of characters, e.g. `Ctrl`.

! Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".



These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

- To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.



Enabling the OpenConnect VPN Client

To enable the OpenConnect VPN Client, proceed as follows:

1. Ensure that the settings under **System > Update > Firmware Update** are correct. The **Server Path** must point to the firmware version that is currently installed. This is required because the software package for the OpenConnect VPN client must be downloaded in order to deploy the feature.
2. Go to **System > Firmware Customization > Features** and activate **VPN OpenConnect (Limited support - functionality "as is", see product documentation for details)**.
3. Confirm the warning dialog with **Ok**.
4. Click **Ok** in the main window.
5. Reboot the thin client.
On reboot, the client downloads and installs the software package for the OpenConnect VPN Client feature.



genucard

Menu path: **Network > VPN > genucard**

The *genucard* VPN hardware offers a choice of preconfigured Internet and VPN connections.

The settings for launching the session are described below.

Session name: Name for the session.

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.



- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.



- “Connections” Window(see page 734)
- Options(see page 735)
- Desktop Integration(see page 736)
- Administrator Session(see page 738)



“Connections” Window

The **Connections** window opens as soon as the *genucard* session is launched. You will find the following menu points there:

- **File**
 - **Change PIN:** Enter your previous PIN as well as your chosen new PIN twice.
 - **Rekeying:** Enter your PIN to generate a new key.
- **Wifi:** Opens the **Wifi** dialog which allows you to configure wireless access for the *genucard*.
 - Select a wireless network from the list. **Scan** updates the list (this can take up to a minute).
 - **Password:** The password for the selected wireless network. **Show** shows the entry in plain text.
 - **Save:** Saves the connection data entered along with the password on the *genucard*.
 - **Saved connections:** Select one of the previously saved connections.
 - **Delete:** Deletes the selected connection.
 - **Edit:** Changes the password for the selected connection.
- **Log:** Allows you to view the log
- **Network connection:** Select one of the network connections preconfigured on the *genucard*, for example LAN or WiFi.

i The network connections listed here have been configured using a *genucard* administration session or the *genucenter*. Connections configured with the *genucenter* are marked with "(GCE)".

► To start the selected network connection, click **Connect**.

- **VPN connection:** Select one of the VPN connections preconfigured on the *genucard*.

i The VPN connections listed here have been configured using a *genucard* administration session or the *genucenter*. Connections configured with the *genucenter* are marked with "(GCE)".

► To start the selected VPN connection, click **Connect**.



Options

Menu path: **Setup > Network > VPN > genucard > Options**

Here, you can prepopulate connection and user data for the genucard.

- **Autostart during boot**

The genucard application is launched during booting. This option increases the waiting time until the network is available.

ⓘ If the user name, password, default Internet connection and the default VPN connection are set in the setup, automatic launching allows firmware updates via VPN too.

The genucard application is not launched during booting. (default)

- **Autostart after USB directory (requires restart)**

The genucard application is automatically launched as soon as the genucard is connected to the thin client. (default)

ⓘ Launching the genucard can take up to 60 seconds.

- **Default Internet connection:** Name of an Internet connection configured on the genucard.

- **Default VPN connection:** Name of an Internet connection configured on the genucard.

- **User name:** User name for the genucard application

- **Password:** Password for the genucard application

- **Internet connection timeout:** Permitted waiting time in seconds (default: 120)

- **VPN connection timeout:** Permitted waiting time in seconds (default: 120)

- **File path for private keys for machine connection:** File path for the key file.



Desktop Integration

Menu path: **Setup > VPN > genucard > Desktop Integration**

- **Session name:** Name for the session

 The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

- **Start menu:**
 - The session can be started with the start menu. (Default)
 - The session cannot be found in the start menu.
- **Application Launcher:**
 - The session can be started with the Application Launcher. (Default)
 - The session cannot be found in the Application Launcher.
- **Desktop:**
 - The session can be started with a program starter on the desktop. (Default)
 - The session does not have a program starter on the desktop.
- **Quick start panel:**
 - The session can be started with the quick start panel.
 - The session cannot be found in the quick start panel. (Default)
- **Start menu's system tab:**
 - The session can be started with the start menu's system tab.
 - The session cannot be found in the start menu's system tab. (Default)
- **Application Launcher's system tab:**
 - The session can be started with the Application Launcher's system tab.
 - The session cannot be found in the Application Launcher's system tab. (Default)
- **Desktop context menu:**
 - The session can be started with the desktop context menu.
 - The session cannot be found in the desktop context menu. (Default)
- **Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.
- **Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.
- **Password protection:** Specifies which password will be requested when launching the session.
Possible values:
 - **None:** No password is requested when launching the session.
 - **Administrator:** The administrator password is requested when launching the session.
 - **User:** The user password is requested when launching the session.
 - **Setup user:** The setup user's password is requested when launching the session.
- **Hotkey:** A hotkey with which the session can be started is defined. It consists of modifiers and a key.
- **Modifiers:** One or two modifiers for the hotkey:
 - **None**



- = Shift
- [Ctrl] = Ctrl
- = Super_L
- [Alt] = Alt

Modifiers can be combined by using the pipe character | :

- [Ctrl]+ = Ctrl|Super_L

- **Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as user and enter xev -event keyboard . Press the key to be used for the hotkey. The text in brackets that begins with keysym contains the character string for the **Key** field. Example: Tab in (keysym 0xff09, Tab)



Administrator Session

The genucard is configured and administered centrally via the genucenter management interface. While VPN profiles can only be configured via genucenter or other remote interfaces, Internet connection profiles can also be configured via a local administration session.

Further information is available from www.genua.de⁵⁰.

Optionally, an administrator session allowing the genucard Internet connection to be configured can be set up:

To configure an Internet connection profile via a local administration session, proceed as follows:

1. Click on **Add instance** under **System > Registry > Sessions > genucard%**.
The genucard icon will appear on the desktop.
2. Click on the genucard icon.
The genucard logon window will open.
3. Enter a **user name** and **password**.
4. Click on **Logon**.
The Internet/VPN page will open.
5. In the **Internet** area, configure the connection with the help of the (Create), (Edit) and (Delete) buttons.

⁵⁰ <https://www.genua.de/en.html>



SCEP Client (NDES)

Menu path: **Setup > Network > SCEP Client (NDES)**

SCEP allows the automatic provision of client certificates via an SCEP server and a certification authority. This type of certificate is automatically renewed before it expires and can be used for purposes such as network authentication (e.g. IEEE 802.1x).

A Microsoft Windows Server (MSCEP, NDES) for example can serve as a queried counterpart (SCEP server and certification body). More information can be found at Microsoft, e.g. in the following Technet article: [Network Device Enrollment Service \(NDES\) in Active Directory Certificate Services \(AD CS\)](#)⁵¹

Manage certificates with SCEP

- Certificate management via SCEP Client (NDES) is enabled. Now carry out the necessary configuration.
 Certificate management via SCEP Client (NDES) is not enabled. (Default)

-
- [Certificate](#)(see page 740)
 - [Certification Authority](#)(see page 742)
 - [SCEP](#)(see page 743)

⁵¹<http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs.aspx>



Certificate

Menu path: **Setup > Network > SCEP Client (NDES) > Certificate**

Here, you can specify the basic data for the certificate to be issued by the certification body.

Type of CommonName/SubjectAltName: The characteristic for linking the certificate to the device.

- IP address: The IP address of the device.
- DNS name: The DNS name of the device.
- IP address (auto): The IP address of the device (inserted automatically).
- DNS name (auto): The DNS name of the device (inserted automatically).
- Email address: An email address.
- DNS name as UPN (auto)

i If the client automatically obtains its network name, **DNS Name (auto)** is a good type for the client certificate.

The following parameter is available if **Type of CommonName/SubjectAltName** is set to **IP address**, **DNS name**, or **Email address**:

CommonName/SubjectAltName: Give a designation which matches the **Type of CommonName/SubjectAltName**. For certain types, this occurs automatically. No entry is then required.

The following parameter is available if **Type of CommonName/SubjectAltName** is set to **IP address (auto)**, **DNS name (auto)**, or **DNS name as UPN (auto)**:

CommonName/SubjectAltName Suffix: Specifies a suffix that will be added to CommonName/SubjectAltName. Possible values:

- "none": No suffix will be added.
- "dot + DNS domain (auto)": The system's current DNS domain name separated with a dot will be added. Example: `.igel.local`
- Free text entry: The manually entered suffix will be added. Take notice that the percent symbol "%" is used for introducing the escape sequence, and thus the following replacements take place automatically:
 - `% D` is replaced by the system's DNS domain name at the time the certificate signing request (CSR) is created. Example: `@% D` will be changed into `@ igel.de` if the system's current DNS domain name is `igel.de`.
 - `%%` will be replaced by %. Example: `A %% B` will be changed into `A % B`.
 - Other combinations with % are currently discarded. Example: `A % BC` will be changed into `A C`.

i If you have to specify the suffix manually, make sure you enter the separator.



Organizational unit: Stipulated by the certification authority.

Organization: A freely definable designation for the organization to which the client belongs.

Locality: Details regarding the device's locality. Example: "Augsburg".

State: Details regarding the device's locality. Example: "Bayern".

Country: Two-digit ISO 3166-1 country code. Example: "DE".

RSA key length (bits): Select a key length (one suited to the certification authority) for the certificate that is to be issued.

Possible values:

- "1024"
- "2048"
- "4096"



Certification Authority

Menu path: **Setup > Network > SCEP Client (NDES) > Certification Authority**

The details for the following fields can be obtained from the certification authority:

CA identifier

CA certificate fingerprint (MD5)



SCEP

Menu path: **Setup > Network > SCEP Client (NDES) > SCEP**

Here, you can give information regarding the SCEP server used.

- ⓘ Because of the need to enter a fingerprint (CA root certificate) and the **Challenge password** (SCEP server), the configuration process is somewhat complicated. Ideally, it should be set up in the UMS as a profile and distributed to the devices. At the same time, the certificate cannot yet be used for communication purposes.

SCEP server URL: Address of the SCEP server. Examples: `http://myserver.mydomain.com/certsrv/mscep/mscep.dll` (Windows Server 2019); `http://myserver.mydomain.com/certsrv/mscep` (before Windows Server 2019)

Proxy server for SCEP requests: Proxy server in the format `host:port`. If this field is empty, no proxy will be used.

Challenge password: Password for queries.

Certificate renewal period (days): Time interval before certificate expiry after which the certificate renewal procedure is started. (Default: 30)

Certificate expiry check interval (days): Specifies how often the certificate is checked against its expiry date. (Default: 1)

- ⓘ As an example, a certificate is valid until 31.12. of a year. If the period for renewal is set to 10 days, a new certificate will be requested for the first time on 21.12. of the same year.

For more information, see the how-to Providing the SCEP Server Data. See also Configuration of the SCEP Client.



Routing

Menu path: **Setup > Network > Routing**

Here, you can enter additional routes if necessary.

Enable: (default: disabled)

Routing is enabled.

Default gateway: Gateway that routes the packets to the target network

Interface: The network interface via which the route is to run

i Predictable Network Interface Names (PNINs)

As of IGEL OS 11.06, the names of Ethernet and WLAN interfaces are predictable network interface names (PNINs), see [Predictable Network Interface Names](#)⁵². This ensures the stability of interface names on reboot and generally improves the reliability of associating configurations with interfaces.

- As "eth0", "eth1", and "wlan0" have been replaced by PNINs, configurations or custom scripts that include the old names of Ethernet and WLAN interfaces, e.g. `eth0`, `eth2`, `wlan0`, have to be adjusted.

The following already existing configurations do NOT require manual adjustment since old names `eth0`, `eth1`, etc. will internally be replaced by the correct PNINs automatically:

- Tcpdump
- **Bind interface** under **Security > Smartcard > Services**, see [Services](#)(see page 818)
- To view the PNINs and the order of the configured interfaces, you can use the following commands. The default interface is always listed first, the second interface is listed second, etc.

Ethernet (LAN): `cat /config/net/en-interfaces`

WLAN: `cat /config/net/wl-interfaces`

(Note: Only the first wireless interface (former `wlan0`) is supported. All other wireless interfaces will be ignored.)

- If you need to configure more than two Ethernet interfaces, go to **System > Registry > network.interfaces.ethernet.device%** and add an instance.
To explicitly assign a configuration instance to a certain interface, enter the corresponding PNIN for the registry key **network.interfaces.ethernet.device%.ifname**.

Routing [1-5]

Enable: (default: disabled)

This route is enabled.

Network route / host route: Type of route

- **Network route:** The routing relates to a (sub) network
- Host route: The routing relates to the address of a computer

⁵² <https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/>



Network / host IP or name: The address of the network (for a network route) or the IP address or the name of the host (for a host route)

Network mask: Mask for the desired IP range, e.g. 255.255.255.0

Gateway: Gateway that routes the packets to the target network

Interface: The network interface via which the route is to run



Hosts

Menu path: **Setup > Network > Hosts**

If no DNS (Domain Name Service) is used, you can specify a list with computers in order to allow translation between the fully qualified host name, the short host name and the IP address.

To manage the list of computers, proceed as follows:

- Click to create a new entry.
- Click to remove the selected entry.
- Click to edit the selected entry.
- Click to copy the selected entry.

Add

- **IP address:** IP address of the host you would like to add
- **Fully qualified host name:** Host name along with the domain, e.g. `mail.example.com`
- **Short host name:** E.g. `mail`



Network Drives

Menu path: **Setup > Network > Network Drives**

Here, you can configure both the drives that are to be connected during booting and the associated login data.

- [NFS](#)(see page 748)
- [Windows Drive](#)(see page 750)



NFS

Menu path: **Setup > Network > Network Drives > NFS**

In this area, you can integrate network drives using the Network File System (NFS).

You can find a sample configuration at the end of this page.

To manage the network drives, proceed as follows:

- Click to create a new entry.
- Click to remove the selected entry.
- Click to edit the selected entry.
- Click to copy the selected entry.

Add

- **Enabled:** Here, you can enable and disable configured entries.
 The network drive will be integrated. (default)
- **Local Mount Point:** The local directory under which the server directory is to be visible (default: `/nfsmount`)
- **Server:** NFS server that exports the directory
 - **For Server,** you can provide an IP address, a hostname or a Fully-Qualified Domain Name (FQDN).
- **Directory name:** Path under which the NFS server exports the directory

Sample configuration entry

The picture below shows a sample configuration entry.

- In both the **Local Mount Point** and **Directory Name** only (Linux/Unix-style forward slash) is permitted as a path separator.



Add

<input checked="" type="checkbox"/> Enabled	
Local Mount Point	/nfsmount
Server	192.168.0.1
Directory Name	folders/shared

Ok Cancel



Windows Drive

Menu path: **Setup > Network > Network Drives > Windows Drive**

In this area, you can integrate network drives shared by Windows as well as those from Linux/Unix servers via the SMB protocol (Samba).

You can find a sample configuration at the end of this page.

To manage the drive list, proceed as follows:

- Click to create a new entry.
- Click to remove the selected entry.
- Click to edit the selected entry.
- Click to copy the selected entry.

Clicking will bring up the **Add** dialogue, where you can define the following settings:

- **Enabled:** Defines whether the configuration entry will be applied.
 The network drive will be integrated.
- **Local Mount Point:** The local directory under which the server directory is to be visible
 (default: `/smbmount`)
- **Server:** The IP address, Fully-Qualified Domain Name (FQDN) or NetBIOS name of the server.
- **Share Name:** Path name as exported by the Windows or Unix Samba host.
- **User name:** User name for your user account on the Windows or Unix Samba host.
- **Password:** Password for your user account on the Windows or Unix Samba host.
- **User writable**
 The user can not only read but also write directory contents. Otherwise, only the local root user is able to do this.
 The user can only read directory contents. (default)

Sample configuration entry

The following picture shows a sample configuration entry.

If a NetBIOS name is provided for **Server**, make sure it is not preceded by slashes, e.g. `\myComputer` (wrong) vs. `myComputer` (correct).

For **Local Mount Point**, only `/` (Linux/Unix-style forward slash) can be used as a path separator. Note that if you enter, for example, `\smbmount` as a mount point, a directory called `\smbmount` will be created, because `\` is a legal character in Linux directory names. For **Share Name**, however, `/` (Linux/Unix-style forward slash) or `\` (Windows-style backward slash) can be used as a path separator.



/smbmount

<input checked="" type="checkbox"/> Enabled	
Local Mount Point	/smbmount
Server	192.168.0.4
Share Name	shared/folder1
User name	username
Password	*****
<input type="checkbox"/> User writeable	

Ok Cancel



Proxy

Menu path: **Setup > Network > Proxy**

Here, you can select the communication protocols for which a system-wide proxy server is to be used.

Direct connection to the Internet: The endpoint device is directly connected to the Internet. No proxy is used.

Manual proxy configuration: You can configure one or more proxies in the fields from **FTP proxy** up to **SOCKS protocol version**.

Automatic proxy configuration: The proxy settings are dynamically retrieved via a PAC file (Proxy Auto Config) that you specify under **URL**. For more information on PAC, see e.g. https://en.wikipedia.org/wiki/Proxy_auto-config.

FTP proxy / port: FTP proxy server and port

HTTP proxy / port: HTTP proxy server and port

SSL proxy / port: SSL proxy server and port

SOCKS host / port: Socks proxy server and port

SOCKS protocol version: Selects the SOCKS protocol version. (Default: SOCKS v5)

URL: URL of the PAC file for **Automatic proxy configuration**

No proxy for: List of computers to which the endpoint device is to connect directly, separated by commas (Default: localhost, 127.0.0.1)

Proxy realm for browser: Area in which the browser authenticates itself for the proxy. Together with the user name and password, this information is necessary for authentication. See also [Browser Global Proxy](#)(see page 366)

Use passthrough authentication

The temporarily saved login information (user name and password) will be used to log in to the proxy server.

The login information entered under **User name** and **Password** will be used to log in to the proxy server. (Default)

User name: User name for the proxy login

Password: Password for the proxy login

Enable client-side NTLM authenticating proxy

Client-side proxy is enabled. It stands between the application and the corporate proxy, adding NTLM authentication at the corporate proxy. The credentials specified on this Setup page are used.

Listening port: Port for client-side proxy



Devices

Menu path: **Devices > Hardware Info**

- ▶ Click on **Hardware Info** to view the system information for your IGEL device.

In this area, you can make settings for the following options:

- [Printer](#)(see page 754)
- [Storage Devices](#)(see page 778)
- [Bluetooth](#)(see page 784)
- [USB Access Control](#)(see page 785)
- [Unified Communications](#)(see page 788)



Printer

Menu path: **Devices > Printers**

You can set up a printer for the thin client here.

The printers must be set up under **Devices > Printer > CUPS > Printers** and must be enabled there for mapping in sessions.

- i** Because the thin client merely places incoming print jobs in a queue, you need to install the printer on the server. Please note that you will need to be logged in as administrator to the terminal to which the printer is connected.

- [CUPS\(see page 755\)](#)
- [LPD\(see page 765\)](#)
- [TCP/IP\(see page 766\)](#)
- [ThinPrint\(see page 772\)](#)
- [PrinterLogic\(see page 776\)](#)



CUPS

Menu path: **Devices > Printers > CUPS**

The Common UNIX Printing System™ (or CUPS) is the software that allows you to print from within applications, e.g. from this web browser.

CUPS converts the page descriptions produced by the application, e.g. "Insert Paragraph", "Draw Line" etc., into data that can be read by the printer, and then sends this information to the printer.

With the appropriate configuration, CUPS can use printing devices via the following connections:

- Parallel (LPT 1, LPT 2)
- Serial (COM1, COM2, USB COM1, USB COM2 – with a USB-to-serial adapter)
- USB (1st and 2nd USB printer)
- Network (TCP/IP, LPD, IPP, SMB)

Default Paper Size: Specify a default paper size for print jobs.

Possible values:

- Letter
- Legal
- Executive
- A5
- A4
- A3
- Autodetect

Additional information on CUPS printers can be found under CUPS: Mapping Local Printer to Citrix or RDP Sessions and Installing a Custom CUPS Driver.

-
- [Printers - Configure CUPS Printers in IGEL OS](#)(see page 756)
 - [IPP Printer Sharing](#)(see page 764)



Printers - Configure CUPS Printers in IGEL OS

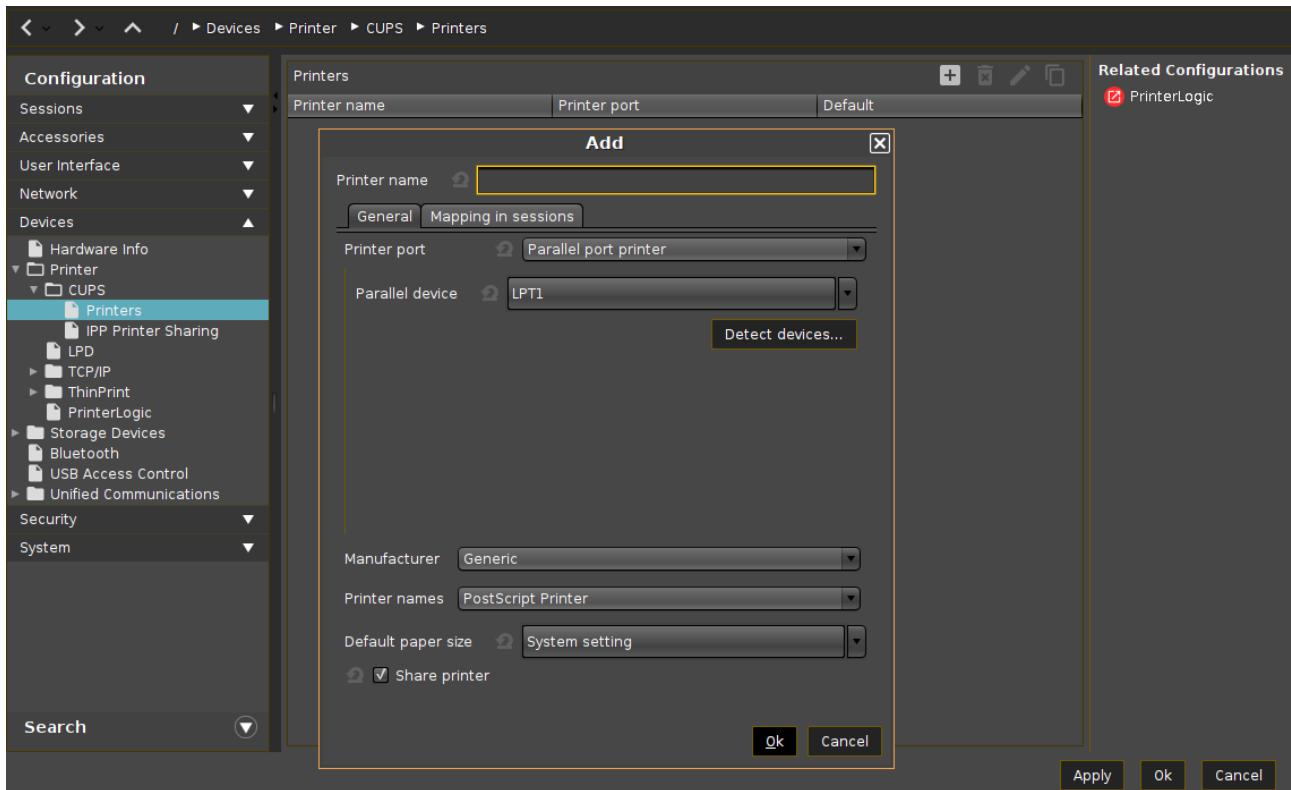
The following article describes settings for configuring CUPS printers for your IGEL OS devices. For general information on CUPS, see [CUPS \(see page 755\)](#).

If you want to automatically set the currently connected printer as the default printer, see also [Dynamic Selection of the Default Printer on IGEL OS](#).

- ⓘ Because the endpoint device merely places incoming print jobs in a queue, you need to install the printer on the server. Note that you will need to be logged in as an administrator to the terminal to which the printer is connected.

- ⓘ Settings made here apply to local printing (e.g. PDF, Firefox, etc.) and to mapping a local printer into a session.

Menu path: **Devices > Printer > CUPS > Printers**



Printers can be created and edited here.

- ▶ Click on **[+]** to open the **Add** dialog.
- ▶ In the edit dialog, specify a **Printer name** which begins with a letter.



General

Printer port

Interface type for locally connected printers or the network protocol for network printers.

Possible values:

- **Parallel port printer***
- **Serial port printer**
- **USB printer**
- **USB class printer**
- **LPD network printer**
- **TCP network printer**
- **IPP network printer**
- **SMB network printer**

i Depending on the chosen **Printer port** type, different parameters have to be configured, see [Settings to Be Configured for Each Printer Port Type](#)(see page 760).

Manufacturer

List of possible printer manufacturers. When you select a manufacturer here, the relevant selection of models will be provided under **Printer names**. (Default: Generic)

If a custom printer driver is required, see [Installing a Custom CUPS Driver](#).

Printer names

List of possible printer models. (Default: PostScript Printer)

Default paper size

Set the printer-specific paper size that you would like to use as a default.

Possible values:

- **Letter**
- **Legal**
- **Executive**
- **A5**
- **A4**
- **A3**
- **System setting***

Share printer

You can access the printer via the network if you have enabled the print server under **IPP Printer Sharing**, see [IPP Printer Sharing](#)(see page 764).*



Mapping in sessions

Map printer in NX sessions

- The printer is available in NX sessions.
 The printer is not available in NX sessions.*

Map printer in Parallels Client sessions

- The printer is available in Parallels Client sessions.
 The printer is not available in Parallels Client sessions.*

Map printer in ICA sessions

- The printer is available in ICA sessions.*

i Install the HP Color LaserJet 2800 Series PS driver on the server side to redirect the local printer to Citrix sessions, see <https://support.citrix.com/article/CTX140208>.

Map printer in RDP sessions

- The printer is available in RDP sessions.*

Map printer in AVD sessions

- The printer is available in AVD sessions.*

See also [CUPS Printer Redirection](#)(see page 470) for AVD sessions.

Use Windows driver name from list

- A driver name from the following list will be used.*

Manufacturer

List of possible printer manufacturers. (Default: Generic)

Model

List of possible models. (Default: Generic PostScript)

Use custom Windows driver name

- Enter the name of your driver here if it is not mentioned in the list above.

Printer driver

Windows driver name for the printer.

i The name must not contain ";" or ":".
Note that special characters, spaces, and case-sensitive characters are relevant when specifying a driver name.



When printing in ICA and RDP sessions, the print data are normally prepared for the printer model by the Windows printer driver and are passed unchanged from the device to the printer. An exception is made when using the Windows driver in ICA sessions, **Manufacturer** is set to "Generic" and **Model** is set to "Generic PostScript." In this case, the print data are prepared on the device with the help of the printer driver defined above under **Printer** for the printer model. This requires device resources.

*IGEL OS system default



Settings to Be Configured for Each Printer Port Type

Menu path: **Devices > Printer > CUPS > Printers**

Here, you can find the parameters available for configuration for each **Printer Port** (**Devices > Printer > CUPS > Printers > Add > General > Printer port**).

Printer Port: "Parallel port printer"

Parallel device:

- "LPT1"
- "LPT2"

Detect devices...: Opens a dialog for selecting the available devices.

Printer Port: "Serial port printer"

Serial device:

- "COM1"
- "COM2"
- "USB COM1"
- "USB COM2"

Detect devices...: Opens a dialog for selecting the available devices.

Baud rate:

- "9600"
- "19200"
- "38400"
- "57600"
- "115200"

Character size:

- "5"
- "6"
- "7"
- "8"

Parity:

- "None"
- "Even"
- "Odd"

Flow control:

- "None"
- "XON/XOFF"
- "RTS/CTS"
- "DTR/DSR"



Printer Port: "USB printer"

USB device:

- "1st USB printer"
- "2nd USB printer"

Detect devices....: Opens a dialog for selecting the available devices.

Printer Port: "USB class printer"

If you use a lot of different printer models attached via USB, you can assign printer models to CUPS printers without specifying dependencies to a specific USB port. Instead, the USB printer is assigned by matching patterns specified under **Manufacturer pattern** and **Product pattern** with the specific model name. A single printer definition can thus work for a class of different USB printer models.

Pattern matching mode: Specifies the type of the search pattern.

- "pattern": Standard wildcards are used for pattern matching, e.g. "*", "?". The matching is case sensitive. For detailed information on wildcards, see [man7.org⁵³](#) and [tldp.org⁵⁴](#).
- "pattern, case insensitive": Standard wildcards are used for pattern matching, e.g. "*", "?". The matching is case insensitive.
- "regular expression": Regular expressions are used for pattern matching. For detailed information on regular expressions, see [man7.org⁵⁵](#) and [tldp.org⁵⁶](#).

Manufacturer pattern: Pattern matching the manufacturer name of the printer. If the pattern is empty, it is ignored.

Product pattern: Pattern matching the product name of the printer. If the pattern is empty, it is ignored.

Information: Manufacturer and product names can be found in the accessories under **Devices > USB Devices > System Information**.

⁵³ <http://man7.org/linux/man-pages/man7/glob.7.html>

⁵⁴ <http://www.tldp.org/LDP/GNU-Linux-Tools-Summary/html/x11655.htm>

⁵⁵ <http://man7.org/linux/man-pages/man7/glob.7.html>

⁵⁶ <http://www.tldp.org/LDP/GNU-Linux-Tools-Summary/html/x11655.htm>



Product	hp Laserjet 1015
Manufacturer	Hewlett-Packard (www.hp.com)
Speed	12,00Mbit/s
Max Current	2mA
Misc	
USB Version	1,00
Class	0x7
Vendor	0x3f0
Product ID	0xe17
Bus	1

Click to see examples...

Matching all printers whose product name contains "LaserJet":

Pattern matching mode: "pattern"

Product pattern: "*LaserJet*"

Matching all printers whose product name contains "LaserJet":

Pattern matching mode: "regular expression"

Product pattern: "LaserJet"

Matching all printers whose product name contains "LaserJet" or "DeskJet":

Pattern matching mode: "pattern"

Product pattern: "+(*LaserJet*|*DeskJet*)"

Matching all printers whose product name contains "LaserJet" or "DeskJet":

Pattern matching mode: "regular expression"

Product pattern: "LaserJet|DeskJet"

Printer Port: "LPD network printer"

LPD print server: Host name or IP address of the remote LPD printer.

LPD queue name: Name of the LPD printer queue.

Printer Port: "TCP network printer"

TCP print server: Host name or IP address of the remote TCP/JetDirect/Socket printer.

TCP port: TCP port number. (Default: 9100)

Printer Port: "IPP network printer"

IPP URI: URI of the IPP print server. Example: `ipp://myprinter.example.com/printers/printer1`



Printer Port: "SMB network printer"

SMB server: NetBIOS host name of the SMB server.

SMB workgroup: Workgroup or domain name. (Optional)

SMB printer: Share name of the printer.

SMB port: SMB port number. (Default: 0, which stands for standard ports 139 and 445)

Use Kerberos authentication

Kerberos credentials are used for authentication on condition that Active Directory/Kerberos Logon has been configured. See [Active Directory/Kerberos](#)(see page 807).

Kerberos credentials are not used for authentication. (Default)

Use passthrough authentication

Single sign-on authentication is used on condition that Active Directory/Kerberos Logon or IGEL Shared Workplace have been configured. See [Active Directory/Kerberos](#)(see page 807) and [Shared Workplace](#)(see page 810).

Single sign-on authentication is not used. (Default)

SMB user name: User name used for authentication. (Optional)

SMB password: Password used for authentication. (Optional)



IPP Printer Sharing

Menu path: **Devices > Printer > CUPS > IPP Printer Sharing**

The IPP (Internet Printing Protocol) offers the following configuration options:

Network or host for sharing local printers: Access to the printer is possible from this network or host.

Possible options:

- "None"
- "Local network": Allows printing on the local device from the local network.

i This can also be given in the form 192.0.2.* or 192.0.2.0/24 or *.domain.com or 192.0.2.1 or host.domain.com .

- "Global": Allows printing on the local device from the global network.



LPD

Menu path: **Setup > Devices > Printers > LPD**

LPD printers are used by the BSD printing system and are also supported by *Windows* servers.

- **Enable LPD Print Server**

Local printers are provided in the network as LPD printers. The thin client is made the LPD print server. The CUPS printers defined under [Printers\(see page 756\)](#) can be addressed under their printer name as a queue name via the LPD protocol. (default)

- **Print Filter:**

- Automatic: Attempts to automatically recognize whether or not the print data need to be prepared by the local printer driver.
- None: The print data are always forwarded unchanged to the printer.

- **Max. Concurrent Connections**: Limits the number of print jobs that can be accepted at the same time.

- Unlimited
- 1
- 2
- 3

- **Restrict LPD Access** - Specifies the sub-networks or hosts from which print jobs can be accepted.

► Click on to add an LPD network or a host to the list.



TCP/IP

Menu path: **Setup > Devices > Printers > TCP/IP**

You can assign printers connected to your device to a TCP/IP port.

- [COM 1 / 2](#)(see page 767)
- [Additional Serial Ports](#)(see page 768)
- [LPT 1](#)(see page 770)
- [USBLP 1](#)(see page 771)



COM 1 / 2

Menu path: **Setup > Devices > Printers > TCP/IP > COM 1**

- **Activate TCP/IP printers on this port**
 Maps the interface defined below in a TCP/IP port.
 Disabled (default)
- **TCP/IP port number:** Port on which the interface is to be mapped (default: 3004).
- **Poll criterion:** Criterion according to which the interfaces are mapped.
 - Always: Maps constantly without polling.
 - Online: Maps only if the printer is switched on.
- **Poll frequency:** Amount of time between polls (default: 1 sec)
- **Speed:** Input and output speed (default: 9600)
- **Parity:** Parity bits that are to be used. Possible values:
 - None
 - Even
 - Odd
- **Stop bits:** Use up to two stop bits. (default: 1)
- **Word width:** Sets the number of bits used per byte.
 - 5
 - 6
 - 7
 - 8
- **Use RTS/CTS flow control**
 Hardware flow control will be used.
 Not used (default)
- **Use XON/XOFF flow control**
 Software flow control by sending start/stop signs will be used.
 Not used (default)
- **Use DSR flow control**
 Hardware flow control with DSR for output will be used.
 Not used (default)



Additional Serial Ports

Menu path: **Setup > Devices > Printers > TCP/IP > Additional Serial Ports**

TCP/IP printers on additional serial ports

- ▶ Click on to add TCP/IP printers to the list.

A mask with the following settings options will open:

- **Activate TCP/IP printer on this interface**
 - Maps the interface defined below in a TCP/IP port.
 - Disabled (default)

- **Device name:** The printer can be connected to one of the following connections, provided that they are available on the device:
 - USB COM1
 - USB COM2
 - Perle COM1
 - Perle COM2

i Data are forwarded bidirectionally at serial interfaces. This means that other serial devices such as barcode scanners or scales can be operated too.

- **Search for devices...:** Opens a dialog allowing you to select the device file. 3 device files are available for each device; the **Designation** column shows the type of device file:

- (GENERIC) [device designation]: Generic type. The name of the device file ends in a consecutive number which depends on the boot procedure or the order of insertion.
Example: `/dev/ttyUSB0`
- (BY PORT) [device designation]: According to USB port. The device file is in the `/dev/usbserial/` directory. The name of the device file ends in the number of the USB port that the device is plugged into. Example: `/dev/usbserial/ttyUSB_P12`
- (BY USBID) [device designation]: According to USB ID. The device file is in the `/dev/usbserial/` directory. The name of the device file ends as follows: `_V[Vendor ID]_P[Product ID]`. Example: `/dev/usbserial/ttyUSB_V067b_P2303`

- **TCP/IP port number:** Port on which the interface is to be mapped (default: 9100).

- **Poll criterion:** Criterion according to which the interfaces are mapped.

- Always: Maps constantly without polling.
- DSR (M1): Maps only if the relevant line is set by the serial device.
- DCD (M5): Maps only if the relevant line is set by the serial device.

- **Poll frequency:** Amount of time between polls (default: 1 sec)

- **Speed:** Input and output speed (default 9600 baud).

- **Parity:** Parity bits that are to be used. Possible values:

- None
- Even
- Odd

- **Stop bits:** Use up to two stop bits. (default: 1)

- **Word width:** Sets the number of bits used per byte.

- 5



- 6
- 7
- 8
- **Use RTS/CTS flow control**
 Hardware flow control will be used.
 Not used (default)
- **Use XON/XOFF flow control**
 Software flow control by sending start/stop signs will be used.
 Not used (default)
- **Use DSR flow control**
 Hardware flow control with DSR for output will be used.
 Not used (default)



LPT 1

Menu path: **Setup > Devices > Printers > TCP/IP > COM 1**

- **Activate TCP/IP printers on this interface**

- Maps the interface defined below in a TCP/IP port.
- Disabled (default)
 - **TCP/IP port number:** Port on which the interface is to be mapped (default: 3004).
 - **Poll criterion:** Criterion according to which the interfaces are mapped.
 - Always: Maps constantly without polling.
 - Online: Maps only if the printer is switched on.
 - **Poll frequency:** Amount of time between polls (default: 1 sec)



USBLP 1

Menu path: **Setup > Devices > Printers > TCP/IP > USBLP 1**

- **Activate TCP/IP Printers on this Port:**

- Maps the interface defined below in a TCP/IP port.
- Disabled (default)

- **TCP/IP Port Number:** Port on which the interface is to be mapped (default: 3004).

- **Poll Criterion:** Criterion according to which the interfaces are mapped.

- Always: Maps constantly without querying.

- Online: Maps only if the printer is switched on.

- **Poll Frequency:** Amount of time between status queries (default: 1 sec)



ThinPrint

Menu path: **Devices > Printer > ThinPrint**

ThinPrint allows the bandwidth provided for the transfer of print jobs to be reduced depending on the resources available. The ThinPrint client prints either on printers connected to a local interface (serial, parallel or USB), on an LPD network printer or on a CUPS printer defined on the thin client.

In this area, you will find the following parameters:

Port Number: Port number via which the ThinPrint daemon will communicate (default: 4000).

- ⓘ Make sure that the port number on the ThinPrint client and the ThinPrint server is the same (communication will otherwise not be possible).

Bandwidth: A bandwidth value (in bits per second) which is lower than or equal to the value specified on the ThinPrint server. A higher value, the disabling of client control or no entry at all means that the ThinPrint server values will be used (default: 0).

Open Printer Interval: Maximum waiting time in seconds if a printer is unavailable (default: 165).

Open Printer Tries: Number of attempts to contact a printer in order to start a print job (default: 100).

-
- [Printer](#)(see page 773)
 - [Connection Service](#)(see page 774)
 - [Encryption](#)(see page 775)



Printer

Menu path: **Devices > Printer > ThinPrint > Printer**

In this area, the **ThinPrint and ezeep Printers** are shown.

The page provides an overview of pre-configured ThinPrint printers.

- ▶ Click on to add a printer to the list.

A mask with the following settings options will open:

Active: Indicates whether or not the printer is visible.

Printer Name: Name under which the printer can be addressed.

Printer Class Name: Name of the printer class - optional, max. 7 characters without spaces

Device: A device file or the printer name, e.g. /dev/ttyS1 (COM2).

Detect Devices....: Opens a mask for selecting the available devices.

Print Retries: Number of attempts to contact a printer in order to start a print job (default: 10).

Default: Defines the selected device as the default printer.



Connection Service

Menu path: **Setup > Devices > Printers > ThinPrint > Connection Service**

By default, the .print client waits for incoming connections from the print server. If the thin client is unavailable via the network from the print server, the connection can also be established from the thin client.

- **Connection Service Mode:**

- Listen Mode: Receive print jobs without Connection Service. The .print client heeds incoming connections.
- Static Mode: Use connection to receive print jobs. The .print client establishes a connection to the .print Connected Gateway.
- Both: Use both modes.

- **Connection Server Address:** IP address of the computer on which the connection service runs.

- **Connection Service Port number:** The client port of the .print Connected Gateway (default: 4001)

- **Client ID:** The ID of the client must be unique.

- **Connection Service Authentication key:** A value that is defined on the connection server.

- **Connection Service Retry Interval:** Waiting time in seconds until another connection attempt is made if the .print Connection Service is unavailable (default: 300)



Encryption

Menu path: **Setup > Devices > Printers > ThinPrint > Encryption**

In this area, you can enable encryption for print jobs.

- **Enable SSL Encryption:**
 The client can receive print jobs via an encrypted connection.
 Disabled (default)
- **SSL Root Certificate:** Path name of the file that receives the root certificate in the .pem format.
- **SSL Client Certificate:** Path name of the file that receives the client certificate in the .pem format.
- **SSL Client Certificate Password**



PrinterLogic

Menu path: **Setup > Devices > Printer > PrinterLogic**

If you are using PrinterLogic to provision printers, you are replacing the previous direct printer management from the Setup.

Instead, the administrator creates a website (on printercloud.com⁵⁷) with the respective printers of the location(s). The setup user/administrator can then select the desired printers via the browser.

Manage printers by Printer Installer client:

The printers will be managed by the Printer Installer client and not by the IGEL CUPS functionality (**IGEL Setup > Devices > Printers > CUPS**).

No Printer Installer client is activated. The printers will be managed by the IGEL CUPS functionality. (default)

HomeURL protocol

Possible options:

- <https://>
- <http://>

HomeURL hostname: The host name of the web server running the printer cloud. Default: printercloud.com

Authorization code: Authorization code for the printer cloud; generated by the administrator.



If you have successfully set up the printer cloud, this tray icon appears in the system tray.

Mapping in sessions

ICA sessions

Include printers managed by PrinterLogic in ICA sessions. (default)

RDP sessions

Include printers managed by PrinterLogic in RDP sessions. (default)

NX sessions

Include printers managed by PrinterLogic in NX sessions.

Don't include printers managed by PrinterLogic in NX sessions. (default)

Parallels client sessions

Include printers managed by PrinterLogic in Parallels client sessions.

Don't include printers managed by PrinterLogic in Parallels client sessions. (default)

Show CUPS printers: Displays a list of installed printers that can be deleted.

⁵⁷ <http://printercloud.com>



The PrinterLogic menu



Right-click the icon to get the following options:

- **Add Printers...**: Opens the PrinterCloud in the browser. The installed printers are listed and can be installed via double-click.
- **Pull Printing...**: The print job is held and released by the user at each print device that supports this function.
 - **Print Job Management...**: Manages your print jobs.
 - **Secure Print Settings...**: Opens settings for secure printing.
- **Refresh Configurations**



Storage Devices

Menu path: **Setup > Devices > Storage Devices**

Configure your hotplug storage devices here.

Show attached storage devices: Shows a list with registered storage devices.

- [Storage Hotplug](#)(see page 779)
- [Options](#)(see page 782)
- [DriveLock](#)(see page 783)



Storage Hotplug

Menu path: **Setup > Devices > Storage Devices > Storage Hotplug**

In this area you can set up the connection of hotplug storage devices to the device. These can be USB mass storage devices or MMC card readers for example.

Following file systems are officially supported:

ext2, ext3, ext4	Standard Linux file systems
squashfs	a packed read-only file system
vfat	supports all FAT variants
exFAT ¹	supports exFAT (found on SDXC SD-cards)
ISO 9660	CDROM/DVD file systems
udf	CDROM/DVD file systems
ntfs	supported with ntfs-3g (Fuse)

¹ With Firmware 11.03.100 or newer

You can change the following settings:

Storage Hotplug

Hotplug storage devices will be mounted and unmounted automatically. When mounted, a hotplug storage device can be used in sessions like ICA, RDP, VMware Horizon, or in local applications like browser / PDF viewer or media player.

- ❗ Before you unplug a hotplug storage device from the thin client, you must safely remove it. Otherwise, data on the hotplug storage device can be damaged. Depending on the configuration, there is one or several possibilities to safely remove a hotplug storage device:
 - Click on ▲ in the task bar. The taskbar is not available in a fullscreen session.
 - Click on ▲ in the in-session control bar. Depending on the configuration, the in-session control bar may be available in a fullscreen session. For further information, see [In-session Control Bar](#)(see page 661).
 - Function **Accessories > Disk Removal** with further starting possibilities; amongst other things, a hotkey can be defined here.
- If the following warning is displayed: **Volume(s) still in use. Dont' remove the device.**, then the hotplug storage device must not be removed. First, exit the program concerned or close all files or directories that reside on the hotplug storage device.

Hotplug storage devices will be mounted and unmounted automatically. (Default)

Default permission: Default access rights for hotplug storage devices.

Possible values:

- Read only



- Read/Write

Client Drive Mapping: Defines the creation of drives in ICA sessions, RDP sessions or Horizon sessions. The mounting of hotplug storage devices to the local file system is not influenced by this parameter.

Possible values:

- **Dynamic:** Drives are created automatically in a session when a hotplug storage device is connected to the device. When the device is removed, the corresponding drive is removed automatically.
- **Static:** The drives in a session are predefined by the parameters described under [Static Client Drive Mapping](#)(see page 780).

Static Client Drive Mapping

Private drive letter for each storage drive

- A drive letter is assigned to each hotplug storage device.
- A single drive letter will be generated for all hotplug storage devices and each hotplug storage device will be assigned a sub-directory. (default)

Number of drives: The maximum number of hotplug storage devices that can be used simultaneously in the session.

- i When this number is reached, no additional hotplug storage devices will be assigned.

Start storage drives with this drive letter: Letter that is assigned to the first hotplug storage device if automatic drive mapping is enabled (default:A). Further hotplug storage devices are assigned the next letter alphabetically.

ICA read access for storage hotplug devices: Specifies whether read access to hotplug storage devices is allowed in an ICA session.

Possible values:

- Yes: Read access is allowed.
- No: Read access is not allowed.
- Ask user: Read access can be allowed on request.

ICA write access for storage hotplug devices: Specifies whether write access to hotplug storage devices is allowed in an ICA session.

Possible values:

- Yes: Write access is allowed.
- No: Write access is not allowed.
- Ask user: Write access can be allowed on request.

Notification

Hotplug beep

- A signal tone will be heard when connecting and disconnecting hotplug storage devices. (Default)

Hotplug message

- Hotplug messages will be shown when connecting and disconnecting hotplug storage devices. (Default)



Timeout: Period of time in seconds after which the window with the hotplug messages is hidden. If the parameter is set to **No timeout**, the window will be shown until it is closed manually. (Default: [15](#))

You will find further settings options in the HDX / ICA Global setup area under [Drive mapping](#)(see page 60), in the RDP Global setup area under [Drive mapping](#)(see page 119), in the Devices area under [USB access control](#)(see page 785) and in the Accessories area under [Disk Removal](#)(see page 597).



Options

Menu path: **Setup > Devices > Storage Devices > Options**

In this area, you can specify a directory in which external storage devices are accessible to the user. The devices are always mounted in the `/media` directory.

User browse directory

- The directory defined under **Browse directory** is linked to the `/media` directory. (Default)

Browse directory:`:` Local directory in which the devices can be found. (Default: [userhome/media](#))

Support for built-in floppy drives

- Built-in disk drives are active.
 Built-in disk drives are disabled (default)

i This option is only valid for drives which are not connected via USB.



DriveLock

Menu path: **Devices > Storage Devices > DriveLock**

DriveLock allows the control of your USB devices and helps to prevent BadUSB attacks. For details, see <https://www.drivelock.com/>.

Enable DriveLock agent

DriveLock agent is activated.

DES server URL: URL of the DriveLock Enterprise Service server used for the distribution of policies

Tenant: Name of the DES user group to which the policy should apply. (Default: root)



Bluetooth

Menu path: **Devices > Bluetooth**

In this area, you can set up a Bluetooth service.

Bluetooth

- The Bluetooth service is active. The Bluetooth Tool can be used.
- The Bluetooth service is inactive. The Bluetooth Tool cannot be used. (Default)

Tray Icon

- A Bluetooth icon will be shown in the system tray. You can launch the Bluetooth Tool by double-clicking on the Bluetooth icon. Right-clicking on the Bluetooth icon will bring up an overview as to which Bluetooth devices are connected to the thin client and you can enable or disable Bluetooth.

- A Bluetooth icon will not be shown in the system tray. (Default)

Details of the settings options for Bluetooth can be found under **Accessories > Bluetooth Tool**(see page 583).

Here you can find information on the [Bluetooth Wizard](#)(see page 8).



USB Access Control

Menu path: **Devices > USB Access Control**

You can allow or prohibit the use of USB devices on your endpoint. Specific rules for individual devices or device classes are possible. For an example, see How to Configure USB Access Control.

Enable

USB access control is enabled and the following settings can be configured.

USB access control is inactive. (Default)

⚠ The activation of **USB Access Control** and setting the **Default rule** to **Deny** will block the use of USB devices locally and in the session and, thus, might disable devices needed for the users. Therefore, activate the USB access control only if your security policy requires that. In this case, set **Default rule** to **Deny** and configure **Allow** rules for the required USB devices and USB device classes.
It is recommended to make settings for **USB Access Control** as the last step in the device configuration. Before activating the USB access control, check that all your other settings for printers, Unified Communication, USB redirections, mapping settings for USB devices are working as expected. Note that the USB access control is completely separate than USB redirection for remote sessions, see When to Use USB Redirection.
Take also notice that the feature does not disable a USB port physically, i.e. power delivery will still work.

Default rule: Specifies whether the use of USB devices is allowed or prohibited.

- Allow
- Deny

Default permission: Default access rights for USB devices.

- Read Only
- Read/Write

Class Rules

Class rules apply to USB device classes.

► Click on **[+]** to create a new rule.

An input mask with the following options will open:

Rule: Specifies whether the use of the device class defined here is allowed or prohibited.

Class ID: Device class for which the rule should apply. (Examples: **Audio**, **Printers**, **Mass Storage**).

Name: Name of the rule

Device Rules

Device rules apply to specific USB devices.

- ▶ Click on  to create a new rule.

An input mask with the following options will open:

Rule: Specifies whether the use of the device defined here is allowed or prohibited.

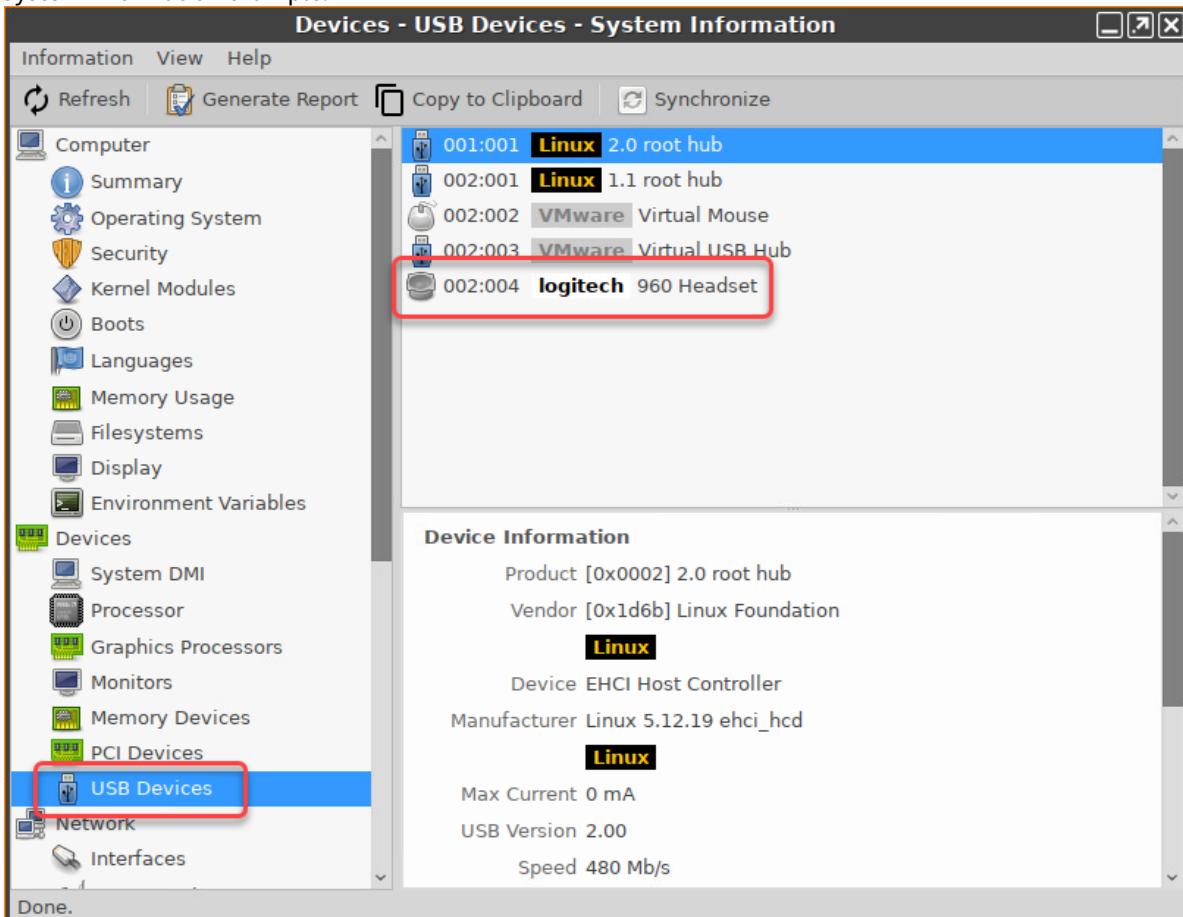
Vendor ID: Hexadecimal ID of the device manufacturer

Product ID: Hexadecimal ID of the device

Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see [Using “System Information” Function\(see page 592\)](#).

System Information example:



Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:



Local Terminal

```
File Edit View Terminal Tabs Help
root@ITC005056930CAD:~# lsusb | grep -i logitech
Bus 002 Device 004: ID 046d:0a45 Logitech, Inc. 960 Headset
root@ITC005056930CAD:~# █
```

Device uuid: Universal Unique Identifier of the device

Permission: Authorizations for access to the device

Possible values:

- Global setting: The default setting for hotplug storage devices is used; see the **Default permission** parameter under **Devices > Storage Devices > Storage Hotplug**.
- Read only
- Read/Write

Name: Name of the rule

Further setting options can be found under [Storage Hotplug](#)(see page 779).



Unified Communications

- [Jabra](#)(see page 789)
- [EPOS Audio](#)(see page 792)



Jabra

- [Jabra Xpress](#)(see page 790)
- [Options](#)(see page 791)



Jabra Xpress

Menu path: **Devices > Unified Communications > Jabra > Jabra Xpress**

Jabra Xpress is a solution for the remote mass-deployment of Jabra USB headsets that enables creating and deploying packages containing a configuration of settings, firmware updates, etc. for Jabra devices. For more information, see <https://www.jabra.com/supportpages/jabra-xpress#/>.

- ⚠** For detailed information on how to deploy a Jabra Xpress package, see How to Deploy a Jabra Xpress Package.

Device Dashboard URL: URL of the dashboard server of the Jabra device.

Package: File name of the Jabra Xpress package. Example: `xpress_package_20190109_144111.zip`.

Source URL: URL to the directory containing the Xpress package. Example: `https://172.30.92.1:8443/ums_filetransfer/`

- i** As a **Source URL**, you can specify any server, e.g. FTP(S) or HTTP(S), where you have placed the Xpress package downloaded from the Jabra Xpress portal.
If you want to use the UMS as a source location, your Jabra ZIP archive has to be registered as a file object in the UMS, see Files - Registering Files on the IGEL UMS Server and Transferring Them to Devices. See also UMS and Devices: File Transfer.

Check SSL certificate: Determines if the SSL certificate is checked. (Default: Enabled)

- i** Disable SSL certificate checking if your HTTPS or FTPS server uses a self-signed certificate.

User name: User name for accessing the Xpress package that resides under the **Source URL**.

Password: Password for accessing the Xpress package that resides under the **Source URL**.

- ✓** For the optimal performance of Jabra headsets (esp. relevant if Skype for Business is used), activate:
- in Citrix sessions: **HDX Realtime Media Engine** under **Sessions > Citrix > Citrix Global > Unified Communications > Skype for Business**;
 - in VMware Horizon sessions: **Virtualization Pack Skype for Business** under **Sessions > Horizon Client > Horizon Client Global > Unified Communications > Skype for Business**;
 - in RDP sessions: **Compression** under **Sessions > RDP > RDP Global > Performance**.



Options

Menu path: **Devices > Unified Communications > Jabra > Options**

Suspend on idle: Determines if the wireless Jabra USB audio device is set to the offline state after 5 seconds of idle time. (Default)



EPOS Audio

- EPOS Connect(see page 793)



EPOS Connect

EPOS provides headset and conferencing solutions. For the supported EPOS headsets and speakerphones, see [EPOS / Sennheiser Compatibility with IGEL OS](#).

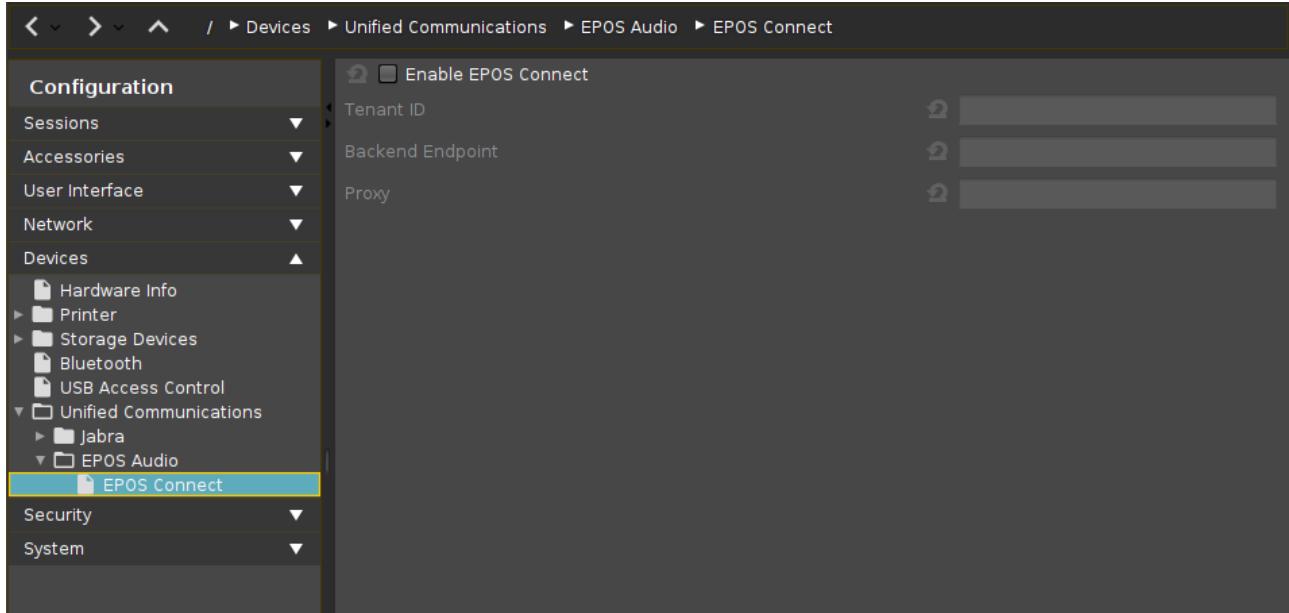
In IGEL OS, you can set up EPOS Connect, a client application that connects with EPOS Manager and sends device information and configuration to it. EPOS Manager performs the following tasks for EPOS devices that are connected to the endpoint:

- Firmware updates
- Remote asset management
- Remote configuration

i "Silent update" must be selected in EPOS Manager during the update. Otherwise, the update will not function.

For more information on EPOS Manager and EPOS Connect, see <https://www.eposaudio.com/en/us/enterprise/software>.

Menu path: **Devices > Unified Communications > EPOS Audio > EPOS Connect**



Enable EPOS Connect

The EPOS Connect client is enabled.



Tenant ID

The customer-specific system ID for your EPOS Manager installation.

A screenshot of the EPOS Manager configuration interface. The main area shows the company name as "Igel Technology GmbH" and the tenant name as "[REDACTED]". Under "Client Configuration", there are three fields: "Backend Endpoint" set to "https://api.enterprise.eposaudio.com", "Initial Heartbeat Time" set to "7200 seconds", and "Tenant ID" set to "[REDACTED]". A red box highlights the "Tenant ID" field. A "Download" button is visible below the configuration section. On the right side, a sidebar menu is open, showing the user is "Tenant Admin". The "Client Config" option in the menu is highlighted with a teal background. Other menu items include "Settings", "Single Sign On", "Administration", "Change Password", "Help", "About", and "Logout".

EPOS

Company Name : Igel Technology GmbH Tenant Name : [REDACTED]

Client Configuration

Backend Endpoint : https://api.enterprise.eposaudio.com

Initial Heartbeat Time : 7200 seconds

Tenant ID : [REDACTED]

Download

Tenant Admin

Settings

Single Sign On

Administration

Client Config

Change Password

Help

About

Logout

Backend Endpoint

URL of EPOS Manager

Proxy

URL of the proxy that connects to EPOS Manager, if applicable. The proxy URL must be provided in the format [ADDRESS] : [PORT] .



Security

Menu path: **Setup > Security**

In order to prevent unauthorized access to the thin client setup, it is important to set up an administrator password after the initial configuration. With an additional user password, you can allow the user to make limited changes to the configuration.

Further information can be found under [Password - Restrict Access to IGEL OS Components](#)(see page 799).

- [Device Encryption for IGEL OS](#)(see page 796)
- [Password - Restrict Access to IGEL OS Components](#)(see page 799)
- [Logon](#)(see page 803)
- [Active Directory/Kerberos](#)(see page 814)
- [Smartcard](#)(see page 817)



Device Encryption for IGEL OS

If you want to strengthen the security of your endpoint device, you can deploy strong device encryption that is derived from a user password. The encryption is applied to all partitions that can contain user data, e.g. browser history or Custom Partitions.

Menu path: **Security > Device Encryption**

Device encryption mode

Possible options:

- **Keep:** If the device is encrypted, it stays encrypted. If it is not encrypted, it will not get encrypted.
- **Activate:** The device will be encrypted when the user enters the password for the first time. The re-encryption may take about 10 to 60 seconds; the duration depends on the hardware performance and the size of the Custom Partition.
- **Deactivate:** The device will be re-encrypted back to the default device encryption on the next boot. The re-encryption may take about 10 to 60 seconds.

⚠ If you want to switch back to the default device encryption, you must have the password. If the password gets lost, you must reinstall IGEL OS 11 on the device, e. g. via OSC (see Installation).

Change password

Only applicable if device encryption is enabled. The user can change the password for device encryption.

Authentication type

Possible options:

- **PW:** Password authentication. In this version of IGEL OS, this is the only available authentication type.

Security level

Possible options:



- **Auto, constant-time:** The password aggregation function that fits best with the defined **Target time delay (ms)** is selected.
- **Auto, at least level:** The security level will be at least as high as the value selected by **Password aggregation function**; if the **Target time delay (ms)** allows for a higher security level, the higher security level will be used.
- **Manual:** The **Password aggregation function** can be set manually, irrespective of the delay time specified by **Target time delay (ms)**.

Target time delay (ms)

Maximum time that should be consumed by the password aggregation function. This delay is effective when the user enters the device encryption password on boot or changes the device encryption password.

Password aggregation function

Security level of the encryption.

Possible options:

- **I: Argon2id, 8M/7 ops**
- **II: Argon2id, 128M/3 ops**
- **III: Argon2id, 256M/3 ops**
- **IV: Argon2id, 512M/3 ops**
- **V: Argon2id, 1024M/4 ops**
- **VI: Argon2id, 128M/4 ops**

Minimum password length

Minimum number of characters the password must be composed of

Unwanted strings in password (comma separated)

Comma-separated list of strings that must not be contained in the password

The password must contain

Defines whether all of the subsequent minimum requirements (minimum amount of lower case letters etc.) must be fulfilled, or 2, or 3 of them.

- **all**
- **2 of**
- **3 of**

Minimum amount of lower case letters

The minimum amount of lower case letters



Minimum amount of upper case letters

The minimum amount of upper case letters

Minimum amount of numbers

The minimum amount of numbers

Minimum amount of special characters

The Minimum amount of special characters

Special characters allowed

List of all non-alphanumeric characters that are allowed in the password, without separators



Password - Restrict Access to IGEL OS Components

The following article provides details on different authorization levels in IGEL OS, which you can configure to protect your endpoint devices against unwanted changes. You will learn the difference between the access for **administrator** and **setup administrator**, for **user** and **setup user**.

For a general overview on securing your devices, see Securing IGEL OS Endpoints.

Menu path: **Security > Password**

You can assign four different authorization levels:

Administrator: The administrator has full access to the IGEL Setup.

- ⓘ The assignment of the administrator password is a prerequisite for all other rights assignments. Even if the administrator wants to leave the administration of the IGEL Setup to the setup administrator, the administrator password must be set.
An administrator password protects the following critical actions/areas from unauthorized access:
 - the [reset to factory defaults](#)(see page 28) in the boot menu
 - the [local terminal](#)(see page 507)
 - the [virtual console access](#)(see page 643).

Setup Administrator: A user to whom rights are assigned for minor administrative tasks. You specify which pages the setup administrator can edit under [Accessories > Setup > Setup Administrator Permissions](#)(see page 518).

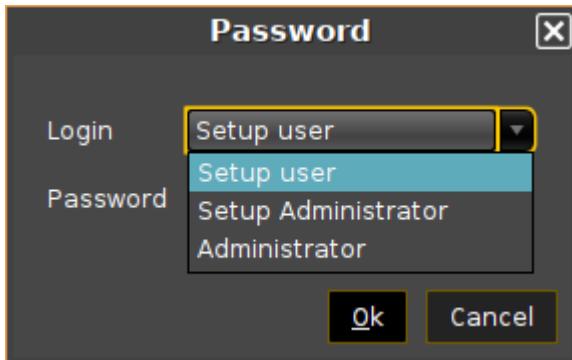
Setup User: A user who can make some unlocked user settings in the IGEL Setup. You specify which pages the setup user can edit under [Accessories > Setup > Setup User Permissions](#)(see page 516).

User: This user has no access to the IGEL Setup. A user password is required in the following cases:



- when logging on to the [terminal session](#)(see page 507)
- when logging on to sessions (see Desktop Integration)
- for unlocking the [screenlock](#)(see page 663)

If you have defined passwords for different authorization levels, a login window appears at the start of the IGEL Setup in which you can select an authorization level:



i When entering a password, ensure that the correct [keyboard layout](#)(see page 672) is enabled.

Administrator

Use password

A password is needed to log in as administrator (`root`).

- A password is also needed for the user, the setup user, and the setup administrator.
- The password is set by clicking **Change Password**.

No password is needed to log in as an administrator. Also, no password is needed for the user (`user`), the setup user, and the setup administrator.*

Change Password

Sets a new password for the administrator (`root`).

i Effects on local terminal access

Setting an administrator password has the following effects on the access to local terminals:

- For logging in as `root`, the administrator password must be entered.
- Logging in as `user` is no longer possible.

However, you can allow access for `user` by making the following settings:

- Enable the registry key `system.security.usershell` (Default: Disabled).
- Set a user password.



For logging in as `user`, the user password will have to be entered. (See the "User" section of this page).

Setup Administrator

Setup Administrator Access

This option is relevant if an administrator password is set.

The setup administrator can access the areas of the IGEL Setup for which he has authorization. Further information can be found under [Setup Administrator Permissions - Define Access to IGEL Setup Areas](#)(see page 518).

- A password is needed to log in as setup administrator.
- The password is set by clicking **Change Password**.

The setup administrator cannot access the IGEL Setup.*

Change Password

Sets a new password for the setup administrator.

Setup User

Setup User Access

This option is relevant if an administrator password is set.

The setup user can access the areas of the IGEL Setup for which he has authorization. Further information can be found under [Setup User Permissions - Define Access to IGEL Setup Areas](#)(see page 516).

- A password is needed to log in as a setup user.
- The password is set by clicking **Change Password**.

The user cannot access the IGEL Setup.*

Change Password

Sets a new password for the setup user.

User

Use Password

This option is relevant if an administrator password is set.

The user (`user`) needs a password in order to log in to the device via the local terminal. The password is set by clicking **Change Password**.



If an administrator password is set, the user (`user`) cannot log in to the device via the local terminal. If no administrator password is set, the user (`user`) can log in to the device via the local terminal without a password.*

Change Password

Sets a new password for the user (`user`).

User Account for Remote Access

Enable Login

The remote user (`ruser`) can log in to the device via SSH. Further information can be found under [SSH Access](#)(see page 833).*

Logging in via SSH is not possible.

Use Password

A password is needed to log in via SSH.

No password is needed to log in via SSH.*

Change Password

Sets a new password for the remote user (`ruser`).

*IGEL OS system default



Logon

Menu path: **Setup > Security > Logon**

- [IGEL Smartcard](#)(see page 804)
- [Taskbar](#)(see page 805)
- [Active Directory/Kerberos](#)(see page 807)
- [Shared Workplace](#)(see page 810)
- [Local User](#)(see page 812)



IGEL Smartcard

Menu path: **Setup > Security > Logon > IGEL Smartcard**

Login with IGEL smartcard

You can log in to the device using a smartcard. Depending on the configuration, a password may also be needed. Sessions stored on the smartcard become available.

The desktop can be used without an IGEL smartcard. (Default)

Enable IGEL smartcard without locking desktop

Enables sessions stored on the smartcard after entering an optional password. The device is not locked – even without a smartcard.

The device will be locked after the removal of the smartcard. (Default)

On smartcard removal, terminate

This parameter is available if **Enable IGEL smartcard without locking desktop** is activated.

Possible options:

- "All sessions": When the card is removed, all sessions are ended.
- "Sessions originating from smartcard": When the card is removed, all sessions stored on the card are ended. Other sessions are not affected.

Company key: A shared code for a smartcard and a device. The code entered must match the code stored on the IGEL smartcard. If two codes do not match, the IGEL smartcard cannot be used on this terminal.

- i** Save the settings before starting to personalize the card.

Start application to write IGEL smartcards:

Smartcard personalization: Opens a window where you can set a login password and add sessions to the card.

- i** Session configurations are stored on the card's integrated circuit, and the session can be used on any IGEL device that reads the card.

- i** Smartcard personalization is possible via the local Setup only. The option is not available via the UMS.

For further information about the smartcard personalization function, see [Using “Smartcard Personalization” function](#)(see page 609).

For information on how to create IGEL smartcards via the UMS, see Authentication with IGEL Smartcard.

See also Smartcard Readers Supported by IGEL Smartcards.



Taskbar

Menu path: **Setup > Security > Logon > Taskbar**

Taskbar settings for the login dialog

- **Show taskbar in login screen**
 The taskbar will be shown during the login dialog. (Default)
 The taskbar will not be shown during the login dialog.
- **Show clock**
 The clock will be shown during the login dialog. (Default)
 The clock will not be shown during the login dialog.
- **Show keyboard layout switcher**
 The switch for the keyboard layout will be shown during the login dialog. (Default)
 The switch for the keyboard layout will not be shown during the login dialog.
- **Show on-screen keyboard button**
 The button for opening the on-screen keyboard is shown during the login dialog.
 The button for opening the on-screen keyboard is not shown during the login dialog. (Default)
- **Start on-screen keyboard automatically**
 The on-screen keyboard is open during the login dialog.
 The on-screen keyboard is not open during the login dialog. (Default)
- **Show reboot button**
 The button for rebooting the thin client is shown during the login dialog.
 The button for rebooting the thin client is not shown during the login dialog. (Default)
- **Show shutdown button**
 The button for shutting down the thin client is shown during the login dialog. (Default)
 The button for shutting down the thin client is not shown during the login dialog.

Taskbar settings when the screenlock is active

- **Show taskbar in screenlock**
 The taskbar is shown while the screen is locked. (Default)
 The taskbar is not shown while the screen is locked.
- **Show clock**
 The clock is shown while the screen is locked. (Default)
 The clock is not shown while the screen is locked.
- **Show keyboard layout switcher**
 The switch for the keyboard layout is shown while the screen is locked. (Default)
 The switch for the keyboard layout is not shown while the screen is locked.
- **Show on-screen keyboard button**
 The button for opening the on-screen keyboard will be shown while the screen is locked.
 The button for opening the on-screen keyboard will not be shown while the screen is locked. (Default)
- **Start on-screen keyboard automatically**
 The on-screen keyboard will remain open while the screen is locked.



- The on-screen keyboard is not open while the screen is locked. (Default)
- **Show reboot button**
 - The button for rebooting the thin client is shown while the screen is locked.
 - The button for rebooting the thin client is not shown while the screen is locked. (Default)
- **Show shutdown button**
 - The button for shutting down the thin client is shown while the screen is locked.
 - The button for shutting down the thin client is not shown while the screen is locked. (Default)
- **Show logoff button**
 - The button for logging off is shown while the screen is locked.
 - The button for logging off is not shown while the screen is locked. (Default)

- ⓘ There is no separate option for enabling/disabling network connection icons in the login dialog and/or on the locked screen. With **Show taskbar in login screen** and **Show taskbar in screenlock** enabled, they appear automatically if the option **Enable tray icon** is activated under **Setup > Network > LAN Interfaces > Interface 1 (or Interface 2, Wireless)** and/or under **Setup > Network > Mobile Broadband** (and/or **VPN**).

ⓘ The network connection icons in the login dialog and on the locked screen, with the exception of the Wi-Fi icon, serve for information purposes only and thus are inactive on clicking. The Wi-Fi icon invokes a [dialog for turning Wi-Fi on/off](#)(see page 701) or the [Wireless Manager](#)(see page 699) in case it is activated under **Setup > Network > LAN Interfaces > Wireless**.

Active Directory/Kerberos

Menu path: **Setup > Security > Logon > Active Directory / Kerberos**

In this area, you can enable local login to the device via the Kerberos protocol. Active Directory/Kerberos must be configured, see [Active Directory/Kerberos](#)(see page 814).

- ⓘ The login can be used for single sign-on in a number of session types (ICA, RDP).

- **Login to Active Directory domain**

- You can log in to the device via Active Directory.
- You cannot log in to the device via Active Directory. (Default)

Login Methods

- **Explicit:**

- You can log in with a user name and password. (Default)
- You cannot log in with a user name and password. If logging in with a smartcard is set up, you can log in with a smartcard.

- **Remember last user name**

- The login dialog will be prepopulated with the last user name that logged on. **Explicit** must be enabled for this.
- The login dialog will not be prepopulated. (Default)

- **Smartcard**

- You can log in using a smartcard.
- You cannot log in using a smartcard. (Default)

- ⓘ Select the smartcard type under **Security > Smartcard > Middleware**.

- **Smartcard removal action:** Specifies what action is performed when the smartcard via which the user is logged in is removed.

Possible actions:

- Log out: The user is logged out from the device.
- Lock device: The screen is locked.

Logout Shortcut Locations

The start options for the logoff function are specified here.

Start menu

- The session can be launched from the start menu.

Application Launcher

- The session can be launched with the Application Launcher.



Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

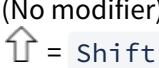
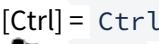
Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
-  = `Shift`
-  = `Ctrl`
-  = `Mod4`



-  When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

-  To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

IGEL Tech 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=JxGOEGAb3LI>



Shared Workplace

Menu path: **Setup > Security > Logon > Shared Workplace**

- **Activate IGEL Shared Workplace**

- You can log in to the thin client via IGEL Shared Workplace.
- You cannot log in to the thin client via IGEL Shared Workplace. (Default)

- **Skip IGEL Shared Workplace login if UMS server is unavailable**

- If the *UMS* server is not available, the user can log in via Active Directory/Kerberos. In order to do this, logging in via Active Directory/Kerberos must be configured; further information can be found under [Active Directory/Kerberos](#)(see page 807).
- Logging in is only possible if the *UMS* server is available. (Default)

- **Remember last user name**

- The login dialog will be prepopulated with the last user name that logged on.
- The login dialog will not be prepopulated. (Default)

Logout Shortcut Locations

The start options for the logoff function are specified here.

- **Start menu:** If this option is enabled, the session can be launched from the start menu.
- **Application Launcher:** If this option is enabled, the session can be launched with the Application Launcher.
- **Desktop:** If this option is enabled, the session can be launched with a program launcher on the desktop.
- **Quick start panel:** If this option is enabled, the session can be launched with the quick start panel.
- **Start menu's system tab:** If this option is enabled, the session can be launched with the start menu's system tab.
- **Application Launcher's system tab:** If this option is enabled, the session can be launched with the Application Launcher's system tab.
- **Desktop context menu:** If this option is enabled, the session can be launched with the desktop context menu.
- **Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.
- **Path in the Application Launcher:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.
- **Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.
- **Password protection:** Specifies which password will be requested when launching the session.
Possible values:
 - **None:** No password is requested when launching the session.
 - **Administrator:** The administrator password is requested when launching the session.
 - **User:** The user password is requested when launching the session.



- **Setup user:** The setup user's password is requested when launching the session.
- **Hotkey:**
 - The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.
- **Modifiers:** A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`. Here, you will find the available modifiers and the associated key symbols:
 - (No modifier) = `None`
 - = `Shift`
 - `[Ctrl]` = `Ctrl`
 - = `Super_L`
 - `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl +` = `Ctrl|Super_L`
- **Key:** Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`



Local User

Menu path: **Setup > Security > Logon > Local User**

Login with local user password

Upon the start of the device, a login screen is shown and authentication with a local user password is enabled. A password specified under **Set password** is deployed to log in. This password will also be used for **User Interface > Screenlock / Screensaver > Options > Local user password** (previously called **Screenlock password**), see [Options](#)(see page 666).

If both [Active Directory \(AD\) login](#)(see page 807) and login with local user password are enabled, you can choose on the login screen which login method you want to use.

Authentication with a local user password upon device startup is disabled.

Logout Shortcut Locations

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.



- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`



Active Directory/Kerberos

Menu path: **Setup > Security > Active Directory / Kerberos**

- **Enable**

- The Kerberos basic configuration will be carried out.
 The Kerberos basic configuration will not be carried out. (default)

- **Default domain (Fully Qualified Domain Name):** This value must match the Windows domain on which the logon is to take place, e.g. EXAMPLE.COM .

The value must be entered in upper case letters.

- **DNS lookup for domain controller**

- In order to find the key distribution centers (KDCs, domain controllers) and other servers for a realm, DNS SRV records are used if they are not explicitly indicated. (default)
 The key distribution centers entered under **Setup > Security > Active Directory/Kerberos > Domain 1 ... Domain 4** will be used.

- **DNS lookup for domain**

- In order to determine the Kerberos realm of a host, DNS TXT records are used. (default)
 The details under **Setup > Security > Active Directory / Kerberos > Domain Realm Mapping** are used.

- **Obtain addressless tickets**

- The first Kerberos ticket is addressless. This may be necessary if the client is located behind an NAT device (Network Address Translation). (default)

-
- **Domain 1 ... Domain 4**(see page 815)
 - **Domain Realm Mapping**(see page 816)



Domain 1 ... Domain 4

Menu path: **Setup > Security > Active Directory/Kerberos > Domain 1 ... Domain 4**

Up to 4 domains where a login is possible can be configured here.

To configure a domain, proceed as follows:

1. Under **Domain name**, give the name of the domain (Kerberos realm).
2. Click to create a new entry.
3. Under **Domain controller**, give the name or IP address of the domain controller (Kerberos key distribution center). A port number can be added to the host name; the port name must be preceded by a colon.
4. Click on **Continue**.

The domain controller will be added to the **Domain controller list**.



Domain Realm Mapping

Menu path: **Setup > Security > Active Directory / Kerberos > Domain Realm Mapping**

With domain realm assignment, a host name is translated into the corresponding Kerberos realm name.

- **Use default DNS domain - Active Directory domain mapping**

- The DNS name and Active Directory domain name match. (default)
 DNS name and Active Directory domain name assignments must be set up.

To set up a DNS name to Active Directory domain name assignment proceed as follows:

1. Click **[+]** to create a new entry.
 2. Under **DNS host or domain name**, enter the host name that is to be assigned to an Active Directory domain name.
 3. Under **Active Directory domain name**, enter the Active Directory domain name that is to be assigned to the host name.
 4. Click on **Continue**.
- The data entered will be added to the **Domain realm mapping** list.



Smartcard

Menu path: **Setup > Security > Smartcard**

Here, you can define settings for logging on using a smartcard.

- Services(see page 818)
- Middleware for Smartcards in IGEL OS(see page 820)



Services

Menu path: **Setup > Security > Smartcard > Services**

The PC/SC service enables the smartcard reader to connect to the device, so that the smartcard is available to an application. This can be a server-side application where the data are forwarded via an RDP or ICA connection or a local application, e.g. the browser.

Enable PC/SC daemon

- The PC/SC service is enabled. The card reader is available for applications. (Default)
- The PC/SC service is disabled. The card reader is not available.

Currently active PC/SC devices: List of smartcard readers currently connected to the device. Internal smartcard readers and a variety of USB smartcard readers are supported.

You will find a list of supported smartcard readers in the [IGEL Hardware Database](#)⁵⁸.

See also Smartcard Readers Supported by IGEL Smartcards.

Cherry USB2LAN proxy

- The Cherry USB2LAN proxy is active and makes Cherry electronic health card devices available in the network via SICCT and HTTPS.
- The Cherry USB2LAN proxy is disabled. (Default)

Bind interface: Network interface used for the proxy.

This parameter is available if **Cherry USB2LAN proxy** is enabled.

Possible options:

- "autoBind IP (see below) is set to "auto".
- "eth0": The Ethernet interface will be used.
- "wlan0": The WLAN interface will be used.
- Free text entry: The manually entered network interface will be used.

i The Ethernet and WLAN interfaces can be configured under **Network > LAN Interfaces**. See [LAN Interfaces](#)(see page 689).

Bind IP: The IP address used for the proxy.

Possible options:

- "autoBind interface is set to "auto".
- Free text entry: The manually entered IP address will be used instead of the network interface specified under **Bind interface**.

HTTPS server port: The TCP port for the HTTPS server. (Default: 443)

SICCT announce IP: The IP address to send the SICCT announce messages to.

Possible options:

⁵⁸ <https://www.igel.com/linux-3rd-party-hardware-database/>



- "broadcast- Free text entry: SICCT announce messages are sent to the manually entered IP address.

SICCT announce port: UDP port for SICCT announce messages. (Default: 4742)

SICCT announce interval: Time interval in seconds for sending out SICCT announce messages.

Value range: 5 to 1800 (Default: 30)

USB fast mode

- Faster connection to a Cherry eGK device is enabled.
 Faster connection to a Cherry eGK device is disabled. (Default)

i In order for the changes of this setting to be applied, the device must be unplugged and connected again.

Alternative initialization method for G87-1505

- Alternative initialization method for Cherry eGK keyboard G87-1505 is enabled.
 Alternative initialization method for Cherry eGK keyboard G87-1505 is disabled. (Default)

Middleware for Smartcards in IGEL OS

In comparison to simply using passwords, two-factor authentication with a smartcard or smart token offers an additional layer of security. When configuring login with a smartcard, you have to define smartcard middleware to be used. In this area of the IGEL Setup, you select the middleware (PKCS#11 module) which matches your card or your token. Alternatively, you can specify here your own PKCS#11 module.

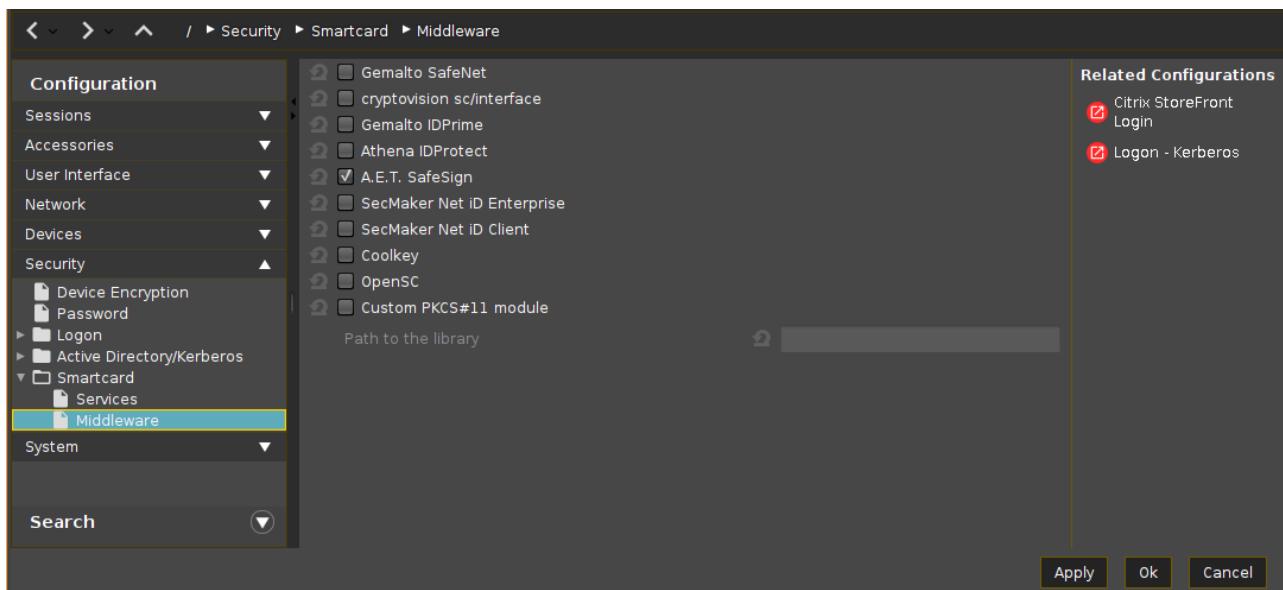
The middleware selected here will be used for the following logins:

- Login to Citrix sessions; see [Citrix Global](#)(see page 52)
- Login to Citrix StoreFront; see [Citrix StoreFront](#)(see page 91)
- Login to an endpoint device via Active Directory; see [Active Directory/Kerberos](#)(see page 807)

For more information on smartcard authentication in IGEL OS, see the how-to Smartcard Authentication in IGEL OS.

If you use IGEL smartcards, see Authentication with IGEL Smartcard.

Menu path: **Security > Smartcard > Middleware**



- i** For smartcard authentication to Citrix and Active Directory / Kerberos, you can use several middleware libraries at the same time. The concurrent usage of multiple smartcard middleware libraries may be required, for example, if multiple users with different smartcard types must have access to the device.
Note: If no middleware is activated, OpenSC is used as a fallback.

Gemalto SafeNet

The middleware for Gemalto/SafeNet eToken, IDPrime smartcards and Token is used.



cryptovision sc/interface

The middleware for cryptovision smartcards is used.

Gemalto IDPrime

The middleware for Gemalto IDPrime smartcards is used.

- ⓘ Enable this Gemalto middleware when you want to operate Gemalto Common Criteria devices in unlinked mode.

Athena IDProtect

The middleware for Athena IDProtect smartcards is used.

A.E.T. SafeSign

The middleware for SafeSign smartcards is used.

SecMaker Net iD Enterprise

The SecMaker Net iD Enterprise middleware, formerly known as "Secmaker Net iD", is used.

- ⓘ Enable this SecMaker middleware if you use Net iD implementation with CID (Certificate Identity Declaration).

SecMaker Net iD Client

The SecMaker Net iD Client middleware is used. SecMaker Net iD Client is the next generation of Net iD Enterprise, see <http://docs.secmaker.com/net-id-client/latest/index.html>.

- ⓘ The SecMaker Net iD Client must also be installed on the server side.

Coolkey

The middleware Coolkey is used.

OpenSC

The middleware OpenSC is used.



90meter

The 90meter middleware is used.

Licensed Feature

This feature requires an add-on license; see Add-On Licenses. Please contact your IGEL sales representative.

Custom PKCS#11 module

The PKCS#11 module stored under the **Path to the library** is used. See also Using a Custom PKCS#11 Library.

- In case of the installation of a custom PKCS#11 library, the file(s) (in `.so` format) must be placed on the endpoint device either via UMS file transfer or Custom Partition.
The use of the `/wfs` folder is NOT recommended because of its space limit.

Path to the library

Path to the custom PKCS#11 module. Example: `/usr/lib/pkcs11/[name of the library].so`



System

Menu path: **Setup > System**

You can configure basic system settings here.

- [Time and Date](#)(see page 824)
- [Update](#)(see page 825)
- [Remote Management](#)(see page 829)
- [Remote Access](#)(see page 832)
- [Logging](#)(see page 839)
- [Power Options](#)(see page 841)
- [Firmware Customization](#)(see page 847)
- [Registry](#)(see page 876)



Time and Date

Menu path: **Setup > System > Time and Date**

- **Timezone Continent/Area:** Continent/Area for your location

Possible values:

- General: Under **Location**, you can select a time zone.
- Africa... Pacific: Under **Location**, you can select a city for the selected continent/area.

- **Location:** Select your location or time zone.

i Please note that the GMT time zones under Linux are usually in POSIX format. This means that you need to invert the actual time difference (e.g. for New York you select the zone "GMT+5" for "5 hours west of Greenwich" although the time in New York is actually 5 hours behind GMT). Defining the time zone by selecting a **Continent** and **Location** is therefore preferable.

- **Use NTP Time Server**

The system clock is set via NTP.

The system clock is not set via NTP. (default)

- **Use NTP Time Server:** IP or name of an NTP time server. If you would like to enter a list of NTP time servers for redundancy purposes, separate the servers with spaces.

- **Set time and date:** Carries over the time and date and sets the hardware clock.

You will find further information regarding the updating of time zone information (e.g. summer time adjustments) in the Updating Timezone Information (Daylight Saving Time, DST) FAQ.



Update

Menu path: **Setup > System > Update**

Here, you can configure settings for the system update.

- [Firmware Update\(see page 826\)](#)
- [Buddy Update\(see page 828\)](#)



Firmware Update

Menu path: **Setup > System > Update > Firmware Update**

Here, you can specify how the device obtains updates for its own firmware.



No Downgrade from IGEL OS 11.03

It is not possible to downgrade from IGEL OS 11.03 or higher to any version before IGEL OS 11.03, except IGEL OS 11.02.200. This is because, from IGEL OS 11.03 onwards, the system partitions are signed to guarantee their integrity; it is not possible to change from a system with signed partitions to a system with unsigned partitions. IGEL OS 11.02.200 is a special variant of IGEL OS 11.02 that has signed system partitions. IGEL OS 11.02.200 is only available from the IGEL Support Team.



Update Can Be Canceled After Timeout

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

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

- **Protocol:** Select the method for accessing the updates.
 - HTTP: Download from a web server.
 - HTTPS: Download from a TLS/SSL-secured web server.
 - FTP: Download from an FTP server. (FTP passive mode is used)
 - Secure FTP: Download via SSH-secured FTP.
 - FTPS: Download from a TLS/SSL-secured FTP server.
 - FILE: The update lies in the device file system, possibly as a shared NFS or Windows update.
You can choose the location by selecting a file below.
- **Server name:** Name or IP address of the server.
- **Port:** Port of the server on which the service is provided.
- **Server path:** The path to the directory with the update files on the server.
- **User name:** User name on the server.
- **Password:** Password for the user account on the server.
- **Automatic update check on boot**
 The device will automatically search for and install an updated firmware version each time that it boots.
 The device will not automatically search for an updated firmware version. (Default)
- **Automatic update check on shutdown**
 The device will automatically search for and install an updated firmware version each time that it shuts down or it reboots.



- The device will not automatically search for an updated firmware version when it shuts down. (Default)
- **Automatic buddy detection**
 - The device will automatically search for further devices in the local network that offer firmware updates as Buddy Servers.
 - The device will not automatically search for Buddy Servers. (Default)
- **Update firmware:** Launches the update process. If you have made changes on this setup page earlier on, click on **Apply** first.



Buddy Update

Menu path: **Setup > System > Update > Buddy Update**

Under **Buddy Update**, you can specify your thin client as an update server for other IGEL thin clients. If you use a thin client as an update server, only the FTP protocol can be used to update the firmware. A number of thin clients can be set up as buddy update servers within the network.

Thin clients without a specified update server search for available servers during the update. The first update server contacted then provides the update.

No Downgrade from IGEL OS 11.03

It is not possible to downgrade from IGEL OS 11.03 or higher to any version before IGEL OS 11.03, except IGEL OS 11.02.200. This is because, from IGEL OS 11.03 onwards, the system partitions are signed to guarantee their integrity; it is not possible to change from a system with signed partitions to a system with unsigned partitions. IGEL OS 11.02.200 is a special variant of IGEL OS 11.02 that has signed system partitions. IGEL OS 11.02.200 is only available from the IGEL Support Team.

Update Can Be Canceled After Timeout

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

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

Enable Update Server

- This thin client serves as an FTP firmware update server for other thin clients.
- This thin client does not serve as an FTP firmware update server for other thin clients. (default)

User Name: User name for FTP access (default: anonymous)

Password: Password for FTP access. The asterisk * allows any password.

Max. Concurrent Logins: Maximum number of simultaneous logons on the FTP server. (default: 10)

For further information, read the Buddy Update how-to.



Remote Management

Menu path: **Setup > System > Remote Management**

Here, you can configure settings relating to the remote administration of the device using the Universal Management Suite (UMS).

Enable remote management

- The endpoint device can be managed via the UMS. (Default)
- Remote management is not allowed.

Universal Management Suite: If the device is registered on a UMS Server, its IP address or hostname will be shown in the list.

- ⓘ The list can contain more than one UMS instance. If the device cannot contact a UMS Server under the hostname `igelrmserver`, and the DHCP option 244 is not set, the device will go through the entries in the list until it can contact a UMS Server successfully.

To add another UMS instance, click on :

- **UMS Server:** Name or IP of the UMS Server
- **Port Number:** Port number of the UMS Server (Default: 30001)

Display “Apply changes” dialog on boot: If new settings were made in the UMS, the device may receive them during the boot procedure. Here you can decide whether the user can influence the application of the new settings.

During the boot procedure, the **Apply changes** dialog will be shown if new settings are available. The user can decide whether the new settings are applied immediately. If the user does not allow them to be applied immediately, they will automatically be applied when the system is next restarted.

The dialog will not be shown. The new settings will be automatically applied or ignored depending on the setting under **Default action on boot**.

Timeout: Number of seconds for which the **Apply changes** dialog is shown (Default: 20). If the timeout is exceeded, the received settings will be automatically applied.

Possible values:

- No timeout: The dialog is shown until the user clicks on a button.
- 1 ... 120 seconds

Default action on boot: Configure the action that is to be performed if the dialog exceeds the time limit or if it is disabled.

Possible values:

- Apply changed configuration immediately: New settings will become active immediately and programs that are running may be restarted.
- Ignore changed configuration: New settings will not be applied. The new configuration will be saved on the device.

Prompt user on UMS actions



The user will be informed via a message window if the device receives new settings from the UMS or is shut down. (Default)

The user will not be informed if the device receives new settings from the UMS or is shut down.

Timeout: Number of seconds for which the notification window is shown

Possible values:

- No timeout: The dialog is shown until the user clicks on a button.
- 1 ... 120 seconds

Structure tag: You can define a structure tag in order to sort the device into a directory in accordance with the UMS directory rules.

UMS Registration: This button opens the [UMS Registration](#)(see page 550) program from the accessories.

Further information regarding the use of structure tags can be found in the how-to Using Structure Tags.

-
- [Options](#)(see page 831)



Options

Menu path: **Setup > System > Remote Management > Options**

- **Log login and logoff events**

(i) Please note: For this option to work, in the UMS Console under **UMS Administration > Globale Configuration > Logging** the option **Log Events** must be enabled.

If a user logs on or off via Citrix or Kerberos, details of this event will be sent to the UMS and can be used there, e.g. to process support queries.

Logoffs from the Shared Workplace will also be logged (logons take place via the UMS anyway).
(default)

Logon and logoff events will not be relayed. (default)

(i) The event logs can be found under the system information for the thin clients in the UMS.

- **Delay session start at boot time in order to apply new UMS settings:** If new settings were made in the UMS, the thin client may receive them during the boot procedure.

The session start will be delayed until the settings have been transferred or the time limit has been exceeded.

- **Timeout:** Delay in seconds (default: 10)

Possible values:

- No time limit: The dialog is shown until the user clicks on a button.
- 1 ... 120 seconds



Remote Access

Menu path: **Setup > System > Remote Access**

In order to allow central administration, the thin client can be configured in such a way that it can be accessed via the WAN.

- [SSH Access](#)(see page 833)
- [Shadow Settings in IGEL OS](#)(see page 835)
- [Secure Terminal](#)(see page 838)



SSH Access

Menu path: **Setup > System > Remote Access > SSH Access**

Remote access to the local system via SSH is permitted by default. However, you can restrict remote access to a specific user from a specific host.

Enable

The SSH service is enabled. (default)

Permit empty passwords

Logging on without a password is allowed.

Logging on without a password is not allowed. (default)

Permit administrator logon:

Logging on as an administrator is allowed.

Logging on as an administrator is not allowed (default)

Port number: Port number for SSH (default: 22)

User access

User name: Permitted user

Possible values:

- root
- user
- ruser

i For the **user name** "ruser" a password has to be assigned under **Security > Password**. The names "root" and "user" work also without passwords.

Hostname: Name of the host from which SSH access takes place (example: `xterm.igel.de`)

Deny

Access is denied.

Access is allowed. (default)

Permit X11 forwarding:

X11 forwarding is enabled.

X11 forwarding is disabled. (default)

Enable applications access for remote user "ruser"

Command line: Command that is allowed or prohibited for the remote user

Enable application



- The application given under **command line** may be executed by the remote user. (default)
- The application given under **command line** may not be executed by the remote user.



Shadow Settings in IGEL OS

IGEL OS offers the ability to observe the endpoint device via shadowing. This is handy for helpdesks, troubleshooting, etc. This is possible via IGEL Virtual Network Computing (VNC) Viewer in the Universal Management Suite (UMS) or another VNC client (e.g. TightVNC), see Shadowing (VNC).

In the following article, you will learn about the **Shadow** settings, which you will require when configuring VNC access to your devices.

Menu path: **System > Remote Access > Shadow**

Remote Access to IGEL OS Devices via Shadowing

For Remote Working, Use Secure Shadowing

If the endpoint device is in a mobile or work-from-home environment, it is highly recommended to use secure shadowing only. Regular shadowing without encryption poses a security risk.

The screenshot shows the IGEL OS configuration interface with the following details:

- Path:** / System > Remote Access > Shadow
- Configuration Tree (Left):**
 - Sessions
 - Accessories
 - User Interface
 - Network
 - Devices
 - Security
 - System
 - Time and Date
 - Update
 - Remote management
 - Remote Access
 - SSH Access
 - Shadow** (selected)
 - Secure Terminal
 - Logging
 - Power Options
 - Firmware Customization
 - Registry
 - Search
- Settings (Right):**
 - Allow remote shadowing:**
 - Secure mode:**
 - Use Password:**
 - Password:** [Redacted]
 - Prompt user to allow remote session:**
 - Allow user to disconnect remote shadowing:**
 - Allow input from remote:**
 - Scale frame buffer:**
 - Scale factor:** 1.0
 - Position of the indicator:** Bottom right
- Buttons (Bottom Right):** Apply, Ok, Cancel

Allow remote shadowing

- Desktop content can be viewed from remote computers with VNC software.
- VNC shadowing is not allowed.*



If **Allow remote shadowing** is activated, you can change the following settings:

Secure mode

- Communication will be secured via SSL/TLS and shadowing will only be possible for UMS administrators.
- Communication will not be secured via SSL/TLS.*

Further information regarding secure shadowing can be found under Secure Shadowing (VNC with TLS/SSL).

Use password

- The remote user must enter a password before shadowing can begin.
- The remote user does not require a password for shadowing.*

Password

Password for the VNC connection

Prompt user to allow remote session

- The local user will be asked for permission before shadowing.*

! In a number of countries, for example, Germany, unannounced shadowing is prohibited by law. Do not disable this option if you are in one of these countries!

Allow user to disconnect remote shadowing

- A **Disconnect** button with which the user can terminate the VNC connection is shown.*

Allow input from remote

- The remote user can make entries using the keyboard and mouse as if they were the local user.*

Scale frame buffer

- The screen content of the shadowed device is reduced or enlarged by the **scaling factor** before being transferred.
- The screen content is transferred in the original size.*

Scale factor

Factor by which the screen content of the shadowed device is enlarged or reduced. (Default: 1.0)

Position of the indicator

Defines the position of the popup notification about being shadowed.

Possible options:



- **Top right**
- **Top left**
- **Bottom left**
- **Bottom right***

ⓘ Further parameters for the VNC server on the device are accessible under **System > Registry > network.vncserver**.

*IGEL OS system default



Secure Terminal

Menu path: **Setup > System > Remote Access > Secure Terminal**

You can establish a secure terminal connection to a thin client.

The thin client must meet the following requirements:

- The firmware of the thin clients is *IGEL Linux Version 5.11.100* or higher or *IGEL Linux Version 10.01.100* or higher.

For IGEL Linux Version 5.11.100 and 10.03.100:

1. In the thin client setup, go to **System > Remote Access > Secure Terminal**
2. Enable **Secure Terminal**

For IGEL Linux Version 10.01.100 or newer:

- Enable the following options in the thin client registry:
 - **network > telnetd > enabled > allow telnet access**
 - **network > telnetd > secure_mode > secure telnet**

ⓘ You can allow access via the secure terminal for all registered thin clients. To do this, enable the **UMS Administration > Global Configuration > Remote Access > Enable Global Secure Terminal** option.



Logging

Menu path: **Setup > System > Logging**

Here you can configure local and remote logging for the device.

Local logging

- The log messages are stored locally in `/var/log`. The format is human-readable. Log rotation is applied.
 The log messages are not stored locally.

Persistent log partition: This parameter is effective only when **Local logging** is activated.

- The log messages are stored in a persistent partition on the device. This partition is encrypted.
 The log messages are stored in temporary files that are deleted on reboot.

Partition size in MB: Size of the persistent log partition

Remote mode

Possible options:

- "Server": The device receives log messages from a remote client.
- "Client": The device sends its log messages to a remote server.
- "Off": The device does not send or receive any log messages.

Remote Mode Switched to "Server"

You can configure the device to act as a syslog server. One or more other clients can send log files to this server; you can create a separate server configuration for each client.

Template for log file storage: Pattern from which the file path for storing the received log messages is created. `%HOSTNAME%` is the name of the sender which is configured under **Name**.

Server: A syslog server can be added by clicking .

Local port: Port on which the local server listens for log messages

Transport protocol: Protocol to be used for the transmission of log messages

Name: Hostname of the sender (optional). This is useful for filtering the log messages based on the clients that have sent them.

Local address: Optional parameter; on multihomed machines (i. e. machines with multiple addresses), this specifies to which local address rsyslog is bound. If no address is specified it defaults to `0.0.0.0`, so that rsyslog listens on every network interface. For more information, see the official documentation at <https://www.rsyslog.com/doc/v8-stable/configuration/modules/imtcp.html>.

Remote Mode Switched to "Client"

You can configure one or more clients, e.g. one server for kernel messages and another server for authentication messages.

Clients: A client can be added by clicking .



Remote address: IP address or hostname of the remote server

Remote port: Port on which the server listens for log messages

Transport protocol: Protocol to be used for the transmission of log messages

Syslog facility: Type of program for which log messages are created

Syslog level: Severity level of the event

Syslog style template: Format in which the messages are sent

TLS enabled

TLS encryption for the transmission of log messages is enabled.

Transmitted log messages are not encrypted.

CA certificate: Path to the local CA root certificate file in PEM format which is used to verify the authenticity of the X.509 certificate of your log collector and analyzer. If the UMS is used to transfer the certificate file to devices (see Logging and Log Evaluation), the same path and file name as in the UMS must be entered. Example: `/wfs/ca-certs/ca.pem`



Power Options

Menu path: **Setup > System > Power Options**

In this area, you will find the settings for energy management.

- [System Power Options in IGEL OS](#)(see page 842)
- [Battery](#)(see page 844)
- [Screen](#)(see page 845)
- [Shutdown](#)(see page 846)



System Power Options in IGEL OS

Here, you can configure settings for energy saving on your IGEL OS endpoint device. This comprises the behavior after a configured time of inactivity and the CPU power plan.

ⓘ Display of Energy Star Logo on Selected HP Endpoint Devices

With selected Hewlett-Packard (HP) endpoint devices, the Energy Star certification mark is displayed on this Setup page,

Menu path: **System > Power Options > System**

System suspend/shutdown on inactivity

Specify how long the user can be inactive before the system switches to standby mode or shuts down, dependent on the option selected under **System action on inactivity**.

Possible values:

- **Never***
- **After 1 minute**
- ...
- **After 24 hours**

System action on inactivity

Possible options:

- **Suspend***: The system is set to standby mode after the timeout defined with **System suspend/shutdown on inactivity** has expired.

ⓘ If Suspend doesn't work, it might be related to a missing ACPI Support: <https://01.org/linuxgraphics/gfx-docs/drm/admin-guide/pm/sleep-states.html>

- **Shutdown**: The system is shut down after the timeout defined with **System suspend/shutdown on inactivity** has expired.

Without dialog

- The user is not asked if the system is to be set to standby mode.
 The dialog will be shown.*

Dialog timeout

Time in seconds, for which the dialog is to be displayed. (Default: 10 seconds)



CPU Power Plan

Specify here which CPU power plan (CPU Governor) the device is to use in battery mode and in AC mode.

- **On Battery**

High Performance: full performance with maximum processor speed

Balanced (Smooth): slower regulation of performance in a balanced manner according to the demands of programs. Suitable for users who are bothered by the fan frequently running at high speed.

Balanced (Recommended)*: rapid regulation of performance according to the demands of programs.

Power Saver: lowest processor speed

- **Plugged in**

High Performance*

Balanced (Smooth)

Balanced (Recommended)

Power Saver

Tray Icon

A CPU icon will be shown in the system tray. This makes it easy to switch between power plans.

No CPU icon will be shown.*

* IGEL OS system default



Battery

Menu path: **Setup > System > Power Options > Battery**

In this area, you can define the rechargeable battery messages.

Battery Notification

- **Critical battery level (percentage):** Percentage of remaining battery charge deemed critical (default: 5)
- **Critical battery action:** Action to be taken in the event of a critical battery level
 - Possible options:
 - Do nothing
 - Show warning
 - Run command
 - Run command in terminal
 - **Critical command:** Command that is executed when a critical charge level is reached (example: Shutdown)
- **Low battery level (percentage):** Percentage of remaining battery charge deemed low (default: 10)
- **Low battery action:** Here you can specify what action is to be taken in the event of a low battery level.
 - Possible options:
 - Do nothing
 - Show warning
 - Run command
 - Run command in terminal
 - **Low command:** Command that is executed when a low charge level is reached (example: Shutdown)

Battery Tray Icon

- **Display percentage:**
 The percentage of remaining energy is shown in the taskbar. (default)
- **Display time**
 The estimated remaining battery life is shown in the taskbar.
 The estimated remaining battery life is not shown. (default)



Screen

Menu path: **Setup > System > Power Options > Display**

In this area, you can configure screen settings which can help to reduce energy consumption.

Display Power Management Settings

- **Handle Display Power Management:**
 You can configure energy saving settings separately for battery or AC operation. (default)
 You cannot configure energy saving settings.
- **Standby Time:** Number of minutes after which the screen switches to standby mode if the user is inactive. (default: 6 minutes)
- **Suspend time:** Number of minutes after which the screen switches to suspend mode if the user is inactive. (default: 8 minutes)
- **Off Time:** Number of minutes after which the screen switches off if the user is inactive. (default: 10 minutes)

Brightness Reduction

i The brightness reduction controls have been added specifically for use of laptops. They have no effect on other devices connected to the power supply.

- **On inactivity reduce to:** Specify to how many percent the screen brightness should be reduced if you are not using the device for battery and AC operation. (default for battery: 20%, default for AC operation: 80%)
- **Reduce after:** Specify a time between 10 and 120 seconds after which the screen brightness will be reduced for battery and AC operation. (default: Never)



Shutdown

Menu path: **Setup > System > Power Options > Shutdown**

Here, you can change the behavior when the device shuts down manually or automatically.

Allow system shutdown

- The device can be shut down by the user. (Default)
 The device cannot be shut down by the user.

Allow system suspend

- The device can be suspended by the user. (Default)
 The device cannot be suspended by the user.

Allow canceling of shutdown process

- The user can cancel the procedure via a button. (Default)
 The user cannot cancel the procedure.

Default action: Action that is carried out when the time is set under **Dialog timeout**.

Possible options:

- Shutdown
- Suspend
- Cancel: No action will be carried out after the time set under **Dialog timeout** expires, see **Allow canceling of shutdown process** parameter.
- Nothing: No action will be carried out after the time set under **Dialog timeout** expires.

Without dialog

- The dialog will not be shown. The action selected under **Default action** will be carried out.
 The dialog will be shown. (Default)

Dialog timeout: After the time (in seconds) set here expires, the dialog will close and the action specified under **Default action** will be carried out. If the value is set to 0, the dialog will be shown until the user selects one of the possible actions. (Default: 10)



Firmware Customization

Menu path: **Setup > System > Firmware Customization**

You can configure the firmware according to your needs.

- [Custom Partition](#)(see page 848)
- [Custom Application](#)(see page 850)
- [Custom Commands](#)(see page 857)
- [Corporate Design](#)(see page 864)
- [Environment Variables](#)(see page 872)
- [Features](#)(see page 875)



Custom Partition

Menu path: **Setup > System > Firmware Customization > Custom Partition**

In IGEL OS, a custom data partition is available for use as required. A download/update function that loads data from a server and, where appropriate, updates them can be set up for this custom storage area.

⚠ The IGEL Support Team offers support for the deployment of Custom Partitions. However, it is not possible to offer support for any third-party software that is installed on a Custom Partition.

❗ If the device is reset to the default settings (factory reset), the custom partition and all data stored on it will be deleted.

- [Download](#)(see page 849)



Download

Menu path: **Setup > System > Firmware Configuration > Custom Partition > Download**

Sources for partition data

In order to load data onto the custom partition, at least one source for partition data must be set up here.

To manage the list, proceed as follows:

- Click to create a new source.
- Click to remove the selected source.
- Click to edit the selected source.
- Click to copy the selected source.

Add

- **Automatic update**
 The contents from this source will be updated automatically.
 The contents from this source will not be updated automatically. (default)
- **URL:** URL of the web server
- **User name:** User name for access to the web server
- **Password:** Password for access to the web server
- **Initialization action:** Action which is performed after mounting the partition (program or script with absolute path). For example, a program downloaded to the partition can be launched.
- **Finalizing action:** Action which is performed before mounting the partition (program or script with absolute path). For example, a program downloaded to the partition can be ended.

The transfer protocols are the same as the ones for updating the firmware, e.g. HTTP and HTTPS. An `INF` file which in turn references a tar archive zipped using bzip2 must be referenced as the target.

The structure of the INF file is as follows:

<code>[INFO], [PART]</code>	Header information
<code>file="test.tar.bz2"</code>	File name of the compressed tar archive
<code>version="1"</code>	Version number - a higher version results in an update if Update automatically is enabled.

The files to be transferred must therefore be zipped in a tar archive which is then compressed using bzip2. This file is referenced in the INF file which is the target of the URL.

The tar archive can be created under Windows, e.g. with the open source program 7-Zip (www.7-zip.de⁵⁹). This program also allows `bzip2` compression. Under Linux, tar and bz2 files can be created using onboard resources.

The procedure makes it possible to replace the file(s) on the server with a new version which the thin client loads the next time it is booted. The `Version` parameter in the `INF` file must be increased for this purpose.

⁵⁹ <http://www.7-zip.de>



Custom Application

Menu path: **System > Firmware Customization > Custom Application**

Applications that were loaded onto a customer partition for example can be launched via the Application Launcher or an icon on the desktop once they have been defined as custom applications. In order for this to be possible, a command to call up the application must be entered under [Settings](#)(see page 853).

- ▶ Click on to define a custom application.
- ▶ Specify the launch options:

Session name: Name for the session.

The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.



Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl|Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: Tab in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.



Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

- For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.
- No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

- If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- The session is started automatically, even when no network is available.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode\(see page 213\)](#).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode [XDMCP for this Display](#))
- **Desktop Context Menu** (not in appliance mode [XDMCP for this Display](#))
- **Application Launcher** (includes [Application Launcher's system tab](#); not in appliance mode [XDMCP for this Display](#))
- **Hotkey**
- **Autostart** (not in appliance mode [XDMCP for this Display](#))

The session cannot be started in appliance mode.

-
- [Settings\(see page 853\)](#)
 - [Desktop Integration\(see page 854\)](#)



Settings

Menu path: **System > Firmware Customization > Custom Application > [Session Name] > Settings**

Enter the command for calling up an application here:

Icon name: Select an icon provided. (default: applications-other).

Command: Give the name and path of the application. (Example: /usr/bin/gpicview).

- ⓘ Only the desktop icon of a session is customizable. The taskbar icon of a session cannot be customized and will remain the default icon. Complete customization is not possible.



Desktop Integration

Menu path: **System > Firmware Customization > Custom Application > [Session Name] > Desktop Integration**

Session name: Name for the session.

The session name must not contain any of these characters: \ / : * ? “ < > | [] { } ()

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.

Desktop

The session can be launched with a program launcher on the desktop.

Quick start panel

The session can be launched with the quick start panel.

Start menu's system tab

The session can be launched with the start menu's system tab.

Application Launcher's system tab

The session can be launched with the Application Launcher's system tab.

Desktop context menu

The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.

Possible values:

- **None:** No password is requested when launching the session.
- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey



The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- `[Ctrl]` = `Ctrl`
- = `Mod4`

i When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- `[Alt]` = `Alt`

Key combinations are formed as follows with `|`:

- `Ctrl + Windows` = `Ctrl | Super_L`

Key: Key for the hotkey

i To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network



If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

The session is started automatically, even when no network is available.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 213).

The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

The session cannot be started in appliance mode.



Custom Commands

Menu path: **Setup > System > Firmware Customization > Custom Commands**

You can define custom commands for specific points in time when the system is starting. You can use configured environment variables(see page 872) in the commands.

- Post Session Custom Commands in IGEL OS(see page 858)
- Base(see page 860)
- Network(see page 861)
- Desktop(see page 862)
- Reconfiguration(see page 863)



Post Session Custom Commands in IGEL OS

In the following article, you will learn how you can configure post-session custom commands in IGEL OS. For a specific session type, you can define an action that is performed when the last session of this type is ended. The defined post-session command can also be used for multiple session types.

For an example of using post-session commands, see Shutdown/Suspend Devices Automatically at the End of a Session.

Menu path: **System > Firmware Customization > Custom Commands > Post Session**

Session type

Session type for which the action is performed.

Possible values:

- **No post-session command***
- **Citrix**
- **Citrix via Browser**

i Post-session commands for **Citrix via Browser** are currently supported for Firefox browser only.

- **RDP (with login dialog)**
- **RDP**
- **VMware Horizon**
- **Browser**
- **NoMachine NX**
- **Parallels Client**
- **PowerTerm terminal emulation**
- **ThinLinc**
- **X session**
- **IBM iAccess**
- **Media player**
- **VNC viewer**
- **AVD**

► If a post-session command has to be applied to multiple sessions, specify the main session in the above **Session type** field and use + to add additional sessions.



At first, specify session here

Session type: Citrix

Additional sessions: RDP, VMware Horizon

Post-session command: Reboot (with dialog timeout)

Add

Session type: AVD

Ok Cancel

Post-session command

Action that is carried out after the end of the session(s) selected above.

Possible options:

- **Logoff***: The user is automatically logged off; a login method must be defined for this purpose. Further information can be found under [IGEL Smartcard](#)(see page 804), [Active Directory / Kerberos](#)(see page 807) and [Smartcard](#)(see page 817).

i The “Logoff” option cannot be used if the Appliance Mode is in use. Further information can be found under [Appliance Mode](#)(see page 213).
- **Shutdown/suspend (system default action)**: The device will be shut down or placed in a standby mode depending on the setting under **System > Power Options > Shutdown > Default action** selection. A dialog allowing the user to cancel the procedure will be shown in the process. Further information can be found under [Shutdown](#)(see page 846).
- **Shutdown/suspend (system default action without dialog)**: The device will be shut down or placed in a standby mode depending on the setting under **System > Power Options > Shutdown > Default action** selection. The user cannot cancel the procedure.
- **Reboot (with dialog timeout)**: The device will reboot. A dialog allowing the user to cancel the procedure will be shown in the process.
- **Reboot (without dialog)**: The device will reboot. The user cannot cancel the procedure.
- **Enter custom command here**: Command to be executed.

*IGEL OS system default



Base

Menu path: **Setup > System > Firmware Customization > Custom Commands > Base**

The commands defined here are executed on a one-off basis during the boot procedure. You can define commands for the execution times described below:

- **Initialization**

- Not all drivers loaded, not all devices available
- Network scripts not launched, network not available
- Partitions available except *firefox profile, scim data, ncp data, custom partition*

- **Before session configuration**

- Not all drivers loaded, not all devices available
- Network scripts launched, network not available
- Partitions available except *firefox profile, scim data, ncp data, custom partition*
- Sessions not configured

- **After session configuration**

- All drivers loaded, all devices available
- Network available
- Partitions available except *custom partition*
- System daemons not launched (CUPS, ThinPrint etc.)
- Sessions configured
- UMS settings retrieved but not yet effective

- **Final initialization command**

- All partitions available
- All system daemons launched
- UMS settings effective



Network

Menu path: **Setup > System > Firmware Customization > Custom Commands > Network**

You can define commands for the execution times described below:

Network initialization

- The commands defined here are executed at the beginning of the network configuration.

The commands in the below fields are executed each time the relevant network interface starts. The `INTERFACE` environment variable contains the name of the network interface started.

After network DNS

- Runs after each change in the IP address or host name
- IP address / name server settings used (e.g. via DHCP)

Before network services

- IP address / name server settings used
- VPN connected (if VPN autostart was enabled in the setup)
- No network / host routing settings used

Final network command

- Network / host routing settings used
- NFS and SMB drives available
- System time synchronized with time server
- UMS settings retrieved but not effective yet



Desktop

Menu path: **Setup > System > Firmware Customization > Custom Commands > Desktop**

The commands defined here are executed when the X server is launched. You can define commands for the execution times described below:

- **Desktop initialization**

- Runs once during the boot procedure
- Desktop environment configured but not launched
- User not logged on (Kerberos, smartcard etc.)

- **Before desktop start**

- Runs once during the boot procedure
- Desktop environment launched
- Message service launched
- Session D-Bus launched
- User not logged on (Kerberos, smartcard etc.)

- **Final desktop command**

- Runs after each user logon and desktop restart
- User logged on (Kerberos, smartcard etc.)
- User desktop launched



Reconfiguration

Menu path: **Setup > System > Firmware Customization > Custom Commands > Reconfiguration**

The commands defined here are executed after settings relating to the local setup or the UMS have been changed. You can define commands for the execution time described below.

- **After reconfiguration:** Runs after an effective change in the endpoint device settings (local setup, UMS)



Corporate Design

Menu path: **Setup > System > Firmware Customization > Corporate Design**

In this area, settings allowing you to adapt the user interface to your company layout are grouped together.

You can place your own logo in the following places:

- [Custom Bootsplash](#)(see page 865)
- [Background \(1st Monitor\)](#)(see page 867)
- [Company Logos](#)(see page 870)

See also the how-to [Customizing IGEL OS Desktop](#).



Custom Bootsplash

Menu path: **Setup > System > Firmware Configuration > Corporate Design > Custom Bootsplash**

With a bootsplash, you can show your company logo or a specific image during the booting procedure. The bootsplash will be shown instead of the console messages.

Please note: You need to provide an image file for your custom bootsplash on a download server.

- i** The file types JPG, JPEG, BMP, PNG, SVG, GIF, and TIFF can be used for a bootsplash. A total storage area of 25 MB is available for all user-specific images. The image is 800 x 600 pixels in size (aspect ratio remains unchanged). It can be positioned vertically and horizontally.

Custom Bootsplash

Enable custom bootsplash

- You can make the following settings in order to configure a custom bootsplash.
 No custom bootsplash is configured. (Default)

Custom Bootsplash - Server Location

Use firmware update server location

- The server configuration will be carried over from the [firmware update](#)(see page 826).
 You can carry out a custom configuration below. (Default)

Protocol: Access method for the image

Possible options:

- HTTP: Download from a web server
- HTTPS: Download from a TLS/SSL-secured web server
- FTP: Download from an FTP server
- Secure FTP: Download via SSH-secured FTP
- FTPS: Download from a TLS/SSL-secured FTP server
- FILE: The image file lies in the file system of the device, possibly as a shared NFS or Windows update. You can choose the location simply by selecting a file below.

Server name: Name or IP address of the server

Port: Port of the server on which the service is provided (Default: 21)

Server path: Path to the directory with the image file on the server

User name: User name on the server

Password: Password for the user account on the server

Custom Bootsplash - Settings

Custom bootsplash file: File name of the custom image

As regards positioning, the following applies: 0 = left-justified, 50 = centered, 100 = right-justified



Custom bootsplash style:

- Original
- Stretched
- Scaled
- Zoomed

Background color: Use the color picker to choose.

Horizontal position of the bootsplash image (Default: 50)

Vertical position of the bootsplash image (Default: 50)

Size of progress indicator (Default 72)

Horizontal position of the progress indicator (Default: 90)

Vertical position of the progress indicator (Default: 90)

Bootsplash update: The user-specific bootsplash will be downloaded from the given server.

- (i)** If you change the image file or even just one of the settings for an existing bootsplash, be sure to click on **Bootsplash update** in order to regenerate the system files used and then on **Apply** or **OK**.



Background (1st Monitor)

Menu path: **Setup > System > Firmware Customization > Corporate Design > Background (1st Monitor)**

Decorate the desktop background with predefined IGEL backgrounds, a fill color or a color gradient or define a custom background image. You can set up a separate background image for each monitor that is connected to the thin client.

Prerequisite: You have provided a custom background image on a server; see [Background Image Server](#)(see page 869).

- ⓘ The file types BMP, JPG, GIF, TIF, PNG and SVG are supported for a background image. A total storage area of 25 MB is available for firmware customization images.

- ⓘ From IGEL Linux Version 10.03.500 both background images and background image server can be defined user-customized via Shared Workplace. Please note the following for this:
- All user-customized background images will be saved on the thin client and therefore require a part of the available 25 MB storage space. Ensure that this storage limit is not exceeded. (When the storage limit is reached, all images except the one currently used will be deleted; with a new logon via Shared Workplace, the previously deleted images will be downloaded again until the storage limit is reached.)
You will find further information on Shared Workplace and background images here:
 - IGEL Linux user manual: [Shared Workplace](#)(see page 810)
 - IGEL UMS user manual: Shared Workplace
 - How-To: Creating your own Wallpaper in the How-To Customizing the IGEL Linux Desktop

- **Wallpaper:** Select one of the predefined background images from the following list:
 - neutral
 - disabled
 - black (4x3)
 - [blue \(4x3\)](#)
 - gray (4x3)
 - orange (4x3)
 - green
 - black (16x9)
 - blue (16x9)
 - gray (16x9)
 - orange (16x9)
- **Wallpaper Style:** If you have set a custom background image, you can display it in a number of ways.
Possible options:
 - Automatic
 - Centered
 - Tiled



- Spread
 - Scaled
 - Zoomed
- **Color Style:** If you have chosen two different colors as the desktop background color, you can define color gradients here. Possible values:
Possible options:
 - Solid color
 - Horizontal gradient
 - Vertical gradient
 - **Desktop Color:** Click on **Choose color** to specify a custom background color for your desktop if you have not chosen a background image.
 - **2nd Desktop Color:** Click on **Choose color** to specify a second background color for your desktop.
 - **Custom wallpaper download**
 You can set up a custom background image.
 No custom background image will be used. (Default)
 - **Custom Wallpaper file:** Name of the background image file

i If you would like to use a custom background image, you need to specify the download server under **System > Firmware Customization > Corporate Design > Background (1st Monitor) > Custom Wallpaper Server**(see page 869). If you have already defined a server for the system update files, you can use the same server settings for downloading the background image.



Background Image Server

Menu path: **Setup > System > Firmware Customization > Corporate Design > Background (1st Monitor) > Custom Wallpaper Server**

Custom Wallpaper - Server Configuration

- **Use firmware update server location**

The server configuration will be carried over from the [firmware update](#)(see page 826).

You can carry out a custom configuration below. (default)

- **Protocol:** Select the method for accessing the image.

- HTTP: Download from a web server.
- HTTPS: Download from a TLS/SSL-secured web server.
- FTP: Download from an FTP server.
- Secure FTP: Download via SSH-secured FTP.
- FTPS: Download from a TLS/SSL-secured FTP server.
- FILE: The image lies in the thin client file system, possibly as a shared NFS or Windows file.
You can choose the location simply by selecting a file below.

- **Server name:** Name or IP address of the server.

- **Port:** Port of the server on which the service is provided.

- **Server path:** The path to the directory with the image file on the server

- **User name:** User name on the server

- **Password:** Password for the user account on the server

- **Wallpaper update:** The user-specific background image will be downloaded from the given server.



Company Logos

Menu path: **Setup > System > Firmware Customization > Corporate Design > Company Logos**

You can show your company logo in the screensaver and in the start menu.

Screensaver

- **Enable image display**

The image defined below will be shown as the screensaver. (default)

- **File for screen saver logo:** Complete path for an image file or a directory that contains a number of image files.

i If you enter a folder instead of a single image file as the source, all images in the folder will be displayed as a slide show. The **image display time** for the images can be configured. If you do not specify a file of your own, the *IGEL* logo will be used.

- **One image per monitor**

The image will be shown on each individual monitor rather than one image across all monitors. (default)

- **Image duration:** Time in seconds until the image changes (default: 10)

- **Image display mode**

- Small-sized hopping: small image that jumps across the screen
- Medium-sized hopping: larger image that jumps across the screen
- Full screen center cut out: Image is displayed across whole screen, edges can be cut off.
- Full screen letterbox: Complete image is shown. A black edge may be visible depending on the format.

Start menu

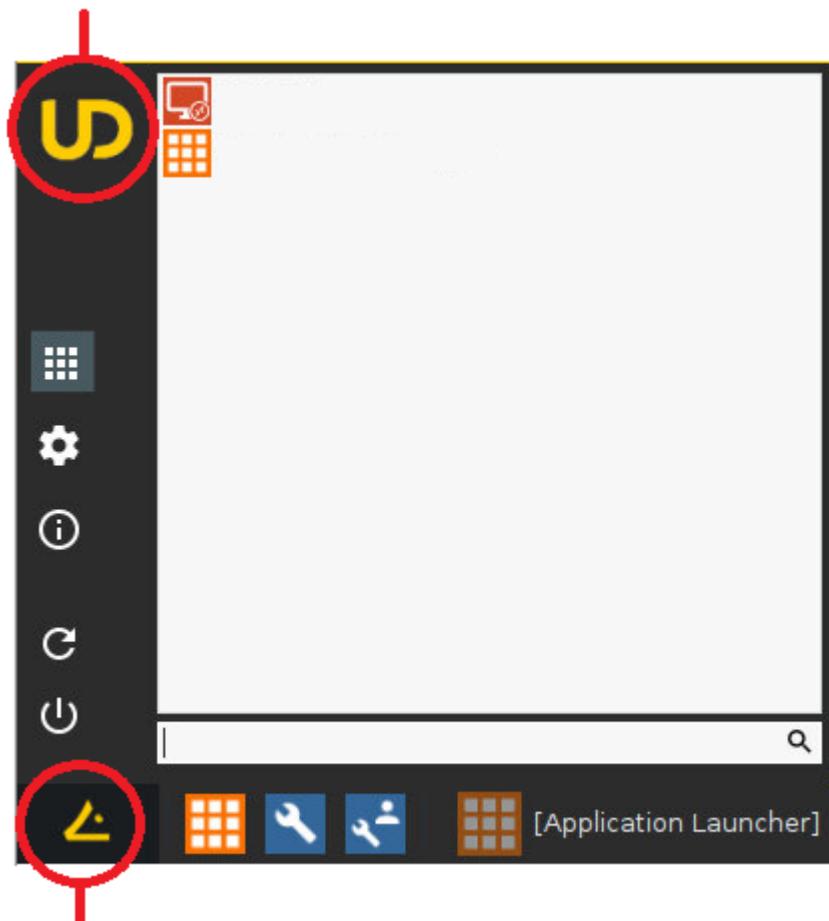
- **Start button icon:** File name with full path to select your logo as the icon for the start menu in the taskbar. Size: 32x32 pixels

- **Company logo in start menu:** File name with full path to show your company logo in the start menu window. Size: 64x64 pixels

i In order to see the company logo in the start menu window, you must set the start menu type to **Advanced**. To do this, click on **User Interface > Desktop > Start Menu**.



Logo in Start Menü



Start Button Icon



Environment Variables

Menu path: **System > Firmware Customization > Environment Variables**

Environment variables allow you to use dynamic parameter values for a number of session types, e.g. so as not to have to enter ICA or RDP servers for every session.

Predefined variables can also be allocated and distributed via the IGEL UMS. Additionally, defined variables can only be used locally on the thin client and may be overwritten by a UMS configuration.

Enable variable substitution in session: (default: disabled)

The use of variables in sessions such as ICA and RDP is enabled. If specific parameters contain a \$, shell substitution will be carried out.

The use of variables in sessions is not enabled. (default)

The environment variables are available in the setup under [Custom Commands](#)(see page 857).

In addition, the following session parameters can be updated through variables:

- Legacy ICA sessions: Citrix Server or published application
- Legacy ICA sessions: User
- RDP session: Server
- RDP session: User

-
- [Predefined](#)(see page 873)
 - [Additional](#)(see page 874)



Predefined

Menu path: **System > Firmware Customization > Environment Variables > Predefined**

- **Variable name:** Name for the variable
- **Value:** Value for the variable

To use environment variables in sessions, proceed as follows:

1. Enable environment variables under **System > Firmware Customization > Environment Variables > Enable variable substitution in session.**
2. Define the variable name and content, e.g.
 - **Variable name:** SERVERNAME
 - **Value:** testServer
3. Enter the variable name in the parameter field of the session with the \$ symbol before it. Example: \$SERVERNAME

i In the case of RDP and ICA sessions, the value is entered in the session file after saving. With XenApp, the setting is not implemented until a session starts and is running.



Additional

Menu path: **System > Firmware Customization > Environment Variables > Additional**

You can define other variables in addition to the 10 predefined ones.

- **Variable name:** Name for the variable
- **Value:** Value for the variable



Features

Menu path: **System > Firmware Customization > Features**

Using this list of available services, you can quickly enable or disable firmware components such as Media Player, Extra Font Services, etc. By deactivating e.g. unused features, you can save storage space.

If a service was disabled, the associated session type will no longer be available when the system is restarted. Existing sessions will no longer be shown but will not be deleted either.

For further information, see Disabling IGEL OS Features to Reduce Firmware Size.

- ⚠** A disabled session type will not be updated during a firmware update. Therefore, you should disable unused services in order to speed up update processes.

ⓘ Features with Limited Support

A number of products feature functions with “limited support”. These functions are offered ‘as is’ without any warranty. Any support for these functions is provided on a non-binding, “best effort” basis.



Registry

Menu path: **System > Registry**

In the registry, you can change virtually any firmware parameter. You will find information on the individual items in the tooltips.

- ⚠ Changes to the registry should only be made by experienced administrators. Incorrect parameter settings can easily destroy the configuration and cause the system to crash. In cases like these, the only way to restore the functionality is to reset the device to the factory defaults!

Search parameter....: Search for setup parameters in the registry.

- **Search criterion:** Criterion for searching.
The following can be selected:
 - Parameter name
 - **Parameter name:** Any search term.
 - Logical search restriction:
 - Contains
 - Exact match
 - Use regular expressions
 - **Ignore case**
 - **Find previous:** Go back if there are a number of hits.
 - **Find next:** Go forwards if there are a number of hits.
- Example: If you would like to find the FTP settings for updating the Linux firmware, you can search for the parameter name `ftp`. The parameter found in the registry structure is highlighted. Click on **Find next** until you find your desired parameter:



A screenshot of the IGEL Setup software interface. The title bar reads "IGEL Setup 11.03.100.rc5.01 (Build 6.3.6)". The left sidebar shows a tree view of configuration categories: Sessions, Accessories, User Interface, Network, Devices, Security, System, and Registry. The "Registry" item is selected and highlighted in blue. The main pane displays a hierarchical registry structure under "System": xdmcp_xephir, xdmcp_xserver, zulu_jre_8, sessions, spice, system, acpi_wakeup, actions, bootsplash, cron, customization, custom_bootsplash, color, enabled, file, filename, and ftp. The "ftp" folder is currently selected, indicated by a blue highlight. A search bar at the top right contains the text "system.customization.custom_bootsplash.ftp". A search dialog box is open, showing the search criteria: "Search criterion: Parameter name", "Parameter name: ftp", and "Contains". There are "Find Previous" and "Find Next" buttons, and a checked "Ignore Case" option. At the bottom of the main pane are buttons for "Add Instance", "Delete instance", "Apply", "Ok", and "Cancel".

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.