

IGEL OS(RPI4)

Exported on 03/31/2021



Table of Contents

1	IGEL OS(RPI4) Articles	13
1.1	Devices.....	13
1.1.1	How to Configure USB Access Control	13
	Enable USB Access Control.....	13
	Create a Class Rule.....	13
	Create a Device Rule	14
	Example	14
1.2	Audio.....	15
1.2.1	Configuring Audio on the NComputing RX420(IGEL)	15
	Overview.....	15
	Selecting a USB Headset on the Endpoint.....	15
	How Do My Audio Devices Appear in the Audiomixer?.....	19
1.3	Desktop and Display	20
1.3.1	Showing and Hiding the On-Screen Software Keyboard Automatically.....	20
	Showing Automatically.....	20
	Hiding Automatically	20
1.4	Citrix.....	20
1.4.1	Configuring Citrix Workspace Hub	21
	Overview.....	21
	Environment.....	21
	Instructions	21
1.5	System	23
1.5.1	YouTube Video Not Playing / Issues With Web Content.....	23
	Symptom	23
	Environment.....	23
	Problem	23
	Solution	23
2	IGEL OS(RPI4) Reference Manual	25
2.1	IGEL Workspace Edition.....	25
2.1.1	Supported Formats and Codecs.....	26
2.2	Devices Supported by IGEL OS 11(RPI4)	26
2.2.1	Core Requirements	26



2.2.2	NComputing	27
2.3	Bluetooth Assistant.....	27
2.3.1	Bluetooth Tool:	27
2.3.2	USB Access Control:	27
2.3.3	Bluetooth.....	27
2.4	Setup Assistant.....	28
2.4.1	Overview	28
2.4.2	Buttons	28
2.4.3	Language	28
2.4.4	Keyboard Layout.....	29
2.4.5	Time Zone Continent/Area	29
2.4.6	Time and Date	29
2.4.7	Wireless.....	30
2.4.8	Connectivity	30
2.4.9	Activate Your IGEL OS	30
	Install License via UMS/ICG	30
	Manual License Deployment	31
	Register for Demo License	31
	Troubleshooting: Proxy Configuration	31
2.4.10	ICG Agent Setup	32
2.4.11	Finish	32
2.5	The IGEL OS Desktop	32
2.5.1	Application Launcher.....	35
2.5.2	Sessions	37
2.5.3	System	37
2.5.4	License.....	38
2.5.5	About Window	38
2.5.6	Restart and Shutdown	39
2.6	Setup.....	39
2.6.1	Starting the Setup	39
2.6.2	End the Setup	40
2.6.3	Quick Setup	40
2.6.4	Setup Search	41
2.7	Sessions	41
2.7.1	Copy Session	41



2.7.2	Global Session Options.....	42
2.7.3	Citrix.....	42
	Citrix Client Selection.....	42
	Citrix Global.....	43
	Citrix StoreFront.....	55
	Citrix Self-Service.....	64
	Citrix Workspace Hub.....	68
2.7.4	SSH Session.....	71
	Starting Methods for Session.....	71
	Command.....	73
	Options.....	74
	Desktop Integration.....	74
2.7.5	Chromium Browser Global.....	76
	General.....	77
	Content.....	78
	Proxy.....	78
	Privacy.....	79
	Security.....	81
	Encryption.....	81
	Menus & Toolbars.....	81
	Window.....	82
	Custom Setup.....	82
	Smartcard Middleware.....	83
2.7.6	Chromium Sessions.....	84
	Starting Methods for Session.....	84
	Settings.....	86
	Desktop Integration.....	86
2.8	Accessories.....	88
2.8.1	ICA Connection Center.....	89
	Starting Methods for Session.....	89
	Using ICA Connection Center.....	91
2.8.2	Terminals.....	92
	Starting Methods for Session.....	92
	Using Local Terminal.....	94
2.8.3	Change Smartcard Password.....	94



Starting Methods for Session	95
Using Change Smartcard Password Function	96
2.8.4 Change Password.....	96
Starting Methods for Session	97
Using Change Password Function.....	98
2.8.5 Setup.....	98
Starting Methods for Session	99
Setup User Permissions	100
Setup Administrator Permissions	101
Options	102
2.8.6 Quick Settings	102
Starting Methods for Session	102
Setup User Permissions.....	104
2.8.7 Display Switch	104
Starting Methods for Session	104
Options	106
Minimal Dialog.....	108
Advanced Dialog	109
Using Display Switch.....	110
2.8.8 Application Launcher.....	112
Starting Methods for Session	112
Application Launcher Configuration.....	114
2.8.9 Sound Preferences.....	115
Starting Methods for Session	115
Options	117
Using Audio Settings Function	119
2.8.10 UMS Registration.....	119
Starting Methods for Session	119
Using UMS Registration Function.....	121
2.8.11 Task Manager	121
Starting Methods for Session	122
Using Task Manager	124
2.8.12 Screenshot Tool	127
Starting Methods for Session	128
Special Hotkeys.....	129
Using Screenshot Tool.....	130



2.8.13 On-Screen Keyboard	130
Starting Methods for Session	131
Appearance	132
2.8.14 Monitor Calibration	133
Starting Methods for Session	133
2.8.15 Commands	135
2.8.16 Bluetooth Tool	137
Starting Methods for Session	137
Using Bluetooth Tool	139
2.8.17 System Information	142
Starting Methods for Session	142
Using System Information Function	144
2.8.18 Disk Utility	145
Starting Methods for Session	146
Using Disk Utility	148
2.8.19 Disk Removal	148
Starting Methods for Session	148
2.8.20 Mobile Device Access	150
Starting Methods for Session	150
2.8.21 Firmware Update	152
Starting Methods for Session	153
Using Firmware Update Function	155
2.8.22 Smartcard Personalization	155
Starting Methods for Session	155
Using Smartcard Personalization Function	157
2.8.23 Webcam Information	158
Starting Methods for Session	158
Using Webcam Information	160
2.8.24 ICG Agent Setup	160
Starting Methods for Session	161
Using ICG Agent Setup	162
2.8.25 Licensing	163
2.9 User Interface	165
2.9.1 Display	166
Screen Configuration	166



Advanced	167
Power Options.....	167
Access Control	168
Gamma Correction.....	169
Options	169
2.9.2 Desktop.....	170
Desktop fonts	170
Background	171
Taskbar	173
Taskbar Background.....	174
Taskbar Items.....	175
Pager.....	176
Start Menu	176
2.9.3 Language	177
2.9.4 Screenlock / Screensaver	177
Starting Methods for Session	177
Options	179
Taskbar	180
Screensaver	181
2.9.5 Input	182
Keyboard	183
Additional Keyboard Layouts	184
Mouse.....	184
2.9.6 Hotkeys.....	185
Commands	185
2.9.7 Font Services	188
XC Font Service.....	188
NFS Font Service	188
2.10 Network	189
2.10.1 LAN Interfaces	189
Individual Interface.....	190
Wireless.....	193
2.10.2 Mobile Broadband.....	198
2.10.3 DHCP Client	200
Standard Options.....	200



Custom Options	200
2.10.4 VPN.....	201
OpenVPN	201
2.10.5 SCEP Client (NDES)	208
Certificate	209
Certification Authority	210
SCEP	210
2.10.6 Routing	211
Routing [1-5].....	211
2.10.7 Hosts	211
Add.....	211
2.10.8 Network Drives.....	212
NFS.....	212
Windows Drive.....	213
2.10.9 Proxy	214
2.11 Devices.....	215
2.11.1 Printer	215
CUPS	215
LPD.....	221
TCP/IP	221
2.11.2 Storage Devices.....	224
Storage Hotplug.....	224
Options	226
2.11.3 Bluetooth.....	227
2.11.4 USB Access Control	227
Class Rules.....	228
Device Rules	228
2.12 Security.....	229
2.12.1 Password	229
Administrator	230
Setup Administrator	230
Setup User	230
User	231
User account for remote access	231
2.12.2 Logon	231



IGEL Smartcard	232
Taskbar	232
Active Directory/Kerberos	234
Shared Workplace	236
2.12.3 Active Directory/Kerberos	238
Domain 1 ... Domain 4	238
Domain Realm Mapping	239
2.12.4 Smartcard	239
Services	239
Middleware	241
2.13 System	241
2.13.1 Time and Date	241
2.13.2 Update	242
Firmware Update	242
Buddy Update	243
2.13.3 Remote Management	244
Options	245
2.13.4 Remote Access	246
SSH Access	246
Shadow	247
Secure Terminal	248
2.13.5 Power Options	249
System	249
Battery	250
Display	251
Shutdown	251
2.13.6 Firmware Customization	252
Custom Partition	252
Custom Application	255
Custom Commands	259
Corporate Design	262
Environment Variables	267
Features	269
2.13.7 Registry	269
3 IGEL OS(RPI4) Release Notes	271



3.1	Notes for Release 11.01.110.....	271
3.1.1	Supported Devices 11.01.110	271
3.1.2	Component Versions 11.01.110.....	271
	Clients	271
	Smartcard.....	271
	System Components.....	272
	Features with Limited IGEL Support	272
	Services.....	273
3.1.3	Known Issues 11.01.110	273
3.1.4	New Features 11.01.110	274
3.1.5	Resolved Issues 11.01.110	277



- [IGEL OS\(RPI4\) Articles](#)(see page 13)
- [IGEL OS\(RPI4\) Reference Manual](#)(see page 25)
- [IGEL OS\(RPI4\) Release Notes](#)(see page 271)



1 IGEL OS(RPI4) Articles

- [Devices](#)(see page 13)
- [Audio](#)(see page 15)
- [Desktop and Display](#)(see page 20)
- [Citrix](#)(see page 20)
- [System](#)(see page 23)

1.1 Devices

- [How to Configure USB Access Control](#)(see page 13)

1.1.1 How to Configure USB Access Control

You can allow and prohibit the use of USB devices on your device. Specific rules for individual devices or device classes are possible.

Enable USB Access Control


1. Open the Setup and go to **Devices > USB Access Control**.
2. Enable the option **Enable**.
3. Select the **Default Rule**. The default rule specifies whether the use of USB devices is generally allowed or prohibited.

 **Tip**

It is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

4. Create one or more rules for classes of devices or individual devices.

Create a Class Rule

1. To create a new rule, click  in the **Class Rules** area.
2. Choose a **rule**. The rule specifies whether use of the device class defined here is allowed or prohibited.
3. Under **Class ID**, select the class of device for which the rule should apply. Examples: **Audio**, **Printer**, **Mass Storage**.
4. Under **Name**, give a name for the rule.
5. Click **OK**.
6. Save the changes.
The rule is active.



Create a Device Rule

i When a rule is defined, at least one of the properties **Vendor ID** or **Product ID** or **UUID** must be given.

1. To create a new rule, click **+** in the **Device Rules** area.
2. Choose a **rule**. The rule specifies whether use of the device defined here is allowed or prohibited.
3. Give the **Vendor ID** of the device as a hexadecimal value.
4. Give the **Product ID** of the device as a hexadecimal value.
+
5. Give the **Device UUID** (Universal Unique Identifier) of the device.
6. Specify **Permissions** for the device.
Possible values:
 - Global setting: The default setting for hotplug storage devices is used; see **Default permission** parameter under **Devices > Storage Devices > Storage Hotplug**.
 - Read only
 - Read/Write
7. Under **Name**, give a name for the rule.
8. Click **OK**.
9. Save the changes.
The rule is active.

Example

- The set rule prohibits the use of USB devices on the device.
- A class rule allows the use of all entry devices (HID = Human Interface Devices).
- A device rule allows the use of the USB storage device with the UUID 67FC-FDC6.
- The use of all other USB devices, for example, storage devices or printers, is prohibited.

Enable

Default rule Deny

Default permission Read/Write

Class Rules		
Rule	Class ID	Name
Allow	HID (Human Interface Device)	Allow HID

Device Rules					
Rule	Vendor ID	Product ID	Device uuid	Permission	Name
Allow			67FC-FDC6	Read/Write	Storage Device



1.2 Audio

- [Configuring Audio on the NComputing RX420\(IGEL\)\(see page 15\)](#)

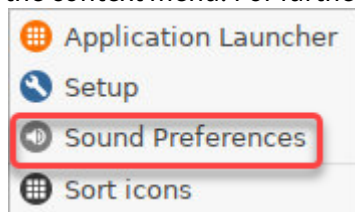
1.2.1 Configuring Audio on the NComputing RX420(IGEL)

Overview

The NComputing RX420(IGEL) supports digital audio via USB and HDMI and analog audio via a 3.5mm jack. The user can select a device using the audiomixer.

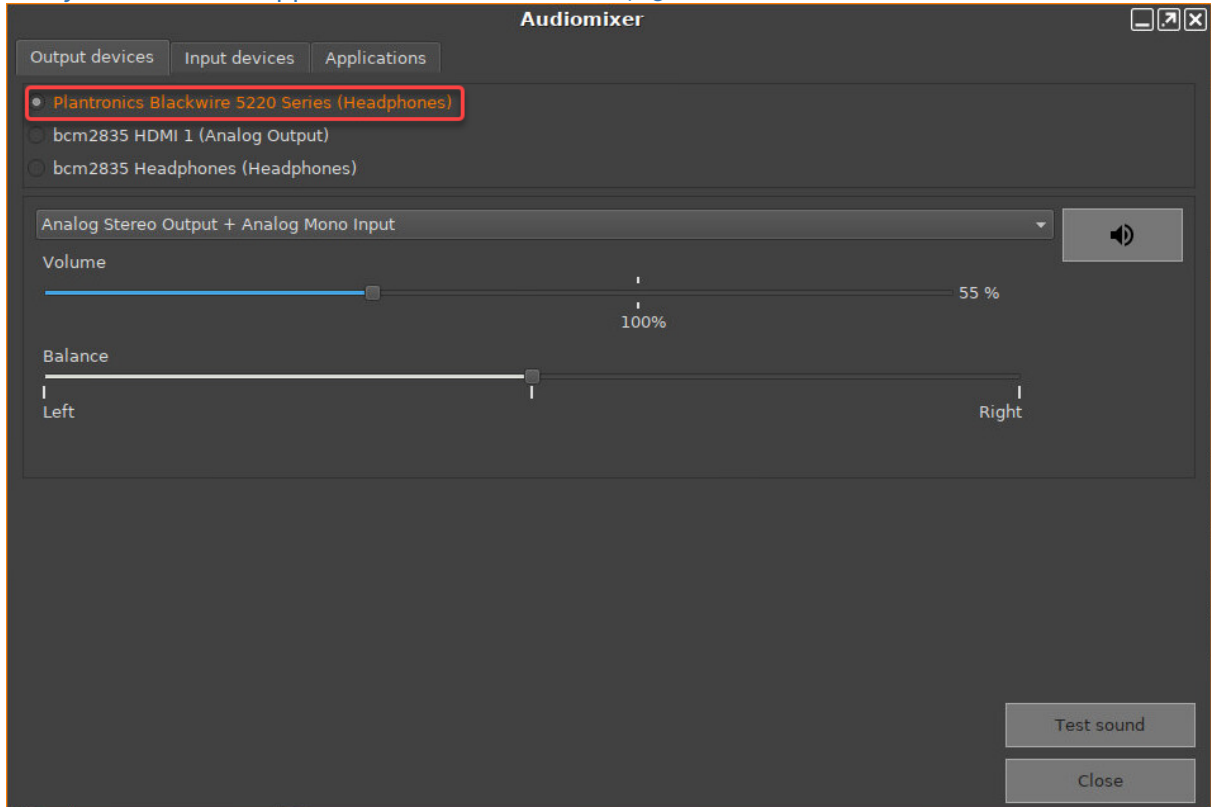
Selecting a USB Headset on the Endpoint

1. Open the audiomixer, e.g. by right-clicking on the desktop and selecting **Sound Preferences** from the context menu. For further starting methods, see [Sound Preferences\(see page 115\)](#).



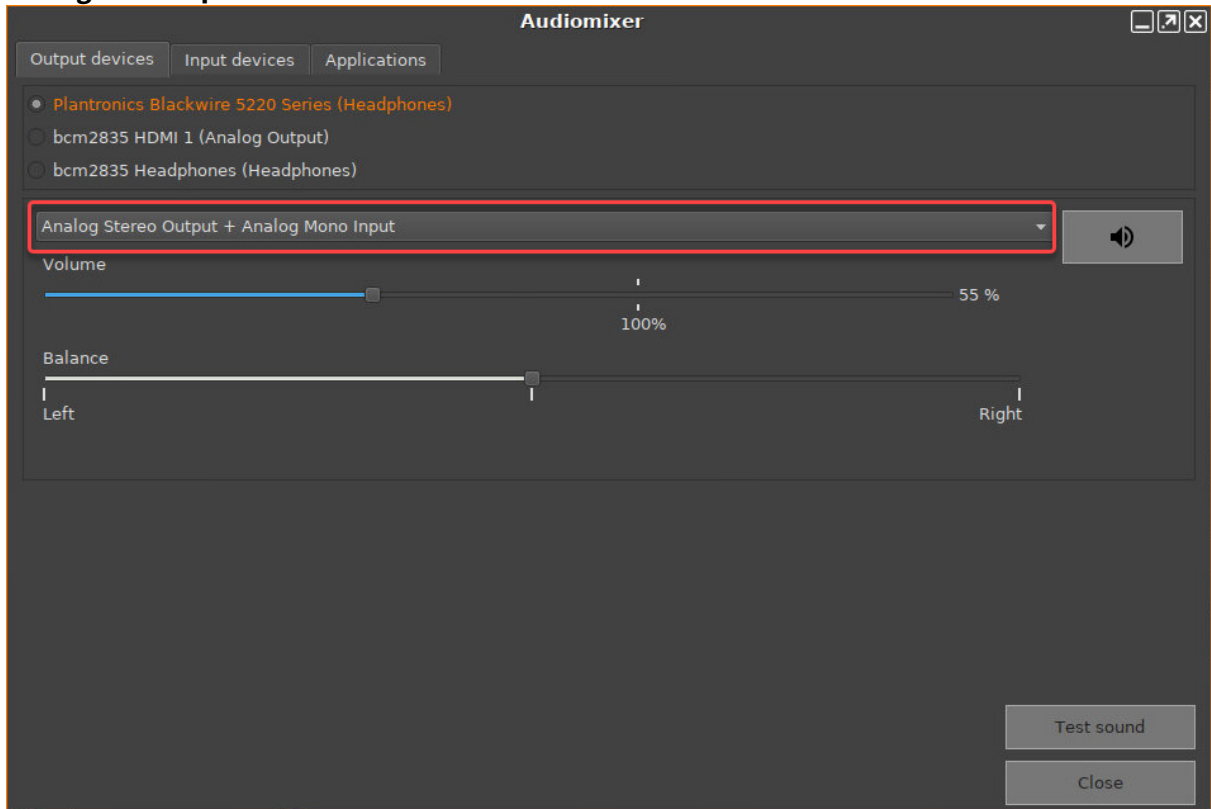


2. In the **Audiomixer** dialog, select the desired device. If in doubt about the device naming, see [How Do My Audio Devices Appear in the Audiomixer?](#)(see page 19).



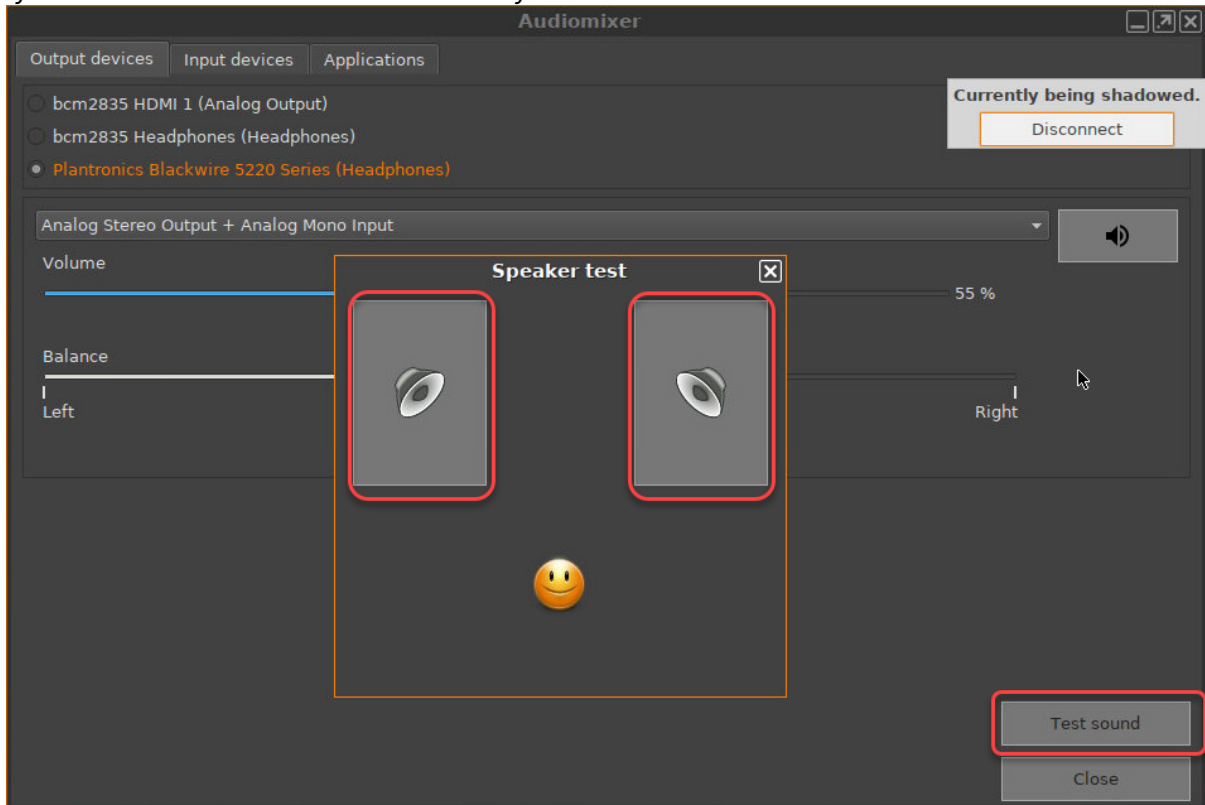


3. Check if the appropriate profile is selected. For a headset, this should be **Analog Stereo Output + Analog Mono Input**.





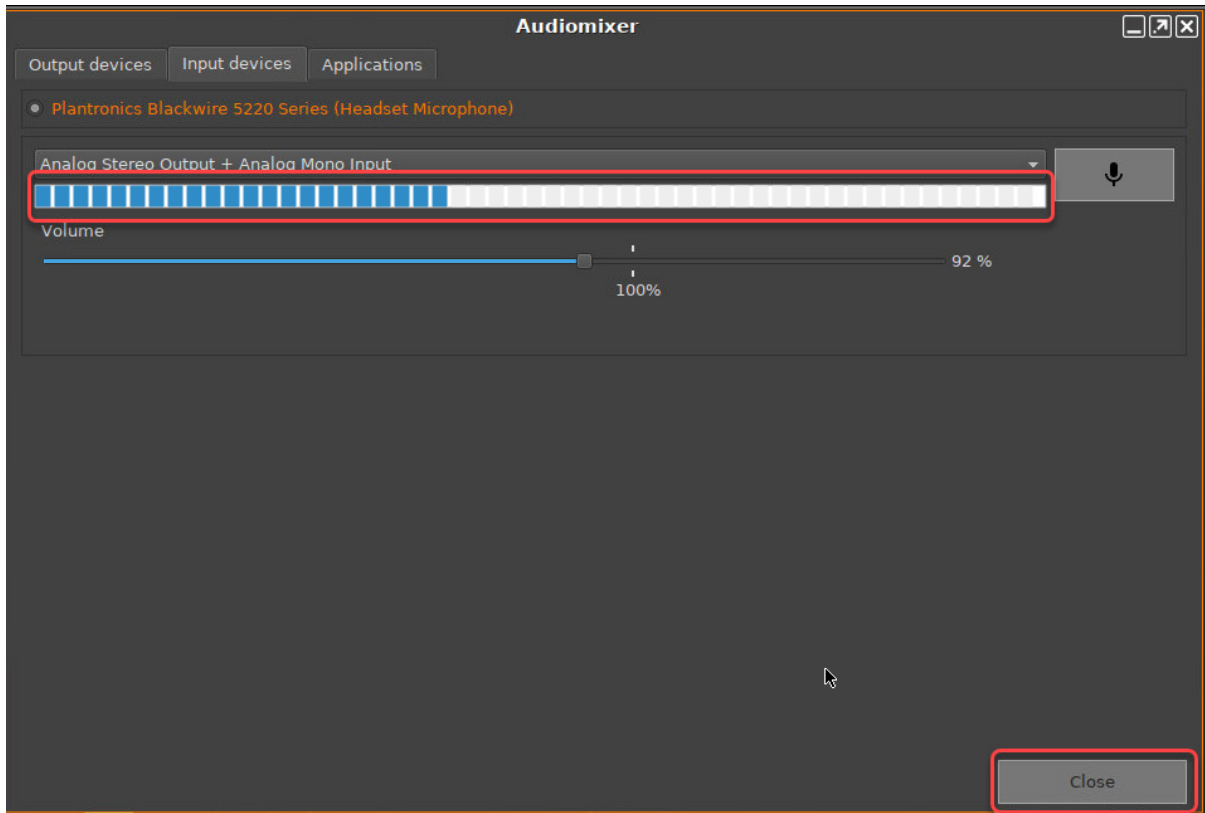
4. To make sure that the audio output is working, click **Test sound** and then click the speaker symbols. You should hear a test sound on your headset.



5. To make sure that the audio input is working, click the **Input devices** tab and speak into your headset's microphone. If the VU meter is reacting, the sound input is working correctly, and you



can click **Close**.



How Do My Audio Devices Appear in the Audiomixer?

Output Devices

Name in Audiomixer	Physical Audio Output
[Device name] (Headphones) Example: Plantronics Blackwire 5220 Series (Headphones)	USB
bcm2835 HDMI 1 (Analog Output)	HDMI
bcm2835 Headphones	3.5mm audio jack



Input Devices

Name in Audiomixer	Physical Audio Input
<p>[Device name] (Headset Microphone)</p> <p>Example: Plantronics Blackwire 5220 Series (Headset Microphone)</p>	<p>USB</p>

1.3 Desktop and Display

- [Showing and Hiding the On-Screen Software Keyboard Automatically](#)(see page 20)

1.3.1 Showing and Hiding the On-Screen Software Keyboard Automatically

You can configure the on-screen software keyboard to appear or disappear automatically when an input box is selected or deselected (e. g. Firefox or screenlock).

Showing Automatically

With the following setting, a software keyboard will be shown automatically when an input box is focused.

1. In the Setup, go to **Registry > userinterface > softkeyboard > autoshow** (parameter: `userinterface.softkeyboard.autoshow`).
2. Enable **Automatically show on-screen keyboard when text field is selected**.

Hiding Automatically

With the following setting, the software keyboard will be hidden automatically when an input box is not focused anymore.

1. In the Setup, go to **Registry > userinterface > softkeyboard > autohide** (parameter: `userinterface.softkeyboard.autohide`).
2. Enable **Automatically hide on-screen keyboard when text field is deselected**.

If there are any problems, e. g. the keyboard does not hide automatically, you have to disable **Automatically hide on-screen keyboard when text field is deselected** and make sure that the following Setup parameters have been enabled:

- **Accessories > On-Screen Keyboard > Autostart**
- **Accessories > On-Screen Keyboard > Restart**

1.4 Citrix

- [Configuring Citrix Workspace Hub](#)(see page 21)



1.4.1 Configuring Citrix Workspace Hub

Overview

⚠ Feature in Beta Status (Experimental)
In this version of IGEL OS(RPI4), the integration of Citrix Workspace Hub is in beta status (experimental).

With Citrix Workspace Hub, you can log in to a Citrix session via a mobile device app and then run this session on any endpoint device that provides Citrix Workspace Hub (hot-desking).

Initially, the Citrix Workspace Hub application must be started on the endpoint device. The Citrix Workspace Hub application displays a launcher screen with a QR code that identifies the endpoint device and signals that the endpoint device is available. On the mobile device app, the user authenticates himself for a Citrix session (session roaming) or has a Citrix session that is already running (session casting). To connect with the endpoint device of choice, the user takes a photo of the QR code. When the mobile device app has recognized the QR code, it connects to the relevant endpoint device via Wi-Fi, and the Citrix session is started on the endpoint device (session roaming) or handed over to the endpoint device (session casting).

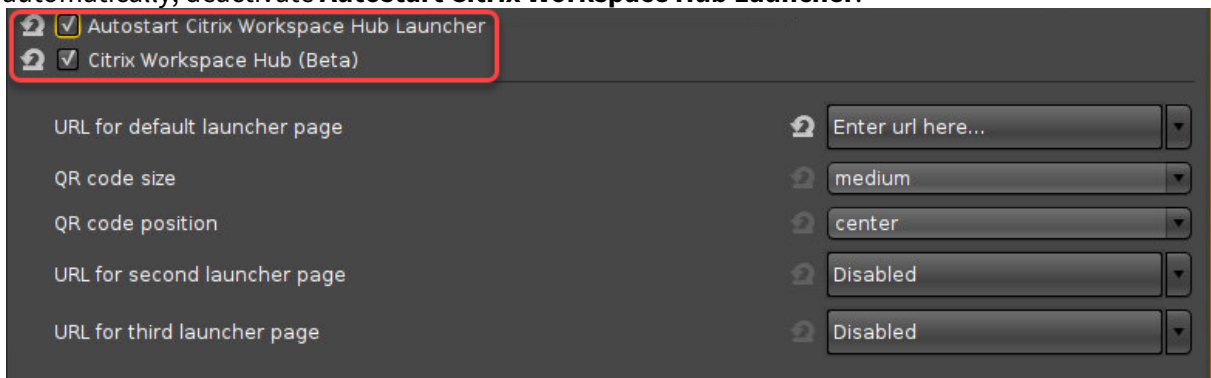
Environment

For a detailed list of prerequisites, see <https://docs.citrix.com/en-us/citrix-ready-workspace-hub/system-requirements.html>

- Endpoint device with IGEL OS(RPI4)
- Mobile device with Citrix Workspace
- Mobile device and endpoint device are on the same Wi-Fi network
- Wi-Fi network is an open IPv4 network (no ports blocked)
- If the launcher page is a page on the Internet, the endpoint device must have Internet access.

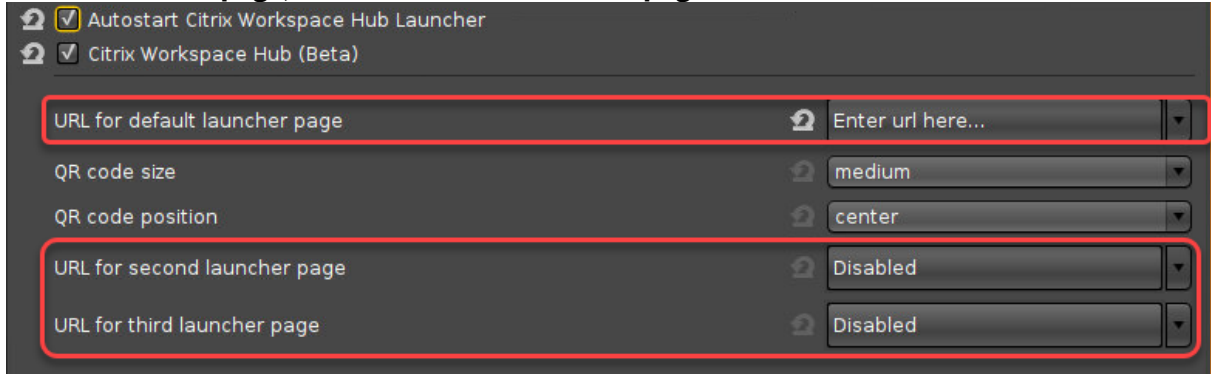
Instructions

1. Open the Setup and go to **Sessions > Citrix > Citrix Workspace Hub > Options**.
2. Activate **Citrix Workspace Hub (Beta)**. If you do not want Citrix Workspace Hub to start automatically, deactivate **Autostart Citrix Workspace Hub Launcher**.

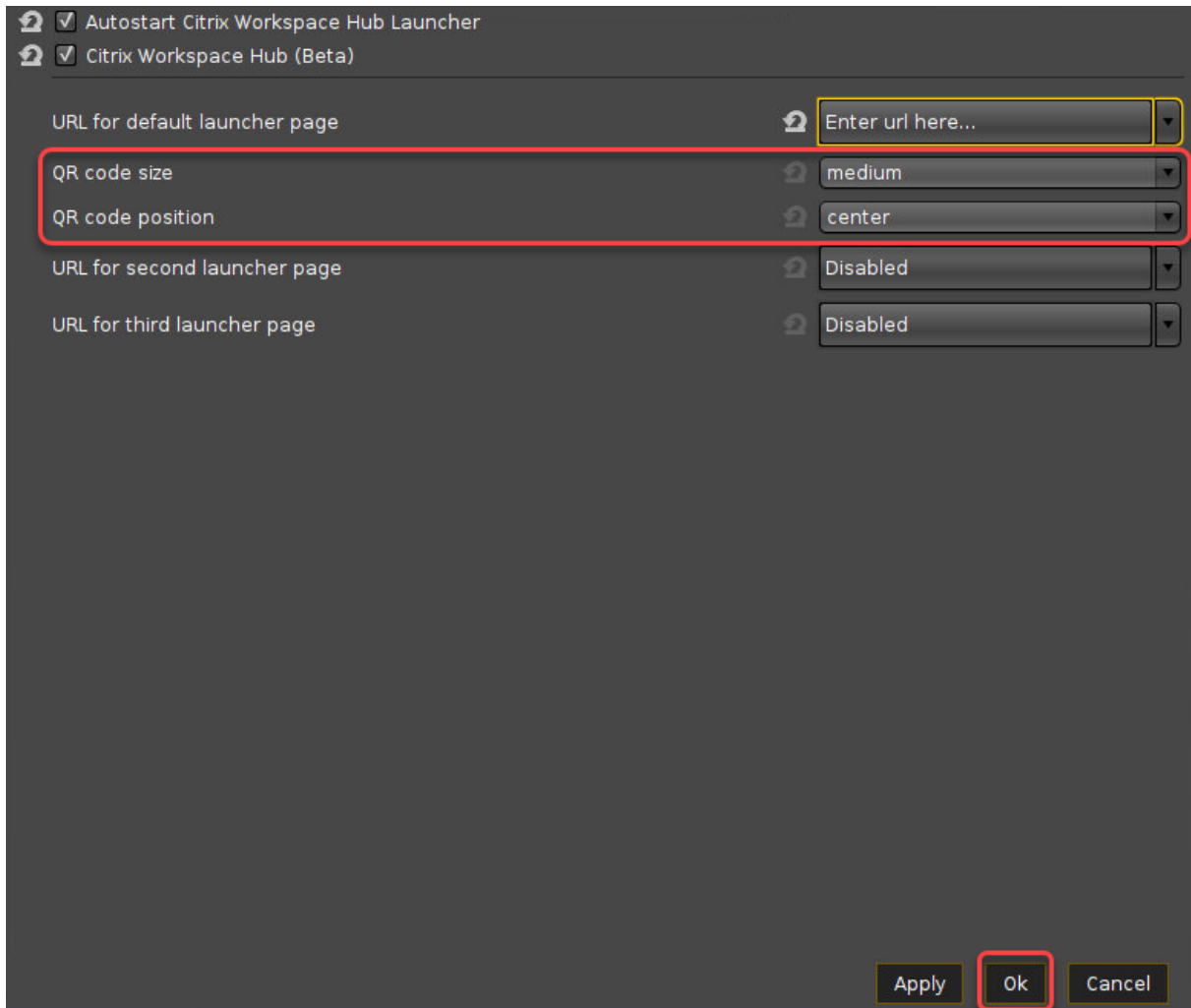




- 3. To configure the background of the launcher screen that contains the QR code, define one or more launcher pages. For details, see [Options](#)(see page 68), **URL for default launcher page**, **URL for second launcher page**, and **URL for third launcher page**.



- 4. To configure the display of the QR code, set **QR code size** and **QR code position** accordingly, and confirm with **Ok**.





1.5 System

- [YouTube Video Not Playing / Issues With Web Content](#)(see page 23)

1.5.1 YouTube Video Not Playing / Issues With Web Content

Symptom

Videos on YouTube won't play, or other web content is not displayed as expected.

Environment

- IGEL OS(RPI4) on devices with no battery-backed real-time clock

Problem

Certificate issues arise because of incorrect time and date settings. Devices without a battery-backed real-time clock lose the current time and date when they are powered off.

Solution

1. In the Setup or UMS configuration dialog, go to **System > Time and Date**.

✔ It is recommended to use a profile. For details, see [Profiles](#)¹.

2. Edit the following settings:
 - **Use NTP time server:** Activate this option.
 - **NTP time server:** Define one or more NTP time servers. To define multiple NTP time servers, separate them by spaces. Example: 0.de.pool.ntp.org 1.de.pool.ntp.org

¹ <https://kb.igel.com/display/endpointmgmt606/Profiles>



3. Confirm the settings with **Ok**.

A screenshot of the IGEL OS time settings dialog box. The dialog has a dark grey background. At the top, there are two dropdown menus: "Timezone continent/area" set to "Europe" and "Location" set to "Berlin". Below these is a checked checkbox labeled "Use NTP Time Server". Underneath the checkbox is a text field for "NTP Time Server" containing the addresses "0.de.pool.ntp.org 1.de.pool.ntp.org". A red rectangular box highlights the "Use NTP Time Server" checkbox and the text field. Below the text field is a button labeled "Set time and date". At the bottom right of the dialog are three buttons: "Apply", "Ok", and "Cancel". The "Ok" button is highlighted with a red rectangular box.



2 IGEL OS(RPI4) Reference Manual

- [IGEL Workspace Edition](#)(see page 25)
- [Devices Supported by IGEL OS 11\(RPI4\)](#)(see page 26)
- [Bluetooth Assistant](#)(see page 27)
- [Setup Assistant](#)(see page 28)
- [The IGEL OS Desktop](#)(see page 32)
- [Setup](#)(see page 39)
- [Sessions](#)(see page 41)
- [Accessories](#)(see page 88)
- [User Interface](#)(see page 165)
- [Network](#)(see page 189)
- [Devices](#)(see page 215)
- [Security](#)(see page 229)
- [System](#)(see page 241)

For supported devices, see [Devices Supported by IGEL OS 11\(RPI4\)](#)².

✔ Getting Started

To get started, see [IGEL OS\(RPI4\) for NComputing RX420\(IGEL\) - STEP-BY-STEP GETTING STARTED GUIDE](#)³

2.1 IGEL Workspace Edition

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](#)⁴.

i 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 26)

² <https://kb.igel.com/display/hardware/Third-Party+Devices+Supported+by+IGEL+OS+11+RPI4>

³ <http://files.igelcommunity.com/igel/igel%20os-rpi4-for-ncomputing-rx420-getting-started-guide.pdf>

⁴ <https://www.igel.com/software-downloads/igel-universal-management-suite/>



2.1.1 Supported Formats and Codecs

As supplied, IGEL OS(RPI4) supports the following multimedia formats and codecs:

- Ogg/Vorbis
- Ogg/Theora
- WAV
- FLAC

The following codecs can be added with the optional [Multimedia Codec Pack](#)⁵:

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.

2.2 Devices Supported by IGEL OS 11(RPI4)

2.2.1 Core Requirements

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

⁵ <https://www.igel.com/multimedia-codec-pack/>



2.2.2 NComputing

Name	Memory (RAM)	Storage	Processor	Supported from IGEL OS(RPI4) Version	Datasheet
RX420 (IGEL)	2 GB	16 GB internal Micro SD card	Broadcom BCM2711	11.01.100	RX420-IGEL.pdf ⁶

2.3 Bluetooth Assistant

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

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

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

2.3.1 Bluetooth Tool:

Path: [Accessories > Bluetooth Tool](#)(see page 137)

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

2.3.2 USB Access Control:

Path: [Devices > USB Access Control](#)(see page 227)

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.

2.3.3 Bluetooth

Path: [Devices > Bluetooth](#)(see page 227)

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.

i 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.

⁶ <https://kb.igel.com/download/attachments/43097666/RX420-IGEL.pdf?api=v2&modificationDate=1614164245869&version=1>



For more information about enabling Bluetooth services, see [Bluetooth](#)(see page 227).

2.4 Setup Assistant

2.4.1 Overview

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

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

2.4.2 Buttons

Next: Go to the next configuration step

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

Back: Go back to the previous step

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

-
- [Language](#)(see page 28)
 - [Keyboard Layout](#)(see page 29)
 - [Time Zone Continent/Area](#)(see page 29)
 - [Time and Date](#)(see page 29)
 - [Wireless](#)(see page 30)
 - [Connectivity](#)(see page 30)
 - [Activate Your IGEL OS](#)(see page 30)
 - [ICG Agent Setup](#)(see page 32)
 - [Finish](#)(see page 32)

2.4.3 Language

Language: Select the language for the user interface.



2.4.4 Keyboard Layout

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

2.4.5 Time Zone Continent/Area

Timezone continent/area: Select the continent/area for your location.

Possible values:

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

Location: Select your location or time zone.

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".

2.4.6 Time and Date

Date: Select the current date.

Time: Set the current local time.

Use NTP Time Server

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

⚠ NTP Server Highly Recommended

Raspberry Pi-based devices like NComputing RX420(IGEL) have no battery-backed real-time clock. After a power outage, the system time will reset to the build time of the IGEL OS firmware. If the time and date are not correct, certificate issues may arise, which causes problems with websites, for instance.

Therefore, it is highly recommended to specify an NTP server. When an NTP server is configured, the system is always provided with the correct time and date.

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](https://kb.igel.com/display/endpointmgmt606/Using+Profiles)⁷.


Next: Sets the system clock according to what is entered above.

⁷ <https://kb.igel.com/display/endpointmgmt606/Using+Profiles>





2.4.7 Wireless

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


 If you carry out the WLAN configuration and exit the Setup Assistant by selecting **Finish**, the connection will be saved and WLAN will be permanently enabled. If you skip this configuration step or cancel the configuration, WLAN will not be permanently enabled.

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

 : Searches again for WLAN access points.

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

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

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

2.4.8 Connectivity

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

Follow the instructions on the screen.

2.4.9 Activate Your IGEL OS

In this step, you select the method for licensing the device.

If the device has no license yet, the following options are available:

- **Install license via UMS/ICG**
- **Manual license deployment**
- **Register for demo license**

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

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

The options are described in detail further below.

Install License via UMS/ICG

The device will request a license from the UMS. If the device is outside the company network, the IGEL Cloud Gateway (ICG) will be used for connecting the device to the UMS. In this case, ICG access must be set up; see [ICG Agent Setup](#)(see page 32).



Manual License Deployment

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

To deploy a license from a URL:

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

To deploy a license via FTP:

1. Click **FTP**.
2. Define the access data for you FTP server:
 - **Host/Port:** URL of the FTP server on which the license file is located
 - **User:** User for accessing the FTP server
 - **Password:** Password associated with the **User**
3. Click **Browse**.
4. In the dialog, go to the license file and select it.
5. Click **Install**.

To deploy a license from a USB memory stick.

1. Click **File**.
2. Connect the USB flash drive that contains the license to the device.
3. Under **Storage Device**, select the USB flash drive that contains the license.
4. Click **Browse**.
5. In the dialog, go to the license file, select it and click **Open**.
6. Click **Install**.

Register for Demo License

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

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

1. Make your choice as required and fill in all fields.
2. Activate the checkbox near **I agree to the terms + conditions and privacy policy**.
3. Click **ACTIVATE YOUR OS 11**.

Your device fetches a demo license from IGEL.

Troubleshooting: Proxy Configuration

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

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



- **Port:** Port of the HTTP proxy
- **SSL Proxy:** Address of the SSL proxy
- **Port:** Port of the SSL Proxy
- **SOCKS Host:** Address of the SOCKS Host
- **Port:** Port of the SOCKS host
- **User name:** User name for authentication
- **Password:** Password for authentication

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

2.4.10 ICG Agent Setup

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

You will find instructions for this under [Using ICG Agent Setup](#)(see page 162).

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

2.4.11 Finish




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

2.5 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

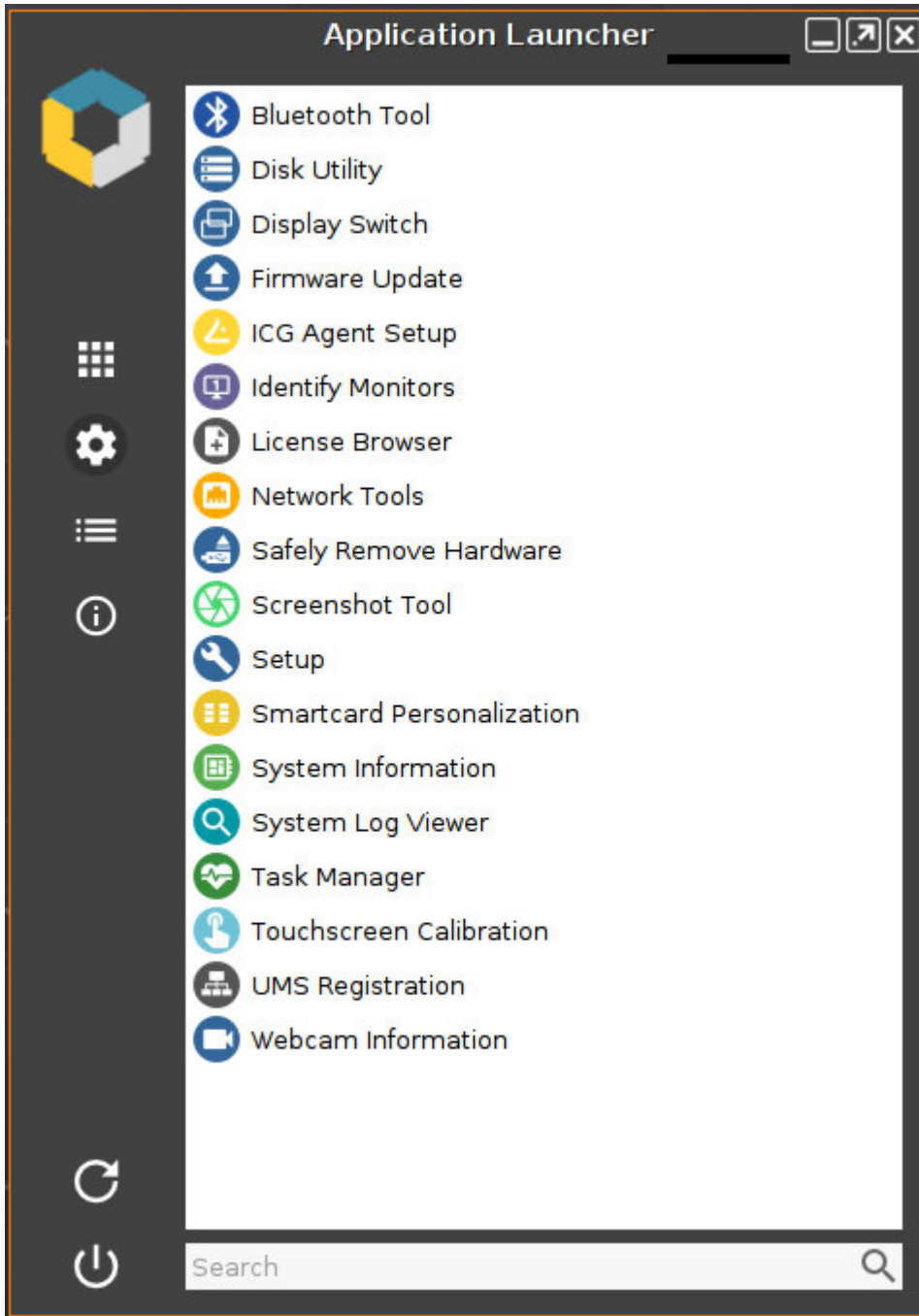


- [Application Launcher](#)(see page 35)
- [Sessions](#)(see page 37)
- [System](#)(see page 37)
- [License](#)(see page 38)
- [About Window](#)(see page 38)
- [Restart and Shutdown](#)(see page 39)

2.5.1 Application Launcher

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







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



The sub-areas of the Launcher provide access to:

	Listing of the sessions (see page 37) that have been set up
--	---




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

You will find information regarding the configuration here [Application Launcher](#)(see [page 35](#)).

2.5.2 Sessions


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

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


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

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

It is also possible, to build a file structure for the sessions in the application launcher. Therefore, 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.

2.5.3 System

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

The following tools are available:

- **Identify Monitors:** Shows the screen's number and manufacturer details.
- **Screenshot Tool:** Takes photos of the screen content.
- **Bluetooth Tool:** Starts the Bluetooth tool.



- **Firmware Update:** Carries out the update with the settings made during the setup.
- **Savely 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.

2.5.4 License



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

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

2.5.5 About Window


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

- **Product:** Information regarding the installed firmware
 - Copyright
 - Firmware Version
 - Product ID
 - Product Name
 - Website
- **Network:** Computer name, hardware address and IP address of the device
 - Local Name
 - Standard 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
 - Unid 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).


2.5.6 Restart and Shutdown

Within the **Application Launcher** you will find two buttons for  **rebooting** or  **shutting down** the device. Both actions can be disabled for the user and will then be available to the administrator only.

You can change the default action when shutting down the device using the button on the screen or the on/off button on the device itself in the setup under **System > Power Options > Shutdown**.

2.6 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 39)
- [End the Setup](#)(see page 40)
- [Quick Setup](#)(see page 40)
- [Setup Search](#)(see page 41)


2.6.1 Starting the Setup

You can open the setup in the following ways:

- Double-click  in the **Application Launcher**
- or click on **Run**.
- Double-click  on the desktop (if available based on the settings).



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

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

2.6.2 End the Setup

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


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

2.6.3 Quick Setup


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

To create a quick setup session, proceed as follows:

1. Enable the password for the administrator in IGEL Setup under **Security** > [Password](#).(see page 229)

 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 102), define the name and options for calling up the quick setup.
3. Under **Accessories** > **Quick Settings** > [Page Authorizations](#),(see page 104) enable those areas to which the user is to have access.

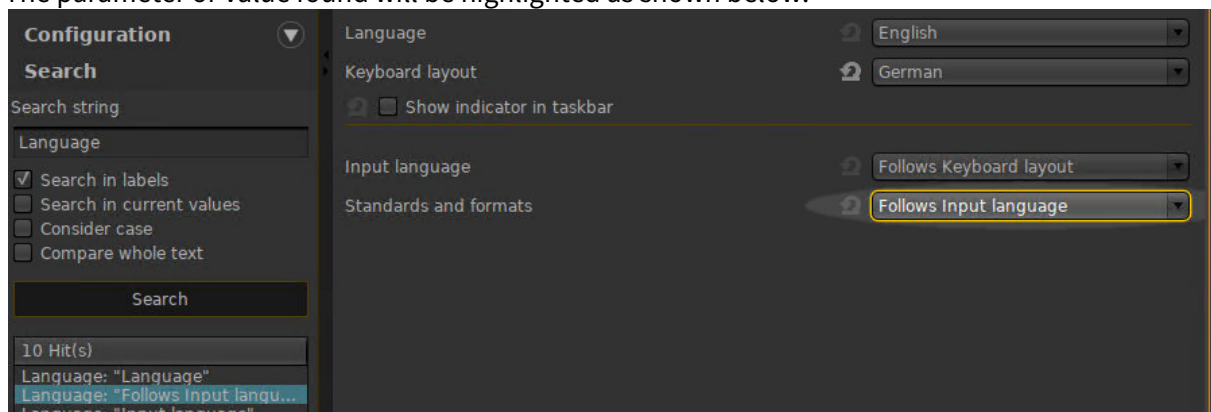
 You can set up a hotkey to start quick setup in appliance mode. Instructions for setting up the hotkey can be found under [Quick Settings](#)(see page 102).



2.6.4 Setup Search

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

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



2.7 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 41)
- [Global Session Options](#)(see page 42)
- [Citrix](#)(see page 42)
- [SSH Session](#)(see page 71)
- [Chromium Browser Global](#)(see page 76)
- [Chromium Sessions](#)(see page 84)


2.7.1 Copy Session

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

To copy a session, proceed as follows:

1. In the setup, open the menu path **Sessions > [Session Type] > [Session Type] Sessions**.
Example: **Sessions > RDP > RDP Sessions**
The existing sessions are shown.



2. Highlight the session that you want to copy.
3. In the **[Session Type] Sessions** area, click . Alternative: Open the context menu of the session by right-click and select **Copy**.
A copy of the session will be created.

2.7.2 Global Session Options

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

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

2.7.3 Citrix

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

- [Citrix Client Selection](#)(see page 42)
- [Citrix Global](#)(see page 43)
- [Citrix StoreFront](#)(see page 55)
- [Citrix Self-Service](#)(see page 64)
- [Citrix Workspace Hub](#)(see page 68)

Citrix Client Selection

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

Select which of the installed Citrix client versions is to be used for Citrix sessions.

Citrix client version

- Default (20.10.0)
- 20.06.0



- 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 [Storefront Login failed because of expired AD password](#)(see page 43).

- [StoreFront Login](#)(see page 43)
- [Window](#)(see page 45)
- [Keyboard](#)(see page 45)
- [Mapping](#)(see page 46)
- [Firewall](#)(see page 49)
- [Options](#)(see page 50)
- [Native USB Redirection](#)(see page 51)
- [HDX Multimedia](#)(see page 53)
- [Codec](#)(see page 54)

StoreFront Login

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

In this area, you can define session-specific login options.

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

- Password authentication: Suitable for on-premises connections; connections via Citrix NetScaler or to a cloud environment may cause problems.
- Kerberos passthrough authentication: Uses local login data for listing and launching applications. The option enables single sign-on if login with AD/Kerberos is configured on the device.
- Smartcard authentication (StoreFront only, not Web Interface)
- Citrix authentication mechanism (instead of IGEL), Smartcard disabled
- Citrix authentication mechanism (instead of IGEL), Smartcard enabled

- i** If you have set an authentication type with smartcard, select the type of card on the [Smartcard](#)(see page 239) page.

Additional options include the following:



Use passthrough authentication


- Cached login data are used for listing and starting applications.
- No passthrough authentication (default)

Auto login

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

User name: Can only be filled in with password authentication

Password: Can only be filled in with password authentication

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

Domain: Can only be filled in with password authentication

Remember username and domain:

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

Synchronize Citrix password with screen lock:

- Synchronizes the screen lock password with that of the Citrix application.
- No synchronization (default)

Relaunch Citrix login after logout:


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

Start a single published application automatically: This parameter is relevant if exactly 1 published application is provided for the user whose login is configured here.




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

Start following applications automatically after server connection is established: A list of applications to be started in the session.

To edit the list, proceed as follows:

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

 You can also enter part of the name followed by an asterisk (*).

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



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

Window

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

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

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

i 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**.

i 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 Connectionbar**
 - Off: Disabled (Default)
 - On: Shows a control bar for minimizing and closing a Citrix full-screen session.

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 46)
- [COM Ports](#)(see page 47)
- [Printer](#)(see page 48)

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.



i Local (USB) devices which are to be used for drive mapping purposes must first be set up as [storage devices](#)(see page 224).

⚠ 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.
- 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.

i 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.

i 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)

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"
- "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

 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.

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)

i After enabling the alternative address, add the server to the address list under **Sessions > Citrix > Citrix Global > Legacy ICA Server Location**.

SOCKS / Secure Proxy

- **Proxy type**
 - None (Direct Connection)
 - **SOCKS:** A proxy that uses the SOCKS protocol
 - **Secure (HTTPS):** An HTTP proxy with TLS/SSL encryption.
- **Proxy server:** Name or IP address of the proxy server
- **Proxy port:** TCP port of the proxy server (default: 1080)



Secure Gateway (relay mode)

- **Secure gateway address:** If you would like to use a Citrix Secure Gateway in relay mode, you must give the full DNS name – the IP address is not sufficient in this case.
- **Port:** TCP port of the gateway (default: 443)

Options

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

In this area, you can set up additional options to optimize the system's general behavior and its performance.

Use server redraw

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

Disable Windows alert sounds

- Switches off the Windows warning sounds.
- The warning sounds remain enabled. (Default)

Backing store

- The X Server temporarily stores hidden window content.
- Window content is not stored. (Default)


Deferred screen update mode

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

Cache size in kB: (default: 1024)

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

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

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

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

Audio bandwidth limit in StoreFront sessions

- High
- Medium
- Low



i Higher quality requires more network and computing resources.

Auto reconnect

- Automatically attempt to reconnect if connection is terminated. (Default)
- Do not attempt to reconnect.

Maximum retries: (default: 3)

Delay in seconds before reconnecting: (default: 30)

Allow Kerberos passthrough authentication in StoreFront sessions

- Kerberos passthrough authentication is allowed. (Default)
- Kerberos passthrough authentication is not allowed.

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. (Default)

HDX Adaptive Transport over EDT

Possible options:

- UDP with fallback to TCP
- TCP Only - UDP disabled
- UDP without fallback to TCP

Native USB Redirection

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

USB devices can be permitted or prohibited during a Citrix session on the basis of rules. Sub-rules for specific devices or device classes are also possible. The use of rules is described under [USB Access Control](#)(see page 227).

Native USB redirection

- Native USB redirection is enabled globally.

i Enable either **native USB redirection** or **Fabulatech USB redirection**, but not both together.

i Disable USB redirection if you use DriveLock. Further information can be found under [Using DriveLock with IGEL Devices](#)(see page 51).



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

- [Deny](#)
- [Allow](#)







Tip

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

Class Rules

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

To manage rules, proceed as follows:

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

Add class rule:

Rule:

- [Allow](#)
- [Deny](#)

Class ID: Selection list

Sub-class ID: Selection list

Name: Free text entry

Device Rules

Device rules apply to specific USB devices.

Add device rule:

Rule:

- [Allow](#)
- [Deny](#)

Vendor ID: Hexadecimal manufacturer number

Product ID: Hexadecimal device number



To find out the **Vendor ID** and **Product ID** of the connected USB device, use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal. You can also use the **System Information** tool, see [Using “System Information” Function](#)(see page 144).



Name: Free text entry

See also an overview and best-practice recommendations for the use of webcams under [Webcam Redirection and Optimization](#)(see page 51).

HDX Multimedia

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

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

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 160).

Resolution grade

Possible options:

- "Very low"
- "Low"
- "Normal"
- "High"
- "Very high"
- "Best"

HDX Webcam frame rate: The frame rate that is requested from the webcam

HDX Webcam quality: The image quality requested from the webcam. Range: 1-63

HDX Webcam width: The image width requested from the webcam

HDX Webcam height: The image height requested from the webcam

HDX Webcam delay time: Time to wait before the webcam is opened, in milliseconds

HDX Webcam delay type

Possible options:

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

Browser content redirection



- The browser content is redirected from the server to the device, e.g. to relieve the load on the server.
- Browser content redirection is disabled. (Default)

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)

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)

Citrix StoreFront





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

Most of the settings were already configured under Citrix Global.

- [Server](#)(see page 55)
- [Login](#)(see page 56)
- [Appearance](#)(see page 57)
- [Reconnect](#)(see page 58)
- [Refresh](#)(see page 60)
- [Logoff](#)(see page 61)
- [Desktop Integration](#)(see page 62)

Server

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





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

Add

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



Domains

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

Handling of domain in login window:

- normal
- locked
- hidden


Login

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

In this area, you can define session-specific login options.

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

- Password authentication: Suitable for on-premises connections; connections via Citrix NetScaler or to a cloud environment may cause problems.
- Kerberos passthrough authentication: Uses local login data for listing and launching applications. The option enables single sign-on if login with AD/Kerberos is configured on the device.
- Smartcard authentication (StoreFront only, not Web Interface)
- Citrix authentication mechanism (instead of IGEL), Smartcard disabled
- Citrix authentication mechanism (instead of IGEL), Smartcard enabled

 If you have set an authentication type with smartcard, select the type of card on the [Smartcard](#) (see page 239) page.

Additional options include the following:

Use passthrough authentication


- Cached login data are used for listing and starting applications.
- No passthrough authentication (default)

Auto login

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

User name: Can only be filled in with password authentication

Password: Can only be filled in with password authentication

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



Domain: Can only be filled in with password authentication

Remember username and domain:

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

Synchronize Citrix password with screen lock:

- Synchronizes the screen lock password with that of the Citrix application.
- No synchronization (default)

Relaunch Citrix login after logout:


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


Start a single published application automatically: This parameter is relevant if exactly 1 published application is provided for the user whose login is configured here.




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


Start following applications automatically after server connection is established: A list of applications to be started in the session.

To edit the list, proceed as follows:

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

 You can also enter part of the name followed by an asterisk (*).

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


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




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] = A l t

Key combinations are formed as follows with |:

- Ctrl +  = C t r l | 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`)

Refresh

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

- **Refresh Session Name:** (default: Update)

Starting Methods for Session

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



- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.
- **Hotkey:** Specifies a hotkey consisting of modifiers and a key which can be used to launch the session. (default: disabled)
 - **Modifiers:** One or two modifiers for the hotkey
 - **Key:** Key for the hotkey

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

Logoff

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

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



Starting Methods for Session

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


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


- **Start menu:**
 - The session can be started with the start menu. (Default)
 - The session cannot be found in the start menu.
- **Application Launcher:**
 - The session can be started with the Application Launcher. (Default)
 - The session cannot be found in the Application Launcher.
- **Desktop:**
 - The session can be started with a program starter on the desktop. (Default)
 - The session does not have a program starter on the desktop.
- **Quick start panel:**
 - The session can be started with the quick start panel.
 - The session cannot be found in the quick start panel. (Default)
- **Start menu's system icon:**
 - The session can be started with the start menu's system icon.
 - The session cannot be found in the start menu's system icon. (Default)
- **Application Launcher's system icon:**
 - The session can be started with the Application Launcher's system icon.
 - The session cannot be found in the Application Launcher's system icon. (Default)
- **Desktop context menu:**
 - The session can be started with the desktop context menu.
 - The session cannot be found in the desktop context menu. (Default)



- **Menu folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.
- **Desktop folder:** If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.
- **Password protection:** Specifies which password will be requested when launching the session. Possible values:
 - **None:** No password is requested when launching the session.
 - **Administrator:** The administrator password is requested when launching the session.
 - **User:** The user password is requested when launching the session.
 - **Setup user:** The setup user's password is requested when launching the session.
- **Hotkey:** A hotkey with which the session can be started is defined. It consists of modifiers and a key.
- **Modifiers:** One or two modifiers for the hotkey:
 - None
 -  = Shift
 - [Ctrl]= Ctrl
 -  = Super_L
 - [Alt]= Alt

Modifiers can be combined by using the pipe character | :


- [Ctrl]+  = Ctrl | Super_L
- **Key:** Key for the hotkey

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

Desktop Integration

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

Login session name: Session name.

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

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher

The session can be launched with the Application Launcher.



Desktop

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

Quick start panel

- The session can be launched with the quick start panel.

Start menu's system tab

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

Application Launcher's system tab

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

Desktop context menu

- The session can be launched with the desktop context menu.

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

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

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

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



Possible values:


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

Hotkey

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


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

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.

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 64)
- [Options](#)(see page 65)
- [Desktop Integration](#)(see page 66)

Server

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

To manage the list, proceed as follows:

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



Server: Web Interface

Add:

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

Server: StoreFront

Add:

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

Server: StoreFront Legacy Mode

Add:

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

Options

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

- **Display mode:** Display type for the Self-Service user interface
Possible values:
 - [Window](#)
 - Full screen

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

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



- The Self-Service user interface reconnects automatically to applications and desktops after being launched.
- The Self-Service user interface does not reconnect automatically.
- **Reconnect to apps after starting an application:**
 - The Self-Service user interface will attempt to reconnect to ongoing sessions if an application is launched or the store is reloaded.
 - The Self-Service user interface will not attempt to reconnect. (default)

Desktop Integration

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

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

Starting Methods for Session

Start menu

- The session can be launched from the start menu.

Application Launcher

- The session can be launched with the Application Launcher.

Desktop

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

Quick start panel

- The session can be launched with the quick start panel.

Start menu's system tab

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

Application Launcher's system tab

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

Desktop context menu

- The session can be launched with the desktop context menu.

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

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

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

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

Possible values:

- **None:** No password is requested when launching the session.






- **Administrator:** The administrator password is requested when launching the session.
- **User:** The user password is requested when launching the session.
- **Setup user:** The setup user's password is requested when launching the session.

Hotkey

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


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



Citrix Workspace Hub

Menu path: **Sessions > Citrix > Citrix Workspace Hub**

Feature in Beta Status (Experimental)

In this version of IGEL OS(RPI4), the integration of Citrix Workspace Hub is in beta status (experimental).

When your IGEL OS(RPI4) device is configured as a Citrix Ready Workspace Hub, you can use it for session roaming, session casting, and screen casting.

- [Options](#)(see page 68)
- [Desktop Integration](#)(see page 69)

Options

Menu path: **Sessions > Citrix > Citrix Workspace Hub > Options**

Feature in Beta Status (Experimental)

In this version of IGEL OS(RPI4), the integration of Citrix Workspace Hub is in beta status (experimental).


Autostart Citrix Workspace Hub Launcher

- The Citrix Workspace Hub Launcher is started automatically on system start.
- The Citrix Workspace Hub Launcher is not started automatically.

Citrix Workspace Hub (Beta)

- The Citrix Workspace Hub is enabled. When enabled, **Autostart Citrix Workspace Hub Launcher** is enabled as well but can be disabled separately.

URL for default launcher page

 The user can switch between the default launcher page, the second launcher page, and the third launcher page by clicking an arrow on the screen border.

- Default launcher page: System default launcher page; IGEL OS(RPI4) default background
- <https://myworkprod0.cloud.com> : Citrix launcher page; requires Internet access
- <https://www.igel.com>: IGEL homepage; requires Internet access
- Enter url here...: Custom URL of the launcher page of your choice; requires Internet access if external

QR code size

Possible options:

- small
- medium
- large



QR code position

Possible options:

- top left
- top right
- bottom left
- bottom right
- center: Exactly in the middle, both horizontally and vertically

URL for second launcher page

Possible options:

- Disabled: This page cannot be selected.
- Default launcher page: System default launcher page; IGEL OS(RPI4) default background
- <https://myworkprod0.cloud.com>: Citrix launcher page; requires Internet access
- <https://www.igel.com>: IGEL homepage; requires Internet access
- Enter url here...: Custom URL of the launcher page of your choice; requires Internet access if external

URL for third launcher page

Possible options:


- Disabled: This page cannot be selected.
- Default launcher page: System default launcher page; IGEL OS(RPI4) default background
- <https://myworkprod0.cloud.com>: Citrix launcher page; requires Internet access
- <https://www.igel.com>: IGEL homepage; requires Internet access
- Enter url here...: Custom URL of the launcher page of your choice; requires Internet access if external

Desktop Integration

Feature in Beta Status (Experimental)

In this version of IGEL OS(RPI4), the integration of Citrix Workspace Hub is in beta status (experimental).

Citrix Workspace Hub Session: Name for the Citrix Workspace Hub 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. Here, you will find the available 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



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 Citrix Workspace Hub Launcher

Citrix Workspace Hub Launcher 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.

2.7.4 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. Here, you will find the available 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



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 71).

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 73)
 - [Options](#)(see page 74)
 - [Desktop Integration](#)(see page 74)

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**

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. Here, you will find the available modifiers and the associated key symbols:

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


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

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super_L

Key: Key for the hotkey

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

Autostart

- The session will be launched automatically when the device boots.

Restart



- The session will be restarted automatically after the termination.

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

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

- For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.
- No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

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

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 74).

- 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.

2.7.5 Chromium Browser Global

Menu path: **Sessions > Chromium Browser > Chromium Browser Global**

Here, you can change settings that will be valid for all Chromium sessions.

Use IGEL Setup for configuration

- The settings made in the IGEL Setup or the UMS configuration dialog will be effective.
- The settings made in the IGEL Setup or the UMS configuration dialog will not have any effect on the behavior of Chromium.

H.264 decoding

- Hardware acceleration will be used for H.264 decoding.
- Hardware acceleration will not be used.

Automatic browser restart on exit

- Chromium is restarted when the user closes it.
- Chromium is not restarted on exit.



Show browser splash screen

- The Chromium splash screen is shown on start.
- Chromium starts without a splash screen.

- [General](#)(see page 77)
- [Content](#)(see page 78)
- [Proxy](#)(see page 78)
- [Privacy](#)(see page 79)
- [Security](#)(see page 81)
- [Encryption](#)(see page 81)
- [Menus & Toolbars](#)(see page 81)
- [Window](#)(see page 82)
- [Custom Setup](#)(see page 82)
- [Smartcard Middleware](#)(see page 83)

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.

Incognito mode

- Chromium is started in incognito mode.
- Chromium is started in normal browsing 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**

In this area, you can define settings for preventing phishing and malware.

Enable phishing and malware protection

- The browser will check each address entered as to whether it can be found in the blacklist of fraudulent websites that use phishing. If this is the case, you will be given a warning.
- The browser will not check whether an address is on the blacklist of fraudulent websites.

Encryption

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Encryption**

In this area, you can define the settings for encryption methods.

Minimum SSL/TLS version: This protocol will be used to establish a secure connection if no higher protocol is available. Higher protocols are preferred.

Possible options:

- TLS 1.0
- TLS 1.1
- TLS 1.2
- TLS 1.3

Maximum SSL/TLS version: This protocol is requested when negotiating the connection. If this protocol is not available, the next lowest protocol will be requested.

Possible options:

- TLS 1.2
- TLS 1.3

Menus & Toolbars

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Menus & Toolbars**

In this area, you can change the browser's menus and toolbars.

Hide home button

- The home button will not be shown.
- The home button will be shown.

Hide bookmarks toolbar

- The bookmarks menu will not be shown in the menu bar.
- The bookmarks menu will be shown in the menu bar.



Window

Menu path: **Sessions > Chromium Browser > Chromium Global > Window**

In this area, you can define the window settings for a Chromium session.

Enable kiosk mode

Chromium starts in kiosk mode.

Chromium starts in normal mode.

Start maximized

Chromium starts in a maximized window.

Chromium starts in a window with default size.

Chromium translation: Changes the default language when Chromium offers to translate a web page.

File access

Chromium can access local files on the endpoint device.

Local files cannot be accessed by Chromium.

Block Chromium settings

The settings menu of Chromium can not be accessed by the user.

The user can access the settings menu.

Custom Setup

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Custom Setup**

- [Policies](#)(see page 82)
- [Preferences](#)(see page 82)
- [Commandline Options](#)(see page 83)

Policies

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Custom Setup > Policies**

Here, you can define policies for Chromium. For further information, see https://chromium.googlesource.com/chromium/src/+master/docs/enterprise/add_new_policy.md.

► Click on **Add** to create a policy.

Policy name: Name of the policy

Policy value: Value of the policy

Preferences

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Custom Setup > Preferences**

Here, you can define preferences for Chromium.



- ▶ Click on **Add** to create a preference.

Preference name: Name of the preference.

Preference value: Value of the preference.

Commandline Options

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Custom Setup > Commandline Options**

Here, you can define command line options that are passed to Chromium on startup.

- ▶ Click on **Add** to create a command line option.

Commandline option: Name of the command line option

Commandline value: Value of the command line option

Smartcard Middleware

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Smartcard Middleware**

In this area, you can activate or deactivate smartcard middleware that is to be used for encryption.

Gemalto SafeNet security device

- Gemalto/SafeNet eToken will be used for encryption.
- Gemalto/SafeNet eToken will not be used for encryption.

cryptovision sc/interface security device

- cryptovision sc/interface will be used for encryption.
- cryptovision sc/interface will not be used for encryption.

Gemalto IDPrime security device

- Gemalto IDPrime will be used for encryption. Enable this Gemalto middleware when you want to operate Gemalto Common Criteria devices in unlinked mode.
- Gemalto IDPrime will not be used for encryption.

Athena IDProtect security device

- Athena IDProtect will be used for encryption.
- Athena IDProtect will not be used for encryption.

A.E.T. SafeSign security device

- A.E.T. SafeSign will be used for encryption.
- A.E.T. SafeSign will not be used for encryption.

SecMaker Net iD security device

- SecMaker Net iD will be used for encryption.
- SecMaker Net iD will not be used for encryption.

Coolkey security device



- Coolkey will be used for encryption.
- Coolkey will be not used for encryption.

OpenSC security device

- OpenSC will be used for encryption.
- OpenSC will not be used for encryption.

90meter security device

i **Licensed Feature**

This feature requires an add-on license; see [Add-On Licenses](#)⁸. Please contact your IGEL sales representative.

- 90meter will be used for encryption.
- 90meter will not be used for encryption.

Use a custom security device

- The PKCS#11 module stored under the **Path to the library** is used.
- The custom security device will not be used for encryption.

Name of the security device: Name of the custom security device that uses the library specified under **Path to the library**

Path to the library: Path to the custom PKCS#11 module

2.7.6 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

⁸ <https://kb.igel.com/display/licensesmoreigelos11/Add-on+Licenses>



- 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. Here, you will find the available modifiers and the associated key symbols:

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


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

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super_L

Key: Key for the hotkey

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

Autostart



The session will be launched automatically when the device boots.

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

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

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

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

- [Settings](#)(see page 86)
- [Desktop Integration](#)(see page 86)

Settings

Menu path: **Sessions > Chromium Browser > Chromium Sessions > [Session Name] > Settings**

In this area, you can change the following settings:

On startup: Specifies what pages are shown when Chromium is launched.

Possible options:

- "Global setting"
- "Open the new tab page"
- "Open a specific page or set of pages": The page or set of pages specified under **Startup page** are opened.
- "Continue where you left off": All tabs from the last session are reopened.


Startup page: Specifies the URL of the start page. You can specify a set of start pages by separating the URLs of the start pages with a vertical dash "|". This setting is active only when "Show my home page" is chosen under **On startup**.

Desktop Integration

Menu path: **Sessions > Chromium Browser > Chromium Sessions > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the Chromium session.

Session name: Name for the session.

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

Starting Methods for Session

Start menu

The session can be launched from the start menu.

Application Launcher



- The session can be launched with the Application Launcher.

Desktop

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

Quick start panel

- The session can be launched with the quick start panel.

Start menu's system tab

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

Application Launcher's system tab

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

Desktop context menu

- The session can be launched with the desktop context menu.

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

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

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

Hotkey

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

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



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**.

2.8 Accessories

- [ICA Connection Center](#)(see page 89)
- [Terminals](#)(see page 92)
- [Change Smartcard Password](#)(see page 94)
- [Change Password](#)(see page 96)
- [Setup](#)(see page 98)
- [Quick Settings](#)(see page 102)
- [Display Switch](#)(see page 104)
- [Application Launcher](#)(see page 112)
- [Sound Preferences](#)(see page 115)
- [UMS Registration](#)(see page 119)
- [Task Manager](#)(see page 121)
- [Screenshot Tool](#)(see page 127)
- [On-Screen Keyboard](#)(see page 130)
- [Monitor Calibration](#)(see page 133)
- [Commands](#)(see page 135)
- [Bluetooth Tool](#)(see page 137)
- [System Information](#)(see page 142)
- [Disk Utility](#)(see page 145)
- [Disk Removal](#)(see page 148)
- [Mobile Device Access](#)(see page 150)
- [Firmware Update](#)(see page 152)
- [Smartcard Personalization](#)(see page 155)
- [Webcam Information](#)(see page 158)
- [ICG Agent Setup](#)(see page 160)
- [Licensing](#)(see page 163)




2.8.1 ICA Connection Center

Menu path: **Accessories > ICA Connection Center**

With the *Citrix ICA Connection Center*, you are given an overview of the existing connections to *Citrix* servers as well as information regarding connection properties. You can also terminate server connections and log off from *Citrix* servers. For details of how to use the **ICA Connection Center**, see [Using ICA Connection Center](#) (see page 91).

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. Here, you will find the available modifiers and the associated key symbols:

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


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

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super_L

Key: Key for the hotkey

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

Autostart

- The session will be launched automatically when the device boots.

Restart

- The session will be relaunched automatically after the termination.

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

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

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

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

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#) (see page 89).

- 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 91)

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 89). All applications are shown in a tree structure with the associated *Citrix* servers.

i 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 89).
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 89).
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 89).



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.

2.8.2 Terminals

Menu path: **Accessories > Terminals > Local Terminal**

With the local terminal, you can execute local commands on your device. For details of how to use the local terminal, see [Using Local Terminal](#)(see page 94).

i 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. Here, you will find the available modifiers and the associated key symbols:

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


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

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super_L

Key: Key for the hotkey

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

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

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

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

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

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



Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 92).

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 94)

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 92).
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.

2.8.3 Change Smartcard Password

Menu path: **Accessories > Change Smartcard Password**

With this function, you can change the password for your IGEL smartcard. For details of how to use the function, see [Using "Change smartcard password" Function](#)(see page 96).

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. Here, you will find the available modifiers and the associated key symbols:

- (No modifier) = None




-  = Shift
- [Ctrl] = Ctrl
-  = Mod4


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

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super_L

Key: Key for the hotkey

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

- [Using Change Smartcard Password Function](#)(see page 96)

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 94).
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.

2.8.4 Change Password

Menu path: **Accessories > Change Password**

With this function, the user can change the password or PIN for the login method he used for his current session, provided one of the following login methods was used:

- Active Directory with username and password
- Active Directory with third-party smartcard
- IGEL smartcard
- Local user with screen lock 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 98).

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. Here, you will find the available modifiers and the associated key symbols:

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


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

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super_L

Key: Key for the hotkey

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

- [Using Change Password Function](#)(see page 98)

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 screen lock password), proceed as follows

1. Start the **Change password** function. The start options are described under [Change password](#)(see page 96).
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.

2.8.5 Setup


Menu path: **Accessories > Setup**



With the IGEL Setup, you can configure your endpoint device. For details of how to allow the user access to the individual areas of the Setup, see [Setup User Permissions](#)(see page 100). For details of how to change the setup options, see [Options](#)(see page 102).

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. Here, you will find the available 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)`

- [Setup User Permissions](#)(see page 100)
- [Setup Administrator Permissions](#)(see page 101)
- [Options](#)(see page 102)

Setup User Permissions

Define which areas should be visible and/or configurable for the setup user.

If a password was set up for the administrator, the IGEL Setup can only be opened with administrator rights, i.e., after entering the password (see [Password](#)(see page 229)). However, individual areas of the setup can be enabled for the user, e.g. to allow them to change the system language or configure a left-handed mouse.

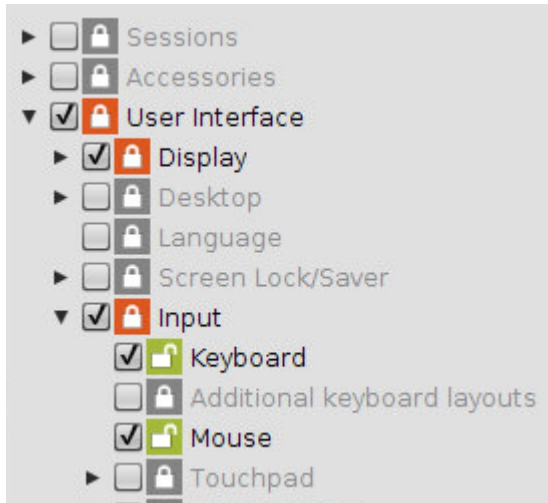
To enable setup pages for the user, proceed as follows:


1. Here, enable those areas to which the user is to have access.

Possible settings:


Node	Setup Page
<input type="checkbox"/> not visible	not visible
<input checked="" type="checkbox"/> visible	not visible
<input checked="" type="checkbox"/> 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).

2. Under **Security > Password**, enable the password for the **administrator** and the **setup user**.

 If users are to be allowed to edit parts of the setup even without a password, create a [quick setup](#)(see page 40) session, the password for the **setup user** will not be enabled in this case.

Setup Administrator Permissions



Configure which area should be visible for the setup administrator.

If a password was set up for the administrator, the IGEL Setup can only be opened with administrator rights, i.e., after entering the password (see [Password](#)(see page 229)). However, individual areas of the setup can be enabled for the setup administrator.


To enable setup pages for the setup administrator, proceed as follows:


1. Here, enable those areas to which the setup administrator is to have access.

Possible settings:


	Node	Setup Page
	not visible	not visible
	visible	not visible



	visible	configurable
---	---------	--------------

 If you enable a setup page on the lower levels, the node points required for access will automatically be marked as visible (but blocked for editing purposes).

2. Under **Security > Password**, enable the password for the **administrator** and the **setup administrator**.

 If administrators are to be allowed to edit parts of the setup even without a password, create a [quick setup](#)(see page 40) 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.


2.8.6 Quick Settings

Menu path: **Accessories > Quick Settings**

With the IGEL Setup, you can allow the user access to individual areas of the Setup. Instructions can be found under [Setup User Permissions](#)(see page 100).

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. Here, you will find the available 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



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 102).

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 104)

Setup User Permissions

Menu path: **Accessories > Quick Settings > Setup User Permissions**

Define which setup pages are visible to users.

You will find instructions for this function under [Setup User Permissions](#)(see page 100).

2.8.7 Display Switch

Menu path: **Accessories > Display Switch**

With this function, you can configure the display on several screens. For details of how to set the function, see [Options](#)(see page 106). For details of how to use the function, see [Using "Display Switch" Function](#)(see page 110).

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. Here, you will find the available 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

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 104).

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 106)
 - [Minimal Dialog](#)(see page 108)
 - [Advanced Dialog](#)(see page 109)
 - [Using Display Switch](#)(see page 110)

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 108)
- [Advanced Dialog](#)(see page 109)
- [Using Display Switch](#)(see page 110)

or the how-to Tip-Trick : [Display Switch](#)(see page 106).

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.



	<p>Rotates the selected display to the left or to the right.</p>
--	--

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 110).

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 110).

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 104).

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.

2.8.8 Application Launcher

Menu path: **Accessories > Application Launcher**

With the Application Launcher, you can launch predefined sessions and device functions/tools. You are also given information regarding the device and the licenses used.

Further information can be found under [Application Launcher](#)(see page 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. Here, you will find the available 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

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 112).

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 114)

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)


2.8.9 Sound Preferences

Menu path: **Accessories > Sound Preferences**

With this function, you can configure your device's audio system. For details of how to change the presets for the audio system, see [Options](#)(see page 117). For details of how to use the function, see [Using "Audio Settings" Function](#)(see page 119).

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. Here, you will find the available 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

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 115).

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 117)
- [Using Audio Settings Function](#)(see page 119)


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 119).

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 115).

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 audio device that has been selected last will be used, if present.

 The other options are not working properly in this version of IGEL OS(RPI4).


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 audio device that has been selected last will be used, if present.

 The other options are not working properly in this version of IGEL OS(RPI4).



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 Audio Settings Function

- ▶ Start the **Audio Settings** function. The start options are described under [Sound Preferences](#)(see page 115).

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.


2.8.10 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 121).

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. Here, you will find the available modifiers and the associated key symbols:


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

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


- [Alt] = Alt

Key combinations are formed as follows with |:



- Ctrl +  = Ctrl|Super_L


Key: Key for the hotkey

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

- [Using UMS Registration Function](#)(see page 121)

Using UMS Registration Function

1. Start the **UMS Registration** function. The start options are described under [UMS Registration](#)(see page 119).
2. Enter the following data:
 - **Server Address:** IP address or host name of the UMS Server.
 - **Port Number:** Port of the UMS Server.
 - **Structure Tag:** Character string for assigning the device to a specific UMS directory.
 - **New Hostname:** Name under which the device is registered in the UMS.
 - **Login:** User name for logging in to the UMS Console.
 - **Password:** Password for logging in to the UMS Console.

 Any UMS user with sufficient rights can be specified under **Login** and **Password**.
Example: If a device has to be registered in a particular folder, the user must have "move" permission for this folder.

3. If you want to assign a specific UMS directory to the device, click on **Click to select directory** and then select the desired directory from the list.
4. Click on **Register**.


2.8.11 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 124).

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. Here, you will find the available 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] = A l t

Key combinations are formed as follows with |:

- Ctrl +  = C t r l | 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 121).

- 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 124)



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 121).

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:

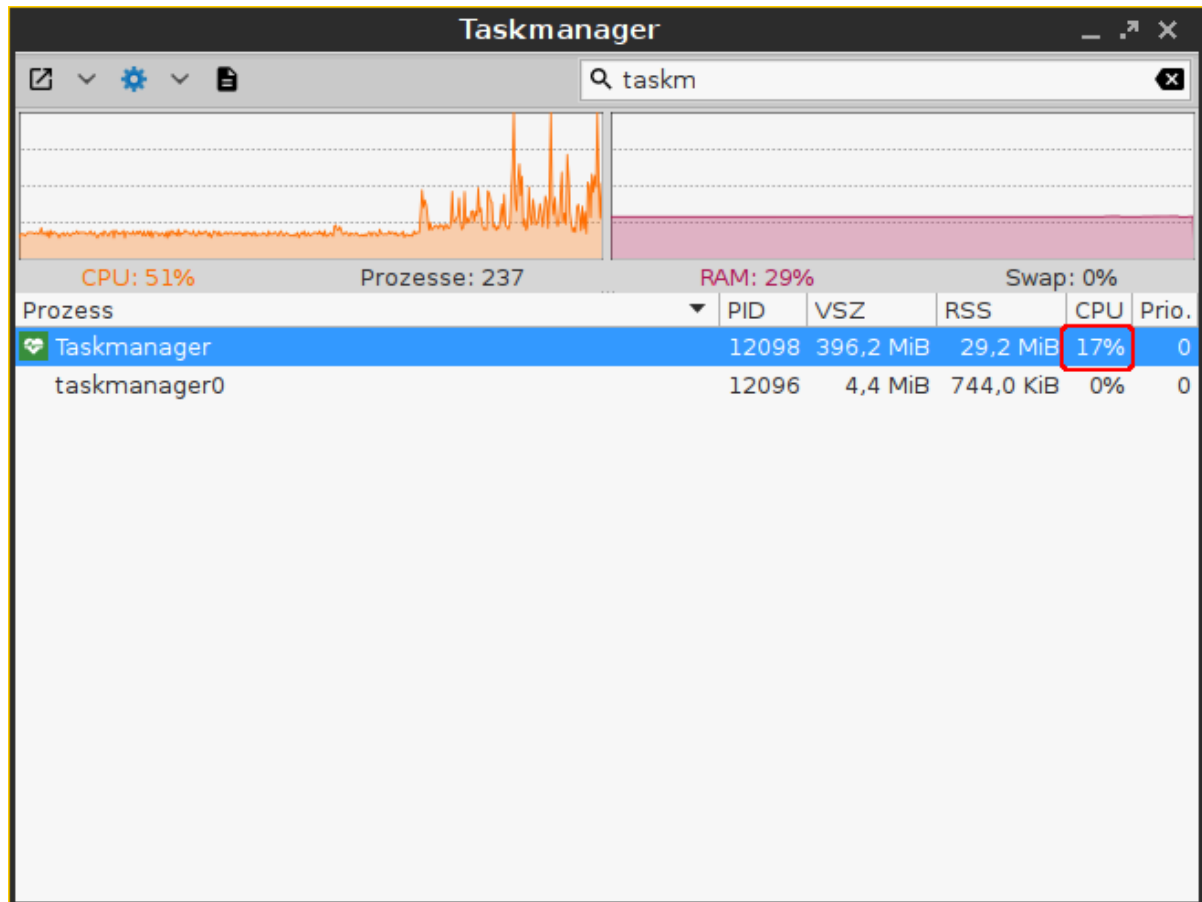
▶ Read the percentage value under **RAM:**.





▶ To calculate the value in bytes, click on  and enable the option **Show memory usage in bytes**.

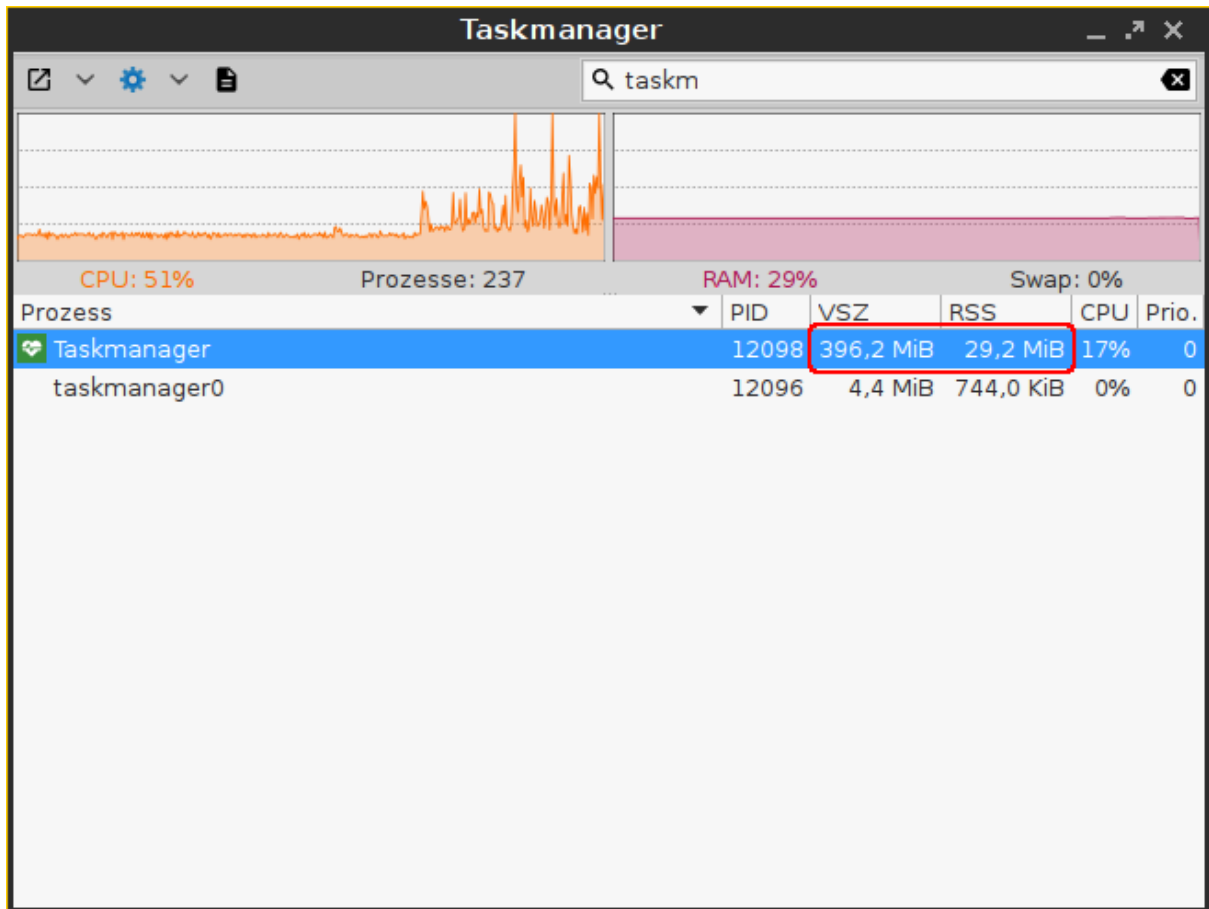
To determine the extent to which a specific application contributes to processor usage, proceed as follows:

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).



i 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:

i 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.

i 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.

2.8.12 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 130).

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. Here, you will find the available 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] = A l t

Key combinations are formed as follows with |:

- Ctrl +  = C t r l | 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 127).

- 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 130)

Using Screenshot Tool

1. Launch the **Screenshot Tool** function. The launch options are described under [Screenshot Tool](#)(see page 127).
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.

2.8.13 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 130).

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 132)

Appearance

Menu path: **Accessories > On-Screen Keyboard > Appearance**

- **Show Function Keys**

The on-screen keyboard features the function keys [F1] ... [F12]. (default)

- **Show Navigation Keys**

The on-screen keyboard features the arrow keys for navigating on the screen. (default)

- **Show Numpad**

The on-screen keyboard features the number block.

The on-screen keyboard does not feature the number block. (default)

- **Enable switching to alternative layout**

 This option is available from IGEL Linux *version 10.04.100* onwards.

The on-screen keyboard has an additional key by which the user can toggle between the normal layout and a reduced layout. The reduced layout resembles the numpad, with the following differences:

- Additional backspace key [←]
- Additional tab key [⇧⇨]
- Additional space key []
- Additional escape key [Esc]
- Return key [↵] instead of [Enter] key



- Switching to the reduced layout is not possible. (default)

2.8.14 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`. Here, you will find the available modifiers and the associated key symbols:

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


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

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super_L

Key: Key for the hotkey

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

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

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

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

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

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



Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 133).

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.

2.8.15 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. Here, you will find the available 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)`

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 135).

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.

2.8.16 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 139).

 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. Here, you will find the available modifiers and the associated key symbols:

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


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

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super_L

Key: Key for the hotkey

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

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

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



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

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

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

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 137).

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 139)

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.

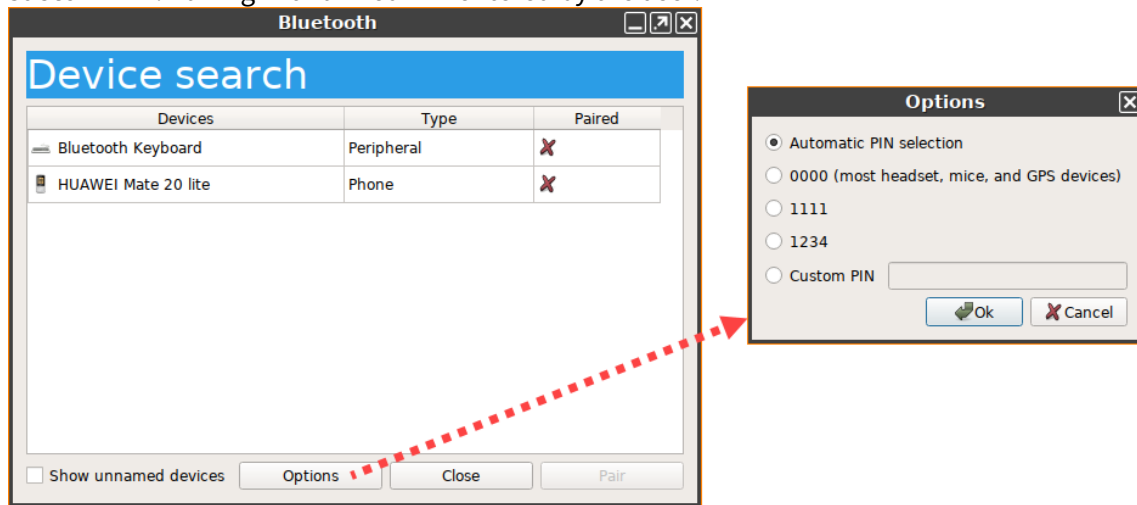
i If your endpoint device (e.g. UD2 D220) does not support Bluetooth, it is necessary to connect a Bluetooth USB adapter to it.

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 137). 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 \(1\)](#)(see page 139).

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 137). 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.



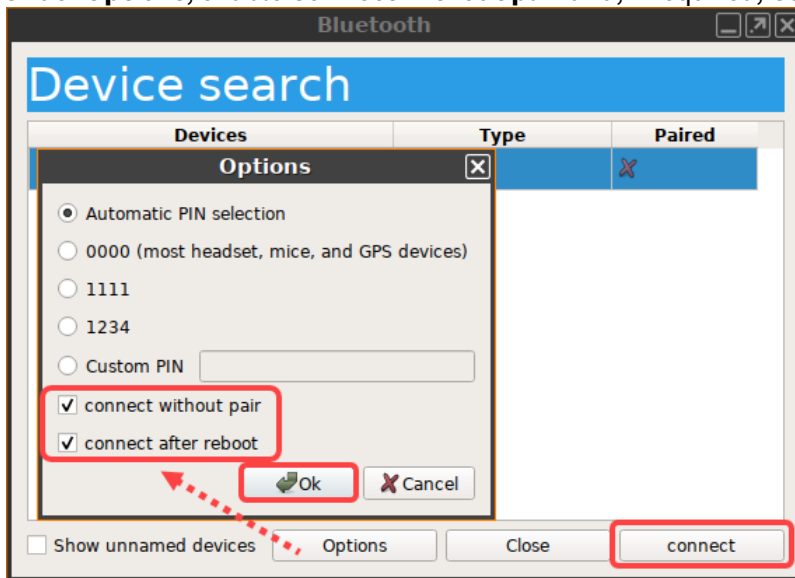
5. Under **Options**, select one of the specified PINs or enable **Custom PIN** and enter the PIN for the Bluetooth device. You will find this PIN in the documentation for your Bluetooth device.
6. Click on **Pair**.
In a few seconds, the status of the connection will be shown.
7. On successful connection, close the dialog.

Canceling Coupling to a Bluetooth Device

1. Start the **Bluetooth Tool**. The start options are described under [Bluetooth Tool](#)(see page 137). 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 137). 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).

2.8.17 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 144).

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. Here, you will find the available modifiers and the associated key symbols:

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


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

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super_L

Key: Key for the hotkey

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

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be restarted automatically after the termination.

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



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

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

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

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 142).

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 144)

Using System Information Function

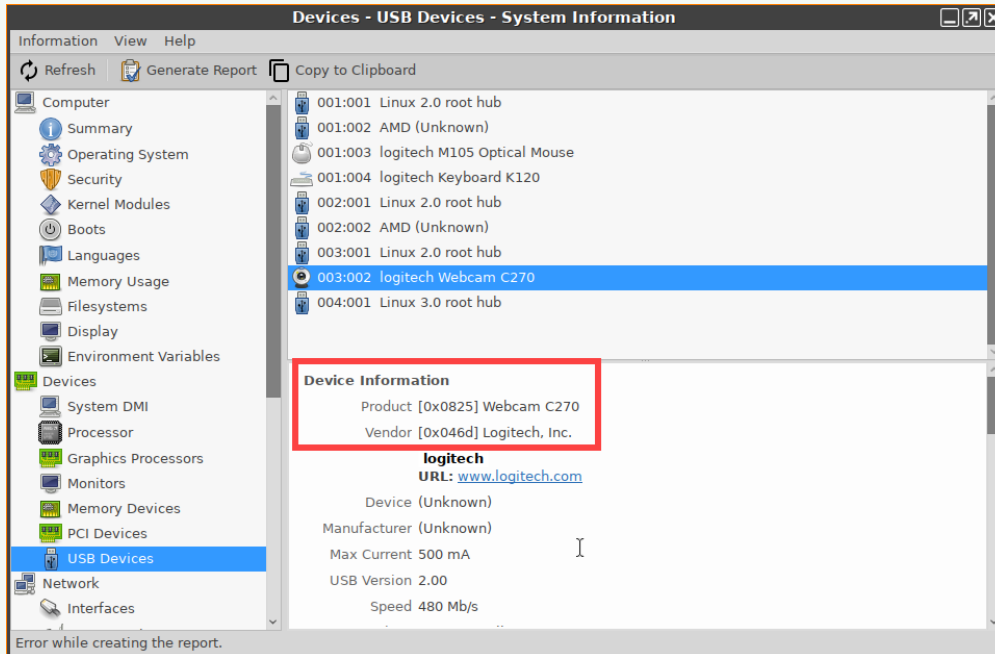
Menu path: **Accessories > System Information**

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 142).
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 227) or [RDP Global Native USB Redirection](#)(see page 144).



See also [Issues with USB IDs in USB Devices Rules](#)(see page 144).

2.8.18 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 148).

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. Here, you will find the available 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] = A l t

Key combinations are formed as follows with |:

- Ctrl +  = C t r l | 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 145).

- 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 148)



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 145).
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 145).
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 224).

2.8.19 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. Here, you will find the available 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`)

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 148).

- 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 148).

2.8.20 Mobile Device Access

Menu path: **Accessories > Mobile Device Access**

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).

With this function, you can access the directories and files of a mobile device.

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

i The functionality may differ according to the specific device and operating system version.

To use the mobile device access feature, you must first activate the function. For information about the activation and use, see [Using Mobile Device Access](#)(see page 150).

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. Here, you will find the available modifiers and the associated key symbols:


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

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


- [Alt] = Alt

Key combinations are formed as follows with |:



- Ctrl +  = Ctrl|Super_L

Key: Key for the hotkey

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

Autostart

- The session will be launched automatically when the device boots.

Restart

- The session will be restarted automatically after the termination.

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

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

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

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

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 150).

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.


2.8.21 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 155).

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. Here, you will find the available 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] = A l t

Key combinations are formed as follows with |:

- Ctrl +  = C t r l | 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 152).

- 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 155)



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 242).
2. Start the **Firmware Update** function. The start options are described under [Firmware Update](#)(see page 152).
3. Confirm this by clicking **Yes**.
The latest firmware will be loaded onto your endpoint device. The device will restart in the process.

2.8.22 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 157).

Further information regarding the IGEL smartcard can be found in the [Authentication with IGEL Smartcard](#)(see page 155) 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. Here, you will find the available modifiers and the associated key symbols:

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


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

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super_L

Key: Key for the hotkey

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

Autostart

- The session will be launched automatically when the device boots.

Restart



- The session will be relaunched automatically after the termination.

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

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

- For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.
- No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.


-
- [Using Smartcard Personalization Function](#)(see page 157)

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 155).
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.



2.8.23 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 160).

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. Here, you will find the available modifiers and the associated key symbols:

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


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

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super_L

Key: Key for the hotkey

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

Autostart

The session will be launched automatically when the device boots.

Restart

The session will be relaunched automatically after the termination.

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

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

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

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

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#) (see page 158).

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 160)

Using Webcam Information

You can determine and change the width, height and frame rate for the webcam connected.

i 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.

2.8.24 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 162).

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. Here, you will find the available 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] = A \bar{l} t

Key combinations are formed as follows with |:

- Ctrl +  = Ctr \bar{l} | Super_L

Key: Key for the hotkey

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

Autostart

- The session will be launched automatically when the device boots.

Restart

- The session will be relaunched automatically after the termination.

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

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

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

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

- [Using ICG Agent Setup](#)(see page 162)



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 160).
 - **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:

- Go to **IGEL Setup > System > Registry > system > remotemanager > icg_try_ums_connect** (Search parameter: **system.remotemanager.icg_try_ums_connect**).
- Enable **Prefer UMS over ICG**.
- Confirm your setting with **Ok**.

2.8.25 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 31).

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. Here, you will find the available 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] = A l t

Key combinations are formed as follows with |:

- Ctrl +  = C t r l | S u p e r _ 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 163).

- 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.

2.9 User Interface


- [Display](#)(see page 166)
- [Desktop](#)(see page 170)
- [Language](#)(see page 177)
- [Screenlock / Screensaver](#)(see page 177)
- [Input](#)(see page 182)
- [Hotkeys](#)(see page 185)
- [Font Services](#)(see page 188)




2.9.1 Display

Menu path: **User Interface > Display**








Every screen connected to the IGEL UD device can be configured independently. The position of the individual screens can be determined in relation to Screen 1.

- ▶ Click on  to show the screen identifier on each device.

 For details of the display resolution supported by your IGEL thin client, please see the relevant data sheet.

Screen Configuration

Number of screens: Select how many monitors you would like to use.

	Identifies each screen connected and specifies the connection and display resolution for each screen.
	Arranges the screens in a single row.
	Arranges the screens in two rows.
	Rotates the selected screen anti-clockwise.
	Rotates the selected screen clockwise.
	Removes the screen which was last added.
	Adds a screen.



The selected screen is highlighted with a blue frame. The black bar at the bottom edge of the screen represents the physical orientation of the monitor.

Selected screen: Selects a screen using this selection box to configure the following settings.

Screen resolution: Move the slider to the resolution which the selected screen is to have. The resolution is shown in the right-hand box.



- i** You have the option of defining your own resolutions via the registry (`x.xserver0.custom_resolution`). In order for the values set there to take effect, the resolution must be set to "Automatic" (slider at the far left). The following parameters apply to the entry in the registry:
- `WxH` : W = width, H = height (example: 1920x1080)
 - `WxH@R` : W = width, H = height, R = refresh rate (example: 1920x1080@60 or 1920x1200@59.8)

Advanced

Detect refresh rate automatically

- A refresh rate for the monitor is identified automatically. (Default)
- A refresh rate for the monitor is to be set manually.

Refresh rate: Number of individual images per second.

Possible values:

- 30 ... 100. (Default: 60)

Graphic card: Graphics card assigned to the selected screen. A graphics card can have more outputs than are actually used. In order to ensure transparency, you may need to assign the graphics cards manually.

- i** 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 167)
- [Access Control](#)(see page 168)
- [Gamma Correction](#)(see page 169)
- [Options](#)(see page 169)

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)



i Make sure that all screens connected to the thin client support the color setting.

2.9.2 Desktop

Menu path: **Setup > User Interface > Desktop**

On this page, you can configure general settings for the appearance of the desktop:

- **Local window manager for this display:** Here, you can disable the window manager if you only work in full-screen sessions and do not require this service.
- **User interface theme:** The colors of windows such as the Application Launcher, the start menu, the local terminal, the taskbar and messages can be varied. You can either select one of our predefined color schemes or define a color scheme of your own.
 - IGEL Dark: The frame color is dark gray, IGEL logos are yellow.
 - IGEL Light: The frame color is light gray, IGEL logos are dark gray.
 - Custom Colors: Define your own color combinations below.
- **Desktop icon size:** Specify the size in which you would like the icons to be displayed on the desktop (default 64).
- **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 specially 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 (default: 10).
- **Desktop icon font size:** Specify your desired font size for desktop icons in pt (points) here (default: 11).
- **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 (default: 11).

-
- [Background](#)(see page 171)
 - [Taskbar](#)(see page 173)
 - [Taskbar Background](#)(see page 174)
 - [Taskbar Items](#)(see page 175)
 - [Pager](#)(see page 176)
 - [Start Menu](#)(see page 176)

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.

i You can set up a separate background image for each monitor that is connected to the thin client.

i **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**.

i 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**.

i 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](#)(see page 175).

- **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).

i 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](#)(see page 177).

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](#)(see page 173).
 - **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



Pager

Menu path: **Setup > User Interface > Desktop > Pager**

In this area, you can enable the use of a number of virtual workstations.

The **Pager** is a tool with virtual desktops which can be used as an easy way of switching between open applications. This window is shown at the right of the taskbar. You can use up to 25 virtual desktops. If you use a **Pager**, you can switch between full-screen applications for example at the click of a mouse.

Instead of minimizing/maximizing sessions or switching between them using key combinations, you simply click on the desired screen using the mouse. The screen is then shown as it was when you closed it (unless you restarted the system beforehand).

- **Use Pager**
 - Several virtual desktops may be used.
 - Pager is not used. (default)
- **Number of Screens - Horizontal:** Specifies how many pages will be shown next to each other.
- **Number of Screens - Vertical:** Specifies how many pages will be shown above each other.
- **Names of the workspaces:** Give names for the individual desktops.
- **Paging Resistance:** Specifies how many pixels the cursor needs to be moved over the edge of the screen before it triggers a switch of desktop. You only need to make this setting if you enable at least one of the following options:
 - **Wrap workspaces while dragging a window:** The desktop is switched as soon as a window is dragged out of view.
 - **Wrap workspaces with pointer:** The desktop is switched as soon as the mouse reaches the edge of the screen.

Start Menu

Menu path: **Setup > User Interface > Desktop > Start Menu**

In this area, you can configure the desktop start menu:

- **Start menu type:**
 - **Auto:** A default setting that automatically selects the advanced or legacy type of the start menu depending on the processor.
 - **Advanced:** An expanded start menu featuring a search function and a more attractive design. It requires more resources, which is particularly noticeable on slow devices.
 - **Legacy:** A start menu resembles the one from Windows 95 – a list of available sessions and options.

Options in Start Menu

Select which options are to be shown in the start menu:

- **Screenlock**
- **Logout**
- **Reboot**
- **Shutdown**
- **System tab**



- **About**
- **Show current user name in About, Application Launcher and start menu**

- The current user will be shown at the top edge of the relevant window.
- The current user will not be shown.

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**

2.9.3 Language

Menu path: **Setup > User Interface > Language**

In this area, you can configure the country-specific language settings.

- **Language:** The language of the user interface.
- **Keyboard layout:** When the language is changed for the first time, the keyboard layout is automatically set to the same language.
- **Show indicator in taskbar**
 - Shows a country abbreviation for the keyboard layout in the taskbar.
 - No indicator is shown (default)
- **Input language:** The keyboard layout is used by default.
- **Standards and formats:** Specifies how country-specific formats for the time and currency for example are displayed. The default setting is geared to the input language selected.

2.9.4 Screenlock / Screensaver

Menu path: **User Interface > Desktop > Screen Lock/Saver**

You can set up the screen saver so that it is activated automatically after a time limit expires, via a button or in response to a key combination (hotkey). You can also select a password option. The look of the taskbar can be configured separately for the logon dialog and the locked screen.

The screen can be locked via icons in the Quick Start Panel and on the desktop or via the hotkey [Ctrl-Shift-L].

Session name: Name for the session.

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

Starting Methods for Session

Start menu

- The session can be launched from the start menu.

Application Launcher



- The session can be launched with the Application Launcher.

Desktop

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

Quick start panel

- The session can be launched with the quick start panel.

Start menu's system tab

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

Application Launcher's system tab

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

Desktop context menu

- The session can be launched with the desktop context menu.

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

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

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

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



Possible values:


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

Hotkey

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

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

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 177).

- 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 179)
- [Taskbar](#)(see page 180)
- [Screensaver](#)(see page 181)

Options

Menu path: **Setup > User Interface > Screenlock / Screensaver > Options**

- **Start automatically**
 - The screenlock or screensaver starts automatically if there is no activity on the thin client within this time limit. The screenlock can be overridden by the user or administrator with the relevant password (see: Password). (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. If Active Directory (AD) login is enabled, an AD user password is deployed instead of the user password.
- **Screenlock password:** A separate password specified under **Set** is deployed to unlock the screen. If Active Directory (AD) login is enabled, the AD user password is deployed instead of the screenlock password.
- **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. (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 181). 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\(see page 195\)](#) or the [Wireless Manager\(see page 194\)](#) 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.

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 **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.

2.9.5 Input

Menu path: **Setup > User Interface > Input**



These setup pages allow you to set the keyboard layout and other input options.

The following input devices can be set up:

- [Keyboard](#)(see page 183)
- [Additional Keyboard Layouts](#)(see page 184)
- [Mouse](#)(see page 184)

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](#)(see page 130).

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.



2.9.6 Hotkeys

Menu path: **Setup > User Interface > Hotkeys > Commands**

In order to make it easier to use your thin client, hotkeys are available for frequent operating routines. A hotkey is a combination of one or more modifiers and an alphanumeric key.

You can enable or disable hotkeys and change the keys used. For more information, see [Commands](#)(see page 185).

- [Commands](#)(see page 185)

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. Here, you will find the available modifiers and the associated key symbols:

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


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

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super_L

Key: Key for the hotkey

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



Available Hotkeys and their Default Settings

Hide all windows and show desktop

Default:

- activated
- **Modifiers:** Ctrl|Mod4
- **Key:** d
- **Appliance Mode Access:** deactivated

Mapping Ctrl+Alt+End to Ctrl+Alt+Del for Citrix sessions

Default:

- deactivated
- **Modifiers:** Ctrl|Alt + End
- **Key:** End
- **Appliance Mode Access:** deactivated

Open start menu

Default:

- deactivated
- **Modifiers:** Shift + Super
- **Key:** Super_L
- **Appliance Mode Access:** deactivated

Open start menu (alternative):

Default:

- deactivated
- **Modifiers:** Shift + Super
- **Key:** Super_L
- **Appliance Mode Access:** deactivated

Screenshot of active window

Default:

- deactivated
- **Modifiers:** Ctrl|Alt
- **Key:** Print
- **Appliance Mode Access:** deactivated

Screenshot of entire screen

Default:

- deactivated
- **Modifiers:** Ctrl|Shift
- **Key:** Print

Switch between active windows using Task Switcher

Default:

- activated
- **Modifiers:** Ctrl|Alt
- **Key:** Tab



- **Appliance Mode Access:** deactivated

Switch between active windows using Task Switcher (backwards)

Default:

- activated
- **Modifiers:** Ctrl|Alt|Shift
- **Key:** Tab
- **Appliance Mode Access:** deactivated

Switch focus to next window

Default:

- activated
- **Modifiers:** Ctrl
- **Key:** Escape
- **Appliance Mode Access:** deactivated

Switch focus to next window (alternative)

Default:

- activated
- **Modifiers:** Ctrl|Alt
- **Key:** Up
- **Appliance Mode Access:** deactivated

Switch focus to next window (reverse order)

Default:

- activated
- **Modifiers:** Ctrl|Alt
- **Key:** Down
- **Appliance Mode Access:** deactivated

Volume down (multimedia key)

Default:

- activated
- **Modifiers:** (none)
- **Key:** XF86AudioLowerVolume

Volume mute (multimedia key)

Default:

- activated
- **Modifiers:** (none)
- **Key:** XF86AudioMute
- **Appliance Mode Access:** deactivated

Volume up (multimedia key)

Default:

- activated
- **Modifiers:** (none)
- **Key:** XF86AudioRaiseVolume



- **Appliance Mode Access:** deactivated

2.9.7 Font Services

Menu path: **Setup > User Interface > Font Services**

You can import further fonts in addition to the ones provided by IGEL:

- [XC Font Service](#)(see page 188)
- [NFS Font Service](#)(see page 188)

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.



2.10 Network

In this area, you can configure thin client network connections.

- [LAN Interfaces](#)(see page 189)
- [Mobile Broadband](#)(see page 198)
- [DHCP Client](#)(see page 200)
- [VPN](#)(see page 201)
- [SCEP Client \(NDES\)](#)(see page 208)
- [Routing](#)(see page 211)
- [Hosts](#)(see page 211)
- [Network Drives](#)(see page 212)
- [Proxy](#)(see page 214)

2.10.1 LAN Interfaces

Menu path: **Setup > Network > LAN Interfaces**

Here, you can configure the LAN interfaces.

- **Activate default interface (Ethernet)**
 - The default interface is enabled. (Default)
 - The Ethernet interface is not enabled.

i If a number of Ethernet interfaces are available, the device designated as `/dev/eth0` by Linux will be used as the default interface.

- **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 200).
- **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.
 - 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)
 - **Method for dynamic DNS registration:**
 - DHCP: Updates the terminal name through DHCP option 81.
 - DNS: Sends updates to the DNS server in accordance with RFC 2136.
 - **Private TSIG key for DNS authentication:** Path to the private key if TSIG-based DDNS registration is used.

-
- [Individual Interface](#)(see page 190)
 - [Wireless](#)(see page 193)

Individual Interface

Menu path: **Setup > Network > LAN Interfaces > [Interface]**

- **Activate default interface (Ethernet)**
 - The default interface will be enabled. (Default)
 - The Ethernet interface will not be enabled.

i If a number of Ethernet interfaces are available, the device designated as `/dev/eth0` by Linux will be used as the default interface.

- **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 200).
- **Specify an IP Address:** The IP address and the network mask are entered manually.
 - **IP Address:** IP address of the device.
 - **Network Mask:** Network mask of the device.
- **IPv6 Configuration**
 - Compatibility mode: Behavior of earlier firmware versions.
 - Disabled: IPv6 completely disabled.
 - Automatic: IPv6 auto configuration based on router advertisements (can include DHCPv6).

For further information, see [RFC 4861](#).⁹

 - DHCPv6: IPv6 configuration using DHCPv6 if router advertisements are not available.

This is mentioned in [RFC 4862 Section 5.5.2](#).¹⁰
- **Network Link Type**
 - Auto sense
 - 1000 Mb/s full duplex
 - 100 Mb/s full duplex

⁹ <https://tools.ietf.org/html/rfc4861>

¹⁰ <https://tools.ietf.org/html/rfc4862#section-5.5.2>



- 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 191)
 - [Wake-on-LAN](#)(see page 192)

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](#)
 - TLS
- **Auth Method:** For the **EAP type** PEAP, the following phase 2 authentication methods are available to choose from under **Auth Method:**
 - [MSCHAPV2](#)
 - TLS
 - GTC
 - MD5
- **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 **user name** 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 208).
 - Client certificates will not be managed with [SCEP](#)(see page 208). (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
- **Password:** Password for network access

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](#)¹¹.

- **Wake on magic packet**
 - The thin client can be started with a Wake-on-LAN magic packet. (default)
- **Wake on ARP packet**
 - The thin client can be started with a Wake on ARP packet.
 - The thin client cannot be started with a Wake on ARP packet. (default)
- **Wake on broadcast message**
 - The thin client can be started with a Wake on broadcast message.
 - The thin client cannot be started with a Wake on broadcast message. (default)
- **Wake on multicast message**
 - The thin client can be started with a Wake on multicast message.
 - The thin client cannot be started with a Wake on multicast message. (default)
- **Wake on physical activity**
 - The thin client can be started with a physical activity.
 - The thin client cannot be started with a physical activity. (default)
- **Wake on unicast message**
 - The thin client can be started with a Wake on unicast message.
 - The thin client cannot be started with a Wake on unicast message. (default)


¹¹ <https://kb.igel.com/display/endpointmgmt605/Wake-on-LAN>



Wireless

Menu path: **Setup > Network > LAN Interfaces > Wireless**

In this area, you can configure everything relating to your wireless connections.

 Configure the [wireless frequency range](#)(see page 198) 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](#)¹².

- **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 client will be obtained automatically using DHCP. (Default)
DHCP options can be specified under [DHCP Client](#)(see page 200).
- **Specify IP address:** The IP address and the network mask are entered manually
 - **IP address:** IP address of the thin client
 - **Network mask:** Network mask of the thin client
- **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](#)¹³.

- DHCPv6: IPv6 configuration using DHCPv6 if router advertisements are not available.

You will find further information in [RFC 4862 Section 5.5.2](#)¹⁴.

- **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 194) is enabled. This tool allows the user to establish a connection to a wireless network quickly. (Default)
 - The Wireless Manager is disabled.

 If you use wireless regularly, it is recommended that you enable the following options: **Tray icon, Enable context menu, Enable Wireless Manager**. Via the **Wireless Manager**, you can use [IGEL Café Wireless](#)(see page 193).

¹² <https://www.igel.com/linux-3rd-party-hardware-database/>

¹³ <https://tools.ietf.org/html/rfc4861>

¹⁴ <https://tools.ietf.org/html/rfc4862#section-5.5.2>



- [Wireless Manager](#)(see page 194)
- [Switch for the Wi-Fi Connection](#)(see page 195)
- [Default Wi-Fi Network](#)(see page 196)
- [Additional Wi-Fi Networks](#)(see page 198)
- [Wireless Regulatory Domain](#)(see page 198)

Wireless Manager

The Wireless Manager tool allows the user to connect quickly to available wireless networks.

i The Wireless Manager can be enabled under **Network > LAN Interfaces > Wireless.**

You can bring up the Wireless Manager from the tray icon for wireless:




1. Click on the tray icon for wireless and select **Manage wireless networks** from the context menu.




2. Search for available networks.
 - The list of active networks is sorted according to the quality of their signal strength.
 - Previously configured connections are flagged with a tick in the **Configured** column.
 - The connection currently active is likewise flagged with a symbol under **Connected**.



3. Double-click on a network in the list in order to open the entry mask. You can either **permanently save** the logon information or enter it each time you establish a connection to this network.

 Click on the key symbol in order to display the key phrase while you are typing.

4. Click on the **Connect network** button in order to establish the previously configured connection: The tray icon will change to show the connection quality. Hidden networks appear in the Wireless Manager with the network name empty or can be defined using the **Search for network** button. In order to connect to a previously unknown hidden network, you must first enter the SSID before the access data are retrieved:

 If you have configured the available connections, you will no longer need the Wireless Manager in order to establish a connection.

In the context menu for the tray icon, all available networks are listed and can be brought up from here.

5. The IGEL Setup shows all connections configured by the local user under **Network > LAN Interfaces > Wireless > Additional Wi-Fi Networks**.

Switch for the Wi-Fi Connection

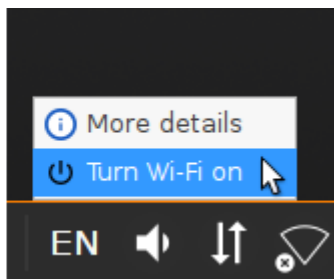
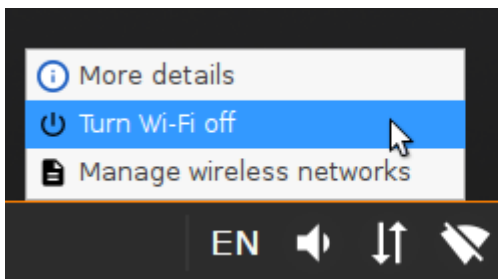
You can turn Wi-Fi off or on.

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 194](#)) 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 Personal encryption

- **Network authentication:**
 - WPA Personal: Wi-Fi Protected Access Pre-Shared Key (WPA / IEEE 802.11i/D3.0)
 - WPA Enterprise: Wi-Fi Protected Access with 802.1X authentication (WPA / IEEE 802.11i/D3.0)
 - WPA2 Personal: Wi-Fi Protected Access Pre-Shared Key (WPA2 / IEEE 802.11i/RSN)
 - WPA2 Enterprise: Wi-Fi Protected Access with 802.1X authentication (WPA2/IEEE 802.11i/RSN)
- **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
 - TLS: Transport Layer Security with client certificate
 - TTLS: Tunneled Transport Layer Security (from IGEL *Linux 10.04.100* onwards)
- **Auth Method:** Method for authentication that is available for the selected EAP type

Possible options for PEAP:

 - MSCHAPv2: Microsoft Challenge Handshake Authentication Protocol
 - TLS: Transport Layer Security with client certificate
 - GTC: Generic Token Card
 - MD5: MD5-Challenge

Possible options for TTLS:

- MSCHAPv2: Microsoft Challenge Handshake Authentication Protocol
- PAP: Password Authentication Protocol
- **Validate Server Certificate**
 - The thin client 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

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 196).

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
 - 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.

2.10.2 Mobile Broadband

Menu path: **Setup > Network > Mobile Broadband Network**

Here, you can change the settings for a modem or a surf stick. This function is available from IGEL Linux *Version 10.03.100*.






 Ensure that data traffic is adequately secured. You can do this in the following ways:

- Use a private APN.
- Use OpenVPN and block traffic that would circumvent VPN with firewall rules.


If the device is already inserted and has been configured, the network connection will be established after the thin client boots. It can take between a few seconds and around 1 minute to establish a connection. The network connection will remain in place until the surf stick is removed or the thin client is put on standby or shut down.



The status of the network connection is shown in the system tray:

-  The network connection is established; the thin client is online This symbol is only shown if "Modem" is selected as the device type. If "Router" is selected as the device type, the symbol for a LAN connection  will be shown.
-  The network connection was interrupted; the thin client is offline This symbol is only shown if "Modem" is selected as the device type. If "Router" is selected as the device type, the corresponding symbol for a LAN connection will be shown.



You can change the following settings:

- **Enable mobile broadband**
 - The mobile broadband network can be used if a supported modem is connected.
 - The mobile broadband network cannot be used. (default)
- **Device type**
Possible options:
 - **Modem:** The device will be operated as a modem. The access data can be changed with the parameters **number**, **user name**, **password**, **APN**, **network ID** and **PIN**.
 - **Router:** The device will be operated as a router. The device must be configured in advance in such a way that it is ready for use when it is inserted.

 Select the "Router" device type if you use a device from Huawei in the HiLink mode; example: Huawei E3372.

- **Number:** Access number for your network connection. If you do not know the access number, ask your mobile communications operator for it.
- **User name:** User name for your network connection. If you do not know the user name, ask your mobile communications operator for it.
- **Password:** Password for your network connection. If you do not know the password, ask your mobile communications operator for it.
- **APN:** APN (Access Point Name) for your network connection. If you do not know the APN, ask your mobile communications operator for it.
- **Network ID:** Network ID for your network connection. If you do not know the network ID, ask your mobile communications operator for it.
- **PIN:** PIN for the SIM card used.
- **Enable tray icon**
 - The current status of the network connection is shown with the symbol  or .
 - The current status of the network connection is not shown with a symbol.



- **Enable context menu**
 - If you click on  or , a context menu can be opened.
 - No context menu can be opened.
- **Enable network info dialog**
 - Via the context menu, you can bring up detailed information regarding the network connection.
 - No detailed information regarding the network connection can be brought up.
- **Enable mobile broadband configuration dialog**
 - Via the context menu, you can open a configuration dialog in order to change the access data.
 - The configuration dialog cannot be opened.

2.10.3 DHCP Client

Menu path: **Setup > Network > DHCP Client**

Here, you can change the advanced settings for the firmware's built-in DHCP client.





-
- [Standard Options](#)(see page 200)
 - [Custom Options](#)(see page 200)

Standard Options

Menu path: **Setup > Network > DHCP Client > Default Options**

- **User Class:** A freely definable character string which can serve as a criterion for allocating specific settings for the DHCP server.
- **List of standard options:** Options with which the client can request information from the DHCP server.
You will find information regarding the various DHCP options in [RFC 2132 DHCP Options and BOOTP Vendor Extensions](#)¹⁵.

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.

Custom Options

Menu path: **Setup > Network > DHCP Client > User-Defined Options**

- ▶ To create a new entry, click on  in the **List of custom options** area.

¹⁵ <https://tools.ietf.org/html/rfc2132>



i 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

2.10.4 VPN

Menu path: **Setup > Network > VPN**

Remote users securely access company networks via virtual private network protocols (VPN).

- **Enable tray icon**
 - A tray icon for the network interface will be shown. (default)
- **Enable context menu**
 - A context menu will be shown when you click on the tray icon. (default)
- **Enable network info dialog**
 - A dialog window with information regarding the network connection will be shown when you click on the context menu. (default)

-
- [OpenVPN](#)(see page 201)

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.

- **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 202)
 - [Options](#)(see page 204)
 - [TLS Options](#)(see page 205)
 - [Proxy](#)(see page 205)
 - [IPv4](#)(see page 206)
 - [Route](#)(see page 206)
 - [Desktop Integration](#)(see page 206)

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

i 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.

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.

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](#)¹⁶ which is maintained by the OpenVPN project.

- **Gateway port:** Local gateway port (default: 1194)
- **Custom renegotiation interval:** Renegotiate data channel key after given number of seconds (default: 0)
- **Use LZO data compression**
 - The client will use LZO compression. Necessary if the server uses compression.
 - The client will not use LZO compression. (default)
- **Protocol used for communication to the host**
 - udp: UDP will be used.
 - tcp-client: TCP will be used.

 If you use a proxy, select **tcp-client**.

- **Virtual network type**
 - tun: Routing will be used
 - tap: Bridging will be used.
- **Use custom tunnel maximum transmission unit (MTU):** The MTU of the TUN device will be used as a given value. The MTU of the interface will be derived from it.
- **UDP fragment size:** Allow internal data fragmenting up to this size in bytes. Leave this field empty to keep the default value.
- **Restrict tunnel TCP maximum segment size (MSS)**
 - The TCP segment size (MSS) of the tunnel will be restricted.
 - The TCP segment size (MSS) will not be restricted. (default)
- **Randomize remote hosts**
 - The remote gateways will be ordered randomly as a simple type of load balancing.
 - 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)

¹⁶ <https://openvpn.net/index.php/open-source/documentation.html>



TLS Options

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > TLS Options**

- **Subject match:** The computer will only accept connections from a computer whose X.509 name or name matches the one entered. If you leave this field empty, no check will take place.
- **Remote peer certificate TLS type**
 - Do not verify
 - Check for server certificate:
 - Check for client certificate:
- **Key file for additional TLS authentication:** As the path, enter relative to /wfs/OpenVPN or select using the file selection. This adds an additional HMAC legitimization level above the TLS control channel in order to prevent DDOS attacks.
- **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.

Proxy

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > Proxy**

Here, you can set up an optional proxy server for the VPN connection.

i 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: **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. Here, you will find the available 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] = A l t

Key combinations are formed as follows with |:

- Ctrl +  = C t r l | S u p e r _ 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 206).

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.

2.10.5 SCEP Client (NDES)

Menu path: **Setup > Network > SCEP Client (NDES)**

SCEP allows the automatic provision of client certificates via an SCEP server and a certification authority. This type of certificate is automatically renewed before it expires and can be used for purposes such as network authentication (e.g. IEEE 802.1x).

A Microsoft Windows 2008 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 \(AD CS\)](#)¹⁷

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 209)
 - [Certification Authority](#)(see page 210)
 - [SCEP](#)(see page 210)

¹⁷<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 AC.

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.

i 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.

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)

i 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.



2.10.6 Routing

Menu path: **Setup > Network > Routing**

Here, you can enter additional routes if necessary.

- **Enable:** (default: disabled)
 Routing is enabled.
- **Default gateway:** Gateway that routes the packets to the target network
- **Interface:** The network interface via which the route is to run, e.g. eth0

Routing [1-5]





- **Enable:** (default: disabled)
 This route is enabled.
- **Network route / host route:** Type of route
 - Network route: The routing relates to a (sub) network
 - Host route: The routing relates to the address of a computer
- **Network / host IP or name:** The address of the network (for a network route) or the IP address or the name of the host (for a host route)
- **Network mask:** Mask for the desired IP range, e.g. 255.255.255.0
- **Gateway:** Gateway that routes the packets to the target network
- **Interface:** The network interface via which the route is to run, e.g. eth0

2.10.7 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



2.10.8 Network Drives

Menu path: **Setup > Network > Network Drives**

Here, you can configure both the drives that are to be connected during booting and the associated login data.

- [NFS](#)(see page 212)
- [Windows Drive](#)(see page 213)





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

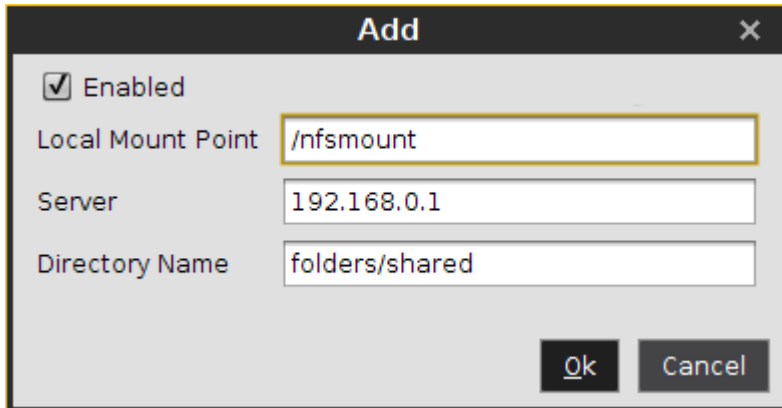
 For **Server**, you can provide an IP address, a hostname or a Fully-Qualified Domain Name (FQDN).

- **Directory name:** Path under which the NFS server exports the directory

Sample configuration entry

The picture belows shows a sample configuration entry.

 In both the **Local Mount Point** and **Directory Name** only / (Linux/Unix-style forward slash) is permitted as a path separator.







Windows Drive


Menu path: **Setup > Network > Network Drives > Windows Drive**

In this area, you can integrate network drives shared by Windows as well as those from Linux/Unix servers via the SMB protocol (Samba).

You can find a sample configuration at the end of this page.

To manage the drive list, proceed as follows:

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

Clicking  will bring up the **Add** dialogue, where you can define the following settings:

- **Enabled:** Defines whether the configuration entry will be applied.
 - The network drive will be integrated.
- **Local Mount Point:** The local directory under which the server directory is to be visible (default: /smbmount)
- **Server:** The IP address, Fully-Qualified Domain Name (FQDN) or NetBIOS name of the server.
- **Share Name:** Path name as exported by the Windows or Unix Samba host.
- **User name:** User name for your user account on the Windows or Unix Samba host.
- **Password:** Password for your user account on the Windows or Unix Samba host.
- **User writable**
 - The user can not only read but also write directory contents. Otherwise, only the local root user is able to do this.
 - The user can only read directory contents. (default)

Sample configuration entry

The following picture shows a sample configuration entry.



⚠ If a NetBios name is provided for **Server**, make sure it is not preceded by slashes, e.g. \\myComputer (wrong) vs. myComputer (correct).

ℹ 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.

2.10.9 Proxy

Menu path: **Setup > Network > Proxy**

Here, you can select the communication protocols for which a system-wide proxy server is to be used.

- **Direct connection to the Internet:** The thin client is directly connected to the Internet. No proxy is used.
- **Manual proxy configuration:** One or more proxies are used.
- **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:** Select the SOCKS protocol version (default: [SOCKS v5](#))
- **No proxy for:** List of computers to which the thin client 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 214)



- **Use passthrough authentication**
 - The temporarily saved logon information (user name and password) will be used to log on to the proxy server.
 - The logon information entered under **User name** and **Password** will be used to log on to the proxy server. (default)
- **User name:** User name for the proxy logon.
- **Password:** Password for the proxy logon.

2.11 Devices

Menu path: **Devices > Hardware Info**

- ▶ Click on **Hardware Info** to view the system information for your endpoint device.

In this area, you can make settings for the following options:

- [Printer](#)(see page 215)
- [Storage Devices](#)(see page 224)
- [Bluetooth](#)(see page 227)
- [USB Access Control](#)(see page 227)

2.11.1 Printer

Menu path: **Devices > Printers**

You can set up a printer for the thin client here.

The printers must be set up under **Devices > Printer > CUPS > Printers** and must be enabled there for mapping in sessions.

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 215)
- [LPD](#)(see page 221)
- [TCP/IP](#)(see page 221)

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
- [Printers](#)(see page 216)
- [IPP Printer Sharing](#)(see page 221)

Printers

Menu path: **Devices > Printer > CUPS > Printers**

Printers can be created and edited here.

- ▶ Click on to open the **Add** dialog.
- ▶ In the edit dialog, specify a **Printer name** which begins with a letter.

General

Printer port: Interface type for locally connected printers or the network protocol for network printers.

Possible values:

- "Parallel port printer" (default)
- "Serial port printer"
- "USB printer"
- "USB class printer"
- "LPD network printer"
- "TCP network printer"
- "IPP network printer"
- "SMB network printer"

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 218).

Manufacturer: List of possible printer manufacturers. When you select a manufacturer here, the relevant selection of models will be provided under **Printer names**. (Example: Generic)



Printer names: List of possible printer models. (Example: PostScript Printer)

Default paper size: Set the printer-specific paper size that you would like to use as a default.

Possible values:

- "Letter"
- "Legal"
- "Executive"
- "A5"
- "A4"
- "A3"
- "System setting"

Share printer

You can access the printer via the network if you have enabled the print server under **IPP Printer Sharing**; see [IPP Printer Sharing](#)(see page 221). (Default)

Mapping in sessions

Map printer in NX sessions

- The printer is available in NX sessions.
- The printer is not available in NX sessions. (Default)

Map printer in Parallels Client sessions

- The printer is available in Parallels Client sessions.
- The printer is not available in Parallels Client sessions. (Default)

Map printer in ICA sessions

- The printer is available in ICA sessions. (Default)

Map printer in RDP sessions

- The printer is available in RDP sessions. (Default)

Use Windows driver name from list

- A driver name from the following list will be used. (Default)


Manufacturer: List of possible printer manufacturers. (Example: Generic)

Model: List of possible models. (Example: Generic PostScript)

Use custom Windows driver name

- Enter the name of your driver here if it is not mentioned in the list above.

Printer driver: Windows driver name for the printer.

 The name must not contain “,” or “.”.

When printing in ICA and RDP sessions, the print data are normally prepared for the printer model by the Windows printer driver and are passed unchanged from the device to the printer. An exception is made when using the Windows driver in ICA sessions, **Manufacturer** is set to "Generic" and **Model** is set to "Generic PostScript." In this



case, the print data are prepared on the device with the help of the printer driver defined above under **Printer** for the printer model. This requires device resources.

Settings to Be Configured for Each Printer Port Type

Menu path: **Devices > Printer > CUPS > Printers**

Here, you can find the parameters available for configuration for each **Printer Port (Devices > Printer > CUPS > Printers > Add > General > Printer port)**.

Printer Port: "Parallel port printer"

Parallel device:

- "LPT1"
- "LPT2"

Detect devices...: Opens a dialog for selecting the available devices.

Printer Port: "Serial port printer"

Serial device:

- "COM1"
- "COM2"
- "USB COM1"
- "USB COM2"

Detect devices...: Opens a dialog for selecting the available devices.

Baud rate:

- "9600"
- "19200"
- "38400"
- "57600"
- "115200"

Character size:

- "5"
- "6"
- "7"
- "8"

Parity:

- "None"
- "Even"
- "Odd"

Flow control:

- "None"
- "XON/XOFF"
- "RTS/CTS"
- "DTR/DSR"

Printer Port: "USB printer"



USB device:

- "1st USB printer"
- "2nd USB printer"

Detect devices...: Opens a dialog for selecting the available devices.

Printer Port: "USB class printer"

If you use a lot of different printer models attached via USB, you can assign printer models to CUPS printers without specifying dependencies to a specific USB port. Instead, the USB printer is assigned by matching patterns specified under **Manufacturer pattern** and **Product pattern** with the specific model name. A single printer definition can thus work for a class of different USB printer models.

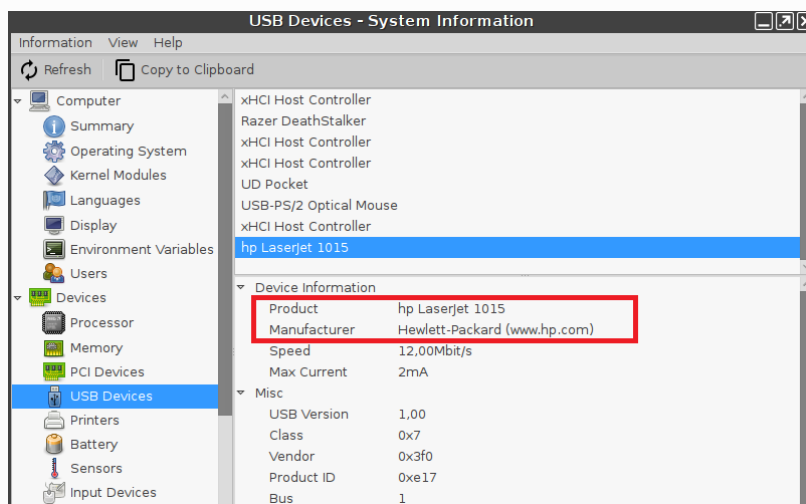
Pattern matching mode: Specifies the type of the search pattern.

- "pattern": Standard wildcards are used for pattern matching, e.g. "*", "?". The matching is case sensitive. For detailed information on wildcards, see man7.org¹⁸ and tldp.org¹⁹.
- "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.org²⁰ and tldp.org²¹.

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.

i Manufacturer and product names can be found in the accessories under **Devices > USB Devices > System Information**.



Click to see examples...

¹⁸ <http://man7.org/linux/man-pages/man7/glob.7.html>

¹⁹ <http://www.tldp.org/LDP/GNU-Linux-Tools-Summary/html/x11655.htm>

²⁰ <http://man7.org/linux/man-pages/man7/glob.7.html>

²¹ <http://www.tldp.org/LDP/GNU-Linux-Tools-Summary/html/x11655.htm>



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 234).

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 234) and [Shared Workplace](#)(see page 236).

Single sign-on authentication is not used. (Default)

SMB user name: User name used for authentication. (Optional)

SMB password: Password used for authentication. (Optional)



IPP Printer Sharing


Menu path: **Devices > Printer > CUPS > IPP Printer Sharing**

The IPP (Internet Printing Protocol) offers the following configuration options:

Network or host for sharing local printers: Access to the printer is possible from this network or host.

Possible options:

- "None"
- "Local network": Allows printing on the local device from the local network.

 This can also be given in the form 192.0.2.* or 192.0.2.0/24 or *.domain.com or 192.0.2.1 or host.domain.com.

- "Global": Allows printing on the local device from the global network.

LPD

Menu path: **Setup > Devices > Printers > LPD**

LPD printers are used by the BSD printing system and are also supported by *Windows* servers.

- **Enable LPD Print Server**

Local printers are provided in the network as LPD printers. The thin client is made the LPD print server. The CUPS printers defined under [Printers](#)(see page 216) 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. Consurent 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 222)



- [Additional Serial Ports](#)(see page 222)
- [LPT 1](#)(see page 224)
- [USBLP 1](#)(see page 224)

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)

2.11.2 Storage Devices

Menu path: **Setup > Devices > Storage Devices**

Configure your hotplug storage devices here.

Show attached storage devices: Shows a list with registered storage devices.

-
- [Storage Hotplug](#)(see page 224)
 - [Options](#)(see page 226)

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 224).
 - 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. 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.

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 226).



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 Citrix Global setup area under [Drive mapping](#)(see page 46), in the Devices area under [USB access control](#)(see page 227) and in the Accessories area under [Disk Removal](#)(see page 148).

Options

Menu path: **Setup > Devices > Storage Devices > Options**



In this area, you can specify a directory in which external storage devices are accessible to the user. The devices are always mounted in the `/media` directory.

User browse directory

- The directory defined under **Browse directory** is linked to the `/media` directory. (Default)

Browse directory/: Local directory in which the devices can be found. (Default: `userhome/media`)

Support for built-in floppy drives

- Built-in disk drives are active.
- Built-in disk drives are disabled (default)

 This option is only valid for drives which are not connected via USB.

2.11.3 Bluetooth

Menu path: **Devices > Bluetooth**

In this area, you can set up a Bluetooth service.

Bluetooth

- The Bluetooth service is active. The Bluetooth Tool can be used.
- The Bluetooth service is inactive. The Bluetooth Tool cannot be used. (Default)

Tray Icon

- A Bluetooth icon will be shown in the system tray. You can launch the Bluetooth Tool by double-clicking on the Bluetooth icon. Right-clicking on the Bluetooth icon will bring up an overview as to which Bluetooth devices are connected to the thin client and you can enable or disable Bluetooth.
- A Bluetooth icon will not be shown in the system tray. (Default)

Details of the settings options for Bluetooth can be found under **Accessories > Bluetooth Tool**(see page 137).

Here you can find information on the [Bluetooth Wizard](#)(see page 27).

2.11.4 USB Access Control

Menu path: **Devices > USB Access Control**

You can allow or prohibit the use of USB devices on your endpoint. Specific rules for individual devices or device classes are possible.

Enable

- USB access control is enabled and the following settings can be configured.
- USB access control is inactive. (Default)

Default rule: Specifies whether the use of USB devices is allowed or prohibited.

- [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. For an example, see [How to Configure USB Access Control](#)(see page 13).

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

i To find out the **Vendor ID** and **Product ID** of the connected USB device, use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal. You can also use the **System Information** tool, see [Using “System Information” Function](#)(see page 144).

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 224).

2.12 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](#)(see page 229).

-
- [Password](#)(see page 229)
 - [Logon](#)(see page 231)
 - [Active Directory/Kerberos](#)(see page 238)
 - [Smartcard](#)(see page 239)

2.12.1 Password

Menu path: **Setup > Security > Password**

You can assign four different authorization levels:

Administrator: The administrator has full access to the IGEL Setup.

i The assignment of the administrator password is a prerequisite for all other rights assignments. Even if the administrator wants to leave the administration of the Setup to the Setup administrator, the administrator password must be set.

An administrator password protects the following critical actions/areas from unauthorized access:

- the [local terminal](#)(see page 94)
- the [virtual console access](#)(see page 168).

Setup Administrator: A user to whom rights are assigned for minor administrative tasks. You specify which pages the setup administrator can edit under **Accessories > Setup > Page Permissions Setup Administrator**.

Setup User: A user who can make some unlocked user settings in the Setup. You specify which pages the setup user can edit under **Accessories > Setup > Page Permissions Setup User**.

User: This user has no access to the Setup. A user password is required in the following cases:

- when logging on to the [terminal session](#)(see page 94)
- when logging on to sessions (see Desktop Integration)
- for unlocking the [screenlock](#)(see page 177)

If you have defined passwords for different authorization levels, a login window appears at the start of the Setup in which you can select an authorization level.



i When entering a password, ensure that the correct [keyboard layout](#)(see [page 183](#)) is enabled.

Administrator

Use password

- A password is needed to log in as administrator (`root`).
 - A password is also needed for the user, the Setup user and the Setup administrator.
 - The password is set by clicking **Change password**.
- No password is needed to log in as an administrator. Also, no password is needed for the user (`user`), the Setup user and the Setup administrator. (default)

Change password: Sets the password for the administrator (`root`).

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

Enable setup administrator access: This option is relevant if an administrator password is set.

- The Setup administrator can access the areas of the Setup for which he has authorization.
 - A password is needed to log in as Setup administrator.
 - The password is set by clicking **Change password**.
 - Further information can be found under [Page authorizations](#)²².
- Setup administrators cannot access the Setup. (default)

Change password: Sets a new password for Setup administrators.

Setup User

Enable user access: This option is relevant if an administrator password is set.

²² <https://kb.igel.com/display/igelos/User+Page+Permissions>



The user can access the areas of the Setup for which they have authorization. Further information can be found under [Page authorizations](#)²³.

- A password is needed to log in as a setup user.
- The password is set by clicking **Change password**.

The user cannot access the *IGEL* setup. (default)

Change password: Sets the password for the setup user.

User

Use password: This option is relevant if an administrator password is set.

The user (user) needs a password in order to log in to the thin client via the local terminal. The password is set by clicking **Change password**.

If an administrator password is set, the user (user) cannot log in to the thin client via the local terminal.

If no administrator password is set, the user (user) can log in to the thin client via the local terminal without a password. (default)

Change password: Sets the password for the user (user).

User account for remote access

Enable login

The remote user (ruser) can log in to the thin client via SSH.

Further information can be found under [Remote access](#)²⁴. (default)

Logging in via SSH is not possible.

Use password

A password is needed to log in via SSH.

No password is needed to log in via SSH. (default)

- ▶ By clicking **Change password**, set up a user password.

2.12.2 Logon

Menu path: **Setup > Security > Logon**

-
- [IGEL Smartcard](#)(see page 232)
 - [Taskbar](#)(see page 232)
 - [Active Directory/Kerberos](#)(see page 234)
 - [Shared Workplace](#)(see page 236)

²³ <https://kb.igel.com/display/igelos/User+Page+Permissions>

²⁴ <https://kb.igel.com/display/igelos/Remote+Access>



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.

 Save the settings before starting to personalize the card.

Start application to write IGEL smartcards:

Smartcard personalization: Opens a window where you can set a login password and add sessions to the card.

 Session configurations are stored on the card's integrated circuit, and the session can be used on any IGEL device that reads the card.

 Smartcard personalization is possible via the local Setup only. The option is not available via the UMS.

For further information about the smartcard personalization function, see [Using "Smartcard Personalization" function](#)(see page 157).

For information on how to create IGEL smartcards via the UMS, see [Authentication with IGEL Smartcard](#)(see page 232).

See also [Third-Party Smartcard Readers Supported by IGEL Smartcards](#)(see page 232).

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)

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 195) or the [Wireless Manager](#)(see page 194) 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 238).

i 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)



i 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. Here, you will find the available modifiers and the associated key symbols:

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


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

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super_L

Key: Key for the hotkey

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

Shared Workplace

Menu path: **Setup > Security > Logon > Shared Workplace**



- **Activate IGEL Shared Workplace**
 - You can log in to the thin client via IGEL Shared Workplace.
 - You cannot log in to the thin client via IGEL Shared Workplace. (Default)
- **Skip IGEL Shared Workplace login if UMS server is unavailable**
 - If the *UMS* server is not available, the user can log in via Active Directory/Kerberos. In order to do this, logging in via Active Directory/Kerberos must be configured; further information can be found under [Active Directory/Kerberos](#)(see page 234).
 - 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`)



2.12.3 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 238)
 - [Domain Realm Mapping](#)(see page 239)

Domain 1 ... Domain 4

Menu path: **Setup > Security > Active Directory/Kerberos > Domain 1 ... Domain 4**

Up to 4 domains where a logon 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.

2.12.4 Smartcard

Menu path: **Setup > Security > Smartcard**

Here, you can define settings for logging on using a smartcard.

-
- [Services](#)(see page 239)
 - [Middleware](#)(see page 241)

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](#)²⁵.
See also [Third-Party Smartcard Readers Supported by IGEL Smartcards](#)(see page 239).

²⁵ <https://www.igel.com/linux-3rd-party-hardware-database/>



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:

- "auto": The first network interface with IPv4 address will be used if **Bind 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. Example: "eth1" if the second Ethernet interface (**Network > LAN Interfaces > Interface 2**) has to be used.

i The Ethernet and WLAN interfaces can be configured under **Network > LAN Interfaces**. See [LAN Interfaces](#)(see page 189).

Bind IP: The IP address used for the proxy.

Possible options:

- "auto": The first network interface with an IPv4 address will be used if **Bind interface** is set to "auto".
- Free text entry: The manually entered IP address will be used instead of the network interface specified under **Bind interface**.

HTTPS server port: The TCP port for the HTTPS server. (Default: 443)

SICCT announce IP: The IP address to send the SICCT announce messages to.

Possible options:

- "broadcast": SICCT announce messages are sent in a broadcast procedure, i.e. to all devices on the network.
- 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

Menu path: **Security > Smartcard > Middleware**

Here, select the middleware (PKCS#11 module) which matches your card or your token. The middleware selected here will be used for the following logins:

- Login to Citrix sessions; see [Citrix Global](#)(see page 43)
- Login to Citrix StoreFront; see [Citrix StoreFront](#)(see page 55)
- Login to thin client via Active Directory; see [Active Directory/Kerberos](#)(see page 238)

The PKCS#11 module can be provided via a Custom Partition. For building a Custom Partition, see [Custom Partition Tutorial](#)(see page 241).

The following options are available:

Coolkey: The middleware Coolkey is used.

OpenSC: The middleware OpenSC is used.

Custom PKCS#11 module: The PKCS#11 module stored under the **Path to the library** is used. See also [Using a Custom PKCS#11 Library](#)(see page 241).

Path to the library: Path to the custom PKCS#11 module

2.13 System

Menu path: **Setup > System**

You can configure basic system settings here.

-
- [Time and Date](#)(see page 241)
 - [Update](#)(see page 242)
 - [Remote Management](#)(see page 244)
 - [Remote Access](#)(see page 246)
 - [Power Options](#)(see page 249)
 - [Firmware Customization](#)(see page 252)
 - [Registry](#)(see page 269)

2.13.1 Time and Date

Menu path: **Setup > System > Time and Date**

- **Timezone Continent/Area:** Continent/Area for your location
Possible values:
 - General: Under **Location**, you can select a time zone.
 - Africa... Pacific: Under **Location**, you can select a city for the selected continent/area.
- **Location:** Select your location or time zone.



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 \(Daylight Saving Time, DST\)](#)²⁶ FAQ.

2.13.2 Update

Menu path: **Setup > System > Update**

Here, you can configure settings for the system update.

-
- [Firmware Update](#)(see page 242)
 - [Buddy Update](#)(see page 243)

Firmware Update

Menu path: **Setup > System > Update > Firmware Update**

Here, you can specify how the device obtains updates for its own firmware.

i **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
 - 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)

²⁶ <https://kb.igel.com/pages/viewpage.action?pageId=23501185>



- 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.

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
- 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 display](#)(see page 243) how-to.


2.13.3 Remote Management

Menu path: **Setup > System > Remote Management**

Here, you can configure settings relating to the remote administration of the client using the Universal Management Suite (UMS).

- **Enable remote management**
 - The thin client can be managed via the UMS. (default)
 - Remote management is not allowed.
- **Universal Management Suite:** If the client is registered on a UMS server, its IP address or host name will be shown in the list.

 The list can contain more than one UMS instance. If the client cannot contact a UMS server under the host name `igelrmsrver`, and the DHCP option 244 is not set, the client 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 thin client 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.

Possible values:

 - No time limit: 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 thin client.
- **Prompt user on UMS actions**
 - The user will be informed via a message window if the client receives new settings from the UMS or is shut down. (default)
 - The user will not be informed if the client receives new settings from the UMS or is shut down.
- **Timeout:** Number of seconds for which the notification window is shown (default: 20)

Possible values:

 - No time limit: 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 thin client into a directory in accordance with the UMS directory rules.
- **UMS Registration:** This button opens the [UMS Registration](#)(see page 119) program from the accessories.
Further information regarding the use of structure tags can be found in the how-to [Using Structure Tags](#)²⁷.

-
- [Options](#)(see page 245)

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.

²⁷ <https://kb.igel.com/display/endpointmgmt605/Using+Structure+Tags>



- 1 ... 120 seconds

2.13.4 Remote Access

Menu path: **Setup > System > Remote Access**

In order to allow central administration, the thin client can be configured in such a way that it can be accessed via the WAN.

-
- [SSH Access](#)(see page 246)
 - [Shadow](#)(see page 247)
 - [Secure Terminal](#)(see page 248)

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

Menu path: **Setup > System > Remote Access > Shadow**

For helpdesk purposes, you can observe the client through shadowing. This is possible via the IGEL UMS or another VNC client (e.g. TightVNC).

⚠ For Remote Working, Use Secure Shadowing

If the endpoint device is in a mobile or work-from-home environment, it is highly recommended to use secure shadowing only. Regular shadowing without encryption poses a security risk.

i The user can terminate the VNC connection at any time by clicking on the **End shadowing** button.

- **Allow remote shadowing:**
 - Desktop content can be viewed from remote computers with VNC software.
 - VNC shadowing is not allowed. (default)

You can change the following settings:


- **Secure mode**
 - Communication will be secured via SSL/TLS and shadowing will only be possible for *UMS* administrators.
 - Communication will not be secured via SSL/TLS. (default)

Further information regarding secure shadowing can be found in the [Secure Shadowing²⁸ How-To](#).
- **Use password**
 - The remote user must enter a password before shadowing can begin.
 - The remote user does not require a password for shadowing. (default)
- **Password:** Password for the VNC connection
- **Prompt user to allow remote session**

²⁸ <https://kb.igel.com/pages/viewpage.action?pageId=23500626>



- The local user will be asked for permission before shadowing. (default)
- The local user will not be asked for permission.

 In a number of countries, for example, Germany, unannounced shadowing is prohibited by law. Do not disable this option if you are in one of these countries!

- **Allow user to disconnect remote shadowing**


- A button with which the user can terminate the connection is shown. (default)

- **Allow input from remote**

- The remote user can make entries using the keyboard and mouse as if they were the local user. (default)

- **Scale frame buffer**

- The screen content of the shadowed client is reduced or enlarged by the **scaling factor** before being transferred.

 Further parameters for the VNC server on the client are accessible in the *IGEL* registry (**Setup > System > Registry > network.vncserver**).

- The screen content is transferred in the original size. (default)

- **Scale factor:** Factor by which the screen content of the shadowed client is enlarged or reduced (default: 1.0)

Secure Terminal

Menu path: **Setup > System > Remote Access > Secure Terminal**

You can establish a secure terminal connection to a thin client.

The thin client must meet the following requirements:


- The firmware of the thin clients is *IGEL Linux Version 5.11.100* or higher or *IGEL Linux Version 10.01.100* or higher.

For IGEL Linux Version 5.11.100 and 10.03.100:

1. In the thin client setup, go to **System > Remote Access > Secure Terminal**
2. Enable **Secure Terminal**

For IGEL Linux Version 10.01.100 or newer:

- Enable the following options in the thin client registry:
 - **network > telnetd > enabled > allow telnet access**
 - **network > telnetd > secure_mode > secure telnet**

 You can allow access via the secure terminal for all registered thin clients. To do this, enable the **UMS Administration > Global Configuration > Remote Access > Enable Global Secure Terminal** option.



2.13.5 Power Options

Menu path: **Setup > System > Power Options**

In this area, you will find the settings for energy management.

-
- [System](#)(see page 249)
 - [Battery](#)(see page 250)
 - [Display](#)(see page 251)
 - [Shutdown](#)(see page 251)

System

Menu path: **Setup > System > Power Options > System**

Here you can configure the settings for standby and for the CPU power plan.

System suspend/shutdown on inactivity: Specify how long the user can be inactive before the system switches to standby mode or shuts down, dependent on the option selected under **System action on inactivity**.

Possible values:

- [Never](#)
- After 1 minute
- ...
- After 24 hours

System action on inactivity

Possible options:

- Suspend: The system is set to standby mode after the timeout defined with **System suspend/shutdown on inactivity** has expired.
- Shutdown: The system is shut down after the timeout defined with **System suspend/shutdown on inactivity** has expired.

Without dialog

The user is not asked if the system is to be set to the standby mode.

The dialog will be shown. (Default).

Dialog timeout: Time in seconds, for which the dialog is to be displayed. (Default: 10 seconds)

CPU Power Plan: Specify here which CPU power plan (CPU Governor) the device is to use in battery mode and in AC mode.

- **On Battery:**
 - High Performance: full performance with maximum processor speed
 - Balanced (Smooth): slower regulation of performance in a balanced manner according to the demands of programs. Suitable for users who are bothered by the fan frequently running at high speed.
 - Balanced (Recommended): rapid regulation of performance according to the demands of



programs.

Power Saver: lowest processor speed

- **Plugged in:**

- High Performance

- Balanced (Smooth)

- Balanced (Recommended)

- Power Saver

Tray Icon

A CPU icon will be shown in the system tray. This makes it easy to switch between power plans.

No CPU icon will be shown. (Default)

Battery

Menu path: **Setup > System > Power Options > Battery**

In this area, you can define the rechargeable battery messages.

Battery Notification

- **Critical battery level (percentage):** Percentage of remaining battery charge deemed critical (default: 5)
- **Critical battery action:** Action to be taken in the event of a critical battery level
Possible options:
 - Do nothing
 - Show warning
 - Run command
 - Run command in terminal
- **Critical command:** Command that is executed when a critical charge level is reached (example: Shutdown)
- **Low battery level (percentage):** Percentage of remaining battery charge deemed low (default: 10)
- **Low battery action:** Here you can specify what action is to be taken in the event of a low battery level.
Possible options:
 - Do nothing
 - Show warning
 - Run command
 - Run command in terminal
- **Low command:** Command that is executed when a low charge level is reached (example: Shutdown)

Battery Tray Icon

- **Display percentage:**
 - The percentage of remaining energy is shown in the taskbar. (default)
- **Display time**



- The estimated remaining battery life is shown in the taskbar.
- The estimated remaining battery life is not shown. (default)

Display

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)

2.13.6 Firmware Customization

Menu path: **Setup > System > Firmware Customization**


You can configure the firmware according to your needs.


- [Custom Partition](#)(see page 252)
- [Custom Application](#)(see page 255)
- [Custom Commands](#)(see page 259)
- [Corporate Design](#)(see page 262)
- [Environment Variables](#)(see page 267)
- [Features](#)(see page 269)

Custom Partition

Menu path: **Setup > System > Firmware Customization > Custom Partition**

In IGEL OS, a custom data partition is available for use as required. A download/update function that loads data from a server and, where appropriate, updates them can be set up for this custom storage area.

 The IGEL Support Team offers support for the deployment of Custom Partitions. However, it is not possible to offer support for any third-party software that is installed on a Custom Partition.

 If the device is reset to the default settings (factory reset), the custom partition and all data stored on it will be deleted.



- [Partition](#)(see page 253)
- [Download](#)(see page 253)

Partition


Menu path: **Setup > System > Firmware Configuration > Custom Partition > Partition**





Here, you can create a partition of your own.

- **Enable partition**

- The customer partition is enabled in the *IGEL Setup* of the thin client or with the *IGEL Universal Management Suite* via the setup path.
- The customer partition is not enabled. (default)

- **Size:** Size of the partition in bytes. The value can have the following multiplicative endings:
 - k for kilobytes
 - K for kibibytes
 - m for megabytes
 - M for mebibytes
 - g for gigabytes
 - G for gibibytes

 Sensible figures are for example 100 K (for 100 KiB = 100 * 1024 bytes) or 100 M (for 100 MiB = 100 * 1024 * 1024 bytes). The size of the partition should be set to at least 100 KiB. However, no more than 300 MiB should be reserved for the customer-specific partition (based on the 1 GB standard CF used in IGEL Linux thin clients). This is because subsequent firmware updates may require more storage space than the current version.

- **Mount point:** Path on which the partition is to be mounted. (default: /custom)
- **Partitions parameters:** From IGEL OS *Version 10.03.100*, you can enter name value pairs which are passed on to the custom partition for further processing.
To manage the list, proceed as follows:
 - Click  to create a new parameter.
 - Click  to remove the selected parameter.
 - Click  to edit the selected parameter.
 - Click  to copy the selected parameter.

Add

- **Name:** Name of the parameter
- **Value:** Value of the parameter

Download





Menu path: **Setup > System > Firmware Configuration > Custom Partition > Download**



Sources for partition data

In order to load data onto the custom partition, at least one source for partition data must be set up here.

To manage the list, proceed as follows:

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

Add

- **Automatic update**
 - The contents from this source will be updated automatically.
 - The contents from this source will not be updated automatically. (default)
- **URL:** URL of the web server
- **User name:** User name for access to the web server
- **Password:** Password for access to the web server
- **Initialization action:** Action which is performed after mounting the partition (program or script with absolute path). For example, a program downloaded to the partition can be launched.
- **Finalizing action:** Action which is performed before mounting the partition (program or script with absolute path). For example, a program downloaded to the partition can be ended.

The transfer protocols are the same as the ones for updating the firmware, e.g. HTTP and HTTPS. An INF file which in turn references a tar archive zipped using bzip2 must be referenced as the target.

The structure of the INF file is as follows:

[INFO], [PART]	Header information
file="test.tar.bz2"	File name of the compressed tar archive
version="1"	Version number - a higher version results in an update if Update automatically is enabled.

The files to be transferred must therefore be zipped in a tar archive which is then compressed using bzip2. This file is referenced in the INF file which is the target of the URL.

The tar archive can be created under Windows, e.g. with the open source program 7-Zip (www.7-zip.de²⁹). 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.


²⁹ <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 257).

- ▶ 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. Here, you will find the available modifiers and the associated key symbols:

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


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

- [Alt] = Alt

Key combinations are formed as follows with |:

- Ctrl +  = Ctrl | Super_L

Key: Key for the hotkey

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

Autostart

- The session will be launched automatically when the device boots.

Restart

- The session will be relaunched automatically after the termination.

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

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

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

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

Autostart requires network

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



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

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see [Appliance Mode](#)(see page 255).

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 257)
- [Desktop Integration](#)(see page 257)


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. Here, you will find the available 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



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 257).

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 267) in the commands.

-
- [Post Session](#)(see page 260)
 - [Base](#)(see page 261)
 - [Network](#)(see page 261)



- [Desktop](#)(see page 262)
- [Reconfiguration](#)(see page 262)

Post Session

Menu path: **Setup > System > Firmware Customization > Custom Commands > Post Session**

For a specific session type, you can define an action that is performed when the last session of this type is ended.

Session type: Session type for which the action is performed.


Possible values:

- [No post-session command](#)
- Citrix
- Citrix via Browser
- RDP
- VMware Horizon
- Browser
- NoMachine NX
- Parallels Client
- PowerTerm terminal emulation
- ThinLinc
- X session
- IBM iAccess
- Media player
- VNC viewer

Post session command: Action that is carried out after the end of the session 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 232), [Active Directory / Kerberos](#)(see page 234) and [Smartcard](#)(see page 239).

 The “Logoff” option cannot be used if the Appliance Mode is in use. Further information can be found under [Appliance Mode](#)(see page 260).

- **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 251).
- **Shutdown/suspend (system default action without dialog):** The device will be shut down or placed in a standby mode depending on the setting under **System > Power Options > Shutdown > Default action** selection. The user cannot cancel the procedure.
- **Reboot (with dialog timeout):** The device will reboot. A dialog allowing the user to cancel the procedure will be shown in the process.
- **Reboot (without dialog):** The device will reboot. The user cannot cancel the procedure.
- **Enter custom command here:** Command to be executed.



Base

Menu path: **Setup > System > Firmware Customization > Custom Commands > Base**

The commands defined here are executed on a one-off basis during the boot procedure. You can define commands for the execution times described below:

- **Initialization**
 - Not all drivers loaded, not all devices available
 - Network scripts not launched, network not available
 - Partitions available except *firefox profile, scim data, ncp data, custom partition*
- **Before session configuration**
 - Not all drivers loaded, not all devices available
 - Network scripts launched, network not available
 - Partitions available except *firefox profile, scim data, ncp data, custom partition*
 - Sessions not configured
- **After session configuration**
 - All drivers loaded, all devices available
 - Network available
 - Partitions available except *custom partition*
 - System daemons not launched (CUPS, ThinPrint etc.)
 - Sessions configured
 - UMS settings retrieved but not yet effective
- **Final initialization command**
 - All partitions available
 - All system daemons launched
 - UMS settings effective

Network

Menu path: **Setup > System > Firmware Customization > Custom Commands > Network**

The commands defined here are executed each time that the relevant network interface (default: `eth0`) starts. The network interface can be selected with the `$INTERFACE` environment variables (`eth0, eth1, wlan0`). You can define commands for the execution times described below:

- **Network initialization**
 - Network authentication successful (802.1x or WPA)
 - No further network settings used
- **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 thin client settings (local setup, UMS)

Corporate Design

Menu path: **Setup > System > Firmware Customization > Corporate Design**

In this area, settings options allowing you to adapt the user interface to your company layout are grouped together.

You can place your own logo in the following places:

- [Custom Bootsplash](#)(see page 263)
- [Background \(1st/2nd Monitor\)](#)(see page 264)
- [Company Logos](#)(see page 266)

Please also see our [Customizing IGEL Linux Desktop](#)³⁰ How-To.

³⁰ <https://kb.igel.com/display/igelos/Customizing+IGEL+Linux+Desktop>



Custom Bootsplash

Menu path: **Setup > System > Firmware Configuration > Corporate Design > Custom Bootsplash**

With a boot splash, you can show your company logo or a specific image during the booting procedure. The boot splash will be shown instead of the console messages.

Please note: You need to provide an image file for your custom boot splash on a download server.

i The file types BMP, JPG, GIF, TIF, PNG and SVG are supported for a boot splash. 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 boot splash

- **Enable custom boot splash**
 - You can make the following settings in order to configure a custom boot splash.
 - No custom boot splash is configured. (default)

Custom boot splash - Server Location

- **Use firmware update server location**
 - The server configuration will be carried over from the [firmware update](#)(see page 242).
 - You can carry out a custom configuration below. (default)
- **Protocol:** Access method for the image
 - HTTP: Download from a web server.
 - HTTPS: Download from a TLS/SSL-secured web server.
 - FTP: Download from an FTP server.
 - Secure FTP: Download via SSH-secured FTP.
 - FTPS: Download from a TLS/SSL-secured FTP server.
 - FILE: The image file lies in the thin client file system, possibly as a shared NFS or Windows update. You can choose the location simply by selecting a file below.
- **Server name:** Name or IP address of the server
- **Port:** Port of the server on which the service is provided
- **Server path:** Path to the directory with the image file on the server
- **User name:** User name on the server
- **Password:** Password for the user account on the server

Custom Bootsplash - Settings

- **Custom boot splash file:** File name of the custom image
As regards positioning, the following applies: 0 = left-justified, 50 = centered, 100 = right-justified
- **Custom Boot splash Style:**
 - Original
 - Stretched
 - Scaled



- Zoomed
- **Background color:** Use the color picker to choose.
- **Horizontal position of the boot splash image** (default: 50)
- **Vertical position of the boot splash 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/2nd 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 [Custom Wallpaper Server](#)(see page 265).

i 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.

i 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 236)
- 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 265). If you have already defined a server for the system update files, you can use the same server settings for downloading the background image.

Custom Wallpaper 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 242).
 - 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

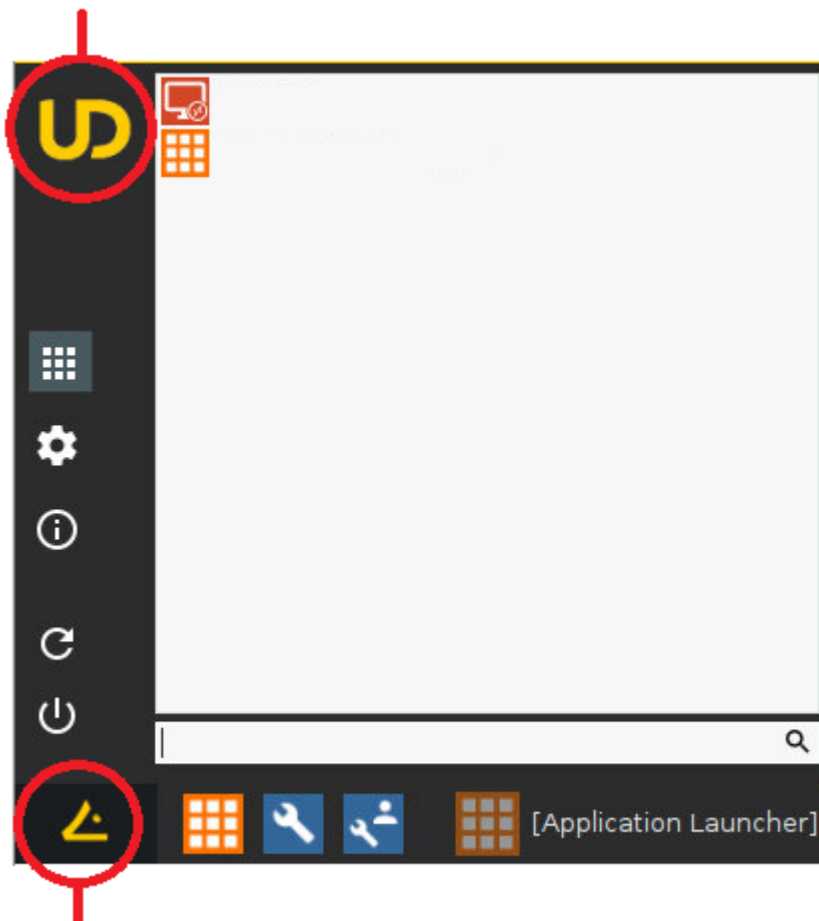
- **Start button icon:** File name with full path to select your logo as the icon for the start menu in the taskbar. Size: 32x32 pixels



- **Company logo in start menu:** File name with full path to show your company logo in the start menu window. Size: 64x64 pixels

 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 259).

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 268)
 - [Additional](#)(see page 268)


Predefined

Menu path: **System > Firmware Customization > Environment Variables > Predefined**

- **Variable name:** Name for the variable
- **Value:** Value for the variable

To use environment variables in sessions, proceed as follows:

1. Enable environment variables under **System > Firmware Customization > Environment Variables > Enable variable substitution in session.**
2. Define the variable name and content, e.g.
 - **Variable name:** SERVERNAME
 - **Value:** testServer
3. Enter the variable name in the parameter field of the session with the \$ symbol before it. Example: \$SERVERNAME

 In the case of RDP and ICA sessions, the value is entered in the session file after saving. With XenApp, the setting is not implemented until a session starts and is running.

Additional

Menu path: **System > Firmware Customization > Environment Variables > Additional**

You can define other variables in addition to the 10 predefined ones.

- **Variable name:** Name for the variable
- **Value:** Value for the variable




Features

Menu path: **System > Firmware Customization > Features**

Using this list of available services, you can quickly enable or disable firmware components such as Media Player, Extra Font Services, etc. By deactivating e.g. unused features, you can save storage space.

If a service was disabled, the associated session type will no longer be available when the system is restarted. Existing sessions will no longer be shown but will not be deleted either.

For further information, see [Disabling Features to reduce Firmware Size](#)(see page 269).

 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.

2.13.7 Registry

Menu path: **System > Registry**

In the registry, you can change virtually any firmware parameter. You will find information on the individual items in the tooltips.

 Changes to the registry should only be made by experienced administrators. Incorrect parameter settings can easily destroy the configuration and cause the system to crash. In cases like these, the only way to restore the functionality is to reset the device to the factory defaults!

Search parameter...: Search for setup parameters in the registry.

- **Search criterion:** Criterion for searching.

The following can be selected:

- Parameter name
- **Parameter name:** Any search term.
- Logical search restriction:
 - Contains
 - Exact match
 - Use regular expressions

- **Ignore case**

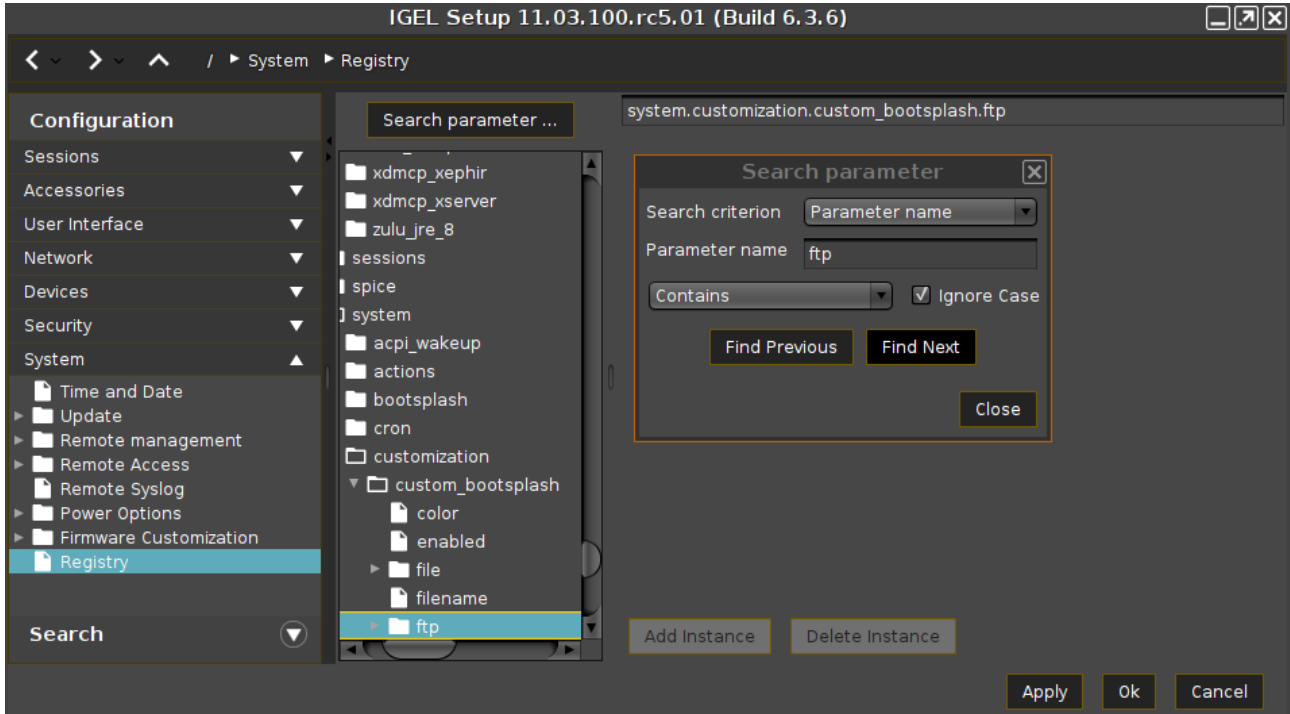
- **Find previous:** Go back if there are a number of hits.

- **Find next:** Go forwards if there are a number of hits.

Example: If you would like to find the FTP settings for updating the Linux firmware, you can search



for the parameter name ftp. The parameter found in the registry structure is highlighted. Click on **Find next** until you find your desired parameter:



Add instance: Adds instances. This is possible with parameters which have a percent sign as their last character, e.g. nfyMount%. The new instances are numbered consecutively: nfyMount1, nfyMount2 etc.

Delete instance: Deletes a previously added instance.



3 IGEL OS(RPI4) Release Notes

- [Notes for Release 11.01.110](#)(see page 271)

3.1 Notes for Release 11.01.110

Software:	IGEL OS(RPI4) Version	11.01.110
Release Date:	2021-02-18	
Release Notes:	Version	RN-1101110-1
Last update:	2021-02-24	

- [Supported Devices 11.01.110](#)(see page 271)
- [Component Versions 11.01.110](#)(see page 271)
- [Known Issues 11.01.110](#)(see page 273)
- [New Features 11.01.110](#)(see page 274)
- [Resolved Issues 11.01.110](#)(see page 277)

3.1.1 Supported Devices 11.01.110

- NComputing RX420 (UC3-RPI4)

3.1.2 Component Versions 11.01.110

Clients

Product	Version
Chromium	86.0.4240.197-rpt1
Citrix Workspace App	20.06.0.15
Citrix Workspace App	20.10.0.6
Citrix Workspace Hub	19.11.100.297
Open VPN	2.4.4-2ubuntu1.3
Zulu JRE	8.48.0.51-2

Smartcard

PKCS#11 Library OpenSC	0.20.0-3igel37
Reader Driver ACS CCID	1.1.6-1igel2
Reader Driver MUSCLE CCID	1.4.31-1igel10



Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.8.26-3igel14

System Components

OpenSSL	1.0.2n-1ubuntu5.4
OpenSSL	1.1.1-1ubuntu2.1~18.04.6
OpenSSH Client	7.6p1-4ubuntu0.3
OpenSSH Server	7.6p1-4ubuntu0.3
Bluetooth Stack (bluez)	5.52-1igel6
MESA OpenGL Stack	20.2.3-1igel128
VDPAAU Library Version	1.4-1igel1003
Graphics Driver FBDEV	0.5.0-1igel1012
Graphics Driver VESA	2.4.0-1igel1010
Input Driver Evdev	2.10.6-1igel1011
Input Driver Synaptics	1.9.1-1ubuntu1igel1009
Input Driver Wacom	0.36.1-0ubuntu2igel1017
Kernel	Linux version 5.9.3-v8~IGEL #1
Xorg X11 Server	1.20.8-2igel1055
CUPS Printing Daemon	2.2.7-1ubuntu2.8igel32
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel12
XFCE4 Window Manager	4.14.2-1~18.04igel1595331607
ISC DHCP Client	4.3.5-3ubuntu7.1
NetworkManager	1.18.0-1ubuntu5igel92
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 1.x	1.18.1-1igel272
WebKit2Gtk	2.28.4-0ubuntu0.18.04.1
Python2	2.7.17
Python3	3.6.9

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.17-3igel5
Mobile Device Access USB (imobile)	1.2.1~git20191129.9f79242-1+b1igel8
Mobile Device Access USB (gphoto)	2.5.25-3igel5



Services

Service Partitions	Size	Services
Java SE Runtime Environment	129.5M	Java SE Runtime Environment
Citrix ICA	59.2M	Citrix Workspace Hub Citrix Workspace app Citrix StoreFront
Internet Printing Protocol (CUPS)	21.8M	Printing (Internet printing protocol CUPS)
Multimedia Codecs	2.8M	Multimedia Codecs
Hardware Video Acceleration	256.0K	Hardware Video Acceleration
Extra Fonts	1.0M	Extra Font Package
Local browser (Chromium)	127.5M	Local Browser (Chromium)
Limited Support Features	256.0K	Limited Support Features Mobile Device Access USB (Limited support)
Mobile Device Access USB	512.0K	Mobile Device Access USB (Limited support)

3.1.3 Known Issues 11.01.110

Citrix

- **Adding smartcard readers during the session** does not work. The reader is visible, but cannot be used due to permanently unknown reader status.
- **Kerberos passthrough authentication** is not supported.
- **Citrix Workspace Hub** CitrixCasting is **limited to 1920x1200** FullHD resolution.
- **Limitations** while running Citrix sessions **with enabled hardware acceleration** (H.264):
 - Notifications are not visible.
 - UMS enhanced messages are not visible.
 - In-session or Citrix toolbar is not visible.
 - Toggle between local windows is not possible.
 - The maximum supported resolution is 2 x 1920x1200 FullHD. There are display corruptions with higher resolutions.
 - Rotated screens are not supported.
 - The Citrix session is not visible via shadowing.
- Workaround: **Disable hardware-accelerated H.264 codec:**

IGEL Setup	Sessions > Citrix > Citrix Global > Codec
Parameter	Accelerated H.264 Deep Compression Codec
Registry	ica.hw-accelerated-h264-codec
Value	enabled / disabled

Base system



- **Custom bootsplash** configuration is not supported.

X11 system

- It is not possible to **hotplug monitors while the system is running**. Monitors must be already connected when boot.

Network

- Wake on Lan is currently not supported on this platform.

3.1.4 New Features 11.01.110

Hardware

- Added support for **Raspberry Pi revision 1.4**
- Reworked **naming for audio outputs**

Citrix

- Integrated **Citrix Workspace Hub 19.11** and **WSH Chrome 0.0.3**
- Added option to **enable Workspace Hub**:

IGEL Setup	Sessions > Citrix > Citrix Workspace Hub > Options
Parameter	Citrix Workspace Hub (Beta)
Registry	ica.workspacehub.enable
Value	<u>disabled</u> / enabled

- Added a **"friendly name" configuration** for the Workspace Hub device. The **empty string** as a default will be **replaced by the hostname** of the device:

Parameter	Friendly name for Workspace Hub device
Registry	ica.workspacehub.friendlyname
Value	(empty string, default)

- Added **autostart** of **WSH Chrome Launcher**. If enabled, using TC Setup Workspace Hub is also activated.

IGEL Setup	Sessions > Citrix > Citrix Workspace Hub > Options
Parameter	Autostart Citrix Workspace Hub Launcher
Registry	sessions.workspacehub0.autostart
Value	<u>disabled</u> / enabled

- Added **default launcher page URL**:

IGEL Setup	Sessions > Citrix > Citrix Workspace Hub > Options
Parameter	URL for default launcher page
Registry	sessions.workspacehub0.launcher.page1.url
Value	<u>Default launcher page</u> /"https://myworkprod0.cloud.com"/"https://www.igel.com"/"Enter url here..."

- Added **flag to activate a QR code** at the launcher page/s:

IGEL Setup	Sessions > Citrix > Citrix Workspace Hub > Options
Parameter	Display QR code



Registry	sessions.workspacehub0.launcher.page1.qrcode
Value	<u>enabled</u> / disabled

- Added hint to **size the QR code**:

IGEL Setup	Sessions > Citrix > Citrix Workspace Hub > Options
Parameter	QR code size
Registry	sessions.workspacehub0.launcher.page1.qcodesize
Value	small / <u>medium</u> / large

- Added hint to **position the QR code**:

IGEL Setup	Sessions > Citrix > Citrix Workspace Hub > Options
Parameter	QR code position
Registry	sessions.workspacehub0.launcher.page1.qrcodeposition
Value	top left / top right / bottom left / bottom right / <u>center</u>

- Added **URL** for a **second launcher page**:

IGEL Setup	Sessions > Citrix > Citrix Workspace Hub > Options
Parameter	URL for a second launcher page
Registry	sessions.workspacehub0.launcher.page2.url
Value	<u>Disabled</u> / Default launcher page/"https://myworkprod0.cloud.com"/"https://www.igel.com"/"Enter url here..."

- Added URL for a **third launcher page**:

IGEL Setup	Sessions > Citrix > Citrix Workspace Hub > Options
Parameter	URL for a third launcher page
Registry	sessions.workspacehub0.launcher.page3.url
Value	<u>Disabled</u> / Default launcher page/"https://myworkprod0.cloud.com"/"https://www.igel.com"/"Enter url here..."

- Integrated **Citrix Workspace app 20.10**

The performance of the Citrix Workspace app was improved and a more detailed logging was implemented.

- New feature added with this release: **multiple audio devices could be mapped** inside the sessions.

Parameter	Multiple Audio Device support
Registry	ica.module.vdcamversion4support
Value	<u>disabled</u> / enabled

- Integrated **centralized Citrix logging** in IGEL OS, so only one parameter is needed to activate logging.

Parameter	Enable logging for Citrix sessions
Registry	ica.logging.debug



Value	off / on
-------	----------

- Since Workspace app 20.09, the tool **setlog** is **used to configure the logging**. For this purpose, parameters are provided in the registry **ica.logging.setlog**, but usually nothing needs to be changed.
- Added automatic configuration of the **Citrix webcam redirection in ICA** sessions.

IGEL Setup	Sessions > Citrix > Citrix Global > HDX Multimedia
Parameter	Automatic HDX webcam configuration
Registry	ica.igel_hdxwebcam.enabled
Value	disabled / <u>enabled</u>
Parameter	Resolution grade
Registry	ica.igel_hdxwebcam.quality
Range	[Very low] [Low] [<u>Normal</u>] [High] [Very high] [Best]
Parameter	Minimal frame rate
Registry	ica.igel_hdxwebcam.framerate
Value	20

- Added configuration for **H264 encoding in the Citrix webcam redirection**:

Parameter	HDX Webcam H264 encoding
Registry	ica.wfclient.hdxh264inputenabled
Value	<u>disabled</u> / enabled
- Added configuration for **native H264 encoding provided by webcam** and used in the Citrix webcam redirection. This parameter **requires** the **ica.wfclient.hdxh264inputenabled** to be set to **"true"**.

Parameter	HDX Webcam H264 native
Registry	ica.wfclient.hdxh264enablenative
Value	<u>disabled</u> / enabled

Chromium

- Updated **Chromium** to version **86.0.4240.197-rpt1**. **Hardware-accelerated video decoding** is **disabled by default** now.

Firmware update

- Added support for the **IGEL automatic update service**.

Registry	update.service.enable
Value	<u>enabled</u> / disabled

Boot

- Boot mode selection during power on:
 - Hold **power button** for '**Emergency boot (setup only)**'
 - Press hotkey '**Ctrl + Space**' for '**Reset to defaults**'
 - Press hotkey '**Ctrl + V**' for '**Verbose boot**'



3.1.5 Resolved Issues 11.01.110

Citrix

- On Citrix sessions with **H.264 HW-Acceleration** (default), **TransparentKeypassThrough=Remote** at ALLRegions . ini is enabled to ensure **all window manager keypress events are directed** to the Citrix session.
- Added new parameter **AckDelayThresh**: Max time (in milliseconds) between sending "resource free" message if any resources free. Default=350

Parameter	AckDelayThresh
Registry	ica.module.AckDelayThresh
Type	Integer
Value	<u>350</u>

- Added new parameter **AudioBufferSizeMilliseconds**: Audio buffer size, in ms. Default=200 ms

Parameter	AudioBufferSizeMilliseconds
Registry	ica.module.AudioBufferSizeMilliseconds
Type	Integer
Value	<u>200</u>

- Added new parameter **AudioLatencyControlEnabled**: Enables latency control. Default=False

Parameter	AudioLatencyControlEnabled
Registry	ica.module.AudioLatencyControlEnabled
Type	Boolean
Value	<u>false / true</u>

- Added new parameter **AudioMaxLatency**: Sets the maximum latency (in ms) before trying to discard audio data. Default=300 ms

Parameter	AudioMaxLatency
Registry	ica.module.AudioMaxLatency
Type	Integer
Value	<u>300</u>

- Added new parameter **AudioLatencyCorrectionInterval**: Defines how often to correct the latency (in ms). Default=300 ms

Parameter	AudioLatencyCorrectionInterval
Registry	ica.module.AudioLatencyCorrectionInterval
Type	Integer
Value	<u>300</u>

- Added new parameter **AudioTempLatencyBoost**: Sets the higher latency band (in ms) above the lower **PlaybackDelayThresh** band. Default=300 ms

Parameter	AudioTempLatencyBoost
Registry	ica.module.AudioTempLatencyBoost
Type	Integer
Value	<u>300</u>



- Added new parameter **CommandAckThresh**: Number of free client command buffers causing a "resource free" message to be sent to the server. Default=10

Parameter	CommandAckThresh
Registry	ica.module.CommandAckThresh
Type	Integer
Value	<u>10</u>

- Added new parameter **DataAckThresh**: Number of free client data buffers causing a "resource free" message to be sent to the server. Default=10

Parameter	DataAckThresh
Registry	ica.module.DataAckThresh
Type	Integer
Value	<u>10</u>

- Added new parameter **MaxDataBufferSize**: Maximum size of each data buffer. Default=2048 bytes

Parameter	MaxDataBufferSize
Registry	ica.module.MaxDataBufferSize
Type	Integer
Value	<u>2048</u>

- Added new parameter **NumCommandBuffers**: Number of client buffers to use for audio commands. Default=64

Parameter	NumCommandBuffers
Registry	ica.module.NumCommandBuffers
Type	Integer
Value	<u>64</u>

- Added new parameter **PlaybackDelayThresh**: Delay (in ms) between being asked to start audio playback and actually starting audio playback in order to build up a backlog of sound. Default=150

Parameter	PlaybackDelayThresh
Registry	ica.module.PlaybackDelayThresh
Type	Integer
Value	<u>150</u>