

Universal Desktop Linux v5

User Manual



IGEL[®]
UNIVERSAL
DESKTOP

Important Information

Please note some important information before reading this documentation.

Copyright

This publication is protected under international copyright laws. All rights reserved. With the exception of documentation kept by the purchaser for backup purposes, no part of this manual – including the products and software described in it – may be reproduced, manipulated, transmitted, transcribed, copied, stored in a data retrieval system or translated in any form or by any means without the express written permission of IGEL Technology GmbH.

Copyright © 2016 IGEL Technology GmbH. All rights reserved.

Trademarks

IGEL is a registered trademark of IGEL Technology GmbH.

Any other names or products mentioned in this manual may be registered trademarks of the associated companies or protected by copyright through these companies. They are mentioned solely for explanatory or identification purposes, and to the advantage of the owner.

Disclaimer

The specifications and information contained in this manual are intended for information use only, are subject to change at any time without notice and should not be construed as constituting a commitment or obligation on the part of IGEL Technology GmbH. IGEL Technology GmbH assumes no responsibility or liability for any errors or inaccuracies that may appear in this manual, including any pertaining to the products and software described in it. IGEL Technology GmbH makes no representations or warranties with respect to the contents thereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose.

IGEL Support and Knowledge Base

If you have any questions regarding an IGEL product and are already an IGEL customer, please contact your dedicated sales partner first. Er beantwortet gerne Ihre Fragen rund um alle IGEL-Produkte.

If you are currently testing IGEL products or your sales partner is unable to provide the help you need, please fill in the support form after logging on at the <http://www.igel.com/de/mitgliederbereich/anmelden-abmelden.html>.

We will then contact you as soon as possible. It will make things easier for our support staff if you provide us with all the information that is available. Please see also our notes regarding support and service information. Please visit our *IGEL Knowledge Base* <http://edocs.igel.com/> to find additional Best Practice and How To documentation as well as the *IGEL Support-FAQ* (<http://faq.igel.com>).

Contents

Important Information	2
1. IGEL Linux user manual	6
2. IGEL Universal Desktop Firmware	8
2.1. Supported formats and codecs	8
3. Quick Installation	9
4. The IGEL Linux desktop	10
4.1. Application Launcher	12
5. Boot Procedure	14
5.1. Boot Menu	14
5.2. Network Integration	16
5.3. X-Server	16
6. Setup Application	17
6.1. Starting the Setup	17
6.2. Ending the Setup	17
6.3. Setup Areas	18
6.4. Enable setup pages for users	19
6.5. Quick setup	19
6.6. Setup Search	20
7. Sessions	21
7.1. Desktop Integration	21
7.2. Citrix Receiver Selection	22
7.3. HDX / ICA Global	22
7.4. Legacy ICA Sessions	32
7.5. Citrix StoreFront / Web Interface	36
7.6. Citrix Self-Service	40
7.7. Citrix Access Gateway	41
7.8. RDP Global	42
7.9. RDP Session	51
7.10. Remote Desktop Web Access	53
7.11. Horizon Client Global	59
7.12. Horizon Client session	62
7.13. vWorkspace Client and AppPortal	66
7.14. Appliance Mode	67
7.15. Leostream Connection Broker	72
7.16. Systancia AppliDis Client	73
7.17. Evidian AuthMgr	73
7.18. NoMachine NX	73
7.19. X Session	74
7.20. Parallels 2X client session	74
7.21. PowerTerm WebConnect	74

7.22.	PowerTerm terminal emulation.....	75
7.23.	IBM iSeries Access.....	76
7.24.	ThinLinc	76
7.25.	SSH Session	82
7.26.	VNC Viewer	83
7.27.	VERDE session	83
7.28.	Firefox browser	83
7.29.	Media Player	101
7.30.	Java Web Start Session	104
7.31.	VoIP Client.....	105
8.	Accessories.....	111
8.1.	ICA Connection Center.....	111
8.2.	Local Terminal	111
8.3.	Change Smartcard Password	111
8.4.	Setup Session	111
8.5.	Quick Settings Session.....	112
8.6.	Display switch	112
8.7.	Application Launcher	115
8.8.	Sound Mixer.....	116
8.9.	System Log Viewer	117
8.10.	UMS Registration	117
8.11.	Touchscreen calibration.....	118
8.12.	Task Manager.....	119
8.13.	Screenshot tool	121
8.14.	Soft keyboard.....	124
8.15.	Java Control Panel.....	124
8.16.	Monitor Calibration.....	125
8.17.	Commands	125
8.18.	Network Diagnostics	125
8.19.	System Information.....	127
8.20.	Disk Utility	127
8.21.	Firmware Update	128
8.22.	Smartcard Personalization	128
8.23.	Identify Monitors	129
8.24.	Upgrade License.....	129
8.25.	Webcam Information.....	130
8.26.	Image viewer.....	131
9.	User Interface.....	132
9.1.	Screen.....	132
9.2.	Desktop	140
9.3.	Language	146
9.4.	Screen Saver and Screen Lock.....	147
9.5.	Input.....	150
9.6.	Hotkeys	156
9.7.	Font Services	157

10.	Network	159
10.1.	Mobile broadband network	159
10.2.	LAN interfaces	160
10.3.	Proxy	178
11.	Devices	179
11.1.	Printers	179
11.2.	USB Storage Devices	182
11.3.	Smartcard	184
11.4.	USB access control	185
12.	Security	187
12.1.	Password	187
12.2.	Login Options	187
12.3.	AD/Kerberos Configuration	192
13.	System Settings	193
13.1.	Time and Date	193
13.2.	Update	194
13.3.	Buddy Update	195
13.4.	Remote management	195
13.5.	Shadow	196
13.6.	Remote Access (SSH / RSH)	201
	Power Options	201
	13.7. Firmware Customization	206
	13.8. IGEL System Registry	217
14.	Index	218

1. IGEL Linux user manual

About this document

All illustrations and descriptions in this manual relate to the current version of the IGEL Linux firmware; this manual is subdivided into the following sections:

- *Quick installation* (page 9): Setting up the thin client for the first time
- *Boot procedure* (page 14): Boot menu, network integration, X-Server
- *Application Launcher* (page 12): Important system data such as the firmware version, list of applications, licensed services, system tools
- *Setup application* (page 17): Setting up sessions and system configuration
- *Sessions* (page 21): Creating and configuring application sessions
- *Accessories* (page 111): Session accessories, card readers, sound control, Java Manager, network tools
- *User interface* (page 132): Language, screen, entry options, font services
- *Network* (page 159): Interfaces, protocols, authentication, drives
- *Devices* (page 179): Hardware, printers, storage devices, interfaces
- *Security* (page 187): Password, logging on, AD/Kerberos configuration
- *System* (page 193): System setting options
- *Firmware configuration* (page 206): Customer-specific partition, applications, commands, start screen, environment variables, features
- *IGEL Smartcard* (page 188): Company keys, saving a user/password/session, testing a card

Formatting and meanings

The following formatting is used in the document:

<i>Hyperlink</i>	Internal or external links
Proprietary names	Proprietary names of products, firms etc.
GUI text	Items of text from the user interface
Menu > Path	Menu paths in systems and programs
Entry	Program code or system entries
<u>Keyboard</u>	Commands that are entered using the keyboard

➡ Reference to other parts of the manual or other eDocs articles.



Note regarding operation



Warning: Important note which must be observed

What is new in 5.09.100?

You will find the release notes for IGEL Linux 5.09.100 as a text file next to the installation programs on our download server and in our Knowledge Base E-Docs.

- New *Citrix Self-Service* (page 40) session type: Allows access to Citrix StoreFront or Web Interface services via the Citrix Self-Service interface. Citrix Receiver 13 is required for this.
- New sessions in the Appliance Mode:
 - *Citrix Self-Service* (page 68)
 - *Caradigm* (page 70)
- *GeNUCard WiFi* (page 172): Wireless access for the VPN Appliance can now be configured.
- *Application Launcher* (page 114): Specific areas can be hidden.
- *Display Switch* (page 112): Includes new functions such as left-handed mode and rotate monitor.
- *ThinLinc session user interface* (page 81), *ThinLinc global options* (page 77) and *ThinLinc session options* (page 80): Access to specific tabs in the ThinLinc client options as well as server-side access to local smartcards can be set. Update to ThinLinc 4.5.
- *Authentication* (page 57): Applications can be launched automatically after logging on; these applications can be selected in the IGEL setup.
- *VoIP client settings* (page 110): Configuration changes made in the VoIP client can be saved in the IGEL setup.
- *Mobile broadband network* (page 159): A mobile network connection via UMTS can be established using the Huawei E3531 HSPA+ surf stick.

2. IGEL Universal Desktop Firmware

IGEL thin clients comprise the latest hardware and an embedded operating system. Depending on the product, this operating system may be based on IGEL Linux or Microsoft Windows Embedded Standard.

The firmware included with every IGEL Universal Desktop product is multifunctional and contains a wide range of protocols allowing access to server-based services. The IGEL Universal Desktop firmware is available on the basis of two possible operating systems.

Depending on the operating system, the following options are available:

Options	IGEL Linux	Windows Embedded Standard 7
Ericom Powerterm terminal emulation	✓	✓
IGEL Shared Workplace	✓	✓
IGEL Universal MultiDisplay	✓	
Codec package	✓	

Management software: Universal Management Suite

For optimum management of your IGEL thin clients, the IGEL Universal Management Suite (UMS) is available on our *download page* http://myigel.biz/index.php?dir=IGEL_UNIVERSAL_MANAGEMENT_SUITE/.



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

2.1. Supported formats and codecs

IGEL Linux supports the following multimedia formats and codecs out of the box:

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

The following codecs are licensed via the separately available Multimedia Codec Pack:

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




AC3 is not licensed.



IGEL Zero Clients (IZ series) have the Multimedia Codec Pack installed by default.

3. Quick Installation

To install the thin client in your network environment, proceed as follows:

1. Connect the thin client as follows to the necessary devices and the network:
 - Monitor (VGA, DVI, DisplayPort)
 - AT-compatible keyboard with PS/2 or USB connection
 - USB mouse
 - LAN via RJ45 plug connection
2. Connect the thin client to the power supply.
3. Start the thin client and wait until the graphical user interface has loaded.
4. Click on  in the taskbar.
5. Specify the system language and keyboard layout under **User Interface > Language**.
6. Specify the resolution and the number of screens under **User Interface > Display**.
7. If you would like to specify the IP address manually, enter it in the **Network > LAN Interfaces** section.
8. Click on **OK** to confirm your changes.

The device will restart if necessary and will use the new settings thereafter.



A handy tool tip is available for virtually every setting. If you would like to know more about a setting or option, move your mouse pointer over it and wait for a moment. You can configure the behavior of tool tips under **User Interface > Desktop**. Further information can be found under *Desktop* (page 140).




4. The IGEL Linux desktop

You can operate the thin client via the taskbar and the IGEL menu.



Figure 1: IGEL Linux desktop

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

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



Symbol for sessions: Launches a session.

3

Window bar

Window buttons

Allows you to switch between open windows.

4

System tray



CPU energy saving plan: Changes the energy saving settings.



Volume control



Allows you to remove a USB stick safely



Local network connection



Pager: Allows you to switch between a number of virtual desktops



Time



Show desktop

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 thin client



- Allows you to restart the thin client

4.1. 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

- **Applications**
- **System**
- **License**
- **Information** regarding the system
- **Network information**

4.1.1. Information

On the **About** page, you will find the following data:

- **Product:** Information regarding the installed firmware
- **Network:** Computer name, hardware address and IP address of the thin client
- **Hardware:** Device type, CPU model etc.
- **Licensed Features:** All firmware features for which a license is available

4.1.2. 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 **Execute**.

Alternatively, you can launch sessions via icons on the desktop, in the Quick Start Panel or from the start menu and context menu.

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



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

4.1.3. System

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

The following tools are available:

- **Disk Utility:** Shows information regarding connected USB drives.
- **Display Switch:** Switches between a number of screens.
- **Firmware Update:** Carries out the update with the settings configured during the setup.
- **Identify Monitors:** Shows the monitor's number and manufacturer details.
- **Network Tools:** Provides detailed information on the network connection and offers a number of problem analysis tools such as Ping or Traceroute.
- **Safely Remove Hardware:** Removes external storage devices without a risk of losing data.
- **Screenshot Tool:** Takes photos of the screen content.
- **Setup:** Launches the IGEL Setup.
- **Smartcard Personalization:** Allows access data and sessions which are to be available to a smartcard user to be written to an IGEL smartcard.
- **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.
- **Taskmanager:** Manages all processes.
- **Touchscreen Calibration:** Allows a connected touchscreen monitor to be calibrated.
- **UMS Registering:** Logs the thin client on to a UMS server (access data for the server are required).
- **Upgrade License:** Reads a new license file from the USB stick and modifies the functions of the firmware accordingly.
- **Webcam Information:** Shows data relating to a connected webcam and allows the camera to be tested.

4.1.4. License

You will find the following here:

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

4.1.5. Network Information

The **Network information** tool allows you to read out data from your local network connections and check the availability of a UMS server:

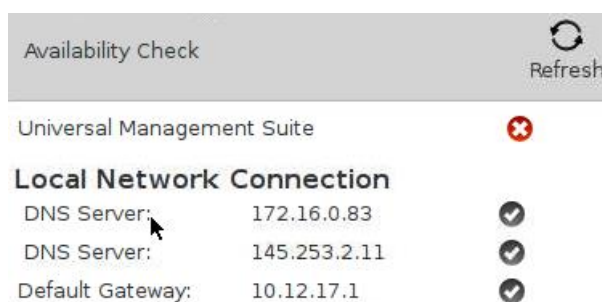


Figure 2: Network information

4.1.6. Shutting Down and Restarting a Device

Within the **Application Launcher** you will find two buttons for **Reboot** and **Shutdown**. 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**.

5. Boot Procedure

The quick installation procedure is complete.

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

5.1. Boot Menu

- During the boot procedure, press the **ESC** key in the **Secondstage Loader** when the **Loading Kernel** message is shown on the screen.

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

- **Quiet Boot (page 14):** Normal boot
- **Verbose Boot (page 14):** Boot with system messages
- **Emergency Boot (page 15):** Setup only
- **Failsafe Boot (page 15):** With CRC check
- **Reset to Factory Defaults (page 15):** Resets the thin client to the default factory settings

5.1.1. Quiet Boot

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

5.1.2. Verbose Boot

Unlike in **Quiet Boot** mode, the boot messages are shown in **Verbose Boot** mode. A diagnostics shell is also available. This can be used to execute common commands (such as `ifconfig` etc.) when searching for and rectifying faults.

- Enter `init 3` to close this shell.

The boot procedure will then resume.

5.1.3. Emergency Boot

Emergency Boot is a setup with default parameters.

If you select **Emergency Boot**, the Secondstage Loader looks for a bootable system in the flash memory and then resumes the boot procedure as in the other boot modes.

Essentially speaking, the X-Server is started without network drivers and with a resolution of 1024 x 768 - 60 Hz during an **Emergency Boot**. The **Setup** menu is then opened directly.

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

5.1.4. Failsafe Boot - CRC check

During a **Failsafe Boot**, a check of the file system is carried out first. The thin client then starts in **Verbose Mode**.

5.1.5. Reset to factory defaults

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



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

Do you know the password?

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

Do you not know the password?

1. Confirm the warning message.
2. When you are prompted to enter the password, press the Enter key three times.
3. Press .

The Terminal Key will appear.

4. Contact us using the IGEL Service RMA form.
5. Enter the Terminal Key shown, the firmware version and your contact details.

Our service department will send you a so-called Reset to Factory Defaults Key specially for your device. To ensure that the process is as straightforward and yet as secure as possible, each key is valid for just one device.



See also the *Resetting a Thin Client with Unknown Administrator Password FAQs* (<http://edocs.igel.com/index.htm#10203461.htm>).

5.2. Network Integration

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

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

Depending on the terminal settings, choose between

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



The network interface can be stopped and restarted on the Linux Console (accessible via **Ctrl+Alt+F11**) with this command:

```
/etc/init.d/network stop  
/etc/init.d/network start
```

5.3. X-Server

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

6. Setup Application

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



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

6.1. Starting the Setup

You can open the setup in the following ways:

- Double-click on **Setup** in the **Application Launcher**
- or click on **Execute**.
- Double-click on **Setup** 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 **Setup** 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.

6.2. Ending 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.

6.3. Setup Areas

The setup application comprises the following main areas:

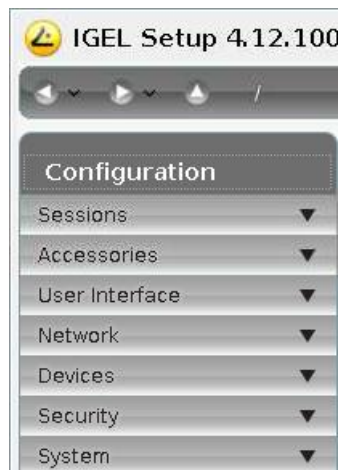


Figure 3: Setup areas

Sessions: Allows you to configure application sessions such as ICA, RDP, PowerTerm, browser and others

Accessories: Allows you to configure various local tools - setup pages for the local shell (Terminal), sound mixer, screen keyboard (for touchscreen monitors), options for the **Application Launcher** and the setup application itself.

User interface: Allows you to configure display settings, entry devices, hotkey commands etc.

Network: Allows you to configure all network settings for LAN/WLAN interfaces and the dial-up connections

Devices: Allows you to configure various devices

Security: Allows you to set the administrator/user passwords and user authorizations etc.

System: Allows you to set various basic system parameters including the date and time, information regarding the firmware update, remote management etc.

➤ Click on one of the areas to open up the relevant sub-structure.

The tree structure allows you to switch between the setup options.

Three navigation buttons are available. The buttons allow you to move back and forth between the setup pages you have visited or reach the next level up within the structure.

You will find a more detailed description of the individual setup options elsewhere. This is merely a brief overview.

6.4. Enable setup pages for users

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* (page 187)). 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. 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 session, the password for the **setup user** will not be enabled in this case.

2. Under **Accessories > Setup > User Page Permissions**, enable those areas to which the user is to have access.
 - A check in the checkbox indicates that the node is visible in the setup.
 - A green symbol (open lock) indicates that the user is able to edit the parameters on this setup page.

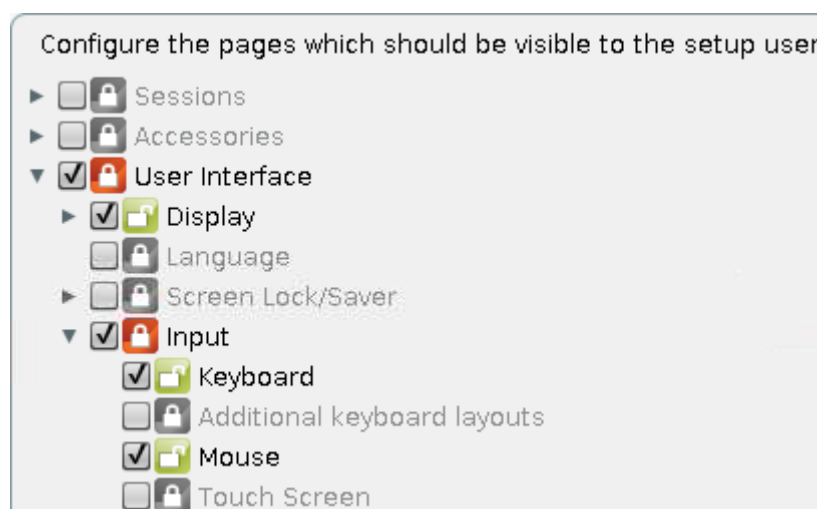


Figure 4: Restricted access to the setup



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).

6.5. Quick setup

To create a quick setup session, proceed as follows:

1. Under **Setup > Security > Password**, enable the password for the administrator.



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 **Setup > Accessories > Quick Setup**, define the name and the options for bringing up the quick setup.
3. Under **Setup > Accessories > Quick Setup > User Page Permissions**, enable those areas to which the user is to have access.



You can set up a hotkey in order to launch quick setup in the appliance mode. You will find instructions for setting up the hotkey under *Desktop Integration* (page 21).

6.6. 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.

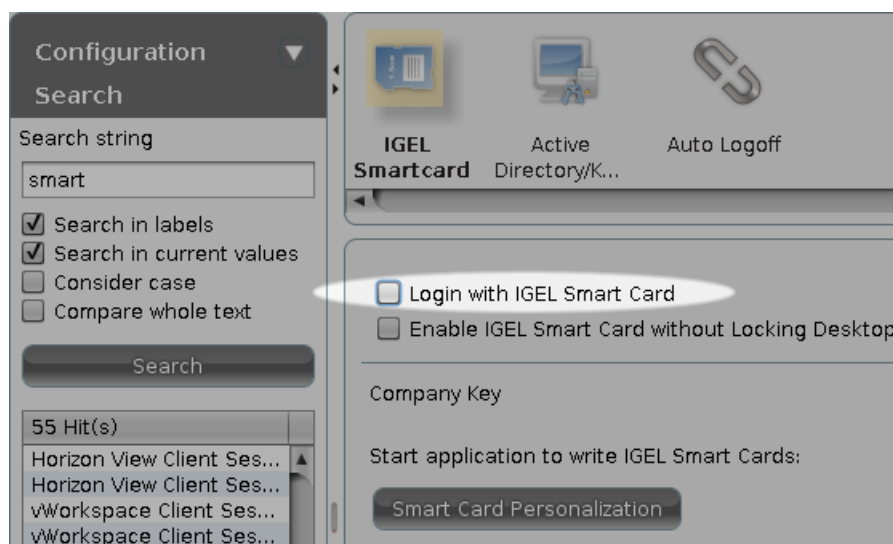


Figure 5: Setup search

7. Sessions

Application sessions can be created and configured in the **Sessions** sub-structure of the IGEL setup application. The **Session Overview** provides an overview of all available session types and existing sessions.

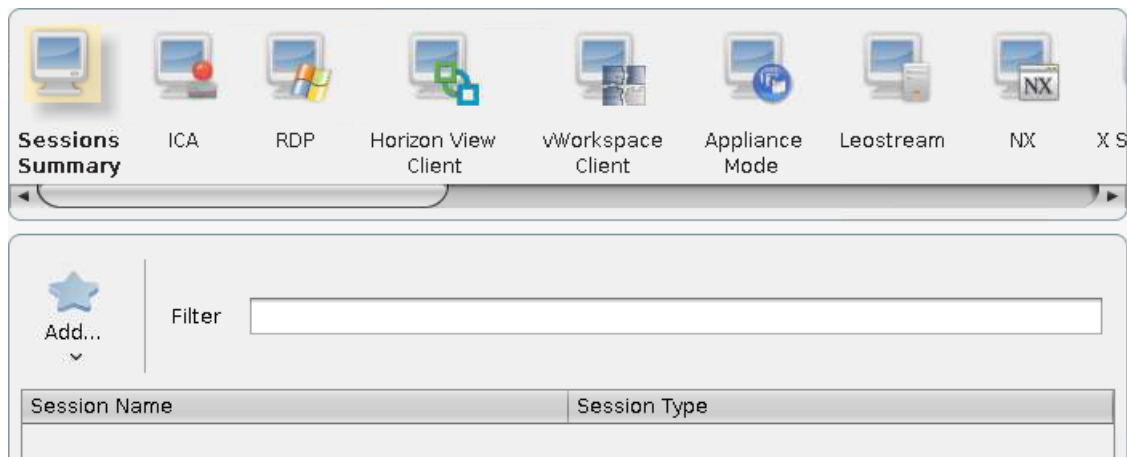


Figure 6: Session overview

- Click on **Add...** to create a new session.



Disabled functions are not shown in the drop-down list.



A number of session functions require the optional Multimedia Codec Pack. This applies in particular to the playback and redirecting of multimedia content. Details can be found in the IGEL Linux Features that Require the Multimedia Codec Pack FAQs.

7.1. Desktop Integration

For each session, there is a **desktop integration** configuration page on which the following actions can be performed:

- Determining the **appearance** of the session on the local desktop.
- Setting up the **name** of the session.



The session name must not contain any of these characters:

\ / : * ? " < > | [] { } ()

- Selecting the **session launch options** (autostart, restart).
- Enabling **hotkey** use.
- Setting a **password** for launching the session (administrator, user, setup user).

7.2. Citrix Receiver Selection

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Citrix Receiver Selection**

Select which of the installed Citrix Receiver versions is to be used for Citrix sessions:

- **Default (13.2.1)**
- **12.1.8**
- **13.1.4**

➡ An FAQ document provides an overview of the features in the different versions.

7.3. HDX / ICA Global

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global**

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

Most of these properties can be changed separately for each session, e. g.:

- Color depth
- Resolution
- Server IP
- Server name



Please note that a number of configuration options depend on the version of the Citrix Receiver selected. A comparison of functions can be found in the FAQs: *Citrix Receiver Feature Matrix* <http://faq.igel.com/otrs-igel/public.pl?Action=PublicFAQZoom;ItemID=619>.



Citrix Receiver 13.0.x and 13.1.x (Linux) supports HTTPS connections only, while the default setting for the Citrix server is HTTP – a connection attempt will thus fail. HTTPS must be enabled on the Citrix server and you must ensure that a valid root certificate for the certification authority (CA) is installed on the thin client. A best practice document regarding distribution of the certificates is available in the IGEL Knowledge Base: *Deploying Trusted Root Certificates* <http://edocs.igel.com/index.htm#10200413.htm>.



Citrix Receiver 13.1 supports Kerberos passthrough authentication for Legacy-ICA sessions only, not for Storefront!

➡ Users can only change an expired password if this option is enabled on the Citrix server too. See *Warning message when changing password* <http://faq.igel.com/otrs-igel/public.pl?Action=PublicFAQZoom;ItemID=621> FAQ.

7.3.1. Server Location

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Server Location**

In this area, you can specify the **master ICA browser**. The Citrix ICA client is connected to the network. It allows you to bring up a list of all Citrix servers and all published applications which are accessible via the network and use the selected browsing protocol.

The address of the first Citrix server to reply then functions as the master ICA browser.

You can specify a separate **address list** for each network protocol. This can be TCP/IP, TCP/IP + HTTP or SSL/TLS + HTTPS.

- **TCP/IP** - If your network configuration uses routers or gateways, or if additional network traffic owing to transmissions is to be avoided, you can specify special server addresses for the Citrix servers from which the list of available servers and/or published applications is to be requested.



You can add a number of addresses to the address list so that the clients can establish a connection and function even if one or more servers are not available.

- **TCP/IP + HTTP** - You can also call up information from the available Citrix servers and published applications via a firewall. To do this, you use the protocol TCP/IP + HTTP as the server location.



The "TCP/IP + HTTP" server location supports the auto-locate function.

- **SSL/TLS + HTTPS** - Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption offer server authentication and data stream encryption. They also allow you to check the integrity of messages.



If you try to establish a non-SSL/TLS connection to an SSL/TLS server, you will not be connected. A **Connection Failed** message will be shown.

7.3.2. Local Logon

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Local Logon**

In this area, you can specify settings for logging on to the ICA client.

Use Kerberos passthrough authentication for all ICA sessions: This option enables single sign-on for all ICA sessions if Log on to the thin client with AD/Kerberos is configured.

The server too must be configured for passthrough authentication. When launching ICA sessions, it is then no longer necessary to enter a user name and password again as the local logon data (domain logon) are transferred for session logon purposes.

Use the local logon module if problems with load balancing occur. The user's logon information is transferred when connecting to the metaframe master browser.

Use local logon window: If this option is enabled, you will need to enter the password again when logging on.

Relaunch mode: The logon module is automatically restarted after being closed.

Type: Here, you can pre-populate the user name and domain in the logon window and choose between the settings from the last logon and the session setup.

Preset login information: The logon window is pre-populated with the user name and domain.

Show domain: Shows the domain entry in the logon window.

Set client name as user name: This setting may help to resolve reconnection problems during load balancing.

Enable Smartcard Logon: Only specific smartcard types are supported. You will find a list of compatible types in the **Smartcard** sub-section of the setup.

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

7.3.3. Window

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Window**

The following settings are configured under **Window**:

Standard number of colors: Specifies the standard color depth - the default setting is a color depth of 256 colors.

Approximate colors: Given the differences between the color palettes used by the ICA client and the "thin client" desktop, the screen may flash annoyingly if you switch between windows on a pseudo-color screen. The ICA client's color adaptation scheme prevents this flashing as it uses the colors from the local desktop palette in order to display the ICA window session. If Approximate Colors is enabled, flashing when switching between windows is avoided.

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

Embed systray icons in window manager taskbar: Inserts an application icon into the local taskbar

Font smoothing: Enables font smoothing - in the event of performance problems, font smoothing should be switched off as it requires additional computing power.

Multi Monitor: Stipulates whether the full-screen mode is to be extended to all monitors.

7.3.4. Keyboard

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Keyboard**

On the **Keyboard** page, you can define alternative key combinations for hotkeys commonly used during ICA sessions. In MS Windows for example, the key combination **Alt+F4** closes the current window. This key combination also 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** is pre-populated but you can also select a country-specific layout. **Default** means that the local keyboard setting will be used in ICA too.
- **File for keyboard layout:** 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**



If you would like to use the PC key combination **Ctrl+Alt+Delete** during an ICA session, use the key combination **Ctrl+Alt+Enter** or **Ctrl+Alt+Return key**.

7.3.5. Mapping

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Mapping**

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

Drive Mapping

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Mapping > Drive Mapping**

Through drive mapping, each directory mounted on the thin client (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.

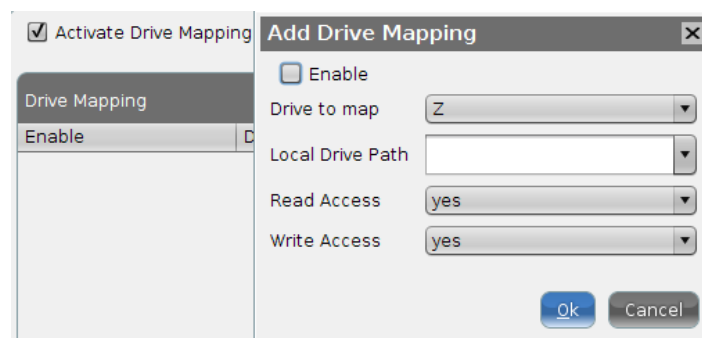


Figure 7: Drive mapping

The **Activate Drive Mapping** option allows you to temporarily enable/disable drive mapping. This offers the advantage that stored settings can be enabled or disabled without being lost.



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

To set up drive mappings, proceed as follows:

1. Click on **Add** to bring up the mapping window.
2. Select a **Drive to map** from the list under which the local device or the folder is to be mapped.



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

3. Give the **Local Drive Path** to which the mapping is to refer.



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

4. Specify the access authorizations for the mapping.

For each mapping, you have the option of granting **read access** or **write access**. You can also select the **Ask** option to query the read/write access rights when each ICA session is accessed for the first time.



The drive mappings and access data defined here are then valid for all ICA connections.

Serial Connections - COM Ports

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Mapping > COM Ports**

Enable Com Port Mapping in order to perform bidirectional mapping between serial devices connected to the thin client (e.g. scanners, serial printers) and the serial ports of the Citrix server.

As a result, programs running on the server can exchange data with the local devices.

- Click on **Add** under **Serial Devices**.
- From the drop-down list, select the serial connector to which a device is connected or click on **Detect Devices...** to select an available device.

/dev/ttyS0	Denotes the local serial connection COM1
/dev/ttyS1	Denotes the local serial connection COM2
COM3 and COM4	Denote possible expansion cards installed in the PCI/ISA slot, e.g. an internal modem
USB COM1 to USB COM4	Denote serial connections to USB-to-serial adapters.

Your selection will be mapped to the virtual COM1 connection. A second device will be mapped to the virtual COM2 connection and so on.



If you would like signature pads, you must enable them beforehand under **User Interface > Signature Pads** (page 155).

Printer

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Mapping > Printer**

You can set up a printer for ICA sessions here.

With the **Enable client printer** function, the locally connected thin client printer is made available for your ICA sessions, provided that it was not disabled on the server side.



The printers must be set up on the **Devices > Printers > CUPS > Printers** page and must be enabled there for mapping in ICA sessions, see *ICA sessions* (page 31).

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

Device Support

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Mapping > Device Support**

Enable virtual ICA channels for communicating with various devices connected to the thin client. These can be card readers, dictation machines or even USB storage devices. Channels of this type allow the device to communicate with the relevant server application.

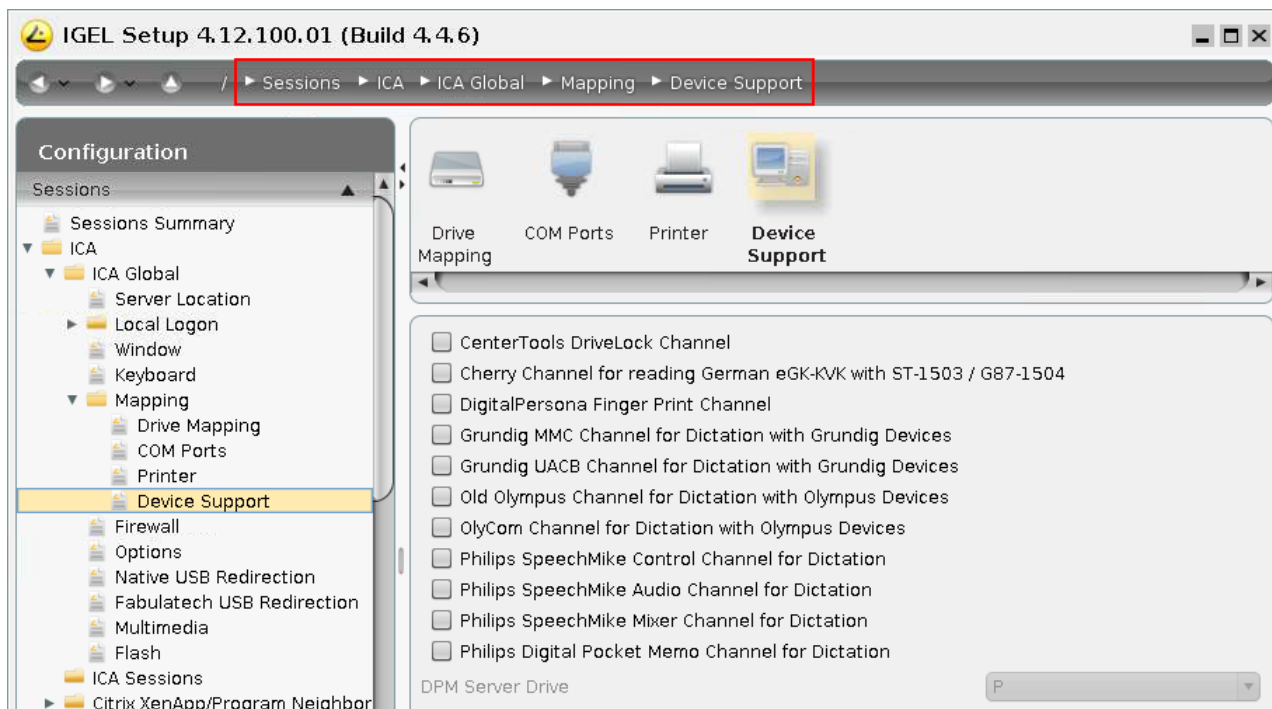


Figure 8: Supported devices



When using CenterTools DriveLock, ensure that the use of USB devices is not universally restricted. Check the settings under: **Devices > USB Access Control**

DriveLock

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Mapping > Device Support**

The virtual CenterTools DriveLock channel (ICA protocol) is included in the UDLX itself and must be installed on the Citrix XenApp server.

DriveLock can read hardware data from local USB devices and transfer these data with the help of the Virtual ICA Channel Extension to the XenApp server. When using whitelists, rules based on the hardware properties of the connected drive (e.g. manufacturer details, model and serial number) are taken into account.

Requirements

The following steps are important in order to be able to define the access rights for drives via the **DriveLock** server configuration:

- Enable the USB devices via drive mapping so that they are available as drives within your terminal session.
 - Check the settings under **Sessions > ICA > ICA Global > Mapping > Drive Mapping**. They should correspond to the DriveLock settings.
 - Disable Citrix USB redirection, because this will otherwise prevent drives being recognized by DriveLock.
 - Check the settings under **Devices > Storage Devices > Storage Hotplug** because they can influence the USB devices in the Citrix session.
 - Install and enable the DriveLock channel in the Universal Desktop setup under **Sessions > ICA > ICA Global > Mapping > Drive Support**.
- ➡ See also this document from CenterTools which describes the configuration of DriveLock on the server side in more detail: [How to use CenterTools DriveLock with IGEL Thin Clients \(PDF\)](#).

DigitalPersona authentication

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Mapping > Device Support**

By integrating DigitalPersona fingerprint readers into the thin client system and using the associated server software, users of IGEL thin clients can identify themselves through their fingerprints when using virtual applications on a Citrix XenApp server. All x86-based IGEL thin clients with the IGEL Linux operating system support the handling of logon data via the DigitalPersona Pro Enterprise Software (Version v5.3 and v5.4).

When used in conjunction with the DigitalPersona U.are.U 4500 fingerprint readers which are connected to IGEL thin clients via USB, the software provides a secure and quick means of authentication on virtual desktops.

- In order to be able to use fingerprint readers in Citrix sessions, enable the relevant virtual channel in **Device Support**.

Softpro SPVC Channel

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Mapping > Device Support**

- Enable the **Softpro SPVC Signature Pad Channel** in order to use Softpro/Kofax pads in Citrix sessions.

➡ You will find detailed information regarding the configuration of signature pads in the Best Practice documents for StepOver Pads and Softpro/Kofax pads.

Nuance channel for dictation

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Mapping > Device Support**

- Enable the **Nuance Channel for Dictation** in order to use dictation solutions from the manufacturer Nuance in Citrix sessions.

7.3.6. Firewall

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Firewall**

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

Use alternate address: Define a proxy or secure gateway server as an alternate address for connections via a firewall. Note the tool tips regarding the individual configuration parameters.

SOCKS / Secure proxy: Select the default proxy settings here or define the settings yourself.

Proxy type: If you use Secure (HTTPS), SSL/TLS or 128-bit encryption must be enabled in order for a secure connection to be established.

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



After enabling the alternative address, add the server to the address list under **Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Server Location**.

7.3.7. Options

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > HDX/ICA 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.

Disable Windows Alert sounds: Allows you to disable Windows alert sounds.

Allow backing store: The X Server temporarily stores hidden window content.

Delayed 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.

Cache size in kB: Allows you to change the settings for the bitmap cache. If you work with images that are displayed over and over again, you can significantly improve the performance of your ICA session(s):

- Specify the maximum amount of local system storage capacity (in kilobytes) used for temporary storage purposes.
- You can specify the minimum size of bitmap files which are to be stored in the cache as well as the directory in which the files are to be stored locally.



Do not make the cache too big otherwise you run the risk of the thin client having too little storage space for its own system and other applications. You may have no alternative but to equip your thin client 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). Setting the value to 100 or higher may help to rectify this problem.

Enable Auto Reconnect: Allows you to specify the parameters for reconnecting the session.

Allow Kerberos passthrough authentication in Program Neighborhood sessions: Allows the use of Kerberos passthrough authentication in the Citrix Program Neighborhood session.

CGP address: Common Gateway Protocol server address

- Select **Use server address** to use the value of the Server parameter as the host name.
- Select **disabled** to leave the server address empty.

7.3.8. Native USB Redirection

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > HDX/ICA 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.

- Use either **Native USB Redirection** or **Fabulatech USB Redirection**.

For **Fabulatech USB Redirection**, a special Fabulatech server component must be installed on the Citrix server (USB for Remote Desktop Igel Edition).

- ➡ More detailed information on the function can be found on the Fabulatech partner site:
<http://www.usb-over-network.com/partners/igel/>.



Enable either native or Fabulatech USB redirection – not both together.
Disable USB redirection if you use CenterTools DriveLock (page 28).

7.3.9. HDX Multimedia Redirection

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > HDX Multimedia**

Citrix HDX multimedia acceleration improves playback via Media Player within an ICA session on the remote desktop and allows isosynchronous transmissions, e.g. of webcams within the session.

➡ See *Supported formats and codecs* (page 8).

To improve multimedia playback on the remote desktop, proceed as follows:

1. To take advantage of improved playback, ensure that the necessary codecs are installed on the remote desktop page.
2. Enable **multimedia redirection** on the thin client.
3. Create the session.
4. Begin playback on the remote desktop.

➡ From IGEL Linux 5.06.100, hardware acceleration for multimedia playback is available on certain devices. You will find more detailed information in an FAQ document on the topic.

7.3.10. HDX Flash

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > HDX Flash**

Depending on the performance of the thin client, Citrix HDX Mediasream Redirection for Flash allows smoother playback of Flash content than is possible within the Citrix session itself.



An installed Flash Player browser plug-in is needed in order to enable flash redirection.

➤ Install the plug-in under **Sessions > Browser > Plug-Ins > Flashplayer**.

7.3.11. Codec

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Codec**

In the Citrix 13.x Versions, two codecs for reproducing screen content are available to choose from:

- The default setting **Automatic** automatically selects the appropriate codec according to the performance of the hardware.
- Alternatively, the codecs **H.264 Deep Compression Codec** for high-quality complex graphics and **JPEG** (less CPU-intensive) as well as their options can also be selected manually.



This setup page can only be seen if you have selected a Citrix Receiver version which is higher than 12.x.

➡ The optional Multimedia Codec Pack is needed to use the H.264 Deep Compression Codec. Further information can be found in the IGEL Linux Features that Require the Multimedia Codec Pack FAQs.

7.4. Legacy ICA Sessions

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Legacy ICA Sessions**

You can set up your own ICA sessions here.

The global ICA session settings can be changed in the individual sessions.

➡ The primary source of further information relating to Citrix connections should always be the relevant Citrix documentation. This manual merely gives general configuration tips.

7.4.1. Server

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Legacy ICA Sessions > ICA Session > Server**

In this area, you can overwrite the following server connection details and thus the default settings:

Browser protocol: The protocol that is to be used when searching for servers and published applications.

Do not use default server location: Lifts the default server requirement – for each protocol separately.

Server: Click on **Search** to send a transmission signal which queries all available servers and published applications.

By selecting the server, the user is connected to the entire desktop as if logging on at the server itself. As a result, all applications, rights and settings contained in the user's profile (local server profile) are available.

If you select a published application, the session is opened in a window which contains just one application. The session is ended if you close this application.

You can also manually enter the IP address or the host name of the server in the **Server** field.

Application: If you have entered the server manually, you can specify a published application here. These fields are automatically filled in if you have selected one of the recognized published applications.

Working directory: Details of the path name of the work directory for the application

7.4.2. Logon

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Legacy ICA Sessions > ICA Session > Logon**

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

Use Kerberos passthrough authentication	Enables single sign-on for this ICA session if Log on to the thin client with AD/Kerberos is configured. The server too must be configured for passthrough authentication. When launching the ICA session, there is no need to enter a user name and password again.
Use passthrough authentication	Enables single sign-on for this ICA session if Log on to the thin client with AD/Kerberos is configured. The fact that the user name and password are temporarily stored when logging on to the thin client means that there is no need to enter them again when launching a session.
User, password, domain	Specifies a user name, password and domain for the ICA session. These details are automatically forwarded to the server and no longer need to be entered on the logon screen.
Do not show password protection window before logon	This option switches the Windows splash screen on and off. This option must be disabled when logging on to Windows using a smartcard.

7.4.3. Window

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Legacy ICA Sessions > Window**

The following settings are configured under **Window settings**:

Number of colors	The color depth is set as a global default . You can change it for this session.
Use default settings for color table	The color table is preset on a global basis. You can approximate it for this session.
Full-screen mode	By disabling the full-screen mode, you can choose between the global default setting and a session-specific setting.
Start monitor	Specifies which monitor in an environment with several monitors is to be used for the session.
Enable seamless mode	The seamless mode can only be used with published applications or with a specified start program for the server connection.
Font smoothing	Font smoothing is preset on a global basis. You can change it for this session.

7.4.4. Firewall

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Legacy ICA Sessions > [Session Name] > Firewall**

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

- **Use alternate address:** Define a proxy or secure gateway server as an alternative address for connections via a firewall. Note the tool tips regarding the individual configuration parameters.
- **SOCKS / secure proxy:** Select the default proxy settings here or define the settings yourself.
- **Proxy type:** If you use Secure (HTTPS), SSL/TLS or 128-bit encryption must be enabled in order for a secure connection to be established.
- **Secure Gateway (relay mode):** If you would like to use a Citrix Secure Gateway in relay mode, you must give the full domain name – the IP address is not sufficient in this case.



After enabling the alternative address, add the server to the address list under **Setup > Sessions > Citrix XenDesktop/XenApp > Legacy ICA Sessions > ICA Session > Server**.

7.4.5. Reconnect

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Legacy ICA Sessions > ICA Session > Reconnect**

In this area, you can specify that ICA sessions automatically reconnect if they were terminated by wireless devices owing to highly fluctuating network latency or area restrictions.

- Enable **Use default Auto Reconnect settings** in order to apply the settings configured under **HDX / ICA Global** in the event of reconnection.
- Alternatively, enable **Auto Reconnect** and you will have the option of specifying the maximum number of attempts and the time delay before a reconnection attempt.

7.4.6. Options

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Legacy ICA Sessions > ICA Session > Options**

Under **Options**, you can optimize performance and system behavior within the ICA session.

Compression	<p>Reduces the quantity of data transmitted via the ICA session.</p> <p>This in turn reduces network traffic to the detriment of CPU performance.</p> <ul style="list-style-type: none"> • Enable compression if you connect your server(s) via WAN. • Disable this option if you use a relatively low-performance server and only work in one LAN.
Caching image data	<p>Enables caching in the cache memory (configured in the global ICA settings) for each session.</p> <p>This makes sense if you use a number of ICA sessions but only one or two sessions are critical with regards to network bandwidth or are used heavily during the day. In this case, you should reserve the cache memory for these sessions.</p>
Encryption method	<p>Encryption increases the security of your ICA connection. Basic encryption is enabled by default. You should therefore ensure that the Citrix server supports RC5 encryption before you select a higher degree of encryption.</p>
Audio transmission	<p>Transfers system sounds and audio outputs from applications to the thin client. These are then output via the speakers connected. The higher the level of audio quality you select, the more bandwidth is needed for transferring audio data.</p>
Mouse click feedback	<p>The mouse pointer immediately turns into an hourglass symbol, thus providing visual feedback in response to a mouse click.</p>
Local text echo	<p>Displays the text entered more quickly and avoids latencies in the network.</p> <p>Select a mode from the drop-down list:</p> <ul style="list-style-type: none"> • Select On for slower connections (connection via WAN) in order to reduce the delay between the user entering text and the text being displayed on the screen. • For faster connections (connection via LAN), select Off. • Select Automatic if you are not sure how fast the connection is.

7.4.7. Desktop integration

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Legacy ICA Sessions > [Session name] > Desktop Integration**

- Give the **name** of the session that you would like to integrate into the desktop.
- From the **Launch Options**, specify how the session is to be made accessible.
- As an option, specify a **hotkey** for starting the session.
- Enable **Autostart** to start this session immediately after the system starts. Specify by how many seconds the session start is to be delayed when Autostart is used.
- Enable **Restart** to restart this session after the connection is terminated.

7.5. Citrix StoreFront / Web Interface

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Citrix StoreFront / Web Interface**

Most of the settings were already configured under HDX ICA Global and *Legacy ICA Sessions* (page 31).

- Select the start options for the Citrix XenApp session, see **Desktop Integration** (page 21).

7.5.1. Server

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Citrix StoreFront / Web Interface > Server**

In this area, you can configure session-specific server connections.

- Under **Citrix server type**, specify the connection type to which the client is to connect.



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.

- Under **Server location**, specify connections to Citrix Stores. Give the server name or the server IP here.
- Add **Domains**.
- Select the **Handling of domain in login window**:
 - Normal
 - Unchanged
 - Hidden



If you select Hidden, the first entry in the domain list will be used to log on.

7.5.2. Logon

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Citrix StoreFront / Web Interface > Logon**

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

- Choose an **Authentication Type**. Depending on the Receiver version, the following types may be available:

- **Password authentication**
- **Kerberos passthrough authentication (Web Interface only, not StoreFront)**

Uses local logon data for listing and launching applications. The option enables single sign-on for XenApp if logon with AD/Kerberos is configured on the thin client.

- **Smartcard authentication (StoreFront only, not Web Interface)**
- **Citrix authentication mechanism (instead of IGEL), without smartcard**
- **Citrix authentication mechanism (instead of IGEL), with smartcard**




If you have set an authentication type with smartcard, select the type of card on the **Smartcard** (page 37) page.

Additional options include the following:

- **Use passthrough authentication:** Uses temporarily saved logon data for listing and launching applications.
 - **Auto logon:** Uses the logon data preset on this page when connecting to the server.
 - **Remember user name and domain:** Saves the user name and domain from the last logon.
 - **Synchronize Citrix password with screen lock:** Synchronizes the screen lock password with that of the Citrix application.
 - **Relaunch Citrix logon after logoff:** Automatically shows the **Logon** dialog again after logging off.
- Give a list of applications which will be launched automatically after a connection to the server has been established.

To select an application for automatic launching, proceed as follows:

1. Click on  in the **Launch following applications automatically after server connection is established** area.
2. In the **Add** dialog, enter the name of the application.



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

3. Click on **Next**.

After a successful logon, the associated desktop icon for each available application will be placed on the thin client 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.

Smartcard

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Citrix StoreFront / Web Interface > Logon > Smartcard**

From IGEL Linux 5.06.100, it is possible to log on to Citrix StoreFront using a smartcard with Version 13.1.3 of Citrix Receiver. A **smartcard** type can be selected or a custom **PKCS#11 module** integrated here.

7.5.3. Options

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Citrix StoreFront / Web Interface > Options**

In this area, you can specify settings which differ from the global settings for Citrix StoreFront / Web Interface.

- **Use server settings for all options:** If this option is enabled, the server settings will be carried over to the client.
- **Client Audio** If this option is enabled, sound will be transmitted.
- **Overwrite local Client Audio with server setting:** If this option is enabled, the server audio settings will be carried over to the client.
- **Audio Bandwidth Limit:** Select between **High**, **Medium** and **Low** - Higher quality requires more network and computing resources.
- **Color Depth:** Choose between **Server setting**, **Global setting**, **16**, **256**, **32 thousand**, **16 million** and **Automatic**.
- **Window size:** Choose between **Seamless | Desktop**, **Server setting**, **Global setting**, Different sizes in pixels, **Work area** and **Full screen**.
- **Restrict full-screen sessions to workarea**
- **Handling of keyboard shortcuts:** Choose between **Server setting**, **Translated**, **Direct in full-screen desktops only** and **Direct**.

7.5.4. Appearance

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Citrix StoreFront / Web Interface > Appearance**

You can configure how Citrix XenDesktop/XenApp applications are displayed.

With the display filter, you can select which applications can be launched in the start menu, in the Application Launcher and on the desktop. You can make a separate selection for the Quick Start Panel.

You can change the following settings:

- **Show applications in start menu:** If this option is enabled, Citrix applications will be shown in the start menu.
- **Show in start menu:** Specifies whether all applications are shown in the start menu or whether the server settings are observed.
- **Resize icons for the start menu:** If this option is enabled, the size of the symbols for the start menu will automatically be adjusted.



Automatic scaling can prolong the logon procedure.

- **Apply display filter to start menu entries:** If this option is enabled, only the applications selected in the display filter will be shown in the start menu.
- **Show applications in the Application Launcher:** If this option is enabled, the applications will be shown in the Application Launcher.
- **Apply display filter to Application Launcher entries:** If this option is enabled, only the applications selected in the display filter will be shown in the Application Launcher.
- **Show applications on desktop:** If this option is enabled, the applications will be shown on the desktop.
- **Keep folder structure on desktop:** If this option is enabled, Citrix sessions will be shown on the desktop in their directory structure.
- **Show desktop shortcuts:** Specifies whether all applications are shown in the Desktop Launcher or whether the server settings are observed.
- **Apply display filter to desktop icons:** If this option is enabled, desktop icons will be created only for the applications selected in the display filter.

To select an application in the display filter, proceed as follows:


1. In the **Display filter: Show only the following applications** area, click on



The **Add** dialog will open.

2. In the **Add** dialog, enter the name of the application that is to be shown.
3. Click on **Ok**.

To select an application that is to be shown in the Quick Start Panel, proceed as follows:

1. In the **Show the following applications in the Quick Start Panel** area, click on . The **Add** dialog will open.
2. In the **Add** dialog, enter the name of the application that is to be shown in the Quick Start Panel.
3. Click on **Ok**.

7.5.5. Password Change

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Citrix StoreFront / Web Interface > Password Change**

In this area, you can specify how a connection is established in order to change a password.

Method for Password Change:

- **Generic session:** Searches for servers/applications and subsequently establishes a connection
- **Predefined ICA session:** Selects a pre-defined ICA session according to session name
- **Citrix XenApp services site:** Allows you to change a password via the Citrix Web Interface itself
- **Use Kerberos to change the password:** If Kerberos authentication is set up on the XenApp Server, the password can also be changed via this route.

7.5.6. Reconnect

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Citrix StoreFront / Web Interface > Reconnect**

In this area, you can select the required option when reconnecting to sessions.

You can establish a connection

- during the logon process and
- through using a reconnect session, e.g. on the desktop.

With the help of the reconnect procedure, you can launch **active and terminated sessions, terminated sessions only** or **sessions on demand**.



An updating session reloads the XenApp session without terminating it.

7.5.7. Log off

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Citrix StoreFront / Web Interface > Logoff**

In this area, you can create a **logoff session** and specify the *desktop integration* (page 21) for it.

7.5.8. Desktop Integration

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Citrix StoreFront / Web Interface > Desktop Integration**

- Give the **name** of the session that you would like to integrate into the desktop.
- From the **Launch options**, specify how the session is to be made accessible.
- As an option, specify a **hotkey** for starting the session.
- Enable **Autostart** to start this session immediately after the system starts. Specify by how many seconds the session start is to be delayed when Autostart is used.

7.6. Citrix Self–Service

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Citrix Self-Service**

The Citrix Self-Service interface allows access to Citrix StoreFront or Web Interface services.

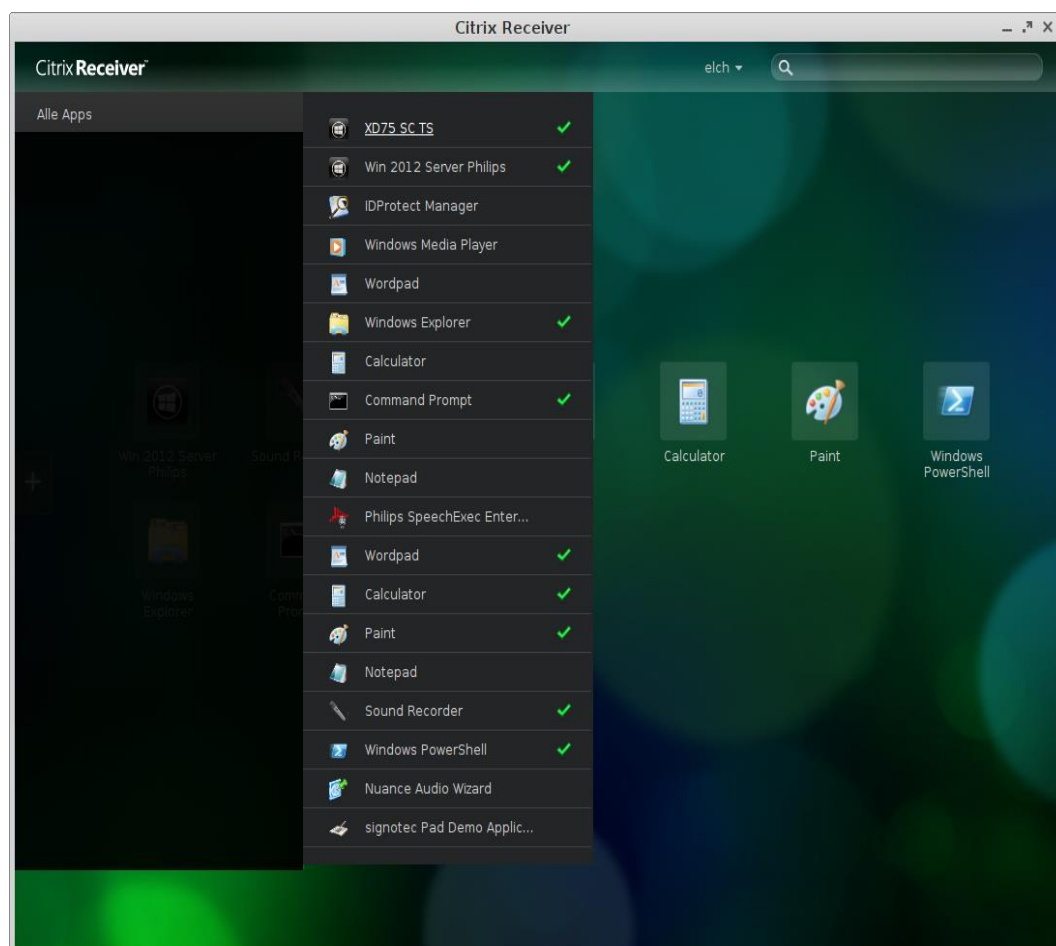


Figure 9: Citrix Self-Service






For this session type, Version 13.1.4. or higher must be selected in the *Citrix Receiver selection* (page 22).

7.6.1. Server

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

- **Use IGEL setup for Citrix Self-Service configuration:** If this option is enabled, the IGEL setup will be used for Self-Service configuration.

You can enter a number of servers below:

- Click  to enter a new server.
- Click  to remove a server.
- Click  to edit a server.

7.6.2. Options

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Citrix Self-Service > Options**

- **Display Mode:** Select whether the Self-Service user interface is shown in a **Window** or in **Full Screen**.
- **Multi User (StoreFront servers only):** If this option is enabled, the user data on the client will be deleted after logging off or terminating Self-Service.
- **Reconnect after logon:** If this option is enabled, the Self-Service user interface will reconnect automatically after the launch.

Reconnect to apps after starting an application: If this option is enabled, the Self-Service user interface will attempt to reconnect to ongoing sessions if an application is launched or the store is reloaded.

7.7. Citrix Access Gateway

Menu path: **Setup > Sessions > Citrix XenDesktop/XenApp > Citrix Access Gateway**

With the **Citrix Access Gateway (CAG)** client, you can establish a VPN connection to a CAG default server. The VPN connection is an SSL tunnel. A certificate is transferred from the server to the client in the process.

Warning when attempting to connect

If the certificate is not trustworthy, a warning will be given when an attempt to establish a connection is made.

- In order to avoid the warning, the server certificate can be stored on the thin client in the `/wfs/cagvpn/cagvpn-trusted-CAs.crt` file.
- The warning can also be disabled in the CAG client configuration.

7.8. RDP Global

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

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



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

7.8.1. Gateway

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

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

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

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

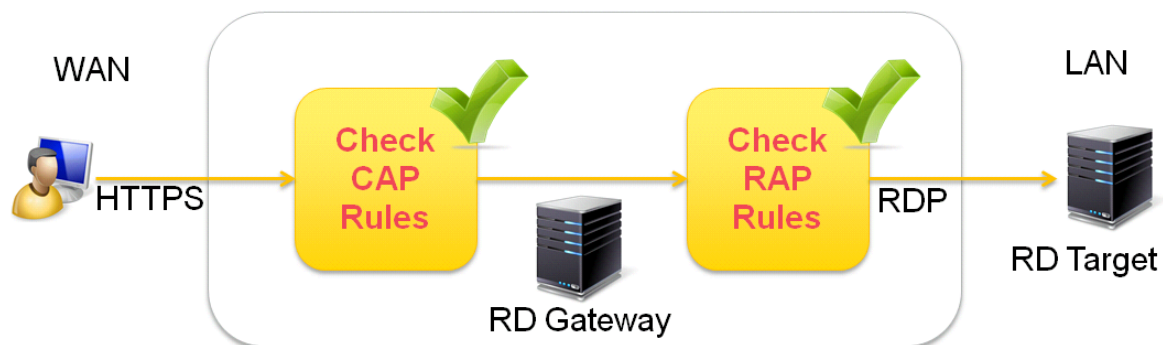


Figure 10: Remote Desktop Gateway

To set up the **RD Gateway**, proceed as follows:

1. Enable **Gateway Support** under **Sessions > RDP > RDP Global > Gateway**.
2. Record the access data. Smartcard is not supported



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

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

- Server 2008R2 Standard (limited to 250 RD Gateway connections)
- Server 2008R2 Enterprise
- Server 2008R2 Datacenter
- Server 2012 Standard
- Server 2012 Datacenter
- Server 2012 Essential (restricted to the RD Gateway role)
- Server 2012R2 Standard
- Server 2012R2 Essential (restricted to the RD Gateway role)



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

7.8.2. Local Logon

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

Under **Local logon**, you can pre-populate user data. As a result, you can avoid users possibly having to log on a number of times.



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

Enable **Use local logon window** to

- Pre-populate user data
- Freely select the server in the logon window of an RDP session.

The following presets can be configured:

Use local logon window	If this option is enabled, you will need to enter the password in the RDP logon window on the terminal side when logging on.
Preset logon information	The logon window is pre-populated with the user name and domain.
Type	Here, you can pre-populate the user name and domain in the logon window and choose between the settings from the last logon and the session setup.
Show domain	Shows the domain entry in the logon window.
Specify client name to user name	This setting may help to resolve reconnection problems during load balancing.
Relaunch mode	The RDP logon window is displayed in restart mode and cannot be closed.
Enable network authentication	Enables network authentication via NTLM. Smartcards are not supported here.
Domains	Allows you to add domains which are to be available. If you enter a number of domains, these will be shown in the Domains drop-down area in the logon module.

7.8.3. Window

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

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

You can change the following settings:

- **Number of Colors:** Specifies the color depth.
- **Window Size:** Specifies the width and height of the window.
 - **Fullscreen:** The session is shown on the full screen. The thin client's taskbar is not visible.
 - **Workarea:** The session is shown on the full screen, minus the area needed by the thin client's taskbar.
 - **Numeric details:** The session is shown in the selected resolution or on the selected percentage of the screen area.
- **Enable Display Control:** If this option is enabled, the window size can be changed during the session.



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



It is not possible to change the window size during the session if the **window size** is set to **full screen** or **work area**.

- **Control bar for RDP sessions:** If this option is enabled, a symbol bar for minimizing and closing a full-screen session will be shown.



If the symbol bar is enabled, a session will be shown on one monitor only, even if **Multi Monitor Fullscreen mode** is set to **Expand fullscreen session onto all monitors**.

- **Enable internal Backing Store:** If this option is enabled, the window content will be saved in an internal buffer. In the event of an expose event, buffering ensures that the window content is obtained from the internal buffer rather than having to be retrieved from the server. This reduces the burden on the network.
- **Multi Monitor Fullscreen mode:** Stipulates whether the full-screen mode is to be extended to all monitors.

7.8.4. Keyboard

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

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

- **Clipboard** (enable or disable)
- **PC keyboard scan codes** (convert or send directly)
- **Override local window manager keyboard shortcuts** (forward or execute locally)



You can select the keyboard layout in the Session Configuration. **Automatic** is the default.

7.8.5. Mapping

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

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

Drive Mapping

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

Through drive mapping, connected mass storage devices can be made available to the user. Specify which folders or drives are mapped during the logon.

Via **Enable drive mapping**, you can temporarily enable/disable drive mapping. This offers the advantage that stored settings can be enabled or disabled without being lost.



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

To set up drive mapping, proceed as follows:

1. Click on **Add** to bring up the mapping window.
2. Select a **Drive to map** from the list under which the local device or the folder is to be mapped.



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

3. Give the **Local Drive Path** to which the mapping is to refer.



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

COM Ports

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

As with locally connected mass storage devices, you can also map the thin client's local serial connections during an RDP session:

1. Click on **Enable Com Port Mapping**.
2. Add the required connection.



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



If you would like signature pads, you must enable them beforehand under **User Interface > Signature Pads** (page 155).

Printers

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

In this area, you can configure printer mapping.

With the **Enable Client Printer mapping** function, the locally connected thin client printer is made available in your RDP sessions, provided that it was not disabled on the server side.



The printers must be set up on the **Devices > Printers > CUPS > Printers** page and must be enabled there for mapping in RDP sessions.

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

Device Support

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

In this area, you can enable virtual RDP channels for communicating with various devices connected to the thin client. These can be card readers (smartcards), dictation machines or even USB storage devices. Channels of this type allow the device to communicate with the relevant server application. Requirements: **Enable plugin support**.



When using CenterTools DriveLock, ensure that the use of USB devices is not universally restricted: **Devices > USB Access Control**.

DriveLock

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

The virtual DriveLock channel (RDP) is included from UDLX Version 5.01.100 or higher and must be installed on the RDP server.

DriveLock can read hardware data from local USB devices and transfer these data to the server with the help of the Virtual RDP Channel Extension. When using whitelists, rules based on the hardware properties of the connected drive (e.g. manufacturer details, model and serial number) are taken into account.

Requirements for configuring DriveLock

The following steps are important in order to be able to define the access rights for drives via the DriveLock server configuration:

- Enable the USB devices via drive mapping so that they are available as drives within your terminal session.
- Check the settings under **Sessions > RDP > RDP Global > Mapping > Drive Mapping**. They should correspond to the DriveLock settings.
- Disable RDP-USB Redirection under **Mapping > USB Redirection**. This would otherwise prevent drive recognition by DriveLock.
- Check the settings under **Devices > Storage Devices > Hotplug Storage** because they can influence the USB devices in the RDP session.

- Install and enable the DriveLock channel under **Sessions > RDP > RDP Global > Mapping > Device Support**.
- ➡ In the Centertools download area, you will find a document which describes in greater detail the procedure for configuring DriveLock on the server side: [How to Use Centertools DriveLock with IGEL Thin Clients \(PDF\)](#)

Audio

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

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

- **Enable Client Audio.**
- Select the **Audio Quality Mode** and the **Audio Compression**.
- **Audio Capture**

7.8.6. Performance

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

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

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



In low-bandwidth environments, you should use **compression** in order to reduce the network traffic.

Please note that the use of compression reduces the burden on the network but does use CPU power.

Graphic settings which you can disable are:

- Desktop background
- Window contents when moving windows
- Menu and window animation
- Desktop themes
- Mouse pointer shadow
- Mouse pointer settings
- Font smoothing

RemoteFX Support

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

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

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



Figure 11: Windows Aero



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



Further information on Remote FX and the server-related requirements is available from Microsoft at <http://technet.microsoft.com/de-de/library/dd736539%28WS.10%29.aspx>.



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

7.8.7. Options

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

In this area, you can configure the following settings:

Disable mouse movement events	Instructs the client not to show "unnecessary" cursor movements in order to conserve power.
Inverted cursor color	Black, White or Dotted are available to choose from. You can also configure your own values 'custom:<foreground color>,<background color>'. The colors must be given in the ARGB8888 format, e.g. 0xFF000000.
Reset license	If you have to remove the MS license from the device, enable this option and restart the device.
Reset confirmed server certificates	Deletes all confirmed server certificates on the client.
RDP legacy mode	Uses the local RDP client from IGEL Linux v4 - see note below.
Client Name	Give a client name for terminal service identification - the default setting is the host name of the computer.
Custom client name	If you have opted for a custom client name, you can enter the name here. If the field remains empty, the MAC address of the client will be used automatically.
Force TLS-encrypted connections	Only TLS-encrypted connections are allowed.
Verify server certificates	Verify server certificate if the connection is TLS-encrypted.



Inform IGEL Support if problems occur with the current RDP client (IGEL Linux v5), even if they can be avoided by using the compatibility mode. The **RDP legacy mode** can be disabled in a later IGEL Linux version.

7.8.8. Native USB Redirection

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

USB devices can be permitted or prohibited during an RDP session on the basis of rules. Sub-rules for specific devices or device classes are also possible.

➤ Use either **Native USB Redirection** or **Fabulatech USB Redirection**.

For **Fabulatech USB Redirection**, a special Fabulatech server component must be installed on the Citrix server (USB for Remote Desktop Igel Edition).

➡ More detailed information on the function can be found on the Fabulatech partner site:
<http://www.usb-over-network.com/partners/igel/>.



Enable either native or Fabulatech USB redirection – not both together.
Disable USB redirection if you use CenterTools DriveLock (page 28).

7.8.9. Multimedia

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

To improve video playback on the remote desktop, proceed as follows:

1. To take advantage of improved playback, ensure that the necessary codecs are installed on the remote desktop page.
2. Enable **Video Redirection** on the thin client.
3. Create the session.
4. Begin playback on the remote desktop.

➡ From IGEL Linux 5.06.100, hardware acceleration for multimedia playback is available on certain devices. You will find more detailed information in an FAQ document on the topic.

7.9. RDP Session

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

You can set up your own RDP sessions here.

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

Server and logon	Allows you to specify a server and a start application for the terminal server session. The necessary logon information is configured here. Otherwise, the terminal server logon window for entering the user and the password will be displayed.
Gateway	Allows you to enable gateway support. Logon data for RD Gateway may also be specified here.
Window	Allows you to specify the size of the session window and the color mode. The local taskbar can be configured so that it remains visible during a full-screen session.
Keyboard	Allows you to specify the keyboard layout, scan codes and the direct connection between keyboard input and the Windows Server.
Mapping	<p>Allows you to specify the audio output device (local/remote) and determine how key strokes and clipboard content are handled. The mapping of serial connections and local drives can be enabled for a session.</p> <p>You can make connected mass storage devices available to the user using the appropriate mapping: Select Enable, choose the drive letter and the device to be mapped.</p>
Performance	Allows you to disable non-essential graphical functions such as skin styles, window animation etc. This is useful in the event of performance problems.
Options	Allows you to specify the start application and the work directory for use during the session (how authentication errors are handled during the logon procedure). If, when connecting to the server, a terminal server gateway is to be used, you can configure the relevant settings here (No Gateway is pre-set).
USB redirection	Allows you to specify native USB redirection
Multimedia	Allows you to specify video redirection.

7.9.1. Server

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

In this area, you can overwrite the following server connection details and thus the default settings:

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

Server

To set up a server, proceed as follows:

1. Give the **Server** name or the IP address.
2. Define the **RDP Port** which is to be used for the connection.
The default port is 3389.
3. Under **Application**, specify a start-up application for the terminal server session.
4. Specify the **Working Directory**.
5. Enable **Changeable Server-URL on Local Logon** in order to allow the server to be entered freely. You must have enabled local logon in order to do this.

Otherwise, the terminal server logon window will be displayed for you to enter a user name and password. If the local logon is used (see above), the thin client's logon window. will be shown.



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

Microsoft RemoteApp

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

- ➡ Detailed instructions regarding server configuration can also be found on the Microsoft website: TS RemoteApp Step-by-Step Guide.

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



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

7.9.2. Display, Keyboard and Mapping

Menu path: **Setup > Sessions > RDP > RDP Sessions > [session name] > Window / Keyboard / Mapping**

- Under **Window**, specify the color depth, window size and the multiscreen behavior.
- Under **Keyboard**, configure the keyboard layout and the hotkey properties.
- Enable/disable the **allocation** of resources for the client, e.g. COM port or printer mapping.

The *global parameters* (page 42) are the default setting.

7.9.3. Performance and Options

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

Specify the performance settings for the session if they differ from the *global configuration* (page 42).

You can influence the following values:

- Enable RemoteFX
- Disable desktop background
- Hide window contents when moving windows
- Disable menu and window animation
- Disable desktop themes
- Disable mouse pointer shadow
- Disable mouse pointer settings
- Disable font smoothing
- Compression

7.10. Remote Desktop Web Access

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access**

With Web Access for Remote Desktop (Web Access for RD), users can access RemoteApp and a Remote Desktop connection via the start menu on a computer or via a web browser.

RemoteApps and Remote Desktop connections therefore provide a modified view of RemoteApp programs and virtual desktops for users.

➡ More information on Web access for Remote Desktop can be found under Microsoft Technet - Web Access for RDP.

7.10.1. Configure Access to RD Connection

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access**

In order to allow users access to RemoteApps, you can configure Web Access in three ways:

In the **Setup** under **Sessions > RDP > Remote Desktop Web Access**, configure:

Pre-Defined Configuration (page 54): Define several server connections with the same user access data. The user must enter their access data and the domain in the logon window.

Ask user (page 54): The connection is pre-configured on the server side. The user only needs to enter their corporate e-mail address.

Or select the third option:

Via browser (page 55): Access via web browser

Pre-defined configuration

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access**

To configure pre-defined configuration, proceed as follows:

1. Click on **Remote Desktop Web Access > Connections**.
2. Select **Pre-Defined Configuration** under **Server Configuration**.
3. Create a new session. See the *Connections* (page 56) section regarding the session settings.

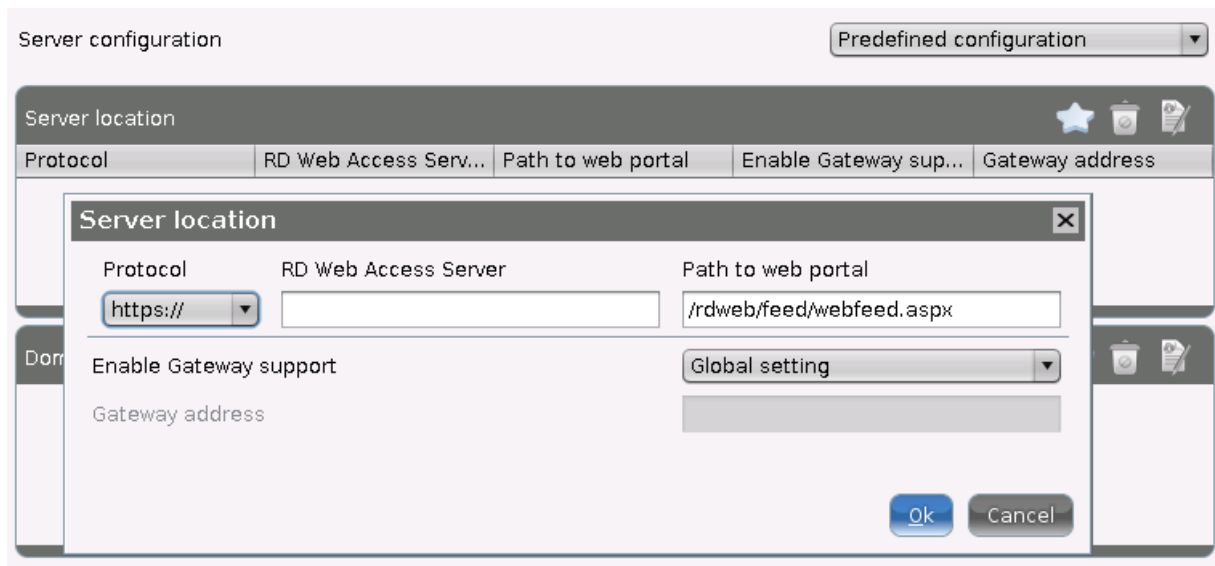


Figure 12: New RD Web Access Session

4. Select a logon option under **Remote Desktop Web Access > Authentication**.

If you have selected **Pre-Defined Configuration**, the **Kerberos Passthrough Authentication** mode will be available for logging on in addition to the normal user authentication process.

5. Under **Logoff / desktop integration** (page 58), you can specify how you would like to log on or off.



You must make a setting for the logon icon because this is not pre-configured and you will not otherwise have access to the Web Access logon.

The applications can be provided in the **Application Launcher**, in the **Start Menu**, in the **Quick Start Panel** or on the **Desktop**. Under **Appearance**, you can choose from the list of available applications for display on the desktop or in the Quick Start Panel.

Ask User

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Server**

This is a very user-friendly Web Access login.

In order to use it, the network connections connected with the user name on the server side must be pre-configured and it must be possible to query them via DNS.

To configure the **Ask user** login, proceed as follows:

- Select **Ask user** under **Server configuration**.

When logging in via RD Web Access, the user will be given a login window where they must only enter their corporate e-mail address, i.e. <name>@<domain>:



Figure 13: Ask User

Via Browser

The Web Access page for Windows Server 2012 and Windows Server 2012 R2 can also be used on a Linux thin client in the Firefox browser.

- The user only needs the corresponding URL which is entered in the address bar.
- They then log on on the browser page using their user name and password.

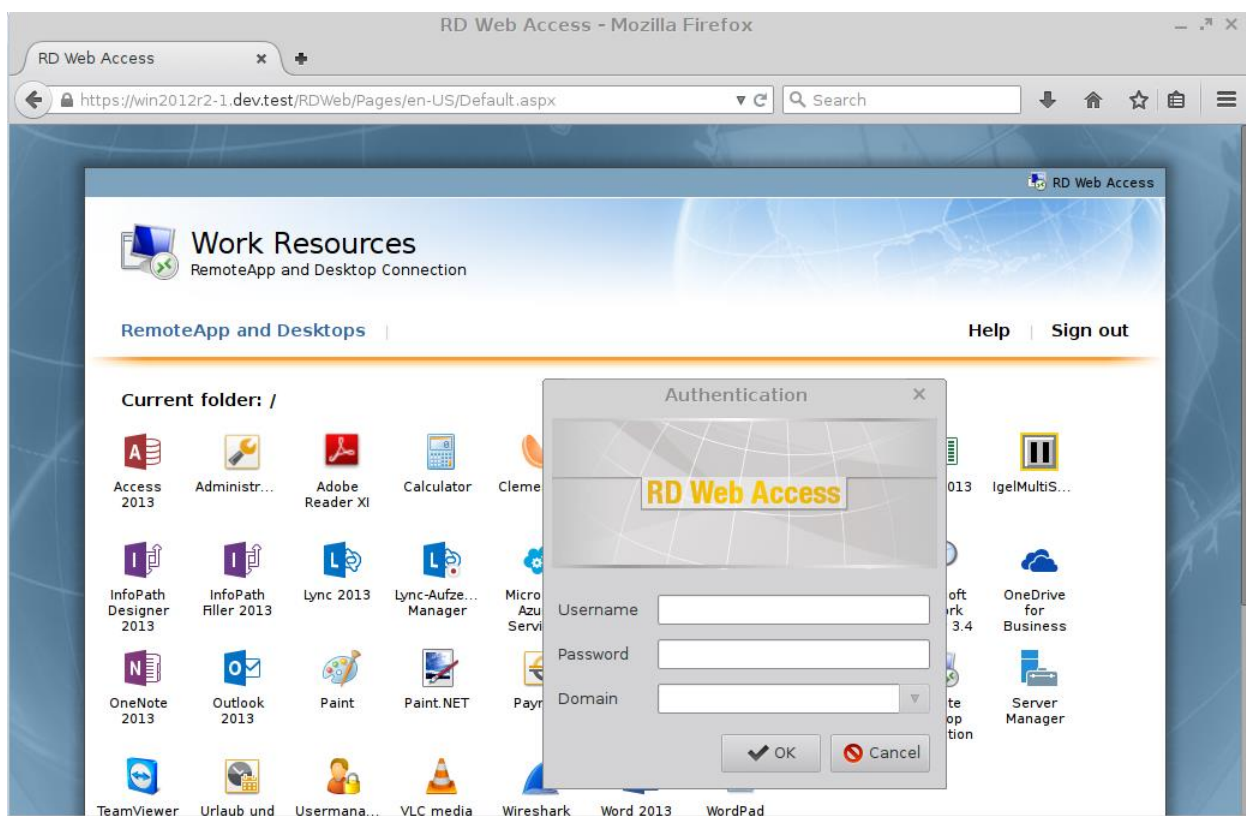


Figure 14: Remotedesktop Web Access in Firefox

If the user clicks on one of the applications offered by Web Access, the thin client will open a logon mask and then a remote desktop session for the chosen application.

7.10.2. Connections

Menupath: **Setup > Sessions > RDP > Remote Desktop Web Access > Connections**

In this area, you can define the connections to server locations and domains:



Figure 15: Remotedesktop Web Access

For the **pre-defined configuration**, specify the following values:

1. Select the **protocol** `http://` or `https://`.
2. Enter the name of the **Remote Desktop Web Access Server** and the path to the **web portal**.
3. If you would like to **Enable gateway support**, you can choose between the settings that you have made globally or in a custom session

If you would like to carry over the **session settings**, you must also specify the **gateway address**.

7.10.3. Authentication

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Authentication**

You can change logon settings on the server and select applications that are launched automatically after logging on.



The logon settings on the server are only effective if the **Server configuration** option under **Sessions > RDP > Remote Desktop Web Access > Connections** is set to **Predefined configuration**. Further information can be found under *Connections* (page 56).

- **Authentication mode:** Specifies how the user authenticates themselves on the server.

Possible values:


- **Kerberos passthrough authentication:** This option can be used if the local thin client logon takes place via Kerberos. The logon data saved temporarily when logging on to the thin client will be used for the user name and password.
- **Auto logon:** The logon data in **user name**, **password** and **domain** will be used to log on.
- **User logon:** The user enters their data in a logon window.
- **User name:** User name when logging on to the server.
- **Password:** Password when logging on to the server.
- **Domain:** Domain in which the **user name** and **password** are valid.

To select an application for automatic launching, proceed as follows:



Ensure that the **Show applications on the desktop** option under **Sessions > RDP > Remote Desktop Web Access > Appearance** is enabled.



1. Click on  in the **Launch following applications automatically after server connection is established** area.
2. In the **Add** dialog, enter the name of the application. Example: `Word 2013`



You can also enter part of the name followed by an asterisk (*). If for example you enter `Word*`, all available versions of Microsoft Word as well as Microsoft WordPad will be opened.

3. Click on **Next**.

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

7.10.4. Appearance

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Appearance**

In this area, you can decide where you would like to display **RD Web Access applications**:

- In the **start menu**
 - In the **Application Launcher**
 - On the **desktop**
- Enable **Use Extended Filter...** in order to restrict the applications shown to a specific selection.
 - Under **Add**, enter the name of the application that you would like to display on the desktop.
 - You can also select applications that you would like to display in the **Quick Start Panel**:

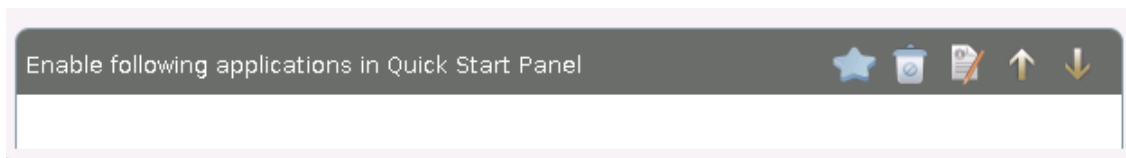


Figure 16: Configuring Quick Start Panel

7.10.5. Logoff / Desktop Integration

Menu path: **Setup > RDP > Remote Desktop Web Access > Logoff**

In these two areas, you can specify how you would like to log on to or log off from the application:

Menu path: **Setup > Sessions > Citrix XenDesktop / XenApp > Legacy ICA Sessions > [Session name] > Desktop Integration**

- Give the **name** of the session that you would like to integrate into the desktop.
- From the **Launch Options**, specify how the session is to be made accessible.
- As an option, specify a **hotkey** for starting the session.
- Enable **Autostart** to start this session immediately after the system starts. Specify by how many seconds the session start is to be delayed when Autostart is used.

Enable **Restart** to restart this session after the connection is terminated.

7.11. Horizon Client Global

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Global**

In this area, you can define the global settings for Horizon Client sessions.

The following settings are carried over from the global settings for RDP sessions; see *RDP Global* (page 42):

- **Drive mapping**; see *Drive mapping (RDP)* (page 45)
- **Number of colors**; see *Window - RDP* (page 44)
- **Window size**; see *Window - RDP* (page 44)
- **Multi-monitor full-screen mode**; see *Window - RDP* (page 44)

7.11.1. Server Options

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Global > Server Options**

In this area, you can specify the settings for the connection between the Horizon Client and the server.

- **Preferred connection protocol**: The selected option is preferred by the client when negotiating the connection protocol.



If the server does not accept the connection protocol preferred by the client, the connection protocol preferred by the server will be used.

Possible values:

- **Server setting**: The client does not give the server details of a preferred connection protocol. The connection protocol preferred by the server is used.
- **RDP**: The client tells the server that it prefers RDP as the connection protocol.
- **PCoIP**: The client tells the server that it prefers PCoIP as the connection protocol.
- **Enable kiosk mode**: If this option is enabled, Horizon Client sessions will be held in kiosk mode.
- **Server certificate verification mode**: Specifies what will happen if server certificate verification fails.

Possible values:

- **Reject if verification fails**
- **Warn if verification fails**
- **Allow unverifiable connections**

7.11.2. Local Logon




Menu path: **Setup > Sessions > Horizon Client > Horizon Client Global > Local Logon**

In this area, you can pre-configure user data. As a result, you can avoid users possibly having to log on a number of times.

You can change the following settings:

- **Use local login window:** If this option is enabled, the local login window of the thin client will be used to log on to the server. If you use the local login window, you can pre-configure login information.
- **Preset login information:** If this option is enabled, login information will appear automatically in the login window. With **Type**, you can specify the source of the login information.
- **Type:**
 - **set user/domain from last logon:** If this option is enabled, the login information from the last session will appear automatically in the login window.
 - **set user/domain from session setup:** If this option is enabled, session-specific login information will appear automatically in the login window. The session-specific login information is described under *Connection Settings* (page 62).
 - **set user/domain from Appliance Mode:** If this option is enabled, the login information specified in the Appliance Mode for VMware Horizon will appear automatically in the login window; see *Appliance Mode* (page 67).
- **Show domain:** If this option is enabled, the domain will be shown in the login window.
- **Restart mode:** If this option is enabled, the login window will be shown in restart mode and cannot be closed.
- **Exit on disconnect or when an error occurs:** If this option is enabled, the session will be ended completely when the connection is terminated. If this option is disabled, the connection overview will be shown when the connection is terminated.

Working with domains:

- To create a domain, click on .
- To remove a domain, click on .
- To change a domain, click on .

➡ Further settings options can be found under *AD/Kerberos Configuration* (page 191) and *AD/Kerberos* (page 190).

7.11.3. USB redirection

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Global > USB Redirection**


In this area, you can enable and configure USB redirection for specific devices.

You can change the following settings:

To enable **USB redirection**, proceed as follows:

1. Enable the option **Enable USB Redirection**.
2. Select a **Default Rule**. The set rule specifies whether USB redirection is allowed or prohibited.
3. Create one or more rules for classes of devices or individual devices.

To create a **class rule**, proceed as follows:


1. To create a new rule, click on  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 **Family**, select the class of device for which the rule should apply. Examples: **Audio**, **Printer**, **Storage Devices**.
4. Under **Name**, give a name for the rule.
5. Click on **Ok**.
6. Click on **Apply** or **OK**.

The rule is active.

To create a **device rule**, proceed as follows:



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

1. To create a new rule, click on  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. Under **Name**, give a name for the rule.
6. Click on **Ok**.
7. Click on **Apply** or **OK**.

The rule is active.

7.11.4. Multimedia

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Global > Multimedia**

You can change the following multimedia settings:

- **Enable VMware Multimedia Redirection**

Possible values:

- **off**: The server renders the multimedia data and sends the individual images to the client.
- **on**: The client renders the multimedia data supplied by the server.

- **Real Time Audio Video (RTAV)**: Specifies the redirection of video data from the client USB webcam.

Possible values:

- **off**: The client does not forward the webcam data as video data.



With USB redirection, data from the webcam can be forwarded to the server even if RTAV is disabled.

- **on**: The client forwards the webcam data as video data.

7.11.5. Performance

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Global > Performance**

In this area, you can optimize the performance of Horizon Client sessions.

You can change the following settings:

- **PCoIP client-side image cache size:** Specifies the size of the cache for images. Caching parts of the display reduces the amount of data to be transferred.



Larger cache sizes of 250 MB or more should only be used if at least 2 GB RAM or more is available.

7.11.6. Smartcard

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Global > Smartcard**

In this area, you can specify which smartcards are authorized when logging on.

7.12. Horizon Client session

7.12.1. Connection settings

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Connection Settings**

In this area, you can specify the settings for the connection between the Horizon Client and the server.

- **Server URL:** URL of the VMware Horizon server
- **Use Passthrough authentication for this session:** If this option is enabled, the user name and password will be temporarily saved and used for authentication during this session.
- **Username:** User name when logging on to the VMware Horizon server
- **User password:** Password when logging on to the VMware Horizon server
- **Domain:** Domain when logging on to the VMware Horizon server
- **Session type:** Specifies whether the session contains a desktop or an individual application.

Possible values:

- **Desktop:** The session contains a desktop.
 - **Application:** The session contains an individual application.
 - **Desktopname:** Specifies a name for the desktop. This option is available if **Session Type** is set to **Desktop**.
 - **Application:** Application that is launched during the session. This option is available if **Session Type** is set to **Application**.
 - **Autoconnect:** If this option is enabled, the connection to the desktop or application will be established automatically when the session starts. For this to be possible, the name of the desktop or application must be defined. If this option is disabled, the overview will be shown when the session starts.
 - **Preferred desktop protocol:** The selected option is preferred by the client when negotiating the connection protocol.
 - **Enable kiosk mode:** If this option is enabled, the session will be held in kiosk mode.
- ➡ Further settings options can be found under *AD/Kerberos Configuration* (page 191) and *AD/Kerberos* (page 190).

7.12.2. Window

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Window**

In this area, you can change the way in which the session is displayed.

- **Window Size:** Specifies the width and height of the window.



The window size is carried over from the global settings for RDP sessions, see *Window* (page 44).

- **Number of Colors:** Specifies the color depth.



The color depth is carried over from the global settings for RDP sessions, see *Window* (page 44).

- **Start Monitor:** Specifies the monitor on which the session is shown.

➡ Further settings options can be found under *Screen* (page 132) and *Window* (page 44).

7.12.3. Mouse and keyboard

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Mouse and Keyboard**

In this area, you can define the settings for the mouse and keyboard.

- **Disable mouse movement events:** If this option is enabled, the mouse pointer will only be shown locally on the thin client. If the user moves the mouse over a session item, no reaction of the item will be shown.

➡ Further settings options can be found under *Language* (page 146) and *Keyboard and Additional Keyboard* (page 150).

7.12.4. Mapping

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Mapping**

In this area, you can specify the data transmission between the thin client and the Horizon Client session.

- **Enable Client Audio:** If this option is enabled, audio data are transmitted.
- **Enable Clipboard:** If this option is enabled, the clipboard will be available.
- **Enable Printer Mapping:** If this option is enabled, the printer will be available.
- **Enable Com Port mapping:** If this option is enabled, the COM port will be available.
- **Enable Drive Mapping:** If this option is enabled, the external drives will be available.
- **Enable USB Redirection:** If this option is enabled, the client's USB data will be forwarded to the server.

➡ Further settings options can be found under *Drive Mapping* (page 45), *Serial Connections (RDP)* (page 45), *Printers (RDP)* (page 46), *Audio* (page 47), *Keyboard* (page 44) and *Printers (Devices)* (page 179).

7.12.5. Performance

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Performance**

In this area, you can save system resources by disabling certain visual functions of the user interface.

- **Disable Wallpaper:** If this option is enabled, no desktop background image will be displayed.
- **Don't show contents of window while dragging:** If this option is enabled, the content of a window will not be shown when the window is moved.
- **Disable Menu and Window animation:** If this option is enabled, transitions for menus and windows will not be animated.
- **Disable Themes:** If this option is enabled, no optional desktop design will be used.
- **Disable Cursor Shadow:** If this option is enabled, the mouse pointer will be shown without a shadow.
- **Disable Cursor Settings**
- **Enable font smoothing:** If this option is enabled, the edges of fonts will be smoothed.

➡ Further settings options can be found under *Performance (Horizon Global)* (page 62) and *Performance (RDP Global)* (page 47).

7.12.6. Options

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Options**

In this area, you can change various settings.

- **Working Directory:** Directory that is used after logging on
- **Compression:** If this option is enabled, the flow of data between the client and server will be compressed.
- **Enforce TLS encrypted connection:** If this option is enabled, the flow of data between the client and server will be encrypted with TLS.
- **Network Level Authentication:** If this option is enabled, the user will authenticate themselves on the network level (network layer authentication) in order to establish an RDP connection.



If network level authentication is enabled, the local logon window is used. This also applies if the **Use local logon window** option under **Setup > Sessions > Horizon Client > Horizon Client Global > Local Logon** is disabled.

➡ Further settings options can be found under *Options (RDP Global)* (page 48), *Performance (RDP Global)* (page 47) and *Local Logon (Horizon Global)* (page 59).

7.12.7. Multimedia

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Multimedia**

You can change the following multimedia setting:

- **VMware multimedia redirection**

Possible values:

- **Global setting:** The global setting for Horizon Client sessions is used, see *Horizon Client Global Multimedia* (page 61).
- **off:** The server renders the multimedia data and sends the individual images to the client.

➡ Further settings options can be found under *Horizon Client Global Multimedia* (page 61).

7.12.8. Proxy

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Proxy**

In this area, you can configure the use of a proxy for the connection between the client and server.

You can change the following settings:

- **Direct connection to the internet:** If this option is enabled, no proxy is used.
- **Manual proxy configuration:** If this option is enabled, a proxy is used. The configuration must be specified in the following fields.
 - **HTTP proxy:** URL of the proxy for HTTP
 - **Port:** Port of the proxy for HTTP
 - **SSL proxy:** URL of the proxy for SSL
 - **Port:** Port of the proxy for SSL
 - **SOCKS host:** URL of the proxy for SOCKS
 - **Port:** Port of the proxy for SOCKS
 - **SOCKS protocol version:** Version of the SOCKS protocol used
 - **No proxy for:** List of URLs for which no proxy is to be used.
- **System-wide proxy configuration:** If this option is enabled, the proxy configured under **Setup > Network > Proxy** will be used.

➡ Further settings options can be found under *System-wide Proxy (Network)* (page 178).

7.13. vWorkspace Client and AppPortal

Menu path: **Setup > Sessions > vWorkspace Client**

By default, **vWorkspace Client** session settings are carried over from the **RDP Global** setup pages. You can change the configuration on the corresponding setup pages for **vWorkspace Client** sessions.



The **vWorkspace Client** is based on hypervisors from other providers and is therefore compatible with VMware, vSphere, Microsoft Hyper-V and XenServer.

➡ All configuration parameters for the **vWorkspace Client** and the **vWorkspace AppPortal Farm** are described in detail in the original documentation for the relevant client version, for Quest, see <https://support.quest.com/Default.aspx>.

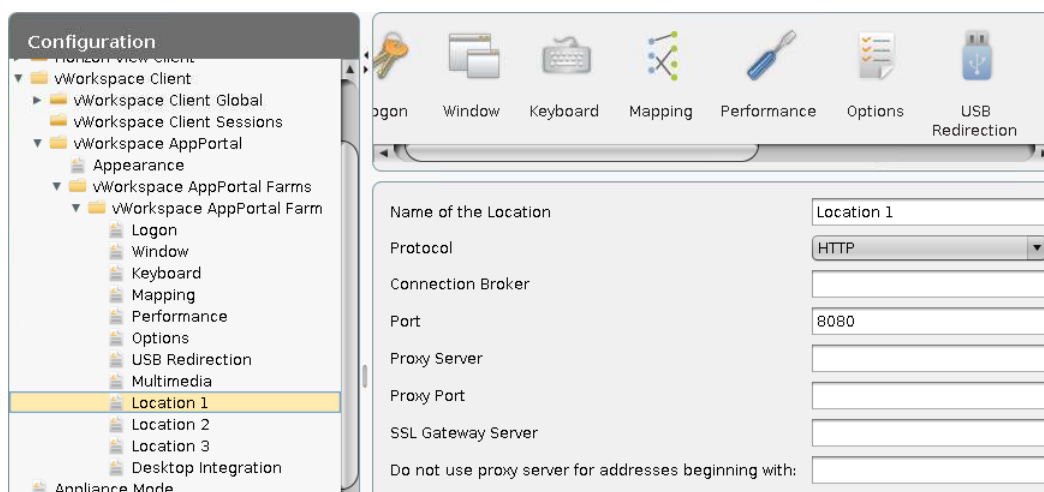


Figure 17: AppPortal farms configuration

7.14. Appliance Mode

Menu path: **Setup > Sessions > Appliance Mode**

In Appliance Mode, only a specific session is shown. Access to other applications is not possible.

To enable Appliance Mode for a session type, proceed as follows.

1. In Appliance Mode pull-down menu, select the session type for which Appliance Mode is to be enabled.

You can enable Appliance Mode for one of the following session types:

- VMware Horizon (page 67)
- Citrix XenDesktop (page 68) (for published desktops only, not for published applications)
- Citrix Self-Service (page 68)
- RHEV/Spice (page 69)
- Imprivata (page 69)
- RDP Multipoint Server (page 70)
- Caradigm (page 70)

2. Enter the necessary configuration data for the selected session type.



The system hotkey **Ctrl+Alt+S** for launching the setup application does not work in the Appliance Mode. Use **Ctrl+Alt+F2** instead.



You can set up a hotkey in order to launch quick setup in Appliance Mode. You will find instructions for setting up the hotkey under *Desktop Integration* (page 21).

7.14.1. VMware Horizon

Menu path: **Setup > Sessions > Appliance Mode > VMware Horizon**

- **Server URL:** URL of the VMware Horizon server
- **Username:** User name when logging on to the VMware Horizon server
- **User password:** Password when logging on to the VMware Horizon server
- **Domain:** Domain when logging on to the VMware Horizon server
- **Desktop name:** Desktop that is to be launched automatically
- **Autoconnect:** If this option is enabled, the desktop given in **Desktop name** will be launched automatically.
- **Network Level Authentication:** If this option is enabled, the user will authenticate themselves on the network level (network layer authentication) in order to establish an RDP connection.



If network level authentication is enabled, the local logon window is used. This also applies if the **Use local login window** option under **Setup > Sessions > Horizon Client > Horizon Client Global > Local Logon** is disabled.

- **Enable on-screen keyboard:** If this option is enabled and a touchscreen is available, an on-screen keyboard will be shown.



If the on-screen keyboard is enabled, the local logon window is used. This also applies if the **Use local logon window** option under **Setup > Sessions > Horizon Client > Horizon Client Global > Local Logon** is disabled.

- **X position of the on-screen keyboard:** Specifies the X position of the on-screen keyboard.
- **Y position of the on-screen keyboard:** Specifies the Y position of the on-screen keyboard.
- **Width of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height.
- **Height of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height.

7.14.2. Citrix XenDesktop

Menu path: **Setup > Sessions > Appliance Mode > Citrix XenDesktop**

- **XenDesktop Delivery Server URL:** URL of the XenDesktop Delivery server
- **Enable Smartcard Login:** If this option is enabled, the user can log on with a smartcard.



When the option is enabled, the browser and Xen will be restarted.

- **Enable on-screen keyboard:** If this option is enabled and the screen is a touchscreen, an on-screen keyboard will be shown.
- **X position of the on-screen keyboard:** Specifies the X position of the on-screen keyboard.
- **Y position of the on-screen keyboard:** Specifies the Y position of the on-screen keyboard.
- **Width of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height.
- **Height of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height.

7.14.3. Citrix Self-Service

Menu path: **Setup > Sessions > Appliance Mode > Citrix Self-Service**

- **Self-Service Delivery Server URL:** Server address including the `http://` prefix.



In the Appliance Mode, only a single server can be used for Self-Service.

- **Multi User (StoreFront servers only):** If this option is enabled, the user data on the client will be deleted after logging off or closing the UI.
- **Reconnect after logon:** If this option is enabled, the Self-Service UI will reconnect automatically after the launch.
- **Reconnect to app after starting an application:** If this option is enabled, the Self-Service UI will attempt to reconnect to ongoing sessions if an application is launched or the store is reloaded.
- **Enable on-screen keyboard:** If this option is enabled and the screen is a touchscreen, an on-screen keyboard will be shown.

- **X coordinate of the on-screen keyboard:** Specifies the X position of the on-screen keyboard.
- **Y coordinate of the on-screen keyboard:** Specifies the Y position of the on-screen keyboard.
- **Width of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height.
- **Height of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height.

7.14.4. RHEV/Spice

Menu path: **Setup > Sessions > Appliance Mode > RHEV/Spice**

- **Connection Broker:** URL of the Connection Broker
- **Enable on-screen keyboard:** If this option is enabled and the screen is a touchscreen, an on-screen keyboard will be shown.
- **X position of the on-screen keyboard:** Specifies the X position of the on-screen keyboard.
- **Y position of the on-screen keyboard:** Specifies the Y position of the on-screen keyboard.
- **Width of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height.
- **Height of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height.

7.14.5. Imprivata

Menu path: **Setup > Sessions > Appliance Mode > Imprivata**

- **Set the URL to the server:** URL of the single sign on server
- **Path to the Appliance:** Path to the appliance on the single-sign-on server
- **Clear Imprivata data partition:** If this option is enabled, information on the Imprivata data partition will be deleted.
- **Enable Logging of the Bootstrap Component:** If this option is enabled, the bootstrap component will generate a log.
- **Bootstrap Component's Logging Verbosity:** Specifies the level of detail for the bootstrap component log.
- **Generic session:** Give the name of the Citrix session that you have configured for Citrix Fast User Switching using generic credentials.
- **Enable on-screen keyboard:** If this option is enabled and the screen is a touchscreen, an on-screen keyboard will be shown.
- **X position of the on-screen keyboard:** Specifies the X position of the on-screen keyboard.
- **Y position of the on-screen keyboard:** Specifies the Y position of the on-screen keyboard.
- **Width of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height.
- **Height of on-screen keyboard in pixels:** It is recommended that you specify either the width or the height.

7.14.6. RDP Multipoint Server

Menu path: **Setup > Sessions > Appliance Mode > RDP Multipoint Server**

- **Connect to the server once it has been found:** The thin client will find one or more RDP Multipoint Servers by itself if these are in the same network as the thin client and obtain their IP address from the same DHCP server as the thin client.

7.14.7. Caradigm

Menu path: **Setup > Sessions > Appliance Mode > Caradigm**

The Caradigm appliance is integrated from IGEL Linux Version 5.09.100.

- **Caradigm Vault VIP** - IP address or host name of the Caradigm authentication server, also referred to as the Vault
- **Caradigm Vault Port** - Port number of the Caradigm authentication server (default port: 8443)



For the certificates that follow, you have to send the certificate files to the client via the file transfer - to the directory `wfs/ca-certs/`. Three files are needed: the thin client certificate, the thin client private key and the Root-CA public key. Now enter the certificates here in the setup. The CA certificates must not be changed because the Root-CA is automatically available after the first reboot via the file `ca-certificates.crt`.

- **SSL Client Private Key** - Path to the thin client private key
- **SSL Client Certificate** - Path to the client certificate
- **CA certs file** - Path to the file which contains the CA certificates. (Default: `/etc/ssl/certs/ca-certificates.crt`)
- **Disable SSL certificate validation:** If this option is enabled, SSL validation will be disabled for test purposes. Normally, the certificates should always be validated.
- **Timeout:** Specifies the number of seconds after which the connection is automatically terminated.
- **Way2Care (EGP):** Name of a group within which the user can log on system-wide with a card without having to authenticate themselves again.



This function only affects desktop sessions.

- **Session type** - Selects the session type. To do this, you must have entered the server in the relevant session beforehand.
- **Default domain** - The following options are available for specifying the domain:
 - The authentication server returns a domain.
 - A default domain for the Caradigm Appliance is set.
 - A system-wide default domain is entered. You will find it under **IGEL Setup > Network > LAN Interfaces > Default Domain**.
 - The user enters the domain manually when logging on.

- **Logout behavior** - The logoff behavior can be specified for Citrix HDX/ICA. The following are possible:
 - **User choice**
 - **Force disconnect**
 - **Force logoff**
- **Company logo** - (optional) Full path of an image file for a logo which is to appear in the logon window.
- **Logging** - Enables local logging.
 - **Logging verbosity** - Specifies how exact logging is to be. The selection options are narrowed down more and more in a downward direction.
- **On-screen Keyboard** - If this option is enabled, an on-screen keyboard will be shown.
 - **X coordinate of on-screen keyboard**: Specifies the X position of the on-screen keyboard.
 - **Y coordinate of on-screen keyboard**: Specifies the Y position of the on-screen keyboard.
 - **Width of on-screen keyboard in pixels**: It is recommended that you specify either the width or the height.
 - **Height of on-screen keyboard in pixels**: It is recommended that you specify either the width or the height.

Smartcard logon

To log on or off using a smartcard, proceed as follows:

- Tap the card on the card reader to log on.
- Tap the card on the card reader once more to log off again.



If you leave the terminal without logging off, you will automatically be logged off as soon as another user logs on.

Forgot your card?

1. Click on the arrow at the bottom right of the logon mask.
The **Enter user data** mask will open.
2. Enter your logon data.

7.15. Leostream Connection Broker

Menu path: **Setup > Sessions > Leostream**

In this area, you can configure settings for the **Leostream Connection Broker**. You have the following options:

Connections	Details of the server and domain for logging on.
Desktop integration	Start option settings for this session.
Options	Setting up the logon prompt and USB redirection.



By default, the RD Desktop client is used for the connection in UDLX – rdesktop must therefore be set as the Leostream API protocol with priority 1 on the server.

LEOSTREAM			
Status Resources Clients Plans			
Protocol Power Control Release Display Printer			
Create Protocol Plan			
Actions	Name	Leostream API Protocols	iTap Protocols
	All		
Edit	Default	rdesktop, RDP, NoMachine NX	RDP
Edit	"Default" policy	rdesktop	RDP, VNC
2 rows			

Figure 18: Leostream-API protocol

➡ More information on the Leostream Connection Broker is available from Leostream by visiting: <http://www.leostream.com/resources/downloads.php>.

7.16. Systancia AppliDis Client

Menu path: **Setup > Sessions > AppliDis**

AppliDis Fusion 4 is a virtualization solution which combines the virtualization of desktops and applications in a single console.

If you create an AppliDis session, you can configure the following settings:

Connections	Details of the Server URL and Connection Type for logging on. If you use AppliDis SLB Linux in the Connector Mode, the name of the application that uses the connector can be specified here.
Options	Allows you to define the language, access data, access path and further settings for the AppliDis client.
Desktop integration	Start option settings for this session.

➡ The original documentation with a description of all parameters for the Systancia AppliDis Fusion 4 Client and the administration manual are available from Systancia Experts.

7.17. Evidian AuthMgr

Menu path: **Setup > Sessions > Evidian AuthMgr**

Using the **Evidian Authentication Manager (AuthMgr)**, you can log on to Citrix ICA, RDP and VMware Horizon roaming sessions using an RFID card. The Evidian AuthMgr can also execute user-defined commands.

➡ You can find setup instructions in a best practice document.

7.18. NoMachine NX

Menu path: **Setup > Sessions > NX > [Session Name]**

If you configure an NX session, retain the NX server data.

Under **NX > [Session Name] > Connections > Server**, select the session type. Depending on the session type chosen, either the Unix Desktop, Windows Desktop or VNC Desktop setup pages are enabled to allow further configuration.

The IGEL setup pages for NX sessions are essentially an adapted graphical user interface for the NoMachine NX Client.

➡ Further information regarding configuration (performance, services etc.) can be found in the original documentation provided by NoMachine: <http://www.nomachine.com/documents.php>

7.19. X Session

Menu path: **Setup > Sessions > X Sessions**

Set up the basic connection data (type, server and command) on the server side and specify the necessary hotkey and window parameters in order to launch an X session.

7.20. Parallels 2X client session

Menu path: **Setup > Sessions > Parallels 2X Client**

Virtual desktops and applications can also be provided via 2X Application Server XG. A suitable client for access is included in IGEL Linux.

A more detailed description of all available parameters as well as information regarding use of the client is available from 2X:

- ➡ http://www.2x.com/docs/en/manuals/html/clientlinux_manual/2XClientForLinux.html
- ➡ <http://www.2x.com/docs/en/manuals/html/client-windows/2XClientForWindows.html>

7.21. PowerTerm WebConnect

Menu path: **Setup > Sessions > PowerTerm WebConnect**

You can access the following applications locally or remotely via **PowerTerm WebConnect**:

- Windows terminal server
 - A virtual desktop (on hypervisors such as VMware, Microsoft, Citrix and Virtual Iron)
 - Blade PCs
 - Legacy hosts
- Enter the host name of the WebConnect server to which you would like to establish a connection.
- ➡ The server configuration is described in Ericom's WebConnect documentation: PtSeriesUsersGuide_LTC.pdf.

7.22. PowerTerm terminal emulation

Menu path: **Setup > Sessions > PowerTerm Terminal Emulation**

The PowerTerm InterConnect software we use in IGEL Linux is the official Linux version from ERICOM Software Ltd.



To use your Ericom PowerTerm Terminal emulation you need a free license key from IGEL. To get to the activation form please register at our support and ticket system.

To configure a session:

1. Click on **Add New Session**.
2. Select **PowerTerm** as the session type.

The **PowerTerm Emulation Setup** window opens.

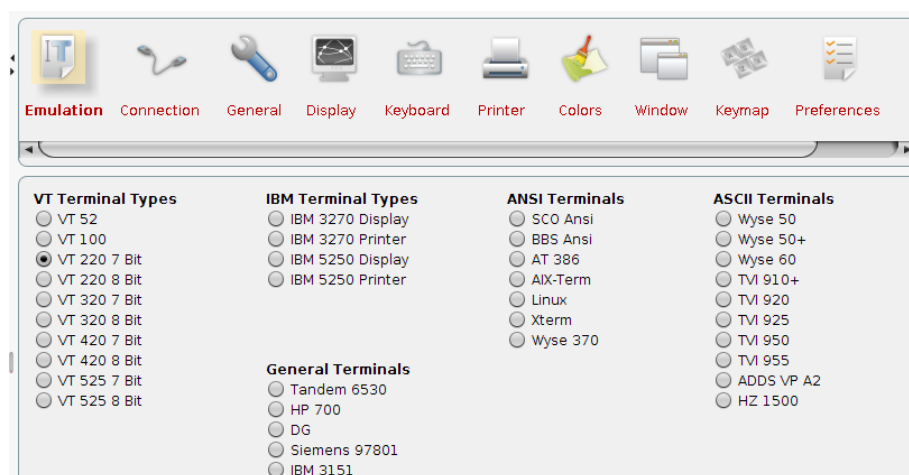


Figure 19: PowerTerm Emulation setup

This setup offers a good overview of the emulation types supported.

The setup pages used here were designed to look as similar as possible to the setup pages described in the original documentation from ERICOM Software Ltd.

➡ You will find detailed information on configuring the PowerTerm software in the PowerTerm manual on the Ericom documentation website.

7.22.1. PowerTerm selection

Two versions of the PowerTerm are available to choose from here:

- 10.1.0.0.20130211.2-_rc_-31580
- 9.2.0.6.20091224.1-_rc_-25848

Default, which corresponds to Version 9.2.0.6.20091224.1-_rc_-25848, is preset.

7.23. IBM iSeries Access

Menu path: **Setup > Sessions > IBM iSeriesAccess**

IBM iSeries Access for Linux (5722-XL1) offers emulation of the IBM-5250 terminal.

- ➡ A full description of the emulation is available from IBM by visiting:
<http://publib.boulder.ibm.com/infocenter/iseriess/v5r4/index.jsp?topic=%2Frzatzv%2FrzatzvI5250.htm>.



The configuration is not accessible until the user confirms that the necessary license is available.

7.24. ThinLinc

Menu path: **Setup > Sessions > ThinLinc**

You can set up one or more Thin Linc sessions.

- ➡ You will find further information on setting up the session in the "Client Configuration" chapter of the ThinLinc administration handbook: <http://www.cendio.com/resources/docs/adminguide.pdf>.

7.24.1. ThinLinc Global

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

In this area, you can change the global settings for ThinLinc sessions.

Server

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > Server**

You can specify the port for communication between the client and server and allow remote monitoring of the client through shadowing.

- **SSH port**
Possible values:
 - **Default SSH (22):** Port 22 is used.
 - **HTTP (80):** Port 80 is used.
 - **Custom:** Under **Custom Port number**, you can enter an alternative port number.
- **User-defined port number:** Alternative port number
- **Enable shadowing:** If this option is enabled, the session can be remote monitored by shadowing via VNC.

Window

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

In this area, you can define the window settings for ThinLinc sessions.

- **Screen size**

Possible values:

- **800x600**
 - **1024x768**
 - **1280 x 1024**
 - **1600x1200**
 - **Current monitor:** The entire display area of the current monitor is used for the ThinLinc session.
 - **All monitors:** The display area of all monitors is used for the ThinLinc session.
 - **Work area (maximized):** The display area of the current monitor minus the height of the taskbar is used for the ThinLinc session.
 - **Custom size:** The display area specified with **Custom Screen Width** and **Custom Screen Height** is used for the ThinLinc session.
- **Custom Screen Width:** Width of the display area for the session in pixels
 - **Custom Screen Height:** Height of the display area for the session in pixels
 - **Full-screen mode:** If this option is enabled, the entire screen area will be used for the ThinLinc session.
 - **Full screen all monitors:** If this option is enabled, the entire screen areas of all monitors will be used for the ThinLinc session.
 - **Control bar for ThinLinc sessions:** If this option is enabled, a session control bar will be shown for a ThinLinc session in full-screen mode. You can minimize or close the session with the control bar.


Options

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

You can change various settings and enable local directories.

- **Enable Sound:** If this option is enabled, the audio output will be forwarded from the server to the thin client. The audio data can then be played back via the built-in loudspeaker or the headset.
- **Redirect Serial Port:** If this option is enabled, the data from the thin client serial port will be forwarded to the server. The serial port can then be used in the ThinLinc session.
- **Enable Printer:** If this option is enabled, local printers can be used in the session.
- **Enable Smartcard Readers:** If this option is enabled, the server will be given access to the local smartcard reader.
- **Enable Drive Access:** If this option is enabled, the server will be given access to local directories. These directories can be selected in the **Exported Paths and Permissions** area.

To select a local directory for server-side access, proceed as follows:

1. Click on .
2. In the **Path** field, enter the local directory path. Example: `/userhome`
3. Select the **Permission** that the server is to have for the directory.

- **Read only:** The server has read rights for the directory but no write rights.
- **Read/Write:** The server has read and write rights for the directory.
- **Disabled:** The server has no read rights and no write rights for the directory.



If you set a directory to **Disabled**, ensure that it is not a sub-directory of a directory for which the server has read or write rights.

4. Click on **Ok**.

Optimization

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization**

You can increase the transmission speed by setting various compression procedures.

- **Enable Custom compression level:** If this option is enabled, you can specify how much the data transmitted between the client and server are compressed. If this option is disabled, compression level 8 will be used.
- **Compression level:** Allows you to select the compression level; 9 is the highest compression
- **Use JPEG Compression:** If this option is enabled, graphical data will be compressed using the JPEG procedure.



A higher JPEG compression level saves bandwidth but reduces the image quality.

- **JPEG Quality:** Allows you to select the image quality. 1 means the highest compression and the lowest image quality, 9 means the lowest compression and the highest image quality.
- **SSH Compression:** If this option is enabled, the data will be compressed using SSH.

VNC Optimization

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > VNC Optimization**

You can change VNC protocol settings in order to optimize transmission.

- **VNC autoselect:** If this option is enabled, the coding and color depth will be set automatically.
- **Preferred encoding:** Specifies how the data to be transmitted are to be coded. The coding is negotiated between the client and server.

Possible values:

- **Tight**
- **ZRLE**
- **Hextile**
- **raw**

- **Color depth:** Allows you to select the color resolution

Possible values:

- **Full (all colors):** The maximum value set on the server is used.
- **Medium (256 colors)**
- **Low (64 colors)**
- **Very low (8 colors)**

7.24.2. ThinLinc Sessions

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name]**

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

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



The session name must not contain any of these characters:

\ / : * ? " < > | [] { } ()

- **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.
- **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:** Specifies a hotkey consisting of modifiers and a key which can be used to launch the session.
- **Modifiers:** One or two modifiers for the hotkey
- **Key:** Key for the hotkey
- **Autostart:** If this option is enabled, the session will be launched automatically when the thin client boots.
- **Restart:** If this option is enabled, the session will be relaunched automatically after termination.
- **Autostart Delay:** Waiting time in seconds between the thin client booting and the session being launched automatically.

Server

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Server**

- **Server:** Name or URL of the ThinLinc server
- **User:** User name for the connection to the ThinLinc server
- **Password:** Password for the connection to the ThinLinc server
- **Use global SSH port settings:** If this option is enabled, the port set under **Setup > Sessions > ThinLinc > ThinLinc Global > Server** will be used for the SSH connection. If this option is disabled, the port set in **SSH Port** or **Custom Port Number** will be used.
- **SSH port**

Possible values:

- **Default SSH (22):** Port 22 is used, the default port for SSH connections.
- **HTTP (80):** Port 80 is used, the default port for HTTP connections.
- **Custom:** Under **User-defined port number**, you can enter an alternative port number.
- **Custom Port Number:** Alternative port number

Window

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Window**

In this area, you can define the window settings for the ThinLinc session. You will find a description under the global settings, see *Window* (page 77).



You can only enable the control bar for ThinLinc sessions in the global settings.

- **Use global screen settings:** If this option is enabled, the settings under **Setup > Sessions > ThinLinc > ThinLinc Global > Window** will be used, see *Window* (page 77).

Options

Menu path: **Setup > Menu Path: Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Options**

You can change various settings, allow access to local directories and allow shadowing.

- **Use global shadowing settings:** If this option is enabled, permission for shadowing will be specified under **Setup > Menu Path: Setup > Sessions > ThinLinc > ThinLinc Global > Server**, see *Server* (page 76).
- **Enable shadowing:** If this option is enabled, the session can be remote monitored by shadowing via VNC.
- **Enable Sound:** If this option is enabled, the audio output will be forwarded to the thin client.
- **Enable Serial Port:** If this option is enabled, the serial interface of the thin client can be used in the session.
- **Enable Printer:** If this option is enabled, local printers can be used in the session.
- **Enable SmartCard Readers:** If this option is enabled, the server will be given access to the local smartcard reader.
- **Enable Srive Access:** If this option is enabled, the server will be given access to local directories. These directories can be selected in the **Exported Paths and Permissions** area.
- **Options Popup Key:** Specifies the key which brings up the options menu.

Optimization

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Optimization**

In this area, you can define the settings for optimizing the ThinLinc session. You will find a description under the global settings, see *Optimization* (page 78).

- **Use global compression level:** If this option is enabled, the settings under **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization** will be used for **Use user-defined compression level** and **Compression level**.
- **Use global JPEG quality settings:** If this option is enabled, the settings under **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization** will be used for **Use JPEG compression** and **JPEG quality**.
- **Use global SSH connection settings:** If this option is enabled, the settings under **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization** will be used for **SSH compression**.

VNC Optimization

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > VNC Optimization**

In this area, you can define settings for the VNC protocol in order to optimize transmission. You will find a description under the global settings, see *VNC Optimization* (page 78).

- **Use global VNC settings:** If this option is enabled, the settings under **Setup > Sessions > ThinLinc > ThinLinc Global > VNC Optimization** will be used.

User Interface

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > User Interface**

You can change the fields and settings options of the logon window as well as the **ThinLinc Client Options** dialog.

- **Lock Server Name:** If this option is enabled, the server name given under **Setup > Sessions > ThinLinc Sessions > Server** will be used and it will not be possible to change it in the logon window.
- **Hide options button:** If this option is enabled, the **Options** button will not appear in the logon window. The **ThinLinc Client Options** dialog therefore cannot be opened.
- **Advanced Mode:** If this option is enabled, the fields which can be opened under **Advanced** will appear when the session is launched.
- **Lock ThinLinc Options Tab:** If this option is enabled, the settings in the **Options** tab cannot be changed in the **ThinLinc Client Options** dialog.
- **Lock Local Devices Options Tab:** If this option is enabled, the settings in the **Local Devices** tab cannot be changed in the **ThinLinc Client Options** dialog.
- **Lock ThinLinc Screen Tab:** If this option is enabled, the settings in the **Screen** tab cannot be changed in the **ThinLinc Client Options** dialog.
- **Lock ThinLinc Optimization Tab:** If this option is enabled, the settings in the **Optimization** tab cannot be changed in the **ThinLinc Client Options** dialog.
- **Lock Security Tab:** If this option is enabled, the settings in the **Security** tab cannot be changed in the **ThinLinc Client Options** dialog.
- **Debug level:** Specifies how detailed the debugging information is to be. 1 is the lowest level, 5 is the highest.

7.25. SSH Session

Menu path: **Setup > Sessions > SSH**

This section describes the procedure for configuring an SSH session.

Use the SSH session to launch a remote application on the host via SSH (Secure Shell) and display it on the terminal. SSH allows secure, encrypted communication between two hosts or host and terminal via an unsecured network. X11 connections can also be routed via this secure channel.

Command	All necessary entries for creating an executable command to remotely launch the application via SSH
User name (remote)	Name of the remote user - The selected user must have a user account on the remote host.
Computer (remote)	Name or IP address of the remote host from which the remote application is launched.
Command line	Allows you to enter the name of the application program which is to be launched.
Options	
Forward X11 connection	X11 connections are automatically forwarded to the remote computer so that each X11 program launched from the shell or the command passes through the encrypted SSH channel. The authentication data are also defined automatically. This option is enabled by default.
Enable compression	Reduces the amount of data transmitted via the data channel - This option is disabled by default.
Get protocol version	You must prove your identity to the remote host using one of the various identification methods. These depend on the protocol version used. In this area, you can obtain details of the protocol version after opting for a particular identification method.

➡ You will find detailed information on SSH and the various authentication methods on the relevant pages of the manual for your server operating system.

7.26. VNC Viewer

Menu path: **Setup > Sessions > VNC Viewer**

Create a **VNC Viewer session** in order to be able to access remote computers (VNC server) via the thin client. Connection options such as the server address or the full-screen mode can be pre-populated for each session or defined individually when the system starts.



If a server address is specified for the session, the connection dialog will not appear when the session starts – the connection will be established immediately.

7.27. VERDE session

Menu path: **Setup > Sessions > VERDE Sessions**

Virtual Bridges VERDE is a scalable virtual desktop solution. It supports traditional virtual desktop environments, available remote branches and both Windows and Linux users. VERDE is the basis for IBM Virtual Desktop.

➡ More information is available from Nimboxx.

7.28. Firefox browser

Menu path: **Setup > Sessions > Browser**

In order to allow central configuration via the IGEL UMS, the original configuration parameters for the Firefox 38.4.0 ESR web browser are assigned to the IGEL setup. These global settings can be changed for each browser session.

7.28.1. Browser Global

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

In this area, you can define the start page, display resolution and font size for the browser.

You can change the following settings:

- **When browser starts:** Specifies what pages are shown when the browser is launched.
 - **Start with a blank page**
 - **Show my home page**
 - **Resume previous session:** All tabs from the last session are reopened.
- **Home page:** Specifies the URL of the start page. You can specify a number of start pages by separating the URLs of the start pages with a vertical dash "|".
- **Display resolution:** Specifies the display resolution for the browser in DPI. Typical values are **72** for medium screens and **96** for large screens.
- **Minimum font size:** Specifies the minimum size of the fonts displayed on websites. The formats of the websites are overwritten in the process.
- **Show browser splash screen:** If this option is enabled, a Firefox logo will be shown in the middle of the screen when the browser is launched.

Tabs

Menu path: **Setup > Sessions > Browser > Browser Global > Tabs**

In this area, you can define settings for the browser tabs.

You can change the following settings:

- **New pages should be opened in:** Specifies how links to new pages are to be opened.
 - **the current window:** The page will open in the current window even if the link defines a new window as the target.
 - **a new window:** If the link does not define a target, the page will open in the current window. If the link defines a new window as the target, the page will open in a new window.
 - **a new tab:** If the link does not define a target, the page will open in the current window. If the link defines a new window as the target, the page will open in a new tab.
- **Warn me when closing multiple tabs:** If this option is enabled, a warning will be shown as soon as you attempt to close a browser window with a number of tabs.
- **Warn me when opening multiple tabs might slow down the browser:** If this option is enabled, a warning will be shown as soon as you open a very large number of tabs.
- **When a link is opened in a new tab, switch to it immediately:** If this option is enabled, the focus will switch to the new tab when a new tab is opened by a link. If this option is disabled, the focus will be retained when a new tab is opened by a link.

Content

Menu path: **Setup > Sessions > Browser > Browser Global > Content**

In this area, you can change settings regarding popups, JavaScript, downloads and the browser display.

- **Block pop-up windows:** If this option is enabled, websites will be prevented from automatically opening popups. With **Exceptions...**, you can allow popups to be opened automatically for specific websites.

To add an exception for the automatic opening of popups, proceed as follows:

a) Click on **Exceptions...**




b) Click on

c) In the **Website** field, give the URL of the website for which the exception is to apply.

d) Click on **Ok**.

- **Load images automatically:** If this option is enabled, websites will be loaded in full, including all images. If this option is disabled, the images will not be loaded and placeholders will be shown instead. As a result of this, websites can be displayed more quickly, but the layout is impaired. With **Exceptions...** you can allow or prevent automatic loading for specific websites.

To add an exception for the automatic loading of images, proceed as follows:

- Click on **Exceptions...**
 - Click on .
 - In the **Website** field, give the URL of the website for which the exception is to apply.
 - Using the **Status** drop-down menu, specify whether the automatic loading of images is to be allowed or prevented for the given website.
 - Click on **Ok**.
- **Type of download directory:** Specifies the directory in which a downloaded file is saved.
 - **userhome:** The file is saved locally on the thin client desktop.
 - **user-defined path:** You can specify whether the downloaded file is to be opened with an application or saved locally.
 - **Download path:** Local directory in which the downloaded file is saved if **Type of download directory** is set to **user-defined path**. Example: /userhome
 - **Enable JavaScript:** If this option is enabled, JavaScript will run on websites.
 - **Raise or lower windows:** If this option is enabled, a website can place windows in the background or foreground via JavaScript.
 - **Move or resize existing windows:** If this option is enabled, a website can move windows or change the window size via JavaScript.
 - **Disable or replace context menus:** If this option is enabled, a website can define a custom context menu via JavaScript; the browser's own context menu will be suppressed in the process.
 - **Languages for Web Pages:** One or more preferred languages for multilingual websites, given in the form of language abbreviations separated by commas. The languages should be given in the order of preference. Example: With `de, en, fr, it`, the website will be shown in German, if available, otherwise in English etc.

Print

Menu path: **Setup > Sessions > Browser > Browser Global > Print**

In this area, you can set the **Default Paper Size** for the printer.

- **Use system settings for default paper size:** If this option is enabled, the paper size set globally will be used when printing websites. If this option is disabled, you can set the paper size via **Default Paper Size**.
- **Default Paper Size:** Preset paper size when printing websites.

Proxy

Menu path: **Setup > Sessions > Browser > Browser Global > Proxy**

In this area, you can change the proxy configuration.

To change the proxy configuration, proceed as follows:

1. In the **Proxy Configuration** pull-down menu, select the type of proxy configuration.

The following proxy configurations are available:

- **Direct connection to the Internet**
- **Manual proxy configuration**
- **Automatic proxy configuration**
- **System-wide proxy configuration**
- **Auto-detect proxy settings for this network**

2. Enter the necessary configuration data for the selected proxy configuration.

Direct connection to the Internet

With this proxy configuration, no proxy is used.

Manual proxy configuration

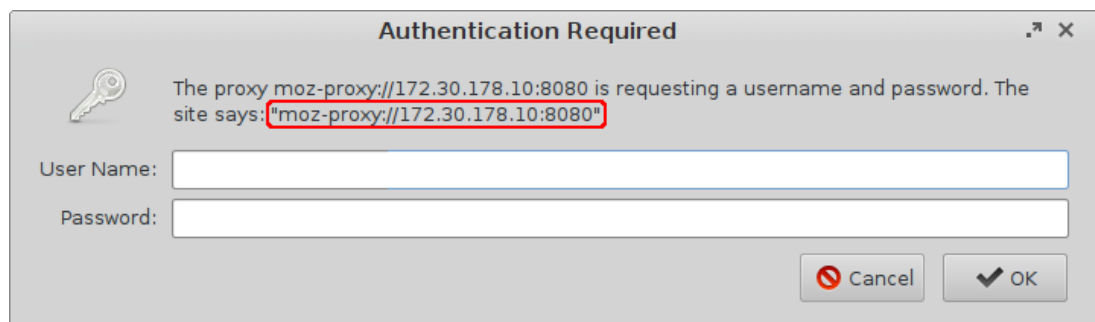
The configuration data must be specified in the following fields.

- **FTP Proxy:** URL of the proxy for HTTP
- **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
- **No Proxy for:** List of URLs for which no proxy is to be used.
- **Proxy Realm:** Area in which the browser authenticates itself for the proxy. Together with the user name and password, this information is necessary for authentication.



The **Proxy Realm** field is internally pre-populated with the value `moz-proxy://[HTTP Proxy] : [Port]`. If the field is empty, this value will be used when authenticating the browser.

If the proxy expects another unknown value for the proxy realm, you can determine this as follows: Leave the **Username** and **Password** fields empty and launch the browser. The dialog window which appears will contain the correct value for the **Proxy realm** field:



In the example above, the value for the **Proxy realm** field is as follows:
`moz-proxy://172.30.178.10:8080`

- **Use Passthrough authentication:** This option can be used if the local thin client logon takes place via Kerberos. If this option is enabled, the logon data temporarily saved when logging on to the thin client will be carried over for the user name and password.
- **Username:** User name with which the browser authenticates itself for the proxy.
- **Password:** Password with which the browser authenticates itself for the proxy.
- **Do not prompt for proxy authentication if credentials are saved:** If this option is enabled and logon data are already saved in the browser, the user will not be asked for a user name and password.



This option should not be enabled in multiuser environments. If this option is enabled in a multiuser environment, a user can use the logon data of a previous user.

Automatic proxy configuration

With this proxy configuration, the PAC file (Proxy Auto Config) available under **URL** will be used.

- **URL:** URL of the proxy configuration file
- **Do not prompt for proxy authentication if credentials are saved:** If this option is enabled, the user will not be prompted to enter a user name and password if the logon data are already saved in Firefox.



This option should not be enabled in multiuser environments. If this option is enabled in a multiuser environment, a user can use the logon data of a previous user.

System-wide proxy configuration

With this proxy configuration, the proxy configured under **Setup > Network > Proxy** will be used.

- **Do not prompt for proxy authentication if credentials are saved:** If this option is enabled, the user will not be prompted to enter a user name and password if the logon data are already saved in Firefox.



This option should not be enabled in multiuser environments. If this option is enabled in a multiuser environment, a user can use the logon data of a previous user.

Automatically recognize proxy configuration for this network

With this proxy configuration, WPAD (Web Proxy Autodiscovery Protocol) will be used. The browser will determine the URL of the WPAD file `wpad.dat` automatically with the help of DNS.

Privacy

Menu path: **Setup > Sessions > Browser > Browser Global > Privacy**

In this area, you can configure settings relevant to data protection.

- **Store Browsing History (in days):** Specifies how long your browsing history will be stored. If you select **Do not save History**, all browsing history data will be lost when the browser restarts.



All browsing history data stored before the period specified here will be lost.

- **Save information entered in forms and the Search Bar:** If this option is enabled, entries in forms and search bars will be retained after the browser restarts.
- **Remember passwords:** If this option is enabled, entered passwords will be retained after the browser restarts.
- **Clear private data when closing browser:** If this option is enabled, any data entered will be deleted when the browser is closed. What data are deleted is specified in the following options.

Select the items to be cleared

- **Browsing & Download History:** If this option is enabled, the addresses (URLs) of visited websites and the list of downloads will be deleted when the browser is closed.
- **Form & Search History:** If this option is enabled, entries in the search window and in website forms will be deleted when the browser is closed.
- **Saved Passwords:** If this option is enabled, any passwords entered will be deleted when the browser is closed.
- **Cookies:** If this option is enabled, any cookies will be deleted when the browser is closed.
- **Cache:** If this option is enabled, the cache for temporarily saving websites will be deleted when the browser is closed.
- **Active Logins:** If this option is enabled, ongoing sessions on websites will be terminated when the browser is closed and will need to be restarted after the browser restarts.
- **Allow private browsing feature:** If this option is enabled, you can open one or more private windows in the browser. All data from private windows will be deleted after the browser is closed.
- **Always start in private browsing mode:** If this option is enabled, the browser will be launched in private mode. All data will be deleted after the browser is closed.
- **Enable "Do Not Track" feature:** If this option is enabled, the browser will inform the website you are visiting that you do not wish to be tracked, i.e. you do not want your surfing history to be recorded.



The browser will use the DNT ("Do Not Track") field in the HTTP header for this purpose.

Observing this setting is voluntary; from a technical point of view, websites can still record the surfing history even when DNT is set to 1.

- **Enable built-in tracking protection:** If this option is enabled, the browser will block specific domains and websites which use tracking. The browser has an internal list for selecting the domains and websites to be blocked.



If tracking protection is enabled, a shield symbol will be shown at the left-hand edge of the address bar.

- **Suggest visited sites in URL bar:** If this option is enabled, 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.
 - **Suggest only typed visited sites:** If this option is enabled, the suggestions will be based only on the websites that were typed directly into the address bar. Websites that were visited via bookmarks or links in other websites will not be used for the suggestions.

- **Suggest bookmarked sites in URL bar:** If this option is enabled, suggestions will be shown while an address is being typed in the address bar. The suggestions will be based on bookmarks.
- **Suggest open pages in URL bar:** If this option is enabled, suggestions will be shown while an address is being typed in the address bar. The suggestions will be based on previously opened tabs.

Security

Menu path: **Setup > Sessions > Browser > Browser Global > Security**

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

- **Safe Browsing:** If this option is enabled, the browser will check each address entered as to whether it can be found in the black list of fraudulent websites which use phishing. If this is the case, you will be given a warning.
- **Malware Protection:** If this option is enabled, the browser will check whether the relevant website can be found in the black list of fraudulent websites which provide malware for downloading before a file is downloaded. If this is the case, you will be given a warning.

Advanced

Menu path: **Setup > Sessions > Browser > Browser Global > Advanced**

In this area, you can change various settings as well as add or change user-defined configuration parameters.

You can change the following settings:

- **Use old searchbar:** If this option is enabled, the logo of the search engine currently set will be shown in the search window. If this option is disabled, the search engine currently set will not be shown in the search window and search suggestions will be shown in the drop-down menu.
- **Always use the cursor keys to navigate within pages:** If this option is enabled, caret browsing will be enabled when the browser is launched. If caret browsing is enabled, you can navigate with the keyboard in websites without using the mouse. With the insertion mark, you can copy text to the clipboard.



You can enable or disable caret browsing at any time by pressing **F7**. To prevent caret browsing being disabled, you will also need to enable the **Setup > Sessions > Browser > Browser Sessions > [session name] > Settings > Hotkeys > Disable Hotkeys for Starting Caret Browsing** option.

- **Find As You Type:** If this option is enabled, search suggestions which match the characters typed will be shown while you type.
- **Warn me when websites try to redirect or reload the page:** If this option is enabled, a message window will be shown as soon as a website tries to get the browser to load another website or reload the current website.
- **Check my spelling as I type**

Possible values:

- **Off:** Your spelling will not be checked while you type.
- **On for multi-line controls:** Your spelling will be checked if you are typing in text fields with multiple lines.
- **On for multi- and single-line controls:** Your spelling will be checked if you are typing in text fields with one line or multiple lines.
- **Use autoscrolling:** If this option is enabled, you can launch automatic page scrolling by clicking on the middle mouse button to place a scroll symbol in the text and then positioning the mouse pointer above or below the anchor.
- **Use smooth scrolling:** If this option is enabled, you can browse through a page using the `Page Up/Down` keys smoothly as with scrolling. If the option is disabled, the display will jump immediately when you press the `Page Up/Down` keys.
- **Disable GStreamer in Browser:** If this option is enabled, GStreamer will not be used to play back videos. This may be a good idea if you experience problems when playing back videos.



We recommend that you disable this option if there is no multimedia codec pack installed on your thin client and you wish to view videos on HTML5 websites.

- **Disable OpenGL acceleration:** If this option is enabled, hardware acceleration with OpenGL will not be used. This may be a good idea if you experience problems with OpenGL applications,

To add a user-defined configuration parameter, proceed as follows:




Changes to the advanced Firefox browser settings can impair its stability, security and speed. IGEL Support is not responsible for problems caused by changing the browser configuration, even if the browser configuration was changed in the IGEL setup.



The configuration parameters can also be changed in the browser via `about:config`. To do this, the **Browser Sessions > [Session Name] > Window Settings > Hide Browser Configuration Page** option must be disabled.



1. In the **Custom preferences** area, click on .
2. Using the **Active** option, specify whether the configuration parameter is to be active.
3. Specify the **Mode** of the configuration parameter.

Possible values:

- **pref:** You can change the value in the browser via `about:config`. When the browser restarts, this change will be lost and the value set here will be used.
 - **defaultPref:** You can change the value in the browser via `about:config`. When the browser restarts, this change will remain.
 - **lockPref:** You cannot change the value in the browser via `about:config`.
 - **clearPref:** You cannot change the value in the browser via `about:config` and the value will not be shown via `about:config`.
4. Under **Custom preference**, give the name of the configuration parameter. Example:
`ui.textSelectBackground`
 5. Specify the **Type** of the configuration parameter.

Possible values:

- **String:** The value is a string of characters.
- **Integer:** The value is a whole number.
- **Boolean:** The value is a Boolean value, i.e. `true` or `false`.

6. Specify the **Value** of the configuration parameter. The possible entries depend on the **Type** selected.

7. Click on **Ok**.

The configuration parameter will take effect the next time that the browser is launched.

➡ You will find information regarding the configuration parameters in Firefox in the MozillaZine Knowledge Base under Firefox About:config entries.

Commands

Menu path: **Setup > Sessions > Browser > Browser Global > Commands**

In this area, you can define commands for the browser.

➤ Click on a command in order to enable the **Edit** button.

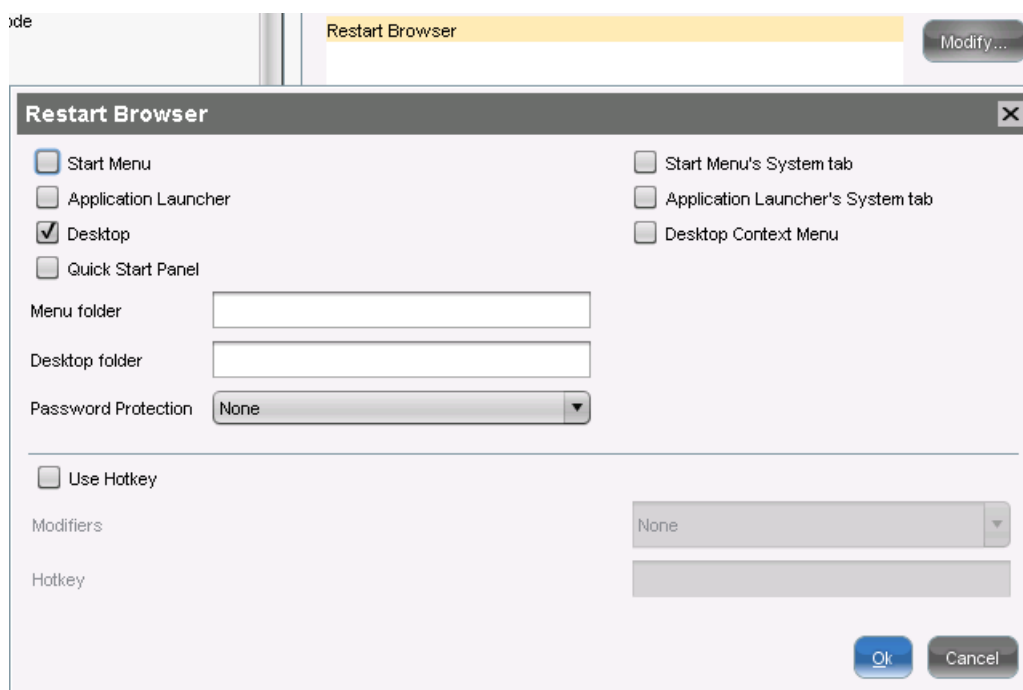


Figure 20: Commands setting

Encryption

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

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

- **Minimum required encryption protocol:** This protocol will be used to establish a secure connection if no higher protocol is available. Higher protocols are preferred.
- **Maximum supported encryption protocol:** This protocol is requested when negotiating the connection. If this protocol is not available, the next lowest protocol will be requested.
- **If a website requires a certificate:** Specifies how the browser behaves if a website requests a security certificate.

Possible values:

- **Select one automatically:** The browser selects a certificate automatically.
- **Ask me every time:** A dialog window requesting the certificate will be displayed.
- **View Certificates:** If you click on this button, the certificates saved in the browser's **Certificate Manager** will be displayed.
- **Certificate Validation:** Specifies the validation of certificates using OCSP (Online Certificate Status Protocol).
 - **Do not use OCSP for certificate validation:** The certificate will not be validated using OCSP.
 - **Validate a certificate if it specifies an OCSP server:** The certificate will be validated with the OCSP server specified in the certificate. If no OCSP server is specified, no certificate validation will take place.
 - **Validate all certificates using the following OCSP server:** All certificates will be validated with the OCSP server specified under the **Service URL**, irrespective of which OCSP server is specified in the certificate.
- **Response signer:** Signer of the response from the OCSP server
- **Service URL:** URL of the OCSP server
- **When an OCSP server connection fails, treat the certificate as invalid:** If, owing to a failed connection to the OCSP server, no validation can take place, the certificate will be treated as invalid. In this case, the browser will show the **This connection is not trusted** error message.
- **Use "Aladdin eToken" Security Device:** If this option is enabled, Aladdin eToken will be used for encryption.
- **Use "Gemalto" Security Device:** If this option is enabled, Gemalto will be used for encryption.
- **Use "IDProtect" Security Device:** If this option is enabled, Athena IPProtect will be used for encryption.
- **Use "SafeSign" Security Device:** If this option is enabled, SafeSign will be used for encryption.
- **Use "SecMaker" Security Device:** If this option is enabled, SecMaker will be used for encryption.
- **Use TCOS 3 NetKey Security Device:** If this option is enabled, TCOS 3 NewKey will be used for encryption.
- **Use TCOS 3 SigG Security Device:** If this option is enabled, TCOS 3 SigG will be used for encryption.
- **Use TCOS 3 Elster Security Device:** If this option is enabled, TCOS 3 Elster will be used for encryption.
- **Use TCOS 3 SD Security Device:** If this option is enabled, TCOS 3 SD will be used for encryption.

7.28.2. Browser Sessions

Menu path: **Setup > Sessions > Browser > Browser Sessions > [Session Name]**

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

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



The session name must not contain any of these characters:

\ / : * ? " < > | [] { } ()

- **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.
- **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:** Specifies a hotkey consisting of modifiers and a key which can be used to launch the session.
- **Modifiers:** One or two modifiers for the hotkey
- **Key:** Key for the hotkey
- **Autostart:** If this option is enabled, the session will be launched automatically when the thin client boots.
- **Restart:** If this option is enabled, the session will be relaunched automatically after termination.
- **Autostart Delay:** Waiting time in seconds between the thin client booting and the session being launched automatically.

Settings

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

In this area, you can define the start page, display resolution and font size for the browser.

You can change the following settings:

- **When browser starts:** Specifies what pages are shown when the browser is launched.
 - **Global setting:** The settings under **Setup > Sessions > Browser > Browser Global** are used.
 - **Start with a blank page**
 - **Show my home page**
 - **Resume previous session:** All tabs from the last session are reopened.
- **Home page:** Specifies the URL of the start page. You can specify a number of start pages by separating the URLs of the start pages with a vertical dash "|".
- **Display resolution:** Specifies the display resolution for the browser in DPI. Typical values are **72** for medium screens and **96** for large screens.
- **Minimum font size:** Specifies the minimum size of the fonts displayed on websites. The formats of the websites are overwritten in the process.

Tabs

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

In this area, you can define settings for the browser tabs. You will find a description under the global settings, see *Tabs* (page 84).

Content

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

You will find a description under the global settings, see *Content* (page 84).



Exceptions for the blocking of popups and for the automatic loading of images can only be defined in the global settings.

Printing

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

In this area, you can set the **default paper size** for the printer. You will find a description under the global settings, see *Printing* (page 85).

Proxy

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

In this area, you can change the proxy configuration. You will find a description under the global settings, see *Proxy* (page 85).

Data Protection

Menu path: **Setup > Sessions > Browser > Browser Sessions > [Session Name] > Settings > Data Protection**

In this area, you can configure settings relevant to data protection. You will find a description under the global settings, see *Data Protection* (page 87).

Security

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

In this area, you can define settings for phishing and malware. You will find a description under the global settings, see *Security* (page 89).

Advanced

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

In this area, you can change various settings. You will find a description under the global settings, see *Advanced* (page 89).



User-defined configuration parameters can only be added and OpenGL acceleration disabled in the global settings.

Encryption

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

In this area, you can define the settings for encryption methods and certificate validation. You will find a description under the global settings, see *Encryption* (page 91).

Restarting

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

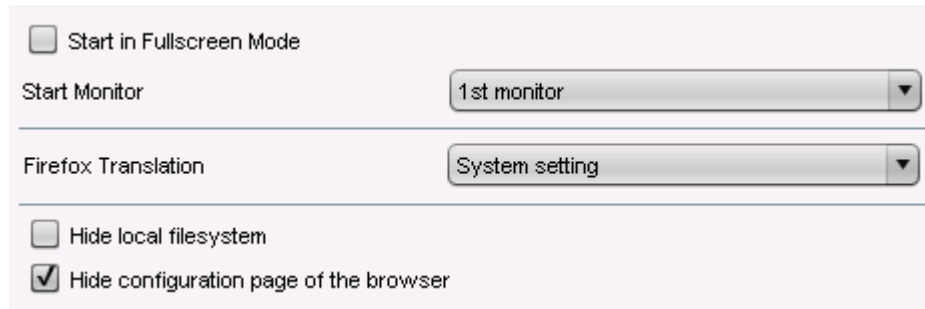
In this area, you can specify whether the browser is restarted after being closed and after what delay time.

- **Restart:** If this option is enabled, the browser will be restarted automatically after being closed.
- **Restart Timeout enabled:** If this option is enabled, the browser will be restarted automatically if, after the time interval defined under **Time limit for restarting**, no action on the part of the user has occurred.
- **Restart Timeout:** Time interval in minutes after which the browser is automatically restarted if in the meantime no action on the part of the user has occurred.

Window settings

Menu path: **Setup > Sessions > Browser > Browser Sessions > Window**

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



☐ Start in Fullscreen Mode

Start Monitor: 1st monitor

Firefox Translation: System setting

☐ Hide local filesystem

☒ Hide configuration page of the browser

Figure 21: Window settings

The **full-screen mode** is disabled by default.

- Check the checkbox in order to enable the full-screen mode.

If you have connected a number of monitors, you can specify the **start monitor** here.

- Under **Firefox translation**, select the language that the Firefox user interface is to be translated into.
- Enable **Hide local file system** if you do not want the local structure to be displayed when you save files.
- Disable **Hide configuration page of the browser** if you would like the configuration page of the browser to be displayed for editing.

Menus and symbol bars

Menu path: **Setup > Sessions > Browser > Browser Sessions > Menus & Toolbars**

In this area, you can adapt Firefox menus and symbol bars to meet your personal needs by

- Hiding items in the menu bar
 - Hiding list items
 - Configuring the symbol bar
-
- Enable **User customization of tool bars** in order to allow the user to configure symbol bars.
 - Configure the **navigation symbol bar**.

The following items are pre-set:

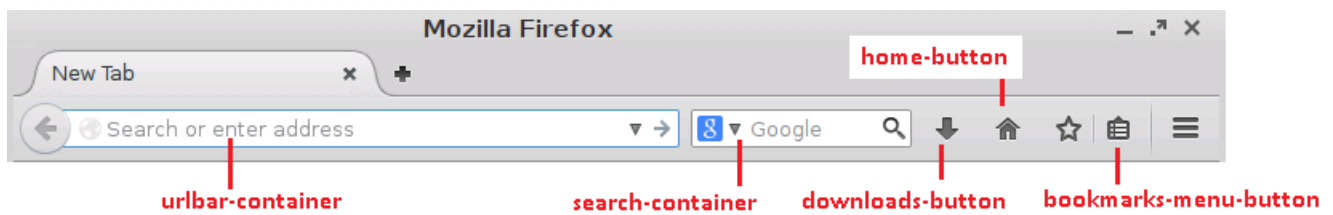


Figure 22: Navigation symbol bar

➤ Configure the **Application menu**:

The following items are pre-set:

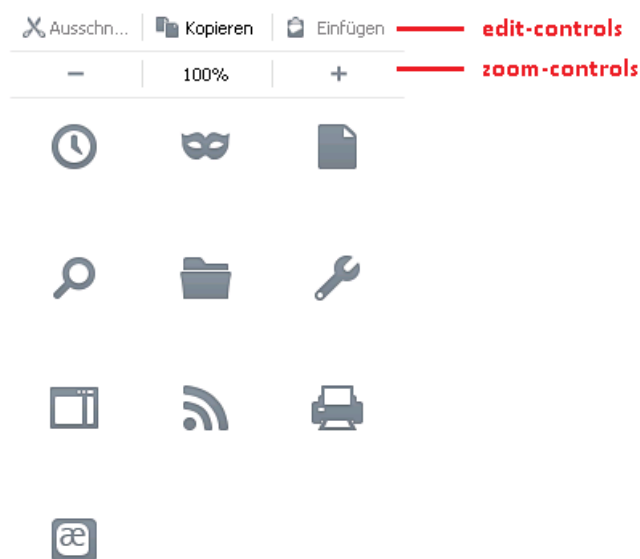


Figure 23: Application menu



Please note that a number of items are only shown if the corresponding feature is enabled.

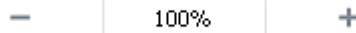
➤ Configure the **Application menu**:

➤ **Other possible items for the navigation symbol bar and the application menu are:**

Loop button



Zoom controls



Edit controls



History panel menu



Private browsing button



Save page button



Find button



Open file button



Developer button



Sidebar button



Feed button



Print button



Character encoding button



Social share button



Panic button



Web apps button



New window button



Fullscreen button



Tab view button



Downloads button



- Click on **Reset icon configuration to default** in order to undo your changes.

Hotkeys

Menu path: **Setup > Sessions > Browser > Browser Sessions > Hotkeys**

In this area, you can disable the following Firefox hotkeys:

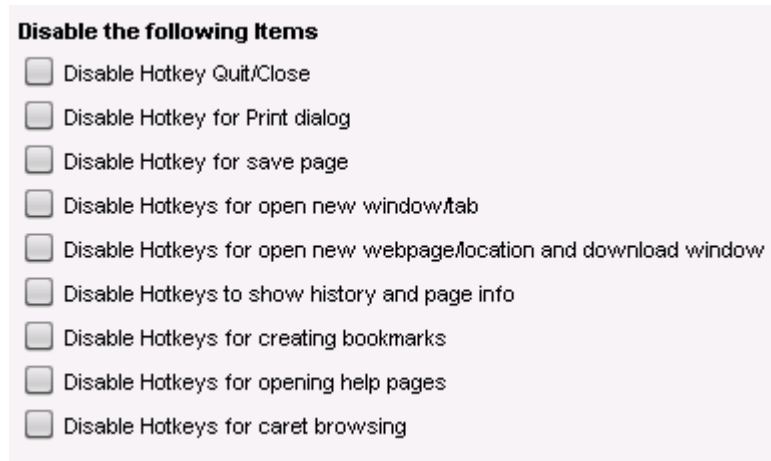


Figure 24: Hotkeys settings

Context menu

Menu path: **Setup > Sessions > Browser > Browser Sessions > Context**

In this area, you can disable various items in the browser context menu.

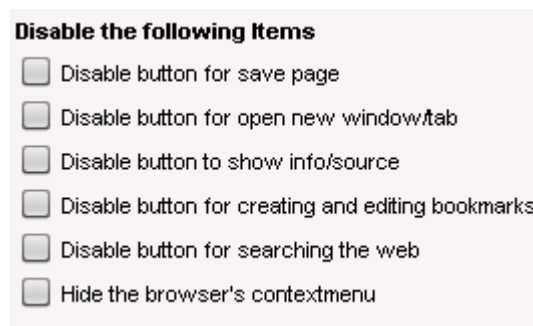


Figure 25: Context menu settings

7.28.3. Browser Plug-ins

Menu path: **Setup > Sessions > Browser > Plugins**

Various plug-ins such as a PDF viewer, Adobe Flash Player or Red Hat Spice are available. However, they may need to be licensed by the user first. Integration of the SecMacer security solution Net iD can also be configured here.

Flash Player

Menu path: **Setup > Sessions > Browser > Plugins > Flashplayer**

Before you can download and install Adobe Flash Player, you need to confirm that the software is licensed - IGEL Universal Desktop Linux does not contain a license to use the Flash Player.

➤ Activate the option **I will license the flashplayer by myself** to activate the **Download Flashplayer** page.

To install Adobe Flash Player:



You can also start the installation using the UMS context menu. For this, select **Other Thin Client commands > Download Flashplayer** in the context menu.

1. Navigate to the **Download Flashplayer** page.
2. Activate the option **I want to download Adobe flashplayer and care about the licensing by myself**.
3. Adjust the following settings:
 - **Use Firmware Update settings for download:** If the option is activated, the parameters **User authentication**, **User name**, **Password**, and **Download URL** are set to the default values and cannot be changed.
 - **User authentication:** If the option is activated, the thin client authenticates with the server using the access data provided in **User name** and **Password**.
 - **Download URL:** URL of the directory in which the Adobe Flash Player is stored. The default value is the official link from Adobe. Alternatively, you can provide the storage location in your company network.



The Adobe link is valid at the time when the firmware is released, but it is subject to change. In case the download fails, modify the URL accordingly.

- **Download File:** Name of the file containing the Adobe Flash Player.
1. Click **Apply** or **Ok**.
- The Adobe Flash Player is downloaded and installed.

PDF viewer

Menu path: **Setup > Sessions > Browser > Plugins > PDF Viewer**

Here, you can specify whether PDF documents are to be embedded in the browser or displayed in a separate window.

RedHat Spice

Menu path: **Setup > Sessions > Browser > Plugins > RHEV/Spice**

In this area, you can define settings for virtual environments.

- Enable **Enable browser plugin** in order to display virtual desktop environments everywhere via the Internet.
- Enable or disable **Enable USB sharing**.

7.29. Media Player

Menu path: **Setup > Sessions > Media Player**

Set up the Media Player for your multimedia applications here.

IGEL Linux supports the following multimedia formats and codecs out of the box:

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

The following codecs are licensed via the separately available Multimedia Codec Pack:

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



AC3 is not licensed.



IGEL Zero Clients (IZ series) have the Multimedia Codec Pack installed by default.

7.29.1. Media Player Global

Menu path: **Setup > Sessions > Media Player > Media Player Global**

- Configure universal settings which will apply by default during all Media Player sessions.



You can override global settings in the individual sessions.

Window

Menu path: **Setup > Sessions > Media Player > Media Player Global > Window**

- Under **Image Aspect Ratio**, specify the required aspect ratio for video playback.

You can also choose the following options:

- Full-screen mode
- Automatically change window size as soon as a new video is loaded
- Main window should remain in the foreground
- Show operating components

Playback

Menu path: **Setup > Sessions > Media Player > Media Player Global > Playback**

- Specify how you would like to play back media files:

Endless loop	Automatically plays back a play list endlessly until you stop it.
Random mode	Plays back the files in a play list in a random order.

- If you wish, choose the visual effects to be used during audio playback.

Visualization type	Determines the visualization plug-in.
Visualization size	Determines the visualization size.

Video

Menu path: **Setup > Sessions > Media Player > Media Player Global > Video**

Video output	GConf:	System-wide configuration
	Auto:	Automatically selects the output
	XVideo:	Hardware-accelerated, uses shared memory to write images to the graphics card memory
	X11:	Not hardware-accelerated, playback via the X Window System display protocol

- Specify the brightness, saturation, contrast and color settings for videos.

Audio

Menu path: **Setup > Sessions > Media Player > Media Player Global > Audio**

Audio output	GConf:	System-wide configuration
	Auto:	Automatically selects the output
	ALSA:	Direct output via kernel driver for sound cards
Audio output type	Select Stereo if you are working with an IGEL thin client.	

Options

Menu path: **Setup > Sessions > Media Player > Media Player Global > Options**

- Specify whether you would like to disable the **screen saver** during audio playback.
- Specify the **network connection speed** in order to influence media file playback.
- Specify the necessary **buffer size** for your network in order to ensure smooth audio and video playback.
- Specify whether you would like to **automatically load subtitles** as soon as a video begins. Currently, the **coding** for subtitles is always UTF-8.
- Specify the **font** and **text size** for the subtitles.

Browser Plugin

Menu path: **Setup > Sessions > Media Player > Media Player Global > Browser Plugin**

If you would like to use the Media Player as a **Browser Plugin**, you can change the configuration values here.



This will affect manually configured Media Player sessions.

7.29.2. Media Player Sessions

Menu path: **Setup > Sessions > Media Player > Media Player Sessions**

You can set up your own personal Media Player sessions here.

1. Click on **Add** to create a new session.
2. Specify a **session name**.
3. Specify which **possible ways of launching the session** you would like. You may choose a number of options here.
4. You may like to select the option of using **hotkeys** and define them.
5. You can also specify whether **autostart** (following a system start) and/or **restart** (after a connection is established) are to be used.
6. For the autostart option, you can also specify by how many seconds the session start is to be delayed.

As soon as you have set up a Media Player session of your own, it will appear in the structure tree under the **Media Player Sessions** directory. Your own session in turn contains three folders: **Playback**, **Options** and **Desktop Integration**.

Playback

Menu path: **Setup > Sessions > Media Player > Media Player Sessions > [Session name] > Playback**

- Under **Medium / File**, give the path of the file which is to be played back when the session is launched. Use the following formats:

`/directory/filename`

or

`http://servername/filename.`

For the window settings, you can choose whether you would like to carry over the global settings or use your own settings for this special session.

Options

Menu path: **Setup > Sessions > Media Player > Media Player Sessions > [Session name] > Options**

If necessary, you can change the pre-configured settings for the operating components here.

7.30. Java Web Start Session

Menu path: **Setup > Sessions > JWS Sessions**

You can set up one or more Java Web Start sessions. This can be for example an IGEL UMS console running as Java Web Start.

To set up a Java Web Start session, proceed as follows:

1. In the **JWS Sessions** area, click on .

A new Java Web Start session will be created.

2. Configure the Java Web Start session. You will find further information under *Java Web Start Session* (page 104).

7.30.1. Java Web Start Session

Menu path: **Setup > Sessions > JWS Sessions > Java Session**

You can change the following settings:

- **Session Name:** Name of the Java Web Start session.
- **Start Menu:** If this option is enabled, the Java Web Start session can be launched in the start menu.
- **Application Launcher:** If this option is enabled, the Java Web Start session can be launched with the Application Launcher.
- **Desktop:** If this option is enabled, the Java Web Start session can be launched with a program launcher on the desktop.
- **Quick Start Panel:** If this option is enabled, the Java Web Start session can be launched in the Quick Start Panel.
- **Start Menu's System tab:** If this option is enabled, the Java Web Start session can be launched in the start menu's system tab.
- **Application Launcher's system tab:** If this option is enabled, the Java Web Start session can be launched in the Application Launcher's system tab.
- **Desktop Context Menu:** If this option is enabled, the Java Web Start session can be launched in 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 Java Web Start session. The menu path will be used in the start menu and in the desktop context menu. Example: "Functions/Screen functions".
- **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 Java Web Start session. The menu path will be used for the program launcher on the desktop. Example: "Functions/Screen functions".
- **Password Protection:** Specifies the password request when launching the Java Web Start session.

Possible values:

- **None:** No password is requested when launching the Java Web Start session.
- **Administrator:** The administrator password is requested when launching the Java Web Start session.
- **User:** The user password is requested when launching the Java Web Start session.
- **Setup User:** The setup user's password is requested when launching the Java Web Start session.
- **Hotkey:** Specifies a hotkey consisting of modifiers and a key which can be used to launch the Java Web Start session.
- **Modifiers:** One or two modifiers for the hotkey
- **Key:** Key for the hotkey
- **Autostart:** If this option is enabled, the Java Web Start session will be launched automatically when the thin client boots.
- **Autostart Delay:** Waiting time in seconds between the thin client booting and the Java Web Start session being launched automatically.

Java Web Start

Menu path: **Setup > Sessions > JWS Sessions > Java Session**

In this area, give the address of the JNLP file which is needed for launching the Java Web Start session. The file is loaded into the cache before being executed.



The browser's global proxy settings are used when downloading the JNLP file. You will find a description of these proxy settings under Browser Global Proxy.

If a proxy is to be used only for the browser but not for the Java Web Start session, give the address of the JNLP file under **Setup > Sessions > Browser > Browser Global > Proxy > No Proxy for**.

- **JNLP file:** Address of the JNLP file. Example: `http://www.server.com/example.jnlp`

7.31. VoIP Client

Menu path: **Setup > Sessions > VoIP Client**

IGEL Linux includes the Ekiga voice over IP client (<http://ekiga.org>). This client allows you to use the SIP (Session Initiation Protocol) and H.323.

➡ You will find a detailed description of all Ekiga options under <http://wiki.ekiga.org/index.php/Manual>.

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

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



The session name must not contain any of these characters:

\ / : * ? " < > | [] { } ()

- **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.
- **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:** Specifies a hotkey consisting of modifiers and a key which can be used to launch the session.
- **Modifiers:** One or two modifiers for the hotkey
- **Key:** Key for the hotkey
- **Autostart:** If this option is enabled, the session will be launched automatically when the thin client boots.
- **Restart:** If this option is enabled, the session will be relaunched automatically after termination.
- **Autostart Delay:** Waiting time in seconds between the thin client booting and the session being launched automatically.

7.31.1. User Account

Menu path: **Setup > Sessions > VoIP Client > User Account**


You can set up or change one or more user accounts as well as specify the name displayed.

- **Full Name:** Name of the user; this name will be shown to the other person. Example: John Doe

To set up an SIP user account, proceed as follows:



Ensure that the VoIP client was terminated before you start setting up or changing a user account. Changes will only be saved if the client is not running.

1. Click on .
2. If the user account is to be active once set up, enable the **Enable Account** option.
3. Enter the following data:
 - **Protocol:** Select SIP.
 - **Name:** Name for this user account.



Choose a name which allows a distinction to be made easily between a number of user accounts.

- **Registrar:** URI with which the VoIP client registers. This can be a DNS name or an IP address.
 - **User name:** Numerical or alphanumerical value. The user name is part of the SIP address. Example: john.doe in john.doe@example.com
 - **Login Name:** Numerical or alphanumerical value. Name with which the VoIP client registers on the registrar. This name can differ from the name given under user name.
 - **Password:** Password with which the VoIP client registers on the registrar
 - **Registration Update Timeout:** Timeout after which the registration should be updated
4. Click on **Ok**.
The user account is set up.

7.31.2. Audio

Menu path: **Setup > Sessions > VoIP Client > Audio**

You can change the audio settings of the VoIP client.




Recommendation: Configure the settings **Device for ringtone**, **Device for audio playback** and **Device for audio recording** in the VoIP client. All available audio devices of the thin client are shown in the VoIP client.

To configure the audio devices in the VoIP client, proceed as follows:

1. In the IGEL setup, ensure that the option **Save configuration changes made in the application** is enabled under **Sessions > VoIP Client > Preferences**.
2. Start the VoIP client.
3. Configure your desired settings in the VoIP client under **Edit > Preferences > Audio > Devices**.



4. To save your settings, close the VoIP client window, right-click on  in the system tray and select **Close**.

The changes will be saved in the IGEL setup once the VoIP client is terminated.

Settings in the setup:

- **Sound Event Output Device:** Specifies which audio device is used for the ringtone.



It is recommended that you select the audio device that is connected to the thin client's built-in loudspeaker.

- **Audio Output Device:** Specifies which audio device is used for playback. Example: the audio device that is connected to the headset's loudspeakers.
- **Audio Input Device:** Specifies which audio device is used for playback. Example: the audio device that is connected to the headset's microphone.
- **Enable Silence Detection:** If this option is enabled, audio transmission will be suppressed in the absence of voice activity. This helps to save bandwidth.



Voice activity detection can reduce the voice quality.

- **Enable Echo Cancellation:** If this option is enabled, the VoIP client will suppress echoes of your own voice.
- **Maximum Jitter Buffer (in Milliseconds):** The jitter buffer improves voice quality by compensating for delay variations when transmitting voice packets. The VoIP client continuously measures delay variations and automatically adjusts the buffer size. The bigger the delay variations are, the bigger the jitter buffer will be set.



A bigger jitter buffer results in greater latency.

7.31.3. SIP

Menu path: **Setup > Sessions > VoIP Client > SIP**

You can change SIP-specific settings for the proxy, forwarding and the multi-frequency dialing process (DTMF).

- **Outbound Proxy:** URI of the SIP proxy that handles outbound calls.
- **Forward URI:** SIP URI to which inbound calls are forwarded if forwarding is enabled. You will find further information on forwarding under *Call Options* (page 109).
- **Send DTMF as:** Specifies how key sequences are transmitted while a connection is in place.

Possible values:

- **INFO:** The key sequence is transmitted as SIP INFO.
- **RFC 2833:** The key sequence is transmitted using RTP (Real-time Transport Protocol).

7.31.4. H.323

Menu path: **Setup > Sessions > VoIP Client > H.323**

You can change H.323-specific settings for forwarding, H.245, quick start and for the multi-frequency dialing process (DTMF).

- **Foward URI:** H.323 URI to which inbound calls are forwarded if forwarding is enabled. You will find further information on forwarding under *Call Options* (page 109).
- **Enable H.245 tunneling:** If this option is enabled, H.245 messages will be packaged in H.225 messages. Port 1720 is needed for this purpose.
- **Enable early H.245:** If this option is enabled, H.245 will be launched at an earlier point in the connection process. The voice connection can be established more quickly as a result.
- **Enable Fast Start procedure:** If this option is enabled, the voice connection will be established in quick start mode (fast connect, part of H.323 v2).
- **Send DTMF as:** Specifies how key sequences are transmitted while a connection is in place.

Possible values:

- **String:** The key sequence is transmitted using H.245 User Input Indication.
- **Tone:** The key sequence is transmitted as a tone sequence in the audio data flow.
- **RFC 2833:** The key sequence is transmitted using RTP (Real-time Transport Protocol).
- **Q.931:** The key sequence is transmitted via the signaling channel.

7.31.5. Call Options

Menu path: **Setup > Sessions > VoIP Client > Call Options**

You can change settings for inbound calls.


- **Always forward calls to the given address:** If this option is enabled, inbound calls will immediately be forwarded to the address defined in **Setup > Sessions > VoIP Client > SIP > Foward URI** (see *SIP* (page 108)) or **Setup > Sessions > VoIP Client > H.323 > Forward URI** (see *H.323* (page 108)).
- **Forward calls to the given address if no answer:** If this option is enabled, inbound calls will be forwarded to the address defined in **Setup > Sessions > VoIP Client > SIP > URI for Forwarding** (see *SIP* (page 108)) or **Setup > Sessions > VoIP Client > H.323 > URI for Forwarding** (see *H.323* (page 108)) after the time specified under **Time limit for calls not taken**. If this option is disabled, inbound calls will be rejected after the time specified under **Time limit for calls not taken**.
- **Forward calls to the given address if busy:** If this option is enabled, inbound calls during a call will be forwarded to the address defined in **Setup > Sessions > VoIP Client > SIP > URI for Forwarding** (see *SIP* (page 108)) or **Setup > Sessions > VoIP Client > H.323 > URI for Forwarding** (see *H.323* (page 108)).
- **No Answer Timeout:** Time in seconds after which calls not taken are rejected or forwarded.

7.31.6. Telephone Book


Menu path: **Setup > Sessions > VoIP Client > Telephone Book**

You can add one or more LDAP address books or local contacts.

To add an LDAP address book, proceed as follows:

1. In the **List of LDAP address books** area, click on .
2. Enter the following data:
 - **Name:** Name with which the LDAP address book will be displayed in the VoIP client
 - **Server Name:** Host name of the LDAP server
 - **Port:** Port for the connection to the LDAP server
 - **Basis DN:** Basis for the search in the LDAP tree
 - **Scope:** Area for the LDAP search
 - **Display Name Attribute:** LDAP attribute that is displayed as the name of the contact in the VoIP client. Example: `cn`
 - **Call Attribute:** LDAP attribute that contains the telephone number.
 - **Filter Template:** Filter for the LDAP search
 - **Bind ID:** Identifier for the LDAP search. This identifier is sent to the LDAP server in a BIND request.
 - **Password:** Password for the user account for the LDAP search
3. Click on **Ok**.

To add a contact to the local contact list, proceed as follows:

1. In the **List of Contacts** area, click on .
2. Enter the following data:
 - **Name:** Name of the SIP or H.323 address displayed
 - **Address:** SIP or H.323 address. Example: `sip:500@example.com`
 - **Group:** Optional group name in order to group contacts

7.31.7. Settings

Menu path: **Setup > Sessions > VoIP Client > Settings**

You can change VoIP client settings.

- **Save configuration changes made in the application:** If this option is enabled, changes made in the VoIP client will be saved in the IGEL setup when the VoIP client is terminated. This applies to all settings available in the IGEL setup, with the exception of settings for the LDAP address book.

7.31.8. Desktop Integration

Menu path: **Setup > Sessions > VoIP Client > Desktop Integration**

In this area, you can configure desktop integration for the VoIP client session, see *VoIP Client* (page 105).

8. Accessories

Menu path: **Setup > Accessories**

Information on other accessories provided by the Universal Desktop can be found [here](#).

8.1. ICA Connection Center

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

The Citrix ICA Connection Center provides an overview of existing connections to Citrix servers. It also allows the server connection to be terminated/canceled and the connection properties to be displayed, e.g. for support purposes.

8.2. Local Terminal

Menu path: **Setup > Accessories> Terminals**

With a terminal session, you can execute local commands via a shell.



It is also possible to access a local shell without a terminal session: You can switch to the virtual terminals tty11 and tty12 by pressing **Ctrl+Alt+F11** / **Ctrl+Alt+F12**.

8.3. Change Smartcard Password

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

Set up a session in order to change your IGEL smartcard password. Details of the setup procedure for your IGEL smartcard can be found under **Security > Login > Smartcard**.

8.4. Setup Session

Menu path: **Setup > Accessories> Setup**

Specific areas of the setup can be made available to the user, even if the overall setup can only be accessed by the administrator. This is useful for example for keyboard and mouse settings or for screen configuration. See *Enable Setup Pages for Users* (page 18).

8.5. Quick Settings Session

Menu path: **Setup > Accessories> Quick Setup**

Specific areas of the setup can be made available to the user, even if the overall setup can only be accessed by the administrator. This is useful for example for keyboard and mouse settings or for screen configuration. See Quick Setup.

8.6. Display switch

Menu path: **Setup > Accessories > Display Switch**

Display switch is a function of the IGEL Linux firmware which allows you to configure settings for the display on various screens.

In order to use the function, you will need to enable it and set it up:

- Enable screen selection by enabling one of the starting methods under **Accessories > Display Switch**.
- Configure a **Hotkey** in order to determine a hotkey or an icon for this session.
- If necessary, specify **Autostart** options.
- Configure the following settings under **Accessories > Display Switch > Options**:
 - **Dialog Type** - Specify how the screen selection dialog is to look:
 - Minimal Dialog** - Basic settings such as **Mirror** or **Expand**, for a maximum of two displays.
 - Advanced Dialog** - The user themselves can change the resolution or rotation outside the setup.
 - **Preserve settings over reboot** - Save the display settings so that they can be reused in the event of a reboot.



This setting has no function under the following condition: You work with **Shared Workplace** and have assigned profiles to various users via the UMS. You can save the default settings for users who are not assigned a profile. With the other users, these settings will be overwritten by the profile from the UMS.

- **Configure new displays when connected** - As soon as you connect a new display, a configuration window will open.

Specify the buttons for the minimal dialog:

- **Mirror displays** - Integrates an icon for shadowing displays.
- **Extend to the left** - Integrates an icon for expanding the the screen content to the left display.
- **Extend to the right** - Integrates an icon for expanding the screen content to the right display.
- **Rotate displays (Page orientation)** - Integrates an icon for rotating the display.
- **Mouse options** - Integrates an icon for mouse settings like lefthand mode, mouse speed or double click time.
- **Advanced** - Allows you to jump to the advanced dialog in the minimal dialog.
- **Reset** - Allows resetting to the setup settings in the dialog.

8.6.1. Advanced settings

Menu path: **Setup > Accessories > Display Switch > Options**

To set up your screens' **Display**, proceed as follows:

1. Open the **Display Switch** that you set up under **Display Switch** (page 112).
The **Displays** mask will open.
2. Click on **Advanced** in order to be able to configure special display options.
The **Display** mask will open:

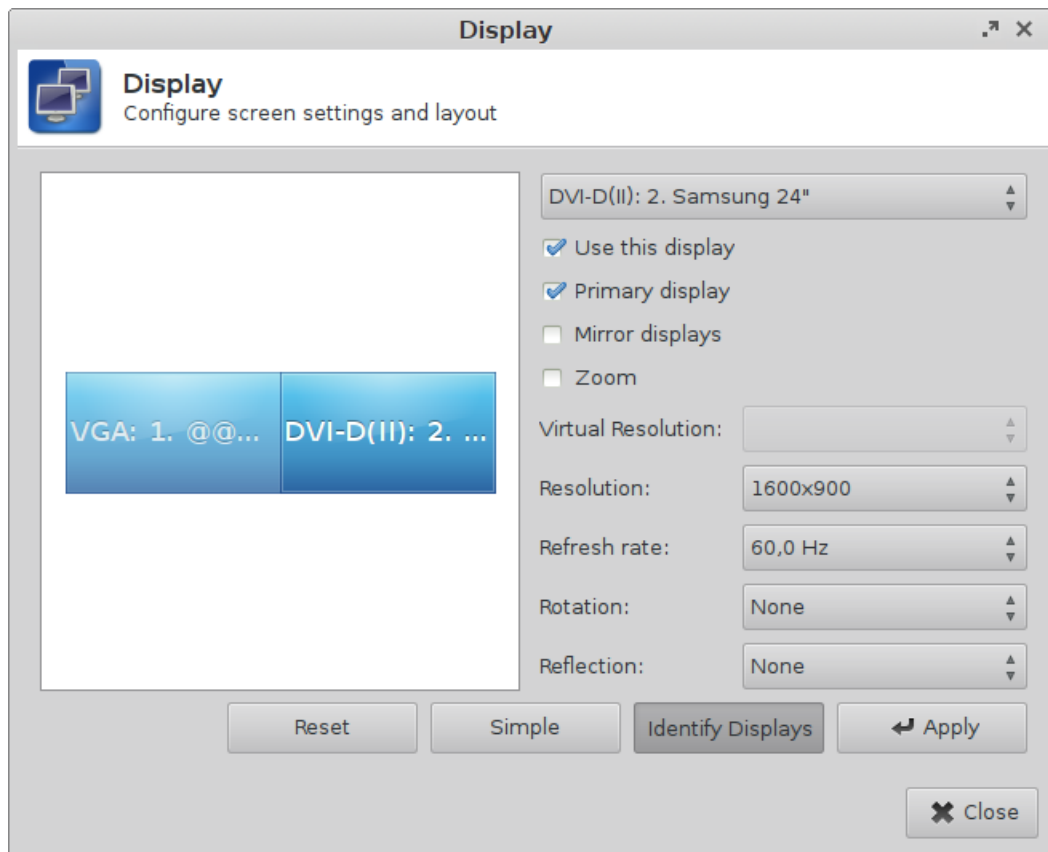


Figure 26: Magnified view

Click on one of the screens shown and configure the settings, e.g.:

- **Use this display** - in order to enable it.
- **Primary display** - in order to specify the first screen, see **Screen 1** in the *Screen Selection* (page 132).
The taskbar appears on the main screen.
- **Mirror displays** - in order to place the screens over each other.
- **Zoom** - in order to set the magnified display.



If you disconnect the only active screen, the one that was active last will be shown again. As a result, you can still configure something even in an emergency.

8.6.2. Enlarged View

You have the option of displaying a magnified setup interface on your screen. This was developed for users with impaired vision.

1. Activate **Zoom** in the **Display** (page 113) window.

The **Virtual Resolution** selection field will become active.

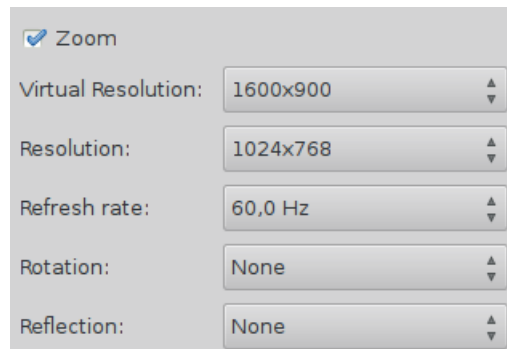


Figure 27: Set resolutions



Under **Virtual Resolution** and **Resolution**, the current resolution value is preset as the default value.

2. Configure the following settings for the magnification function:
 - Under **Virtual Resolution**, select the highest possible value from the selection list.
 - Under **Resolution**, select a much lower value which should simulate the actual resolution of the screen.

The setup interface is now shown as if it would fill a much larger screen. The existing screen thus shows just part of the interface. Essentially, it functions like a magnifying glass or a peephole. The part of the interface that can be seen is highly magnified.



If you selected **Mirror Displays** under the advanced settings, all active screens will be displayed in the same way. They basically lie over each other. However, you can change the way they are displayed in magnification mode by reducing the actual resolution of the mirrored screen.

8.7. Application Launcher

Menu path: **Setup > Accessories > Application Launcher**

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



The session name must not contain any of these characters:

\ / : * ? " < > | [] { } ()

- **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.
- **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:** Specifies a hotkey consisting of modifiers and a key which can be used to launch the session.
- **Modifiers:** One or two modifiers for the hotkey
- **Key:** Key for the hotkey
- **Autostart:** If this option is enabled, the session will be launched automatically when the thin client boots.
- **Restart:** If this option is enabled, the session will be relaunched automatically after termination.
- **Autostart Delay:** Waiting time in seconds between the thin client booting and the session being launched automatically.

Under **Application Launcher > Configuration**, you can hide the following items from the user:

- System page
- "Reboot" button
- "Shut down" button
- Network information page

8.8. Sound Mixer

Menu path: **Setup > Accessories > Sound Preferences**

Use the sound control to adjust the output volume and the input level as well as the balance between the input and output.

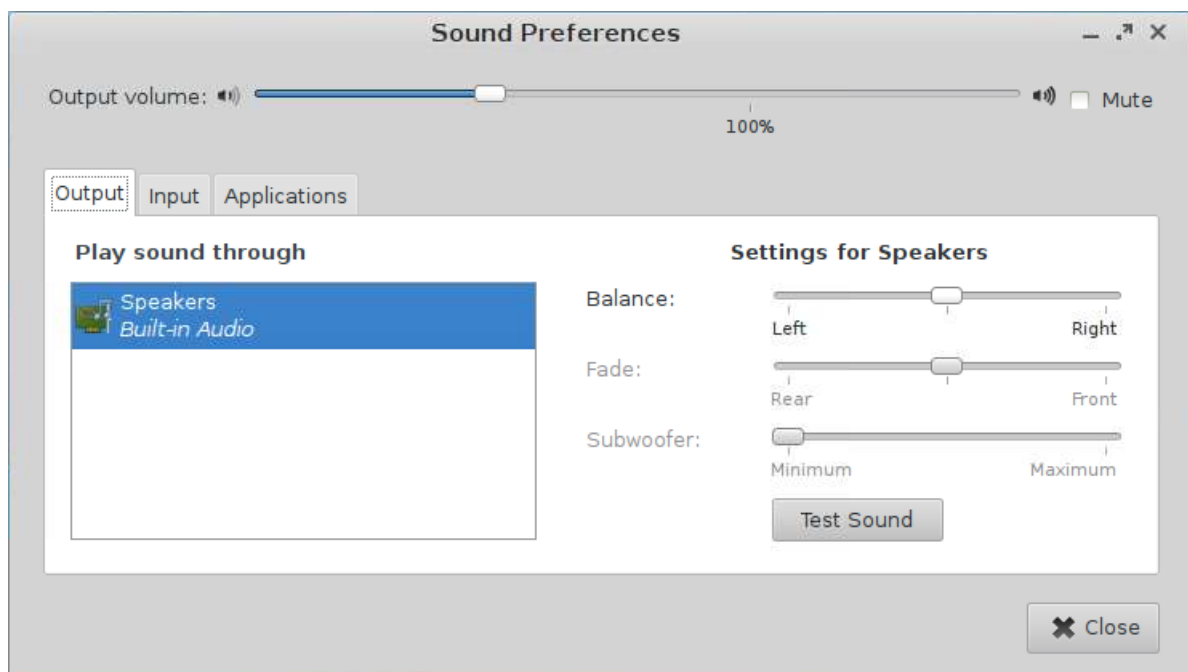


Figure 28: Sound control

The system's default volume can be configured or muted in **Accessories > Sound Mixer > Configuration**. These parameters can also be remotely set via IGEL UMS.

8.9. System Log Viewer

Menu path: **Setup > Accessories > System Log Viewer**

All available system logs are updated and displayed. You can add your own log files in the options. The contents of the selected log can be searched in the viewer and also copied (e.g. for support purposes).

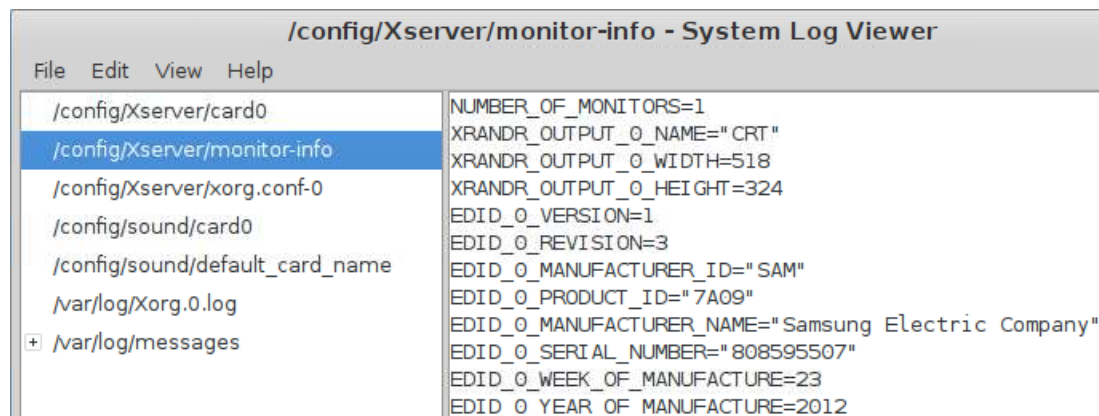


Figure 29: System logs

8.10. UMS Registration

Menu path: **Setup > Accessories > UMS Registration**

Registration of the thin client in the IGEL Universal Management Suite can also be performed locally.

1. Open the **Application Launcher**.

2. In the **System** area, launch the **UMS Registering** application.

Figure 30: Remote Administration

3. Enter the **Server Address**, **Login** and **Password** for your UMS server.



If there is a corresponding DNS entry for the UMS server, you can leave the default value `igelrmserver` in the address field.

4. Optional: Define a **Structure Tag** in order to sort the thin client into a directory in accordance with the UMS directory rules.
 ➡ Further information regarding the use of structure tags can be found in the *"Using Structure Tags" Best Practice* (<http://edocs.igel.com/index.htm#10202089.htm>)
5. Optional: Select a **directory** on the server.
6. Optional: The **New Hostname** specifies the name under which the client will be registered in the UMS.
7. Click **Register**.

8.11. Touchscreen calibration

Menu path: **Setup > Accessories > Touchscreen Calibration**

Enable the calibration program for your touchscreen here and specify how you would like to bring it up.

After launching the calibration program, you will see a pattern with calibration points which must be touched one after another.

- ➡ Further setting options can be found under *Touchscreen* (page 151).

8.12. Task Manager

Menu path: **Setup > Accessories > Taskmanager**

This function provides an overview of the applications and other processes running on the thin client.

Information regarding use of this function can be found under *Using the Task Manager* (page 120). The settings for launching the function are described below.

- To apply a changed setting, click on **Apply**.
- To apply a changed setting and close the setup, click on **OK**.

You can change the following settings:

- **Session Name:** Name for the **Taskmanager** function
- **Start Menu:** If this option is enabled, the Task Manager can be launched in the start menu.
- **Application Launcher:** If this option is enabled, the Task Manager can be launched with the Application Launcher.
- **Desktop:** If this option is enabled, the Task Manager can be launched with a program launcher on the desktop.
- **Quick Start Panel:** If this option is enabled, the Task Manager can be launched in the Quick Start Panel.
- **Start Menu's system tab:** If this option is enabled, the Task Manager can be launched in the start menu's system tab.
- **Application Launcher's System tab:** If this option is enabled, the Task Manager can be launched in the Application Launcher's system tab.
- **Desktop Context Menu:** If this option is enabled, the Task Manager can be launched in 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 Task Manager. The menu path will be used in the start menu and in the desktop context menu. Example: "Functions/Screen functions".
- **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 Task Manager. The menu path will be used for the program launcher on the desktop. Example: "Functions/Screen functions".
- **Password Protection:** Specifies the password request when launching the Task Manager.

Possible values:

- **None:** No password is requested when launching the Task Manager.
- **Administrator:** The administrator password is requested when launching the Task Manager.
- **User:** The user password is requested when launching the Task Manager.
- **Setup user:** The setup user's password is requested when launching the Task Manager.
- **Hotkey:** Specifies a hotkey consisting of modifiers and a key which can be used to launch the Task Manager.
- **Modifiers:** One or two modifiers for the hotkey
- **Key:** Key for the hotkey
- **Autostart:** If this option is enabled, the Task Manager will be launched automatically when the thin client boots
- **Restart:** If this option is enabled, the Task Manager will be relaunched automatically after termination.
- **Autostart Delay:** Waiting time in seconds between the thin client booting and the Task Manager being launched automatically.

8.12.1. Using the Task Manager

The following section explains how to use the Task Manager.

- Launch the **Task Manager** function. The launch options are described under *Task Manager* (page 119).

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:

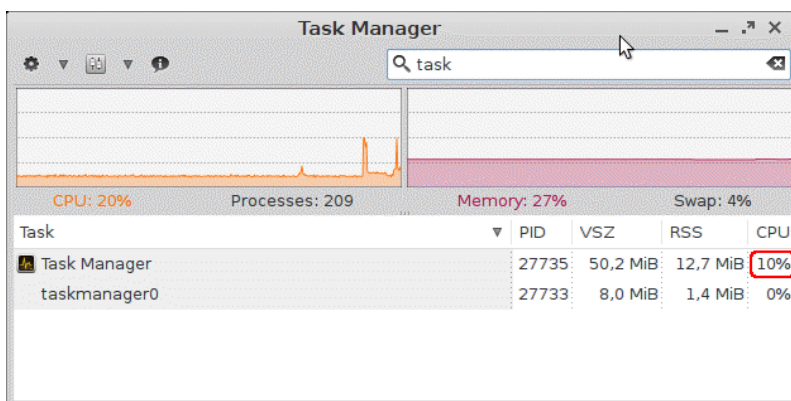
- Read the percentage value under **RAM**:



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

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

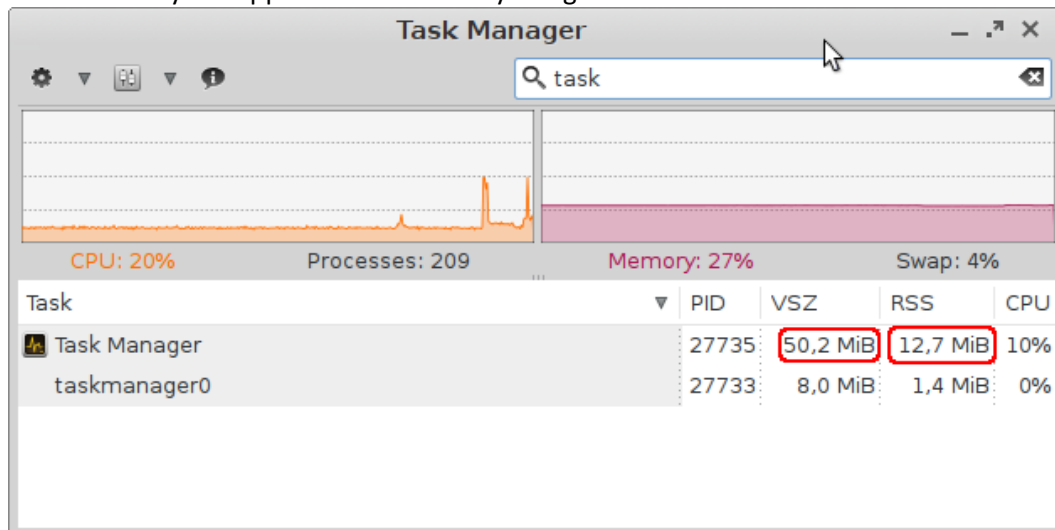
1. In the search window, enter the name of the application or part of the name.
The Task Manager will now show only the relevant applications and processes.
2. Read the percentage value for the relevant application in the **CPU** column.







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

1. 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 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.



- If the **VSZ** column is not shown, click next to  on  and enable the **Virtual Bytes** option.
- If the **RSS** column is not shown, click next to  on  and enable the **Private Bytes** option.

8.13. Screenshot tool

Menu path: **Setup > Accessories > Screenshot Tool**

With this function, you can take a screenshot.

Information regarding use of this function can be found under *Taking a screenshot* (page 122). The settings for launching the function are described below.

- To apply a changed setting, click on **Apply**.
- To apply a changed setting and close the setup, click on **OK**.

You can change the following settings:

- **Session Name:** Name for the **Screenshot Tool** function.
- **Start Menu:** If this option is enabled, the **Screenshot Tool** function can be launched from the start menu.
- **Application Launcher:** If this option is enabled, the **Screenshot Tool** function can be launched with the Application Launcher.
- **Desktop:** If this option is enabled, the **Screenshot Tool** function can be launched with a program launcher on the desktop.
- **Quick Start Panel:** If this option is enabled, the **Screenshot Tool** function can be launched from the Quick Start Panel.
- **Start Menu's System tab:** If this option is enabled, the **Screenshot Tool** function can be launched in the start menu's system tab.
- **Application Launcher's System tab:** If this option is enabled, the **Screenshot Tool** function can be launched in the Application Launcher's system tab.
- **Desktop Context Menu:** If this option is enabled, the **Screenshot Tool** function can be launched in 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 **Screenshot Tool**. The menu path will be used in the start menu and in the desktop context menu. Example: "Functions/Screen functions".
- **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 **Screenshot Tool**. The menu path will be used for the program launcher on the desktop. Example: "Functions/Screen functions".
- **Password Protection:** Specifies the password request when launching the **Screenshot Tool** function.

Possible values:

- **None:** No password is requested when launching the **Screenshot Tool** function.
 - **Administrator:** The administrator password is requested when launching the **Screenshot Tool** function.
 - **User:** The user password is requested when launching the **Screenshot Tool** function.
 - **Setup user:** The setup user's password is requested when launching the **Screenshot Tool** function.
 - **Hotkey:** Specifies a hotkey which can be used to launch the **Screenshot Tool** function.
- ➡ You can also define a hotkey for taking a screenshot under **Setup > User Interface > Hotkeys > Commands**, see *Hotkeys* (page 156).
- **Modifiers:** Combination of modifiers for the hotkey. You can specify a modifier, a combination of an unlimited number of modifiers or no modifier.
 - **Key:** Key for the hotkey
 - **Autostart:** If this option is enabled, the Screenshot Tool function will be launched automatically when the thin client boots.
 - **Restart:** If this option is enabled, the Screenshot Tool function will be relaunched automatically after termination.
 - **Autostart Delay:** Waiting time in seconds between the thin client booting and the Screenshot Tool function being launched automatically.

8.13.1. Taking a screenshot

To take a screenshot of the active window, proceed as follows:

1. Press the keys **Alt+Print** simultaneously.
2. 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.

To take a screenshot of the entire screen or a selectable region, proceed as follows:

1. Launch the **Screenshot Tool** function by pressing **Ctrl+Print** simultaneously. More launch options are described under *Screenshot* (page 121).
2. Select the area you would like to photograph. You have the following options:
 - **Entire screen:** If this option is enabled, the entire screen contents will be photographed.
 - **Active window:** If this option is enabled, the window which is currently the focus will be photographed.
 - **Select a region:** If this option is enabled, you can freely select part of the screen using the mouse.
 - **Capture the mouse pointer:** If this option is enabled, the mouse pointer will be 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.

8.14. Soft keyboard

Menu path: **Setup > Accessories > Soft keyboard**

In this area, you can enable the **On-Screen Keyboard** for use with our IGEL UD10 or any other touchscreen.

In order to display the on-screen keyboard, you can either automatically launch it or show the **On-Screen Keyboard** button in the taskbar. These settings can be configured for the following cases:

- If the logon dialog is visible
- If the screen is locked



This setting has no effect on the on-screen keyboard in the **appliance mode**.

You can also influence which special keys are shown on the keyboard. These also apply for the **appliance mode**. The following three options are available to choose from:

- Function keys
- Navigation keys
- Numeric keys

➡ You will find additional settings under *Keyboard and Additional Keyboard* (page 150).

8.15. Java Control Panel

Menu path: **Setup > Accessories > Java Control Panel**

The Java Control Panel is an operating console which is used for various purposes.

- Specify how Java runs on your computer on the basis of various parameters.
- Manage temporary files used for the Java plug-in.

By doing this, you allow your web browser to use Sun Java to execute applets and Java Web Start. As a result, you can launch Java applications via the network.

- Check certificates via the operating console. This gives you the security you need to use applets and applications via the network.
- Define runtime parameters for applets executed with Java plug-in and applications executed with Java Web Start.

➡ Further information can be found at
<http://java.sun.com/j2se/1.5.0/docs/guide/deployment/deployment-guide/jcp.html>.

8.16. Monitor Calibration

Menu path: **Setup > Accessories > Montor Calibration**

When calibrating your monitor (auto adjust), please use this special pattern. Generally speaking, you will achieve better results than if you calibrate the monitor with a conventional desktop and windows. Clicking on the pattern with the mouse closes the application again.

8.17. Commands

Menu path: **Setup > Accessories > Commands**

The following system commands can be made accessible to the user:

- **Log out**
- **Sort symbols**
- **Switch off terminal**
- **Restart terminal**
- **Restart window manager**

8.18. Network Diagnostics

Menu path: **Setup > Accessories > Network Tools**

The IGEL Universal Desktop Linux firmware features a number of tools for network analysis. These include:

- *Device information* (page 125)
- *Ping* (page 125)
- *Netstat* (page 126)
- *Traceroute* (page 126)
- *Look-up* (page 127)

8.18.1. Device Information

This tool provides information regarding the status of the network device used. This includes:

- MAC and IP address
- Link speed
- Various interface statistics (bytes transferred, errors etc.)

8.18.2. Ping

The **Ping** tool allows you to send contact queries to a network address. You can specify the exact number of queries to be sent. Alternatively, you can enable **Unlimited Requests** which means that the echo requests will be sent until you stop the process.

The Ping result is shown below, and the Ping duration of the last five Pings is illustrated in a bar chart.

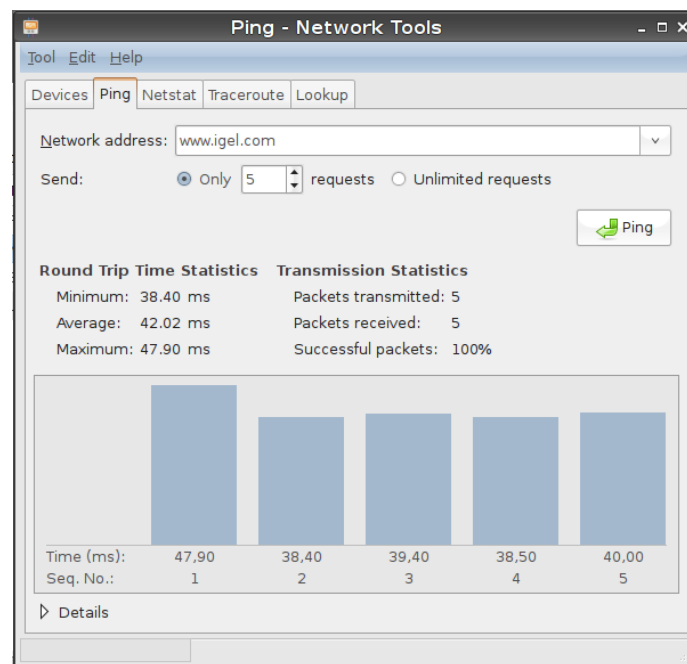


Figure 31: Ping network tools

- Enable **Program→Signal Tone for Ping** to configure the thin client to output an audible signal each time a Ping is sent.

8.18.3. Netstat

Netstat provides information on active network services with protocol and port information as well as a routing table and multicast information for your network devices.

8.18.4. Traceroute

With **Traceroute**, you can trace the route to a network address.

8.18.5. Look-up

The **Look-up** tool shows various information regarding your network address. The available information types are shown in this screenshot.

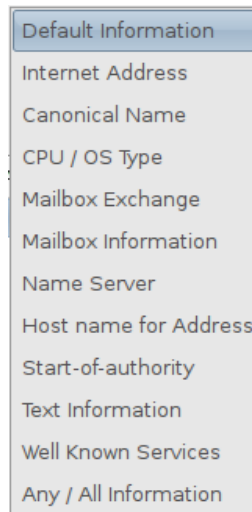


Figure 32: Information types for network address

8.19. System Information

Menu path: **Setup > Accessories > System Information**

The system information provides an overview of all internal and connected thin client hardware components as well as the constituent parts of the Linux system (e.g. kernel modules). The information shown can be copied to the clipboard in order to send it to the IGEL Support department for example.

8.20. Disk Utility

Menu path: **Setup > Accessories > Disk Utility**

Drive management shows all recognized USB drives along with their respective properties (device name, mount point etc.).

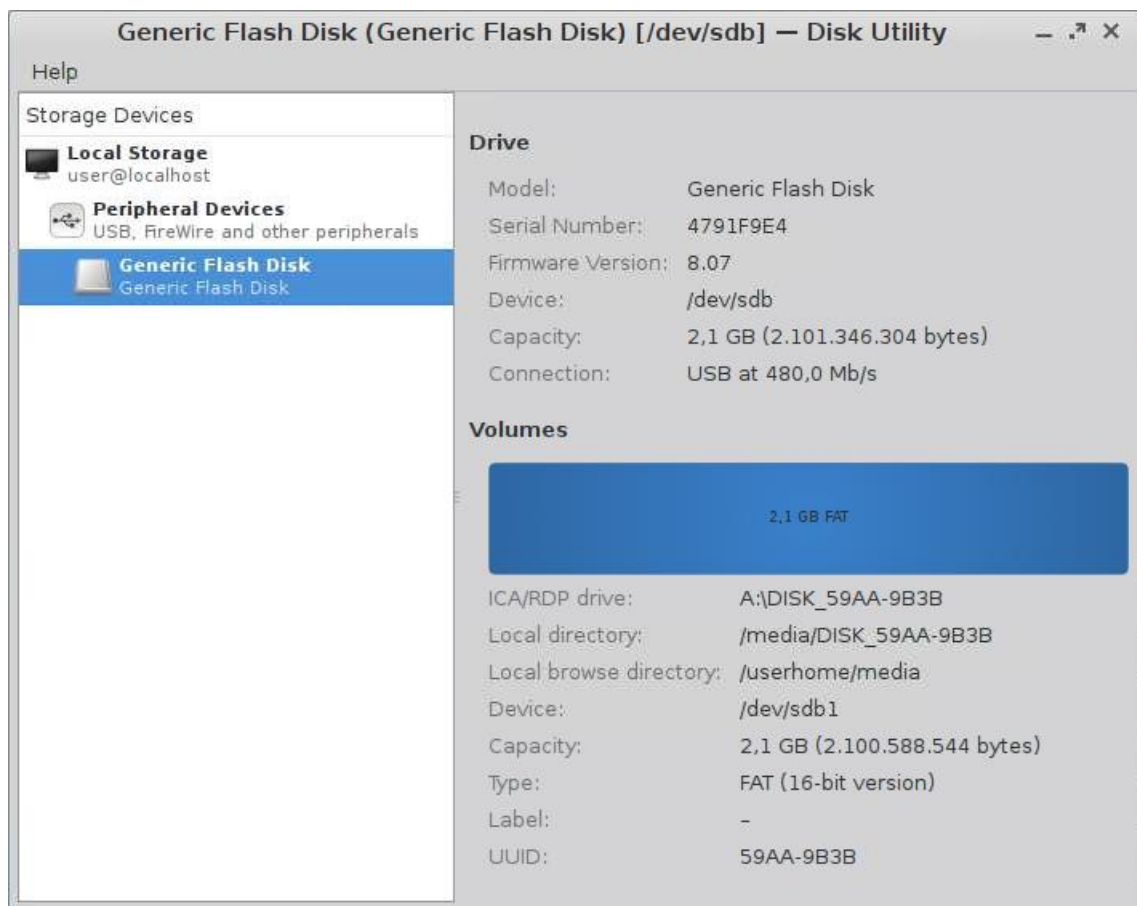


Figure 33: Drive management

- If Dynamic Client Drive Mapping is enabled, you will find a button to safely remove external drives here.
- You can configure a **Hotkey** for opening **Disk Utility**.

8.21. Firmware Update

Menu path: **Setup > Accessories > Firmware Update**

This session updates the firmware with the settings saved in **System > Update > Firmware Update**.

8.22. Smartcard Personalization

Menu path: **Setup > Accessories > Smartcard Personalization**

Configure the options to start the **Smartcard Personalization** (page 188).

8.23. Identify Monitors

Menu path: **Setup > Accessories > Identify Monitors**

Shows the screen number from the IGEL setup and hardware information on every connected screen.



Figure 34: Identify screens

8.24. Upgrade License

Menu path: **Setup > Accessories > Upgrade License**

You can distribute additional firmware functions via the IGEL Universal Management Suite or import licenses locally to a thin client. To do this, an IGEL USB stick with a smartcard or a storage medium containing licenses that have already been produced for this device must be inserted.



Figure 35: Firmware license upgrade

8.25. Webcam Information

Menu path: **Setup > Accessories > Webcam Information**

The **Webcam Information** tool reads information such as the manufacturer, model and supported video formats from a connected webcam. A test image from the camera with the chosen settings can also be displayed.

- Launch **Webcam Information** in the **Application Launcher (System)**.
- Select a resolution and click **Test** in order to display the camera image.

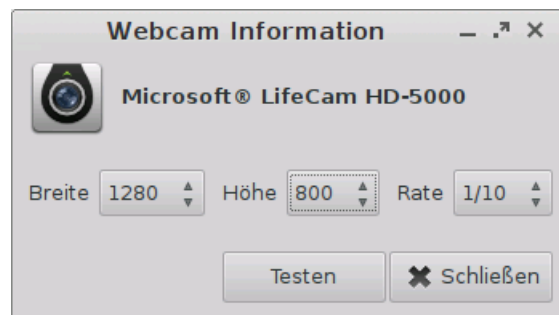


Figure 36: Webcam information



A list with all supported video formats can be created in the Linux Console using the command:
`webcam-info -l`.

```

Local Terminal
root@IGEL-00E0C53627EE:/# webcam-info -l
Microsoft® LifeCam HD-5000
160x120:2/15
160x120:1/10
160x120:1/15
160x120:1/20
160x120:1/30
176x144:2/15
176x144:1/10
176x144:1/15

```

Figure 37: Command webcam-info -l

- ➡ In order to check whether the webcam is functioning in a session (e.g. redirected via Citrix HDX Webcam Redirection), open the website *cameroid.com* (<http://cameroid.com>) in your browser within the session (Adobe Flash must be installed).

8.26. Image viewer

The GPicview image viewer is installed from Igel Universal Desktop Linux 5.06.100.



Applications such as the Firefox browser or the file manager use the image viewer as an auxiliary application. The image viewer does not have a menu entry for opening it directly.

The image viewer can be used to view a wide range of graphic MIME types:

- image/bmp
- image/gif
- image/jpeg
- image/jpg
- image/png
- image/x-bmp
- image/x-pcx
- image/x-tga
- image/x-portable-pixmap
- image/x-portable-bitmap
- image/x-targa
- image/x-portable-greymap
- application/pcx
- image/svg+xml
- image/svg+xml

➡ An entry in the FAQ (<https://faq.igel.com/otrs-igel/public.pl?Action=PublicFAQZoom;ItemID=680>) explains how you can change the way in which they are assigned.

➡ Instructions for using the image viewer can be found on *the Ubuntu Users website*. (<http://wiki.ubuntuusers.de/GPicview>)

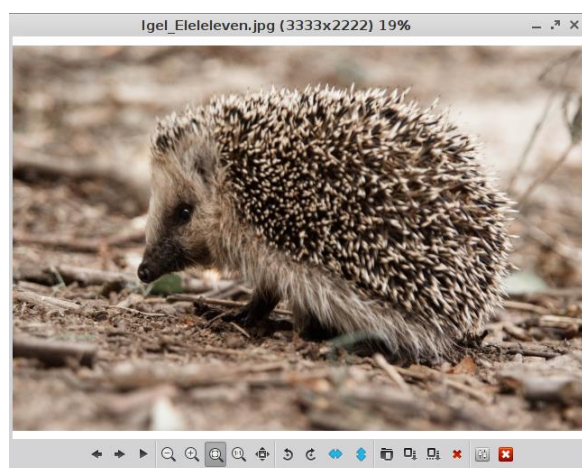


Figure 38: Image Viewer

9. User Interface

You can configure the user interface according to your needs.

9.1. Screen

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

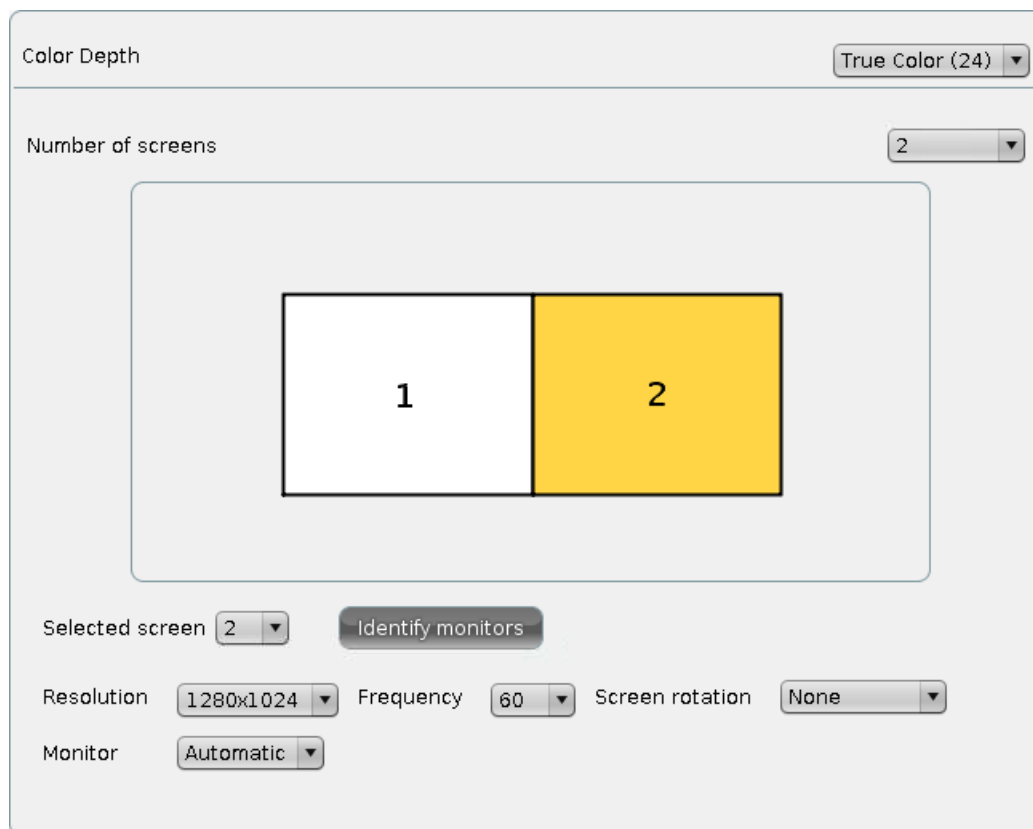




Figure 39: Screen settings

Color Depth	<p>Allows you to select the desktop color depth. The following options are available:</p> <ul style="list-style-type: none"> 16 bits per pixel (High Color / 65,000 colors) 24 bits per pixel (True Color / 16.7 million colors)
 Make sure that all screens connected to the thin client support the color setting.	
DDC	<p>Allows you to activate the Display Data Channel in order to share information between the system and the screen. If screen problems should occur, enable and disable the DDC setting in the Options by way of a test. DDC is enabled by default and the native resolution supported by the screen is determined automatically.</p>
Screen configuration	<p>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 Identify monitors to show the screen identifier on each device.</p>

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

➔ If you use the Shared WorkPlace (SWP) feature with user-specific display resolutions, please note the *best practice on the subject* (<http://edocs.igel.com/index.htm#10202975.htm>).

9.1.1. Energy options

Menu path: **Setup > User Interface > Display > Power Options**

In this area, you can handle display power management. Your screen must support Display power management signaling (DPMS).

Display power management settings

☒ Handle display power management

	On battery	Plugged in
Standby Time	6 Minutes	10 Minutes
Suspend Time	8 Minutes	12 Minutes
Off Time	10 Minutes	15 Minutes

Brightness reduction

	On battery	Plugged in
On inactivity reduce to	20 %	80 %
Reduce after	Never	Never

Figure 40: Display power Management Options

- Enable **Handle display power management** in order to switch on the DPMS energy saving functions.
- 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 reducing the **brightness of the screen**.

- Specify by how many percent the brightness of the screen is to be reduced and how long the period of inactivity before brightness reduction should be. Values between 10 seconds and two minutes are available to choose from.



Naturally, all stages are gone through only if the X-Server does not receive any new entries during this period.

9.1.2. XDMCP

Menu path: **Setup > User Interface > Display > XDMCP**

Enable the XDMCP function for the screen in order to be able to select the appropriate connection type.



Please note that the local setup can then be accessed only using the hotkey **Ctrl+Alt+S**. This should therefore not be disabled for the setup application (**Accessories→Setup**).

☒ XDMCP for this Display

Connection type: indirect via localhost

Name or IP of server:

Figure 41: Display XDMCP

Connection type	Allows you to select the appropriate connection type. If you select broadcast, the graphical logon from the first XDMCP server that responds to a broadcast query will be provided. If you choose the connection type indirect via local host, a list of XDMCP hosts will be shown during the startup procedure. Select from this list the host that provides the graphical logon.
Name or IP of server	This field is enabled if you select the connection type direct or indirect. Give the name or the IP address of the XDMCP server you wish to use. In the direct mode, you are provided with the graphical logon mask straight from the XDCMP server which you specified in the entry field. If you chose the indirect mode, a list of available XDMCP servers will be shown by the server you specified.



Make sure the Display Manager daemon (XDM, KMD, GDM ...) is running and that access authorization is available on the remote host.

9.1.3. Access control

Menu path: **Setup > User Interface > Display > Access Control**

Thin client **access control** is enabled by default. If you highlight **Switch off console access**, it will be possible to access your terminal screen from any UNIX host.

☐ Disable Console switching

☒ Access control

☒ Disable TCP connections

☐ Fixed X-Key

X-Key

List of Trusted X Hosts ★ 🗑️ 📄

Figure 42: Access Control

Fixed X-Key	You can grant specific users permanent remote access to your thin client. To do this, you will need to enable this option, click on the Calculate button and enter the 32-character key you have received into the Xauthority file on the user's computer.
List of Trusted X hosts	Click on the Add button to open the entry mask. Give the name of the remote host (not the IP address) you would like to add and confirm this by clicking on OK .

9.1.4. Gamma correction

Menu path: **Setup > User Interface > Display > 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.

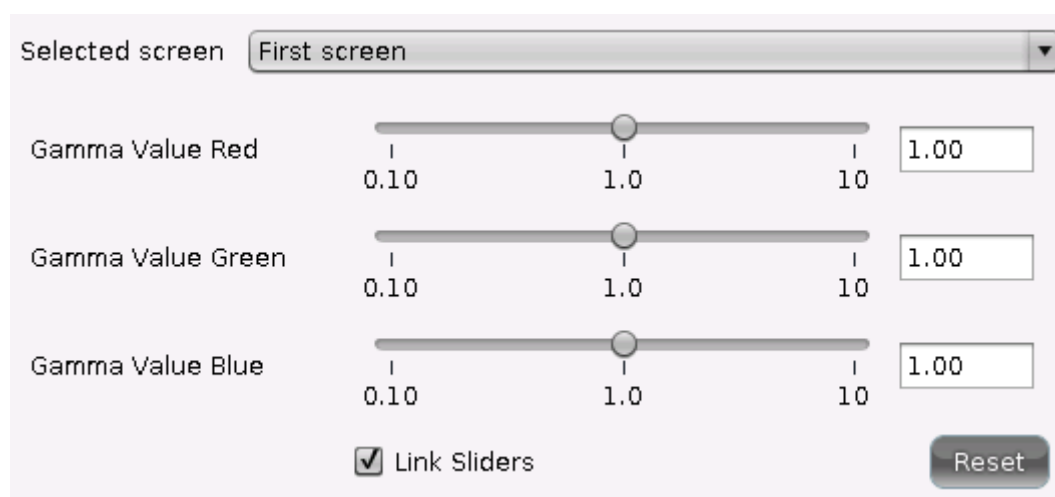


Figure 43: Gamma correction

9.1.5. Options

Menu path: **Setup > User Interface > Display> Options**

Configure the options for the display here:

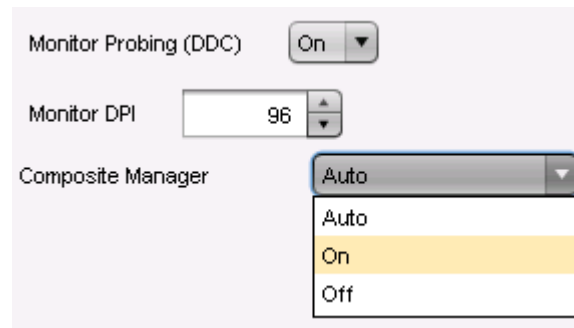


Figure 44: Display options

Monitor Probing (DDC)	Select Off in order to disable the automatic probing of display properties.
Monitor DPI	Enter the DPI resolution (dots per inch) for your monitor. The default setting is 96 DPI.
Composite Manager	<p>You will find three modes for the Composite Manager, the start menu and windows with animations and effects here:</p> <ul style="list-style-type: none"> • Automatic: Disables the Composite Manager during battery operation, if the color depth is low or if the hardware is weak. • On • Off

9.1.6. Universal MultiDisplay

The IGEL Universal MultiDisplay (UMD) solution enables you to set up an extended desktop with up to eight screens in any arrangement (the individual screen areas must however be in contact with each other at one edge and corner, and cannot overlap).

A master thin client (master) can be connected to up to three satellite thin clients (satellite), while one or two screens can be connected to each of the thin clients within the group. Only the master is connected to the company network. The satellites are connected, via their own network, only to the master, which must have a second network card for this purpose.

All other peripherals such as a keyboard, mouse etc. are connected to the master. The entire system is also configured on the master, either via its local setup or the IGEL Universal Management Suite UMS.

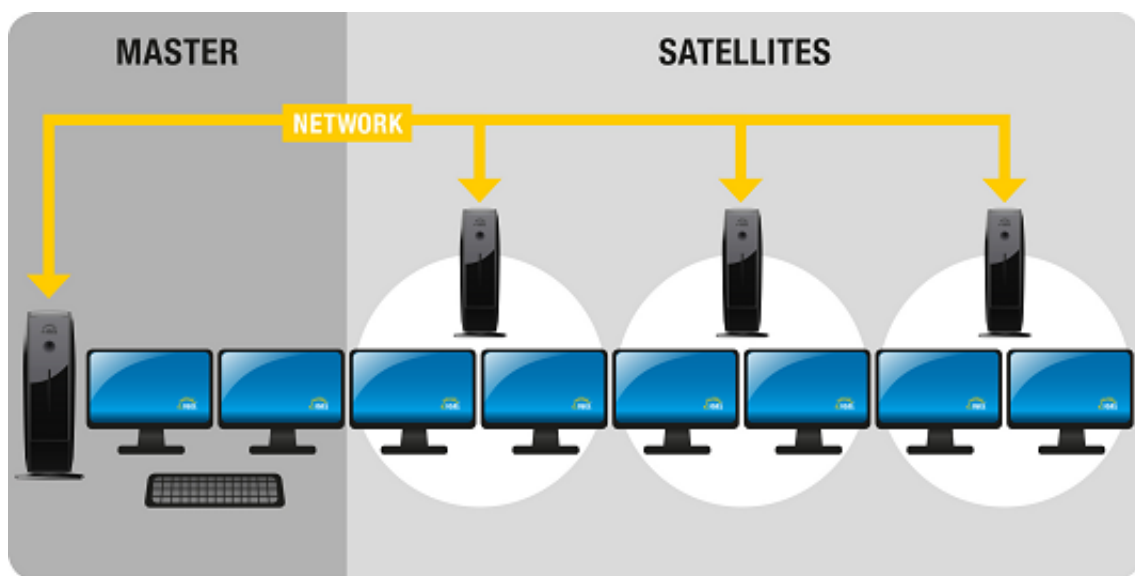


Figure 45: IGEL Universal MultiDisplay Setup

Software Requirements

The following software requirements must be met in order to use IGEL Universal MultiDisplay:

- IGEL UD Linux firmware offering IGEL Universal MultiDisplay support on the master and satellites



Note: Devices with IGEL Universal Desktop OS cannot be used for IGEL Universal MultiDisplay.

- IGEL Universal MultiDisplay Starter Kit license for up to three displays (2x master, 1x satellite)
- IGEL Universal MultiDisplay license for each additional display connected



Note: You will receive the Starter Kit license along with the master thin client. Licenses for additional displays can be added to the master thin client in the IGEL Universal Management Suite Console (**System > License Management**).

Hardware and Network Requirements

The following requirements must be met in order to use IGEL UMD:

- Master: IGEL UD5-x30 LX thin client with PCIe network card installed
- Satellite: Up to 3 IGEL thin clients with Universal Desktop Linux
- The master is connected to the company network via the internal Ethernet port. The additional PCIe network card is used to connect one satellite directly, or a number of satellites via an intermediate switch.
- Depending on the particular hardware configuration, screens can be connected to the master and the satellites via the VGA, DVI or display port.

Advanced Options

In the IGEL Registry under **Setup→System→Registry**, you will find a number of additional parameters which are not yet available in the actual screen configuration:

x.dmx.number_of_screens_master and **x.dmx.number_of_screens_slaveX** allow you to define only one connected monitor for a particular thin client (the default setting is two available monitors per device). This makes sense if two or more UD5s, each with a high-resolution monitor, are to be connected together via the display port for example.

The master saves the list of available satellites. A satellite can be deleted from the list via the **x.dmx.slaveX** parameter by selecting Delete Instance.

The satellites can be arranged in any order by making changes in **x.dmx.slaveX.number**. However, there is no consistency check, so you must therefore carry out a manual check to ensure that the numbering is clear.

With **x.dmx.net**, the automatic configuration of the internal network between the master and clients can also be carried out manually, e.g. the IP address of the master or the address area of its DHCP server.

Configuration

Once you have connected the master and satellites to each other as described above, switch on the master thin client. In the master setup, enable IGEL Universal MultiDisplay under **User Interface→Screen→IGEL Universal MultiDisplay**.

Select the number of screens and set the resolution, rotation etc. for each one. You can select the screens from the list or simply by clicking on them in the arrangement overview.

Using drag & drop, arrange the screens in the overview in the same way as they are physically arranged. When all screens are configured, confirm your choices by clicking on **OK**.

Now switch on the satellites, one after another, starting with satellite 1. After powering up a satellite, wait around 30 seconds before switching on the next one. The satellites will receive their configuration, including IP address, from the master. IGEL Universal MultiDisplay is now ready for use.

Usage

Once you have carried out the initial setup procedure as described above, you will not need to touch the satellites again. The satellites are automatically shut down when you switch off the master and reactivated when the master boots. Subsequent firmware updates will also be distributed automatically to the satellites by the master. All changes to the screens' configuration (arrangement and resolution of the screens, desktop background for each screen, screensaver etc.) should be made on the master (locally or via the UMS). Naturally, this also applies to all other options, e.g. sessions.

You can move application windows freely over all the screens and enlarge the windows so that they cover screen boundaries. If you maximize windows, they are usually enlarged to cover the area of the current screen. Depending on the session type, sessions in full-screen format may be restricted to a specific screen or can be expanded across all screens.

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**
- **Desktop Icon Size:** Specify the size in which you would like the icons to be displayed on the desktop.
- **Single Click Mode:** This option was set up specially for users of touchscreen monitors. Enable this mode in order to open programs with a single click.
- **Default Font:** Choose between serif and sans-serif text and between standard and bold.
- **Default Font Size:** Specify your desired font size in pt (points) here.
- **Desktop Icon Font Size:** Specify your desired font size for desktop icons in pt (points) here.
- **Titlebar Font:** Choose between serif and sans-serif text and between standard and bold.
- **Titlebar Font Size:** Specify your desired font size in pt (points) here.

9.2.1. Background

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

In this area, you can configure the desktop background with pre-defined IGEL backgrounds, a fill color or a color gradient.

You can also select a background image of your own.



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

Own background image - server configuration

- **Wallpaper:** Provides a selection of pre-defined IGEL backgrounds
- **Wallpaper Style:** Provides various design versions:
 - Automatic
 - Centered
 - Tiled
 - Stretched
 - Scaled
 - Zoomed
- **Color Style:** Sets a fill color or a color gradient.
- **Desktop Color:** Sets a desktop color.



You can also use a background image of your own. You can set up a separate background image for each monitor that is connected to the thin client.

- You can provide a user-specific background image on a download server.
1. In the **Desktop > Background** window, enable the option **Own background image**.
 2. Give a name for the background image file.
 3. Specify the download server under **Desktop > Background > Background Image Server**.



If you have already defined a server for the system update files, you can use the same server setting for downloading the background image.

The user-specific background image will be downloaded from the specified server if the function was enabled and if requested manually (Update Background Image). The download can also be launched from the IGEL Universal Management Suite via **Update desktop changes**.

- ➡ A user-specific boot image can be provided on a download server.



The file types BMP, JPG, GIF, TIF, PNG and SVG are supported for an **own background image** and **bootsplash**. A total storage area of 25 MB is available for all user-specific images.

9.2.2. 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:** If this option is enabled, the taskbar will be displayed.
- **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.



If **Number of rows/columns in Taskbar** is set to **Automatic**, the window buttons as well as the symbols 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* (page 143).

- **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: Symbols in the Quick Start Panel, window buttons,
 - **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.
- **Monitor:** Specifies the screen on which the taskbar is shown. This parameter is available if **Multi Monitor Taskbar Size** is set to **Restrict taskbar to one monitor**.
- **Taskbar on top of all windows:** If this option is enabled, the taskbar is always shown, even in sessions with a full-screen window.
- **Taskbar Auto Hide:** If this option is enabled, 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:

- **Intelligently:** 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.
- **Always:** 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.



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 **Taskbar Auto Hide** is enabled.

➡ Further settings can be found under *Screen Lock/Saver* (page 146).

9.2.3. Taskbar background

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

You can specify the background style for the taskbar here.

To incorporate your company logo into the taskbar, proceed as follows:

1. Select **Background Image** under **Background Style**.
2. Give the path of the background image.

➡ See also *Taskbar* (page 141) under User Interface.

9.2.4. Taskbar items

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

- **Taskbar Clock:** If this option is enabled, a clock will be shown in the taskbar.
- **Sorting order in window button list:** Specifies the criteria according to which the window buttons are sorted.

Possible values:

- **Timestamp:** 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'n'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 list:** 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* (page 141).
- **Numeric values:** This value specifies the maximum number of rows.
- **Show labels in window button list:** If this option is enabled, the names of ongoing sessions are shown in the associated window buttons. If this option is disabled, only the symbols are shown.
- **Taskbar System Tray:** If this option is enabled, the system tray will be shown in the taskbar.
- **Size of icons in system tray:** Specifies the size of system tray icons (volume, network connection etc.).

You can choose a pre-defined value or enter a numeric value between 1 and 64.

Predefined values:

- **Automatic:** The size is adjusted to the height and width of the taskbar.
- **Small:** 20 pixels
- **Medium:** 40 pixels
- **Large:** 60 pixels

➡ Further settings can be found under *On-screen Keyboard* (page 123), *Keyboard and Additional Keyboard layouts* (page 150) and *Screen Lock/Saver* (page 146).

9.2.5. 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:** Allow a number of virtual desktops.
- **Number of Screens - Horizontal:** Specify how many pages you want to display next to each other.
- **Number of Screens - Vertical:** Specify how many pages you want to display above each other.
- **Names of the workspaces:** Give names for the individual desktops.
- **Paging Resistance:** Specify 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 when 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.

9.2.6. Start menu

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

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

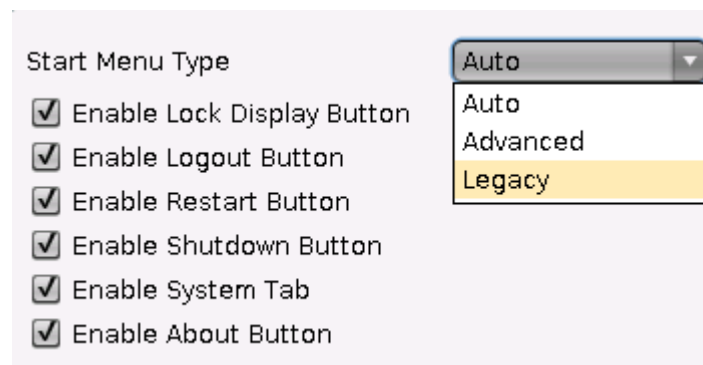


Figure 46: Desktop Start menu

There are three start menu types:

Legacy:	Standard setting which is similar to that from Windows 95 - a list of available sessions and options
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.
Auto:	Automatically select the classic or advanced start menu depending on the processor.

9.2.7. Session Control Bar

Menu path: **Setup > User Interface > Desktop > In-Session Control Bar**


The session control bar allows you to eject a USB drive from a full-screen session, to minimize a session view and to end the session.

- **Use in-session control bar in all supported sessions:** If this option is enabled, the session control bar will be displayed. Depending on the configuration, the session control bar will be permanently visible or will be shown as soon as you move the cursor to the top edge of the screen.

The session control bar is available for the following session types:

- **RDP** - see *RDP Global* (page 42)
- **Citrix** - see *HDX / ICA Global* (page 22), *Legacy ICA Sessions* (page 31) and *Citrix StoreFront / Web Interface* (page 36)
- **ThinLinc** - see *ThinLinc* (page 76)
- **NX** - see *NX* (page 73)
- **Parallel 2X Client** - see *Parallel 2X Client* (page 74)

To use the session control bar, proceed as follows:

- To eject a USB device, click on .
- To minimize the session view, click on .
- To end the session, click on .
- To make the session control bar permanently visible, click on .

9.3. Language

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

Select the system language from the list. You can also set the keyboard layout and the input language depending on the system language.



The language selected is the language for the user interface and therefore applies to all local applications.

9.4. Screen Saver and Screen Lock

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

You can set up the screen saver so that it is activated either automatically 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 login dialog and the locked screen.

Example configuration of a screen lock:

General

The screen can be locked via taskbar or desktop icons or using hotkey **Ctrl-Shift-L**.

Figure 47: Startup Options of Screen Lock

Options

The screen lock starts automatically after 5 minutes without user action at the thin client. The screen lock can be stopped by entering a user password or administrator password (see *Password* (page 187)).

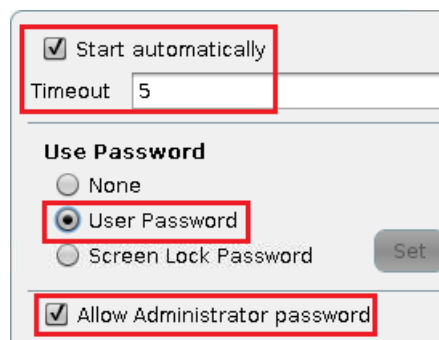


Figure 48: Autostart and Password Settings

Taskbar

The locked screen does not display the taskbar until the login dialog appears. The user can bring up a soft keyboard, e.g. to login using touchscreen monitor.

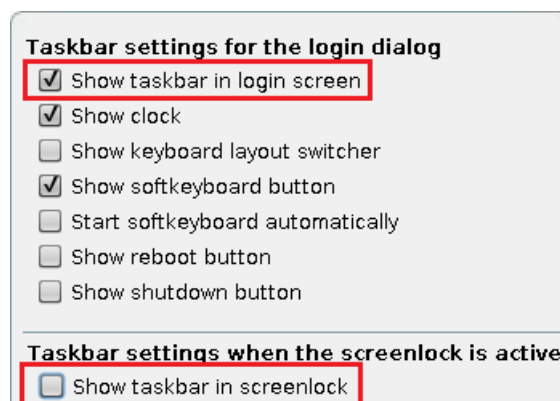


Figure 49: Taskbar on Login Dialog

9.4.1. Example configuration for the screen saver

Menu path: **Setup > User Interface > Screen Lock/Saver > Screensaver**

The session for the **screen saver** can show both a custom image and a configurable clock.

You can select the color of the background, display a custom image (or several images as a slide show) or a digital clock whose size and color can be changed. A combination of a company logo and the clock can also be displayed.

- ➔ In our best practice you will find an example configuration and further instructions on how to customize your IGEL Linux desktop.

1. Connect a network drive with your saved images.



You can also send images to the thin client, e.g. to a /wfs/pix target directory, using UMS file transfer.

2. Enable the displaying of images in the configuration menu for the screen saver and use the network drive connected beforehand as the source.

Figure 50: Select image source



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.

- You can configure a digital clock (size, position on the screen and colors) independently of the screen display. The seconds display can be disabled.

Figure 51: Clock configuration

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 configured:

- *Keyboard* (page 150)
- *Mouse* (page 150)
- *Touchscreen* (page 151)
- *Signaturpad* (page 155)

9.5.1. Keyboard and additional keyboard

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

In this area, you can configure the keyboard.

- **Keyboard layout** – Determines the keyboard layout. The selected layout applies for all parts of the system including emulations, window sessions and X applications.
- **Keyboard type** – Determines the keyboard type.
- **Key repeat** – Determines the automatic repeat behavior for the keyboard:
 - **Repeat delay** – Determines the delay (in milliseconds) before automatic repetition begins.
 - **Repeat rate** – Determines how often a character repeats per second.
 - **Enable dead keys** – Enable this function if the keyboard used supports dead keys for special characters.
- **Start with NumLock on** – Stipulates that **NumLock** is to be automatically enabled during the boot procedure.

Menu path: **Setup > User Interface > Input > Additional Keyboard Layouts**

- You can define **additional keyboard layouts** which can be selected by the user. The layout can be selected in the taskbar or changed via configurable hotkeys.

➡ Further settings can be configured under *On-screen Keyboard* (page 123).

9.5.2. Mouse

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

In this area, you can configure the mouse.

- **Lefthand mode:** Changes the orientation of the mouse by switching the mouse buttons to left-handed mode.
- **Emulate 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:** Cursor will be hidden after the defined timeout.
- **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, considered as double click. The object under the second click receives the double click.

9.5.3. Touchscreen

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

To ensure that you can open the setup and navigate within it, the initial configuration should take place with a mouse and keyboard connected. The setup procedure with an on-screen keyboard is described below.

Touchscreen drivers

The touchscreen types currently supported are:

- Elographics serial touchscreens
- TSharc serial touchscreens
- EvTouch USB touchscreens

➡ You will find the complete list of supported devices in the IGEL Linux 3rd Party Hardware Database.

- **Touchscreen already calibrated**

If you enable the touchscreen function, the touchscreen must be calibrated first. Unless you enable this option, calibration will begin automatically after each system boot.

- **Swap X and Y values**

Enable this option if the mouse pointer moves vertically when you move your finger in a horizontal direction.

- **Minimum/maximum X value/Y value**

These values are determined by the calibration tool. However, you can also change them manually.

- **Let-go limit**

The maximum permitted time (in milliseconds) between two instances of contact in order to still be registered a single touch. When moving windows by drag-and-drop, for example, your contact with the screen may inadvertently be interrupted. Increasing this value prevents the thin client from registering two individual contacts in this case.

- **Contact limit**

Determines how long (in milliseconds) the screen needs to be touched in order for the contact to be recognized.

- **Baud rate (for serial touchscreens only)**

Determines the speed of communication via the selected connection. (If in doubt, read the monitor manual.)

- **Touchscreen connection**

You can connect the touchscreen either to COM1 or COM2. Select your preferred connection here.

- **Set driver-specific default settings**

Click on this button once after changing the touchscreen type or to restore the default settings.

➡ A list of the touchscreens currently supported by IGEL Linux can be found in the IGEL Linux 3rd Party Hardware Database.

➤ Enable the on-screen keyboard for touchscreen use in the setup under **Accessories > On-screen Keyboard**.



The layout for the normal keyboard will also be used for the on-screen keyboard.

➤ Calibrate the touchscreen for optimum contact recognition. The touchscreen calibration application can be found under **Application Launcher > System**.

After launching the calibration program, you will see a pattern with calibration points which must be touched one after another.

9.5.4. Touchpad

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

If you use the Universal Desktop Converter, you have the option of defining touchpad settings.



The actual options depend on the particular touchpad.

You will find these under **User Interface > Input > Touchpad**.

The settings options are subdivided into

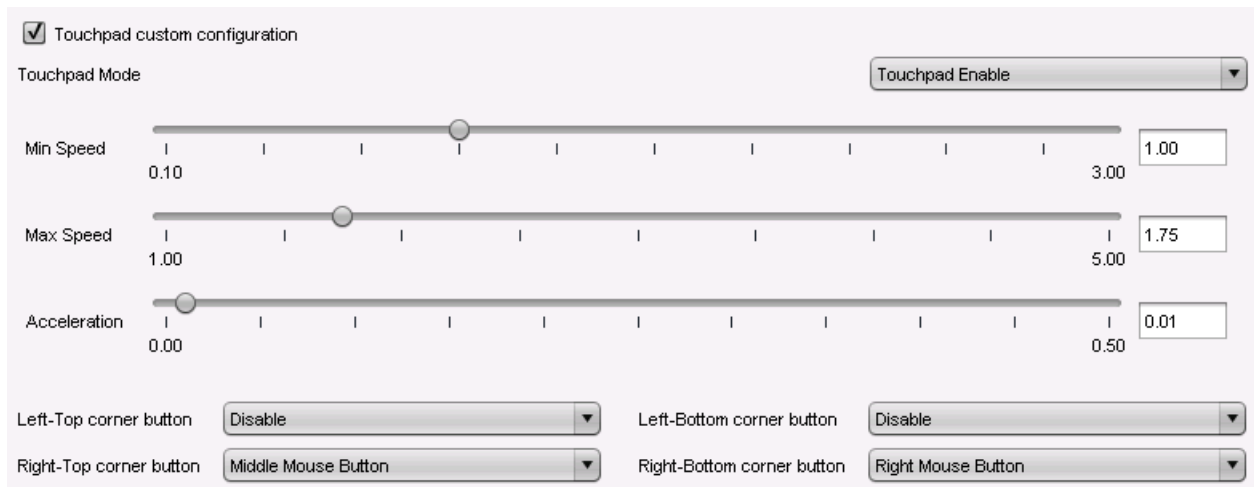
- *Touchpad General* (page 153)
- *Touchpad Scrolling* (page 153)
- *Touchpad Advanced* (page 154)

Touchpad General

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

In this area, you can configure the touchpad according to your needs.

- Enable **Touchpad custom configuration** in order to define personal settings.



☒ Touchpad custom configuration

Touchpad Mode: Touchpad Enable

Min Speed: 0.10 | 1.00 | 3.00

Max Speed: 1.00 | 1.75 | 5.00

Acceleration: 0.00 | 0.01 | 0.50

Left-Top corner button: Disable

Left-Bottom corner button: Disable

Right-Top corner button: Middle Mouse Button

Right-Bottom corner button: Right Mouse Button

Figure 52: General settings for the touchpad

- Select a touchpad mode from:
 - **Enable touchpad** - Decide whether you would like to enable the touchpad by default...
 - **Disable touchpad** - ... or disable it.
 - **Disable tapping and scrolling** - As an alternative, you can disable tapping and scrolling only.
- Use the sliders to set the speed of the mouse pointer in seconds.
- With a number of touchpads, you can assign functions to the four corners. The following settings apply by default:
 - **Left mouse button** - Tap on the relevant corner to highlight objects, place the cursor and move text or objects from one place to another.
 - **Middle mouse button** - Tap on the relevant corner to bring up program-specific functions.
 - **Right mouse button** - Tap on the relevant corner to display the context menu.
 - **Disable** - Tap on the relevant corner to disable the mouse button.

Touchpad scrolling

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

Define the properties for vertical and horizontal scrolling here.

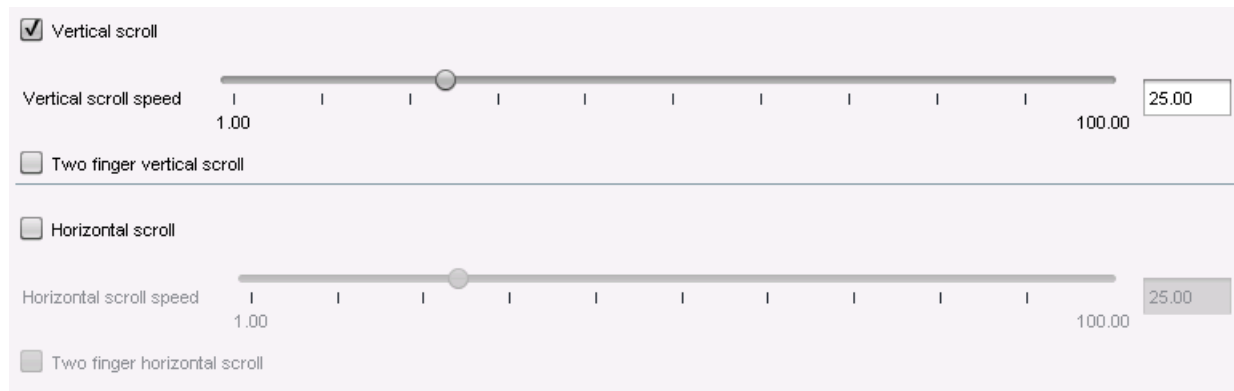


Figure 53: Scrolling properties for the touchpad

- Enable **Vertical scrolling** in order to set the **vertical scroll speed**.
- Enable **Horizontal scrolling** in order to set the **horizontal scroll speed**.

Touchpad Advanced

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

Further settings are possible here:

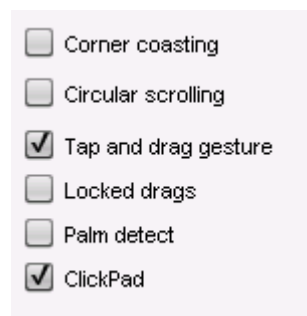


Figure 54: Advanced settings for touchpad

- Enable the following functions in order to:

Corner coasting	continue scrolling if your finger reaches the corner when scrolling vertically or horizontally along the touchpad edges.
Circular scrolling	scroll in a circular fashion. In the selection menu, specify where circular scrolling is to begin.
Tap and drag gesture	move items by tapping and dragging them.
Locked drags	end the tap and drag gesture only after an additional tap; it will otherwise end when you let go.
Palm detection	avoid triggering a function accidentally with the palm of your hand. The function must be supported by the device.
ClickPad	allow ClickPads. These are touchpads with so-called integrated soft buttons on which physical clicks are possible.

9.5.5. SCIM (Input Methods)

Menu path: **Setup > User Interface > Input > SCIM Input Methods Platform**

Smart Common Input Method (SCIM) platform offers entry methods for over 30 languages under Linux. You can enable one of the methods provided by the IGEL system for Chinese character sets (Simplified Chinese, Traditional Chinese) or manage generic tables for describing the entry method.

9.5.6. Signature pad

Menu path: **Setup > User Interface > Entry > Signature Pad**

The following signature pads are available for connection to IGEL Linux thin clients:

- Softpro
- StepOver TCP
- signotec VCOM Daemon



Enable the **Softpro SPVC signature pad channel** in the IGEL Setup under **Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Mapping > Device Support**.

To enable the **StepOver TCP Client** in order to be able to use USB signature pads from this manufacturer in sessions, proceed as follows:

1. Select the checkbox for **StepOver TCP Client**.
If necessary, you can change the TCP port.
2. Click on **Apply**.

- ➡ You will find detailed information regarding the configuration of signature pads in the Best Practice documents for StepOver Pads and Softpro/Kofax pads.

To enable the **signotec VCOM Daemon** in order to be able to use USB signature pads from this manufacturer in sessions, proceed as follows:

1. Select the checkbox for **signotec VCOM Daemon**.
2. Click on **Apply**.
3. Go to **Mapping > Serial Connections** under ICA or RDP Global.
4. Enable **COM Port Mapping**.
5. Click on **Add** and choose one of these devices **Search Devices**.

Under **Select Available Device**, you can choose from the signotec devices `/dev/ttyVST0` and `/dev/ttyVST1`.

6. Select one of these devices.
7. Your signotec signature pad can now be used.

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.

To enable or disable a hotkey, proceed as follows:

1. Highlight the hotkey in the list.
2. Click on **Modify....**
3. Enable or disable the **Hotkey** option in the dialog window.
4. Click on **Continue** in the dialog window.
5. Click on **Apply** or **OK**.

To change the keys used for a hotkey, proceed as follows:

1. Highlight the hotkey in the list.
2. Click on **Modify....**
3. In the **Modifiers** selection list, select a modifier, no modifier or a combination of modifiers.
4. Enter the **Key**.
5. Click on **OK** or **Cancel**.

The following hotkeys are available and can be changed:

- Hide all windows and show desktop
- Screenshot of active window
- Screenshot of entire screen
- Volume up (multimedia key)
- Volume down (multimedia key)
- Volume mute (multimedia key)
- Switch between active windows using Task Switcher
- Switch between active windows using Task Switcher (backwards)
- Switch focus to next window
- Switch focus to next window (2)
- Enable next window (reverse order)
- Open start menu
- Open start menu (2)

9.7. Font Services

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

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

- *XC font service* (page 157)
- *NFS font service* (page 157)

9.7.1. XC Font Service

Menu path: **Setup > User Interface > Fonts Services > XC Font Service**

If you need other fonts in addition to those offered by the thin client, you can use the XC font service.



This service must be installed on a server and fully configured there.

The advantage of using the XC font service rather than NFS is its better performance.

➤ Click on **Enable XC Font Service** in order to enable the following entry fields.

XC font server	Give the name of the server on which the XC font service operates.
Port number	Give the number of the port used by the font service for reception purposes - the default setting is port number 710.
Favor local fonts	Enable this option if local fonts are to be used before a request is sent to the font server.

9.7.2. NFS Font Service

Menu path: **Setup > User Interface > Fonts 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.

- Define and enable an NFS font path entry in order to use the NFS font service.

This will be added to the **list of NFS mounted font directories**.

- Click on **Add** to open the dialog window:

Local directory	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.
Server path	Path on the server under which the fonts are available.
Favor local fonts	If this option is enabled, local fonts are to be used before a request is sent to the font server.

- Click on **Enable** to enable the entry.
- Export the font directory to the server via NFS read-only for the thin client.

10. Network

Menu path: **Setup > Network**

Configure the thin client's network connections here.

10.1. Mobile broadband network

If no LAN or WLAN is available at your location, you can establish a UMTS connection with the Huawei E3531 HSPA+ surf stick.





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 surf stick is already inserted and has been configured, the network connection will be established within approx. 35 seconds after the thin client boots. The network connection will remain in place until the surf stick is removed or the thin client is put on standby or shut down.

Symbols in the system tray indicate the status of the network connection:

-  The network connection is established; the thin client is online
-  The network connection was interrupted; the thin client is offline

To change the settings for the mobile broadband network, proceed as follows:

1. Right-click on  or .
2. In the context menu, select the option **Configure mobile broadband network**.
3. Change the settings:
 - **Enabled:** If this option is enabled, the mobile broadband network is active.
 - **APN:** APN (Access Point Name) for your network connection. If you do not know the APN, ask your mobile communications operator for it.
 - **Network ID:** Network ID for your network connection. If you do not know the network ID, ask your mobile communications operator for it.
 - **Number:** Access number for your network connection. If you do not know the access number, ask your mobile communications operator for it.
 - **User name:** User name for your network connection. If you do not know the user name, ask your mobile communications operator for it.
 - **Password:** Password for your network connection. If you do not know the password, ask your mobile communications operator for it.
 - **PIN:** PIN for your SIM card.
4. Click on **OK**.

10.2. LAN interfaces

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

- Click on **Network > LAN interfaces** in the client setup.
- Choose between automatic network setup with the protocols DHCP and BOOTP or manual network configuration in order to set the thin client for each network interface.

☒ Activate default interface (Ethernet)

☒ Get IP from DHCP Server
☐ Specify an IP Address

IP Address

Network Mask

Default Gateway ☐ enable

Terminal Name

☐ Enable DNS

Default Domain

Nameserver

Nameserver

☐ Manually overwrite DHCP settings
☐ Dynamic DNS Registration

Dynamic DNS Registration Method

TSIG key file for additional DNS authentication

Figure 55: LAN Interfaces

DHCP	Via the Dynamic Host Configuration Protocol, the thin client receives its IP address, network mask, DNS, gateway and other network configurations from a DHCP server. DHCP is enabled by default for LAN 1 (internal). DHCP options can be enabled in the DHCP Client menu. A list of standard options is available. However, you can also define your own options.
BOOTP	Via the BOOTP , the thin client receives its IP address, network mask, DNS, gateway and other network configurations from a BOOTP server database.



The transferring of a `setup.ini` file or a boot script is not supported. BOOTP is not used to call up a boot image from a server and boot this image, in spite of what the term may imply.

Specify IP address manually	Configures the network settings manually instead of searching for a DHCP server. Ensure that the fixed IP address that you enter is not used by another computer in your network. If you have to use a gateway to forward the data packages to and from the target network, click on Enable and enter the gateway IP address.
Terminal name	Give the local name of the thin client. Otherwise, the standard name IGEL <MAC address> will be generated.
Enable DNS	Configures the DNS - Specify the standard domain in which the device will work as well as the IP address of up to two name servers which will be queried one after the other.
Manual overwrite DHCP settings	Manual entries overwrite the standard route, the domain name and the DNS servers.
Dynamic DNS registration	Here, you can automatically report the current IP address of the thin client to the DNS. The DHCP and DNS methods are available. If you select DNS , you may have to specify a private TSIG key for DNS authentication .

➡ You can find instructions for dynamic DNS registration via DNS in an FAQ document.

10.2.1. Individual interface

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

Under the name of the individual interface (for example Interface 1), you can overwrite some of the general settings for LAN interfaces. In addition, there are two further settings:

IPv6 configuration	Here, you can choose a configuration type for operation with IPv6. You will find further details in a best practice document.
Network link type	Specify the network link type for the interface. The default is Automatic Recognition .

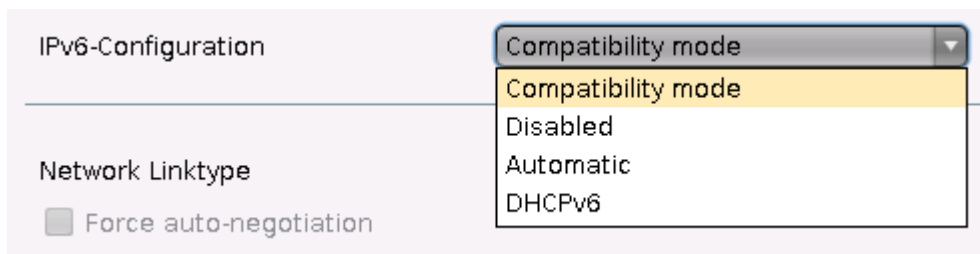


Figure 56: Configuration of an individual interface

Authentication

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

You can enable and configure network port authentication in accordance with the IEEE 802.1x standard here. The following settings are available:

- **Enable IEEE-802.1x authentication:** This option enables network port authentication.
- **EAP Type:** You can choose between the **PEAP** and **TLS** authentication procedures here.



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:** If this option is enabled, the certificate of the server will be checked cryptographically. In order to do this, the path to the CA certificate file is required in **CA Root Certificate**. The file can be in PEM or DER format.



A number of the following fields need to be filled in only for specific combinations of **EAP type** and **Auth Method**.

- **Manage certificates with SCEP (NDES):** Automatically manage client certificates with **SCEP** (page 174)
- **Identity:** The user name for network access
- **Password:** The password for network access



If you leave the **Identity** and **Password** fields empty, an entry mask for authentication purposes will be shown. However, this does not apply to the methods with a client certificate (TLS and PEAP-TLS) where these details are mandatory.

- **Client Certificate:** Path to the file with the certificate for client authentication in the PEM (base64) or DER format. If a private key in the PKCS12 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.

Wake-on-LAN

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

Select the packages or messages with which the thin client can be started via the network.

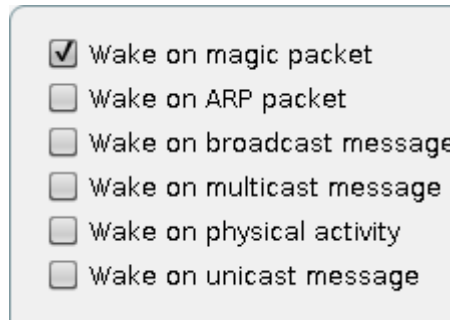


Figure 57: Wake-on-LAN options

10.2.2. Wireless

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

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

➡ You will find details of compatible wireless modules in our IGEL Linux 3rd Party Hardware Database.

If you use mobile devices and regularly spend time in different wireless zones, you will benefit from our new function: IGEL Café Wireless. This means that you can

- easily connect to new, previously unknown wireless networks
- save connections that you have set up and then reuse them later on

straight from the user interface via the *Wireless Manager* (page 165) as you would with a smartphone. This function is irrelevant for stationary desktop devices that are managed centrally. In this case, it is assumed that the network has fixed settings and cannot be influenced by the end user.

To configure the wireless interface, proceed as follows:

1. Open the **IGEL Setup** and click on **Network > LAN Interfaces > Wireless**.

Figure 58: Enable user-defined connections

2. Enable the **Wireless Interface**.
3. Select the configuration for your **IP Addresses** (DHCP or manual).
4. Select a configuration type for operation with **IPv6**.
5. Enable at least the **tray icon**, **context menu** and **Wireless Manager** (page 165) items. Via the *Wireless Manager* (page 165), you can use IGEL Café Wireless.



Ensure that the **Overwrite sessions** parameter is disabled for UMS profiles with this wireless configuration. Otherwise, user-defined connections will be lost when the thin client is rebooted.

6. Configure the wireless network connection in the *Default Wi-Fi network* (page 168) dialog if you do not select it via the *Wireless Manager* (page 165).

Additional connections can be configured in the Additional Wi-Fi networks dialog.

7. Configure your location in the *Wireless regulatory domain* (page 169) dialog.

Once these settings become active on the thin client, a new tray icon for wireless connections will appear:



Figure 59: WiFi symbol

Wireless Manager

You can bring up the **Wireless Manager** from the tray icon:

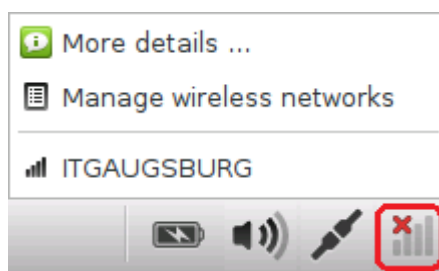


Figure 60: Symbol bar with WiFi context menu



You will need to have switched on the **Wireless Manager** under **Network > LAN Interfaces > Wireless** (page 163)

1. Click on the **Wireless Tray Icon** in the task bar and then on **Manage wireless network connections** in order to bring up the **Wireless Manager**:

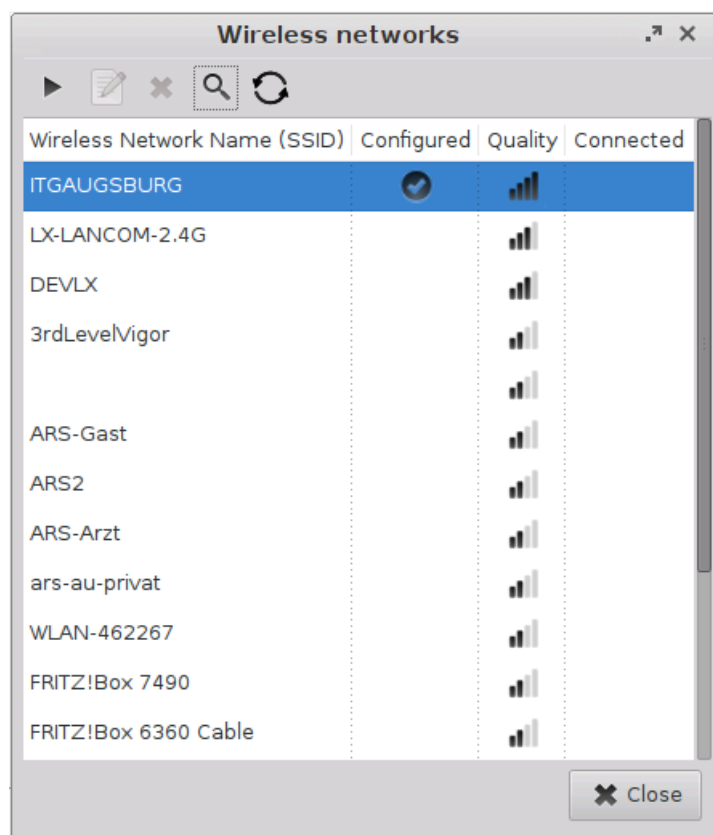


Figure 61: Wireless Manager

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. If you are using the Wireless Manager for configuration, you only need to give the network key – this is considerably easier than using the Setup or the UMS for configuration:

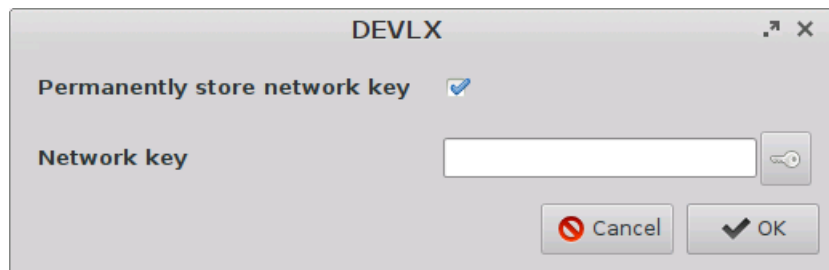


Figure 62: Configure WiFi connection

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:

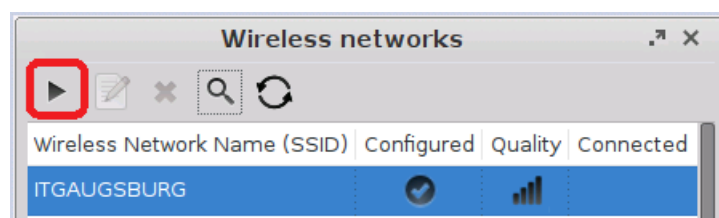


Figure 63: Establish connection to WiFi

The tray icon will change and show the quality of the connection to the active network.

Hidden networks appear in the Wireless Manager with the network name empty or can be defined using the **Search for network** button:

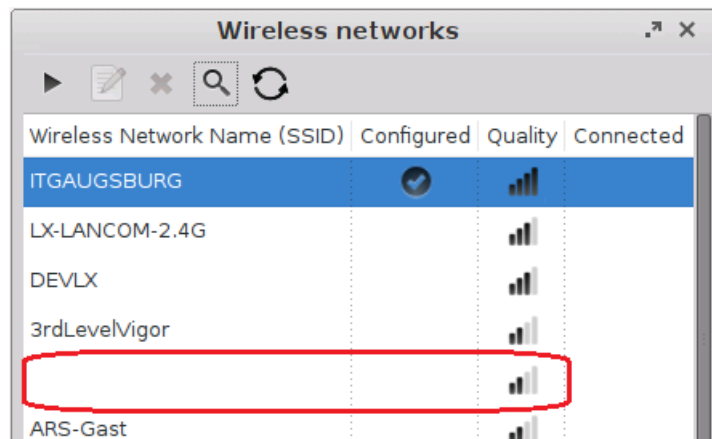


Figure 64: Hidden network

In order to connect to a previously unknown hidden network, you must first enter the SSID before the access data are retrieved:

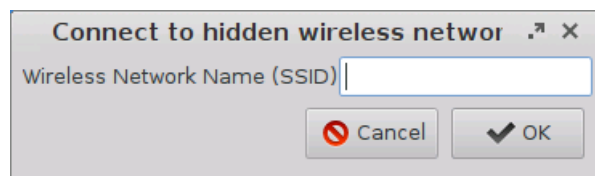


Figure 65: Name of the hidden network



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

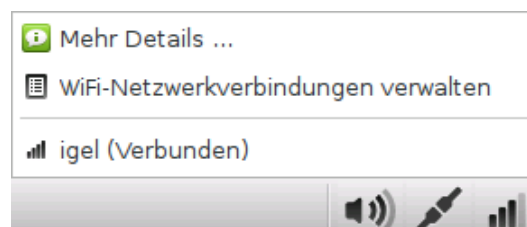


Figure 66: Symbol bar with active connection

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 locally and in the UMS under **Network > LAN Interfaces > Wireless > Other WLANs**:

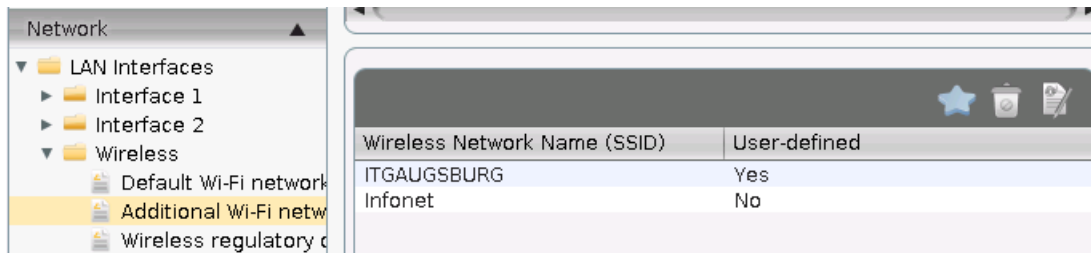


Figure 67: User-defined WiFi connections in the IGEL Setup



A **Yes** in the **User-defined** column means that you can change or delete this connection in the Wireless Manager. A connection that you have set up in the Wireless Manager is automatically user defined. Connections that are specified in the Setup or in the UMS can also be flagged as user defined. In most cases, however, this would not make much sense. After all, the end user should only be able to delete the connections that they themselves have set up, e.g. when traveling.

Configure Connections in the Setup

Menu path: **Setup > Network > LAN Interfaces > Default Wi-Fi network**

In the **Default Wi-Fi network** and **Additional Wi-Fi networks** areas, you can configure wireless network connections:

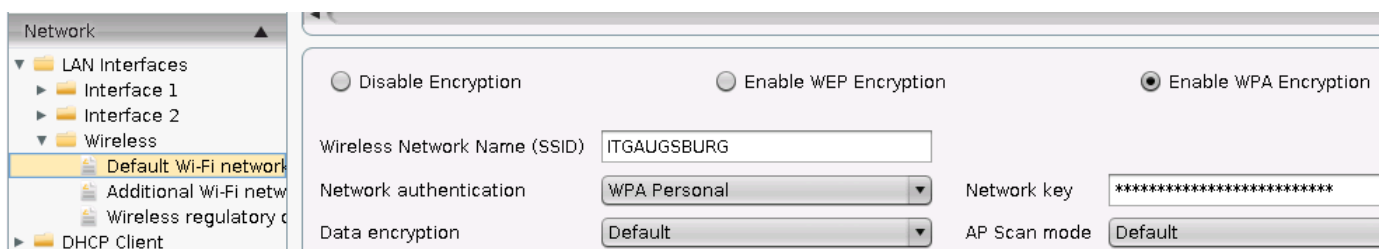


Figure 68: WiFi configuration

1. Select an **Encryption Method**.
2. Enter the **Network Name (SSID)**.
3. Set further parameters depending on the encryption method selected.

- ➔ For WPA(2) Enterprise encryption, the client certificate can also be requested and administered via SCEP. See *Network/SCEP* (page 175) and our *Certificate Enrollment and Renewal with SCEP (NDES)* (<http://edocs.igel.com/#10200572.htm>) best practice.

The connections defined under **Additional Wi-Fi networks** have the same value as the connection entered under **Default Wi-Fi network**. Here, you can pre-configure wireless connections which are available for selection by the user in the *Wireless Manager* (page 165).

The connections configured in the *Wireless Manager* (page 165) are likewise shown in the **Additional Wi-Fi networks** list and are automatically flagged as **User-defined**.

Connection to Hidden Networks

Hidden wireless networks (WLAN without SSID broadcasting) can also be connected to. Pre-defined connections can be used without disclosing the network name to the user. For user-defined connections, the user must however know the name of the hidden network.

To pre-configure connections to hidden networks, proceed as follows:

- In the IGEL Setup, go to **Network > LAN Interfaces > Wireless > Default Wi-Fi network** and set the **AP Scan Mode** parameter to **No Broadcast**.

Figure 69: Connection configuration for hidden networks

Additional connections can be configured in the Other Additional Wi-Fi networks dialog.

Wireless regulatory domain

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

In this area, you can configure your location:

Figure 70: WiFi frequency ranges



Ensure that the **Wireless regulatory domain** is configured correctly in order to prevent your device making unauthorized transmissions.

10.2.3. DHCP Options

Menu path: **Setup > Network > DHCP Client > Standard Options / Custom Options**

Configure the client's use of DHCP options - a number of **standard options** are already set out in a list and can be enabled. **User-defined options** can be set up in a list of your own and managed there.

10.2.4. Virtual Private Network - VPN

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

Remote users securely access company networks via virtual private network protocols (VPN). You can set up your client accordingly for this purpose.

PPTP

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

PPTP (point-to-point tunneling protocol) is one of the most common virtual private network (VPN) protocols allowing remote users to securely access company networks.

Automatically establishing a connection during the boot procedure

In order to set up a client which is fully configured to automatically establish a connection, you may need to dial up first.

1. Enable this option before the desktop is launched.
The client connects to the host.
2. Click on **Add** to set up new connections.
3. Configure the necessary settings in order to dial up the RAS server on the desired remote station.
4. Select the network device and specify whether a dial-up connection is to be used.
5. Specify on the **Options** tab the name service and the IP configuration for the PPTP connection.



These data will normally be transferred from the remote station's RAS server. This means that both DNS and IP address will be set to **automatic** by default.

You can set up additional network routes on the next three setup pages (Routing).

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.

It supports the following authentication methods:

- TLS certificates
- Name/password
- Name/password and certificates
- Static key

- ➡ Click on the star symbol to set up a new OpenVPN connection.
- ➡ A best practice document describes how you can set up OpenVPN connections.

NCP

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

The configuration parameters for the NCP Client are configured exclusively via the client program interface itself.

- ➡ You will find the documentation regarding the NCP Secure Enterprise Client at:
<http://www.ncp-e.com/de/support/produktunterlagen/handbuecher.html>

GeNUCard

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

The GeNUCard VPN hardware offers a choice of pre-configured Internet and VPN connections.

The **Connections** window opens as soon as the GeNUCard session is launched.

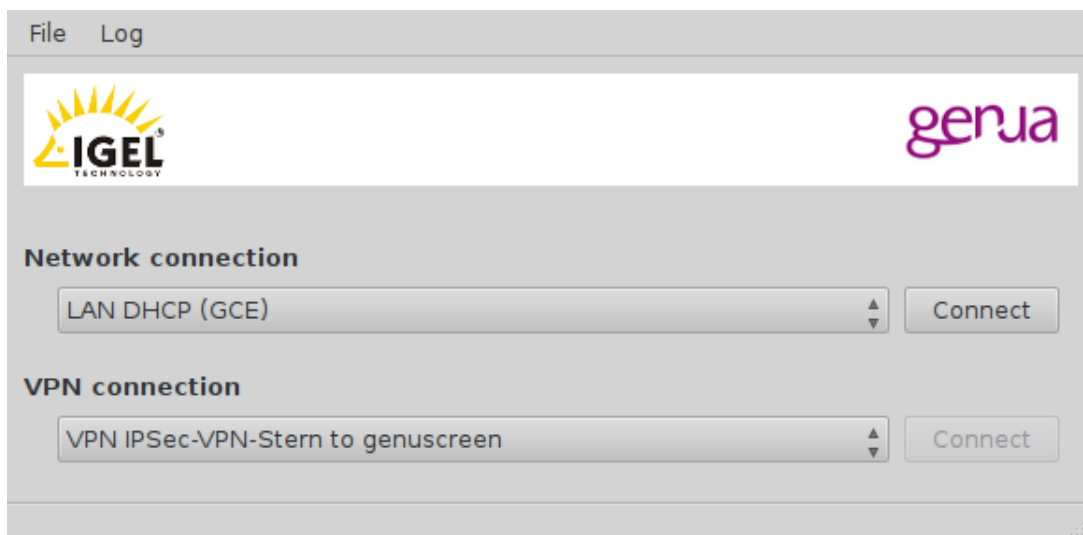


Figure 71: GeNUCard configuration

- **File:**
 - **Change PIN**
 - **Rekeying**
- **WiFi:** Opens the WiFi dialog which allows you to configure the GeNUCard's wireless access.
- **Log:** Allows you to view the log
- **Network connection:** Select one of the network connections pre-configured on the GeNUCard, for example LAN or WLAN.
- **VPN connection:** Select one of the VPN connections pre-configured on the GeNUCard.

WiFi Configuration

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

In this dialog, you can configure how the GeNUCard connects to wireless networks.

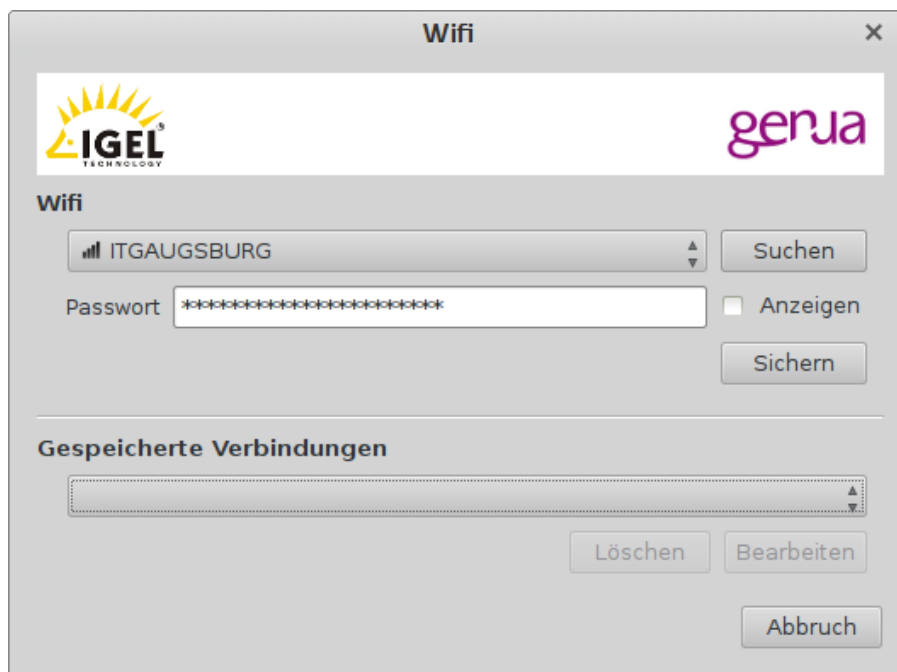


Figure 72: GeNUCard WiFi Configuration

- **WiFi:** Here, you can set the wireless access that the GeNUCard uses.



Unencrypted networks and networks secured with WEP, WPA or WPA2 are supported.

- **Search:** Searches for available wireless networks. This can take up to a minute.
- **Password:** The password for the wireless network set
- **Show:** If this option is enabled, the password will be visible.



Passwords are saved in encrypted form in the IGEL setup.

- **Save:** Saves the complete connection along with SSID and password on the GeNUCard.

- **Saved connections**

- **Delete:** Deletes the selected connection.
- **Edit:** Opens the selected connection for editing.

Options

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

A valid combination of connection and user data can be pre-populated in the IGEL setup: **Network > VPN > GeNUCard > Options**.


<input checked="" type="checkbox"/> Enable Autostart During Boot	
Default internet connection name	telekom
Default VPN connection	test.vpn.genua.de
Username	igeltest
Password	*****
Internet connection timeout	120
VPN connection timeout	120
Private key filepath	/wfs/genua.pem 

Figure 73: Automatically establishing connections

A facility for automatically establishing a connection during the boot procedure can also be enabled. This is necessary when updating the IGEL firmware via the VPN for example.

Administrator Session

- ➡ The GeNUCard is configured and administered centrally via the genucenter management station. Further information is available from www.genua.de.

Optionally, an administrator session allowing the GeNUCard Internet connection to be configured can be set up:

1. Click on **Add instance** under **System > Registry > genucard%**.

The GeNUCard icon will appear on the desktop.

2. Click on the GeNUCard icon.

The GeNUCard logon window will open.

3. Enter a **user name** and **password**.

4. Click on **Logon**.

The Internet/VPN window will open.



Figure 74: Internet/VPN window

5. In the **Internet** area, configure the connection with the help of the **Create, Edit, Delete** buttons.

10.2.5. Simple Certificate Enrollment Protocol - SCEP

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

SCEP allows the automatic provision of client certificates via a 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 authority).

- ➡ More information can be found at Microsoft, e.g. in the white paper
<http://download.microsoft.com/download/a/d/f/adf2dba9-92db-4765-bf2d-34b1c8df9ca3/Microsoft%20SCEP%20implementation%20whitepaper.doc>
- Enable certificate management via SCEP client (NDES) and then make the necessary configuration settings.

Certificate

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

- Under **Certificate**, specify the basic data for the certificate to be issued by the certification authority.

Type of CommonName	If the client automatically obtains its network name, DNS Name (auto) is a good type of thin client certificate.
Organizational unit	Stipulated by the certification authority.
Organization	A freely definable designation for the organization to which the client belongs.
City, state, country	Enter the location of the client here.
RSA key length	Select a key length (one able to be used by the certification authority) for the certificate that is to be issued.

Certification Authority

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

- Enter the name of the certification authority (CA) and the hash value of the root certificate.
 You will receive both of these from the certification authority.

SCEP

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

In addition to a certification authority, an SCEP server must also be defined.

- Enter the **address** and **query password** for the SCEP server here.



The SCEP server generates the password as a one-time password. It is needed when a certificate is requested for the first time. New certificates will be requested before the old ones expire. In this case, the still-valid certificate will serve as a means of authentication.

- For the purpose of checking validity, define an **interval** (checking frequency) and a **period of time** in which certificate renewal must occur.

Example:



A certificate is valid until 31.12 in any one year. The period for renewal is 10 days. This means that a new certificate will first be requested on 21.12 of the same year.



Because of the need to enter a fingerprint (root certificate of the certification authority) and the query password (SCEP server), the configuration process is somewhat awkward. Ideally, it should be set up in the UMS as a profile and distributed to the clients. At the same time, the certificate still cannot be used for communication purposes.

Checking the Client Certificate

If a certificate from the certification authority has been forwarded from the SCEP server to the client, it is then stored there in the `/wfs/scep_certificates` folder.

The data for the certificate (e.g. its validity, creation date and hash value) can be displayed by using the shell command `cert_show_status`.

Example

Certificates issued and managed via SCEP can be used for purposes such as network authentication.

Relevant options can be found when

- configuring IEEE 802.1x authentication

Network→LAN Interfaces→Interface 1→Authentication

- or when setting up the wireless network

Network→LAN Interfaces→Wireless→Authentication, WPA Enterprise Encryption, EAP Type TLS.

One problem when the client certificate is distributed via the network is that the same certificate is needed for communication. The use of the SCEP in conjunction with 802.1x authentication presents no problems to the extent that the initial request for the certificate should also be possible without a certificate.

- Enable the 802.1x authentication method after the SCEP has been configured.

When requesting the certificate, the client will attempt to establish a connection to the SCEP server without using any authentication. It will use the authentication only after having received the certificate.

For WLAN connections, a method of certificate-less PSK encryption must first be set up. The client will then use this connection to obtain the certificate. After this, the WLAN connection can be reconfigured once again.

While the above-mentioned method for Ethernet connections will also function via the UMS, the initial configuration of the WLAN can only be performed on the client as the WLAN is disabled by default.

10.2.6. Routing

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

This setup page allows you to specify additional network routes if necessary.

- In the **Interface** field, specify "eth0", "eth1" or "wlan0", i.e. Interface 1+2 or Wireless LAN.

You can specify up to five additional network routes.

10.2.7. Hosts

Menu path: **Setup > Network > Hosts**

If no DNS (Domain Name Service) is used, you can specify a list with hosts in order to allow translation between your IP address, the full qualified host name and the short host name.

Click on **Add** to open the dialog window.

1. Enter the **IP address** of the host you would like to add.
2. Give the **full qualified host name** (e.g. <mailserver.igel.de>).
3. Give the **short host name** of the host (e.g. <mailserver>).
4. Confirm the details you have entered by clicking on **OK**.

The specified host will now be added to the computer list.

10.2.8. Network Drives

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

Drives shared within the network can be linked to the thin client via NFS or SMB - depending on the protocol offered by the server.

NFS

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

With NFS (Network File System), you can share files via the network. The NFS server exports a system file, and the NFS client (your thin client) links this file to a mount point within its own file system. The exported file system then becomes a logical part of the thin client file system although, in physical terms, it remains on the server.

➡ In order to set up an NFS mount, the server must first be configured. You will find detailed information on NFS on the relevant pages of the manual for your server operating system.

The procedure for sharing files via the NFS server is as follows:

- Click on **Add** to open the dialog window for NFS.

You can then enter the following:

Enabled	The NFS mount is enabled by default and is mounted each time the system boots. Disable this entry if the shared file system is not universally needed.
Local directory	Details of the local directory onto which the shared items are to be mounted on the local thin client file system.
Server	The name or IP address of the NFS server which provides the shared files.
Path name	Details of the path name as exported by the NFS server.

Windows Drive - SMB

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

SMB is used by Microsoft Windows NT, Windows 95/98, Windows 2000 and Windows XP etc. to share hard drives and printers. As Unix (including Linux) can process this protocol with Samba Suite tools, hard drives and printers can be used along with Windows hosts. Consequently, items shared via SMB can be integrated into the thin client by Windows or Unix Samba hosts.



The SMB protocol is used only to share files via the network (not for printers). Shared items which are to be mounted must first be created on the Windows or Unix host.

Local directory: Details of the local directory onto which the shared items are to be mounted on the local thin client file system.

Server: For a Windows host, the Net BIOS name must be entered here. For a Unix Samba host, the host name or the IP address must be used.

Share path name: Path name as exported by the Windows or Unix Samba host.

User name/password: Details of the user name and password for your user account on the Windows or Unix Samba host.

Enabled: The SMB mount is enabled by default and is mounted each time the system boots.

Writable for users: If this option is enabled, the user who is logged on can write data. Otherwise, this is only possible via root.

10.3. Proxy

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

Select the communication protocols for which a system-wide proxy is to be used.

The screenshot shows a window titled 'System-wide proxy' with two radio buttons at the top: 'Direct Connection to the internet' (unselected) and 'Manual proxy configuration' (selected). Below the radio buttons are several input fields: 'FTP Proxy', 'HTTP Proxy', 'SSL Proxy', and 'SOCKS Host'. Below these is a dropdown menu for 'SOCKS Protocol version' currently set to 'SOCKS v5'. At the bottom is a field for 'No Proxy for:' containing the text 'localhost, 127.0.0.1'.

Figure 75: System-wide proxy

11. Devices

Menu path: **Setup > Devices > Hardware info**

- Click on **Hardware Information** for an overview of your IGEL thin client device.

11.1. Printers

Menu path: **Setup > Devices > Printer**

Various printing systems can be used with the thin client.

11.1.1. CUPS - Common UNIX Printing System

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

The Common UNIX Printing System™ (or CUPS) is the software which 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 which 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 USB serial adapter)
- USB (1st and 2nd USB printer)
- Network (TCP/IP, LPD, IPP)

Printers

Printers can be created and edited here.

- In the edit dialog, specify a printer name which begins with a letter.

General

- Under **Printer Connection**, select the interface type for locally connected printers or the network protocol for network printers.
- Depending on the above, enter the relevant configuration data for the interface or network printer.
- Select the local printer driver under **Manufacturer and Printer Name**.

Mapping in sessions

- **Map printer in NX sessions:** Makes the printer available in NX sessions.
- **Map printer in ICA sessions:** Makes the printer available in ICA sessions.
- **Map printer in RDP sessions:** Makes the printer available in RDP sessions.

The remaining parameters are used to select the printer driver in ICA and RDP sessions on Windows servers.

- Give the name of the driver under Windows which is to be used.

If it does not feature in the list, it can be specified under **Use user-defined windows driver name**.

When printing in ICA and RDP sessions, the print data are normally prepared for the printer model by the Windows printer driver and are passed unchanged from the thin client to the printer.



An exception is encountered when using the Windows driver in ICA sessions: Manufacturer: Generic, model: Generic PostScript. In this case, the print data are prepared on the thin client with the help of the printer driver defined above under **Printers** for the printer model. This requires thin client resources depending on the size of the print job.

IPP printer sharing

The IPP (Internet Printing Protocol) offers the following configuration options:

- **Network or host for sharing local printers:** Allows printing on the local device from either the local or the global network.
- **Enable IPP printer browsing:** Allows you to search for shared printers in the local or global network and show your shared printers within the network. A shared printer is visible within the network but it may not be possible to print from the network if you do not have the necessary authorization.

11.1.2. LPD - Line Printer Daemon

Menu path: **Setup > Devices > Printer > LPD**

LPD printers are used by the BSD printing system and are also supported by Windows servers.

Enable LPD print server	Makes the thin client an LPD print server. The CUPS printers defined under 11.2.1.1 can be addressed under their printer name as a queue name via the LPD protocol.
Print data conversion	Attempts to automatically recognize whether or not the print data need to be prepared by the local printer driver. The None option always forwards the print data unchanged to the printer.
Max. simultaneous connections	Limits the number of print jobs that can be accepted at the same time.
Restrict LPD access	Specifies the sub-networks or hosts from which print jobs can be accepted.

11.1.3. TCP/IP

Menu path: **Setup > Devices > Printer > TCP/IP**

You can assign printers connected to your device to a TCP/IP port. The LPT1 (TCP/IP port 3003) is enabled by default. The printer can be connected to one of the following connections, provided that they are available on the device:

- Serial connection (COM 1 or COM 2)
- Parallel connection (LPT 1)
- USB (USBLP 1)
- Additional serial connections: USB adapter or Perle expansion card

Data are forwarded bidirectionally at serial interfaces. This means that other serial devices such as barcode scanners or scales can be operated too.

11.1.4. ThinPrint

Menu path: **Setup > Devices > Printer > ThinPrint**

ThinPrint allows the bandwidth provided for the transfer of print jobs to be reduced depending on the resources available. The **ThinPrint** client prints either on printers connected to a local interface (serial, parallel or USB), on an LPD network printer or on a CUPS printer defined on the thin client.

The following parameters can be found on the **ThinPrint** setup page:

Port number	Specify the port number via which the ThinPrint daemon is to communicate. Make sure that the port number on the ThinPrint client and the ThinPrint server is the same (communication will otherwise not be possible).
Bandwidth	Enter a bandwidth value (in bits per second) which is lower than or equal to the value specified on the ThinPrint server. A higher value, the disabling of client control or no entry at all means that the ThinPrint server values will be used.
Waiting time between print attempts	Maximum waiting time (in seconds) if a printer is unavailable
Number of print attempts	Number of attempts to contact a printer in order to start a print job.

The list of **ThinPrint** printers is shown on the **Printer** page.

➤ Here you can manage printer configurations by adding, editing or deleting printers.

The page provides an overview of pre-configured **ThinPrint** printers:

Active	Indicates whether or not the printer is visible.
Name of the printer	Name under which the printer can be addressed.
Printer class	Name of the printer class - optional, max. 7 characters without spaces
Device	<p>The following options are available here:</p> <ul style="list-style-type: none"> • + /dev/ttyS0, /dev/ttyS1, ... serial interface • + /dev/lp0, /dev/lp1, ... parallel interface • + /dev/usb/lp0, /dev/usb/lp1, ... USB printer • + Name of a CUPS printer with LPD network printer connection: ThinPrint client prints via the network to the LPD network printer. • + Name of another CUPS printer: ThinPrint client forwards print jobs to the appropriate printer in the CUPS printing system.
Standard	Defines the selected device as the standard printer.

11.2. USB Storage Devices

Menu path: **Setup > Devices > Storage Devices**

USB storage devices can be configured here.

11.2.1. Hotplug storage devices

Menu path: **Setup > Devices > Storage Devices > Storage Hotplug**

In this area, you can set up the connection of hotplug storage devices. These can be USB mass storage devices or MMC card readers for example.

You can change the following settings:


- **Default permission:** Default access permissions for hotplug storage devices.

Possible values:

- **Read/Write**
- **Read only**

- **Enable dynamic client drive mapping.** If this option is enabled, hotplug storage devices are automatically added and removed during ICA sessions and RDP sessions.



Before you mechanically disconnect the hotplug storage device from the thin client, you must remove it safely. To do this, click on  in the taskbar.

If the following warning is shown: **The device is still in use! Do NOT disconnect the device.**, the hotplug storage device must not be removed. Close either the named program or close all open files or directories within a session that are located on the hotplug storage device.

- **Number of storage hotplug devices:** The number of hotplug storage devices that can be used in the session.
- **Private drive letter for storage drives:** If this option is enabled, each hotplug storage device will be assigned an individual drive letter. If this option is disabled, a single drive letter will be generated for all hotplug storage devices and each hotplug storage device will be assigned a sub-directory.
- **Start storage drives with this drive letter:** Letter that is assigned to the first hotplug storage device if automatic drive mapping is enabled. Further hotplug storage devices are assigned the next letter alphabetically.
- **ICA read access to hotplug storage devices:** Specifies whether read access to hotplug storage devices is allowed in an ICA session.



This setting is only effective if **Enable dynamic drive mapping** is disabled.

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 to storage hotplug devices:** Specifies whether write access to hotplug storage devices is allowed in an ICA session.



This setting is only effective if **Enable dynamic drive mapping** is disabled.

Possible values:

- **Yes:** Write access is allowed.
 - **No:** Write access is not allowed.
 - **Ask user:** Write access can be allowed on request.
 - **Use storage hotplug beep:** If this option is enabled, a signal tone will be heard when connecting and disconnecting hotplug storage devices.
 - **Show storage hotplug message:** If this option is enabled, hotplug messages will be shown when connecting and disconnecting hotplug storage devices.
 - **Message timeout:** Period of time after which the window with the hotplug messages is hidden. If the time period is set to 0, the window will be shown until it is closed manually.
- ➡ Further settings options can be found under *Drive Mapping (Citrix)* (page 25), *Drive Mapping (RDP)* (page 45) and *USB Access Control* (page 184).

11.2.2. Automount Devices

Menu path: **Setup > Devices > Storage Devices > Automount**

Here you can define the devices which are to be mounted automatically when accessed:

List of automount devices	Overview of the automount devices - The most commonly used devices such as the disk drive, CD-ROM etc. are pre-configured.
Edit	Opens and enables one of the pre-defined devices
Add	Manual configuration of devices not pre-defined in the automount device list .
Name	Name given to a device - This name is also used for the sub-directory created in <code>/autofs/</code> .
Device	Allows you to select a suitable device synonym - This can also be entered manually.
File system type	Definition of the file system - The auto option should normally be used. If, however, you use ext2 or a problem occurs, you should clearly indicate the file system that you use.
Automount time-out	Regulates the time-out period - Specify in seconds how long the system should wait before the devices accessed are unmounted. The time period ranges from 0 to 600 seconds (10 minutes).



Do not set the time-out period to zero! This may result in data loss.

11.3. Smartcard

Menu path: **Setup > Devices > Smartcard**

PC/SC is a service which makes smartcard readers and inserted smartcards available to application programs. RDP and ICA connections make it possible to provide server-side applications with client-side smartcard readers and smartcards. Local applications, e.g. browsers, can also use smartcards in the readers. For these functions to work, the PC/SC daemon must be enabled.

➤ Click on **Enable PC/SC Daemon** to use the PC/SC interface on the thin client.

The **PC/SC Devices Currently Active** window shows the smartcard readers which are currently available. Optional internal readers and a variety of USB smartcard readers are also supported.

11.4. USB access control


Menu path: **Setup > Devices > USB Access Control**

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

To enable **USB access control**, proceed as follows:

1. Enable the option **Enable**.
2. Select the **Default Rule**. The default rule specifies whether the use of USB devices is generally allowed or prohibited.
3. Create one or more rules for classes of devices or individual devices.

To create a **Class Rule**, proceed as follows:


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 **Subclass**, select the subclass for which the rule should apply or **All [device class]** for all subclasses.
5. Under **Name**, give a name for the rule.
6. Click **OK** or **Cancel**.

The rule is active.

To create a **Device Rule**, proceed as follows:



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 *Hotplug Storage Devices* (page 182).
- **Read only**
- **Read/Write**

7. Under **Name**, give a name for the rule.

8. Click on **Next**.
9. Click on **Ok** or **Cancel**.

The rule is active.

Example:

- The set rule prohibits the use of USB devices on the thin client.
- 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.

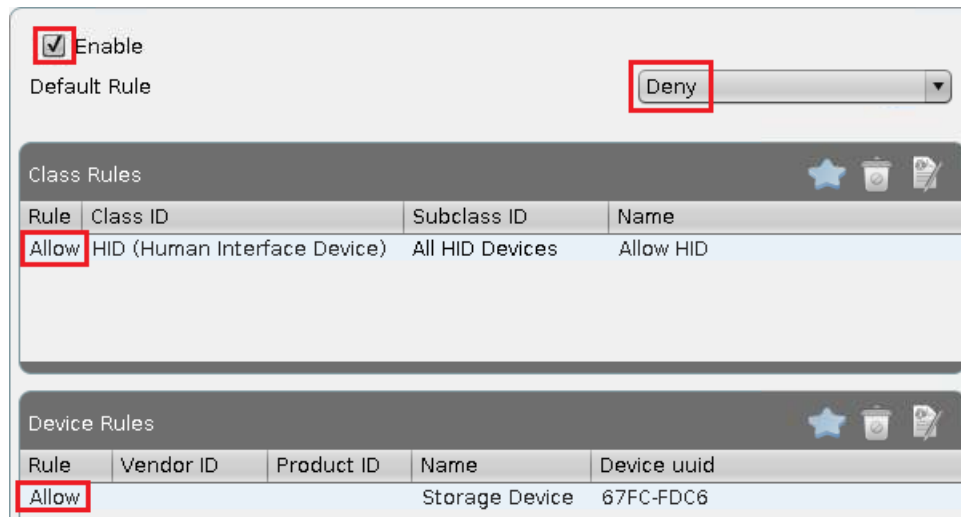


Figure 76: USB access control

➡ Further settings can be found under *Storage Hotplug* (page 182).

12. Security

Menu path: **Setup > Devices > Security**

In order to prevent unauthorized access to the thin client setup which could allow deeper penetration into your network, it is essential that you set up an administrator password following the initial configuration.

- You can also use an additional user password which offers various options for permitting restricted configuration by users.

12.1. Password

Menu path: **Setup > Devices > Security > Password**

- Under **Password**, set up an administrator password and a user password.

Administrator and user password

Sets passwords for the administrator and user accounts. The setup will be protected by the administrator password unless the user has been granted access to specific areas.



By enabling this password, the IGEL setup, shell access to Xterm and access to the console will be restricted to the administrator. The **Reset to Factory Defaults** option may only be used with this password. If the setup is locked by an administrator password single setup pages can be enabled for the user - see *Enable Setup Pages for Use* (page 18)r.

Remote user password

Sets a password for the remote session user (SSH).

Setup user

Allows the user to access the local setup.



When you enter a password, ensure that the correct keyboard layout is enabled. After all, you will only see stars instead of characters when entering the password and will not be able to see why the password was not accepted.

12.2. Login Options

Menu path: **Setup > Devices > Security > Logon**

- Here you can configure the local login procedure for the thin client. You can login via the IGEL smartcard or via the Kerberos protocol, e.g. in a Windows domain.

12.2.1. IGEL Smartcard

Menu path: **Setup > Devices > Security > Logon > IGEL Smartcard**

Logging in with IGEL smartcard	Enables local login to the thin client with the IGEL smartcard. Sessions stored on the smartcard become available. The thin client is locked without the smartcard and optional password.
Enable IGEL smartcard without locking the desktop	Enables sessions stored on the smartcard after entering an optional password. The thin client is not locked – even without a smartcard.
Company key	Shared key for smartcards and thin clients. For more details see <i>smartcard personalization</i> (page 128).

You can use the optional IGEL smartcard for local authentication and personalized session configuration ("Flying Doctor Scenario").



Figure 77: IGEL Smartcard

The procedure when using the IGEL smartcard with the internal card reader or an external reading device (USB) is as follows:

1. Enable the IGEL smartcard solution under **Security**→ **Login**→ **Smartcard** in the setup application.
2. Enter a **company key** to describe your IGEL smartcard.
3. Save your settings before you start personalizing the card.
4. In the **Personalization** window, you can set a login password and add sessions to the card.

Session configurations are stored on the card's IC (integrated circuit) and the session can be used on any IGEL thin client which reads the card.

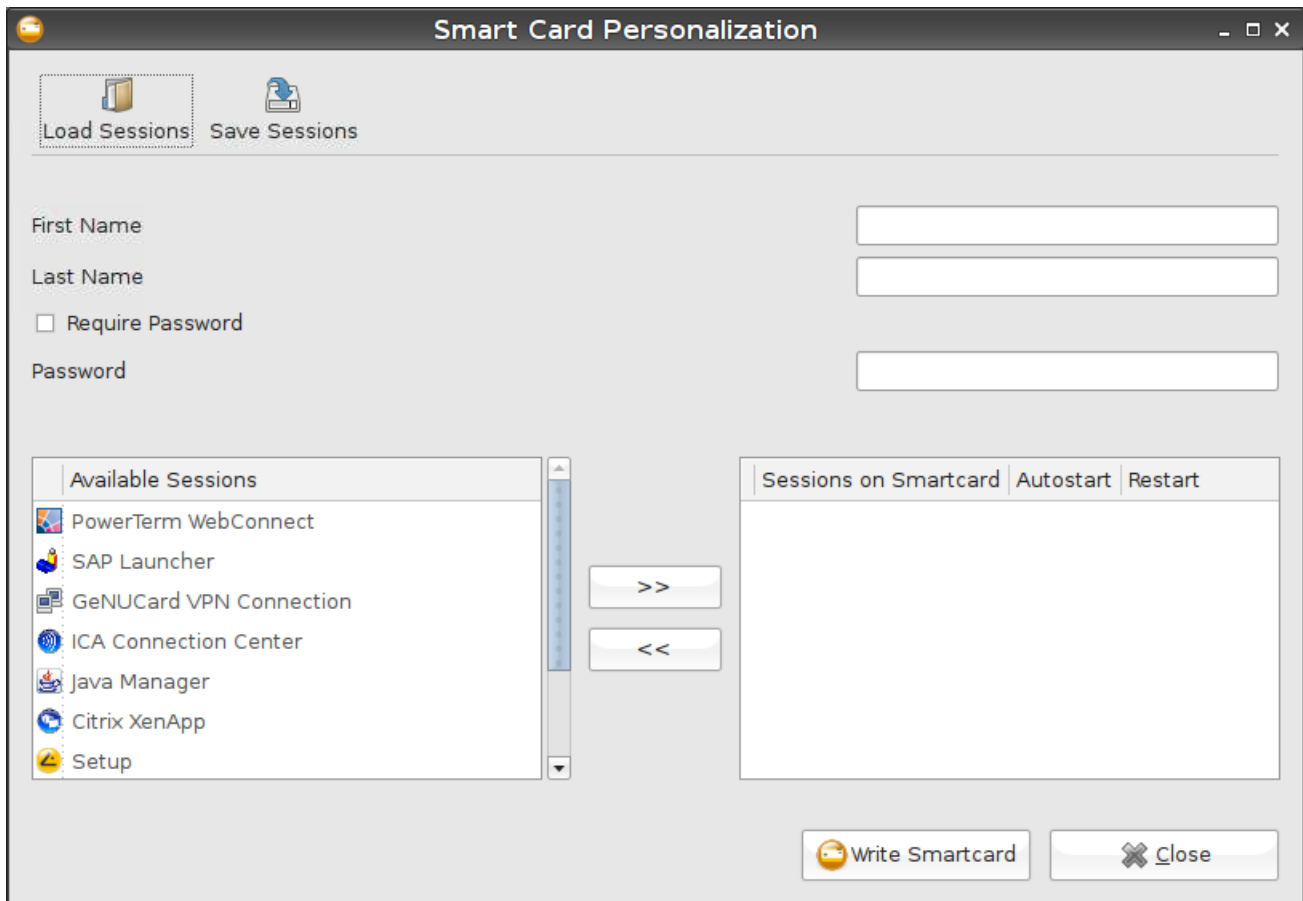


Figure 78: Smartcard personalization

Company Key

The IGEL smartcard solution also contains a **company key**. This is an additional code which is written to the card and which must match the code of the terminal used. If the two codes do not match, the smartcard cannot be used on that particular terminal. This additional security feature ensures that your terminals cannot be accessed from outside your company. It can also be used within the company in order to restrict employees' access to specific terminals.

Save User and Password

The procedure for saving users and passwords for authentication is as follows:

- Enter the first name and surname of the user.

You will then be prompted to enter the password for this name.



If the **Demand Password** option is enabled, a pop-up window will always open when a smartcard is inserted. If the wrong password is entered, access to the terminal will be denied.

If the smartcard is merely used to control access to the terminal, the procedure is as follows:

1. Insert a suitable smartcard.

2. Click on **Write to Card** in order to write the data to the card.
3. Remove the smartcard once the writing operation is complete.

You can now program the next smartcard.

Save Sessions

Saving sessions on the smartcard

If an employee uses a number of different terminals or the terminals are used by many different employees, it may be a good idea to save the sessions used by an employee on his smartcard instead of on the terminal. In this way, the user only needs to call up the applications he requires in order to perform his duties.

The procedure for saving sessions on the smartcard is as follows:

1. Insert the employee's smartcard into the terminal.
The applications used by the employee are shown on the terminal.
2. Create the sessions you would like to add to the smartcard on the terminal (including an autostart option and personalization of login information). On addition to the first name/surname of the card user and an optional password, you can also add to the smartcard the sessions shown in the Available Sessions area.
3. Once you have added all the required sessions, click on **Write to Card** in order to save the data on the smartcard.

Test Smartcard

- Test the card you have created.

After performing a warm start and inserting the smartcard, the sessions will be shown immediately on the desktop. Every session which is set to start automatically when you insert the smartcard will be launched.

12.2.2. AD/Kerberos

Menu path: **Setup > Devices > Security > Logon > Active Directory / Kerberos**

These setup pages allow you to enable local login to the thin client via the Kerberos protocol.

- ➡ AD/Kerberos must also be *configured* (page 191) for this purpose.



The login can be used for single sign-on in a number of session types (ICA, RDP).

- **Login to Active Directory Domain:** Connects the login method with the Active Directory.
- **Login methods:**
 - **Explicit:** Expects login with username and password.
 - **Remember last user name:** Initializes the login mask with the username of the last user. Therefore the option **Explicit** has to be enabled.
 - **Smartcard:** Expects login with smartcard.



Select the type of smartcard under **Active Directory / Kerberos > Smartcard** and decide which **Smartcard Removal Action** shall be executed.

- **Logoff shortcut locations:** Allows you to configure the way(s) in which the user can log off.

12.2.3. Auto Logoff

Menu path: **Setup > Devices > Security > Logon > Auto Logoff**

Define an **Auto Logoff** action which is carried out when you end the last instance of a session type:

1. Bring up the **Security→Login→Auto Logoff** setup page.
2. Choose a **Session Type**.
3. Choose a **command (Auto Logoff Command)**.
4. Save your settings by clicking on **Apply** or **OK**.

If the last session instance of the selected type is ended, the system will carry out the set action.



The **Shutdown** command carries out the set action. You can check this under **System > Energy > Shutdown**.



The **Logout** command has no effect if you have not defined a login method under **Security > Login** (smartcard, active directory/Kerberos or IGEL Shared Workplace). The **Logoff** command cannot be used together with an appliance - in this case, only the **Shutdown/Suspend** and **Reboot** commands will work correctly.



If you use Auto Logout commands in an appliance, ensure that the appropriate session type was selected - e.g. Horizon when using the VMware Horizon Appliance.

12.3. AD/Kerberos Configuration

Menu path: **Setup > Devices > Security > Active Directory / Kerberos**

- Enable and configure Kerberos on these setup pages in order to use this service for login and single sign-on purposes.

Standard realm	Specifies the standard Kerberos realm for the client. Set this value so that it corresponds to your Kerberos realm (Windows domain).
DNS look-up KDC	Specifies whether DNS SRV records should be used to find key distribution centers (KDCs, domain controllers) and other servers for a realm if they are not indicated.
DNS look-up realm	Specifies whether DNS TXT records should be used to determine the Kerberos realm of a host.
No addresses	If this option is set, the first Kerberos ticket is addressless. This may be necessary if the client is located behind an NAT device (Network Address Translation).

12.3.1. Realm 1-4

Menu path: **Setup > Devices > Security > Active Directory / Kerberos > Realm [1-4]**

Up to 4 realms where a login is possible can be configured here.

Realm	The name of the realm/the domains where you would like to authenticate yourself.
KDC list	IP or FQDN list of the key distribution centers (domain controllers) for this realm. An optional port number preceded by a colon can be attached to the host name.

12.3.2. Domain-Realm Mapping

Menu path: **Setup > Devices > Security > Active Directory / Kerberos > Domain Realm Mapping**

Domain Realm Mapping offers translation of a host name into the Kerberos realm name for the services provided by this host.

Standard domain-realm mapping	This should be enabled if the DNS and realm names match. Otherwise, you will need to create user-specific entries in the list.
DNS host or domain name	The entry can be a host name or a domain name. Domain names are indicated by a preceding dot. Host names and domain names should be entered in lower-case letters.
Realm	Kerberos realm name for this host or this domain

13. System Settings

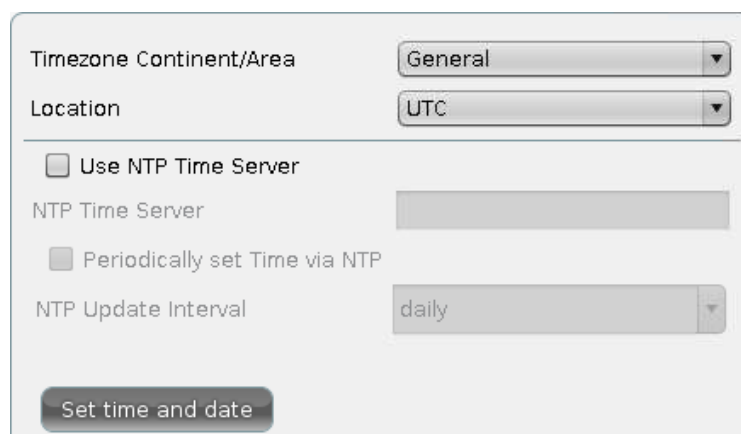
Menu path: **Setup > System**

As previously explained under *Quick installation* (page 9), various basic system settings can be configured in the sub-structure.

13.1. Time and Date

Menu path: Setup > System > Time and Date

1. Go to System > Time and Date



The screenshot shows a configuration window for Time and Date. It has two dropdown menus at the top: 'Timezone Continent/Area' set to 'General' and 'Location' set to 'UTC'. Below these are two checkboxes: 'Use NTP Time Server' (unchecked) and 'Periodically set Time via NTP' (unchecked). There is an 'NTP Time Server' text field and an 'NTP Update Interval' dropdown menu set to 'daily'. At the bottom is a 'Set time and date' button.

Figure 79: Time and Date Configuration

2. Maintain your changes.
3. Click Set time and date to save your settings.



You can use a time server within your network (via Network Time Protocol (NTP)) to set time and date automatically during system boot and with periodic update. Make sure the time zone is configured correctly. Choose the region from the drop-down-menus .

Make sure the time zone is configured correctly. Choose the region from the drop-down-menus .



Note: If choosing General as Time Zone Area you have to set your GMT time zone (Location) following the POSIX standard (as usual in Linux) - which means you have to invert the offset of your common UTC time zone! (See tool tip for Location as well.) Therefore it is preferable to set the system's time zone by choosing the corresponding area and location instead of defining the GMT offset.

Example for America/New York: In POSIX standard GMT+5 is the time zone 5 hours west of Greenwich and corresponds to UTC-5.

➡ FAQ: Updating Timezone Information (Daylight Saving Time, DST)

13.2. Update

Menu path: **Setup > System > Update**

On the **Update** page, a simple dialog for updating your thin client firmware is displayed. The normal procedure for updating your thin client is as follows:

1. Go to www.myigel.biz and download the desired firmware image from the IGEL server.
2. Unzip the ZIP file (the usual format in which updates are provided).
3. Save all files in the directory provided either on your local FTP/HTTP server or on a drive which is accessible from the client (e.g. a USB stick, NFS share etc.).
4. Configure the necessary settings (see below).
5. Save your changes and click on **Update Firmware**.

The update process will now proceed automatically.



The update procedure cannot be carried out via PPP/ISDN connections. In this case, you should use a local storage medium (USB stick) to provide the update.

The following information must be given before the update can start (the details required vary depending on the protocol chosen):

Protocol	Allows you to select the protocol to be used (FTP, HTTP, HTTPS etc.) from the drop-down list.
Server name and port	Details of the name or IP address of the server used as well as the port that is to be used
Path name on the server	Details of the directory in which you have saved the update files - starting from the root directory
User name	The user account name
Password	The password for this user/this account

13.3. 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 found then provides the update.

13.4. Remote management

Menu path: **Setup > System > Remote management**

This Setup page contains settings for managing the thin client remotely via Universal Management Suite (UMS).

- **Enable Remote Management:** If this option is enabled, the thin client can be managed via UMS.
- **Universal Management Suite:** If this client is already registered with a UMS, the UMS server is found in the list. Alternatively, enter a host name or IP address in **UMS Server** along with a **Port Number** in order to make the client register with the specified UMS server.



The list may contain more than one UMS server. If the client cannot reach a UMS Server under the name `igelrmserver` and the DHCP option 244 is not set either, the client will try the list entries until it reaches a UMS server.

- **Enable User Information:** If this option is enabled, the user will be informed via a message window when the thin client receives new settings or a shutdown command.
- **User information Message Timeout:** Time in seconds for which the user message window is displayed.
- **Structural directory tag:** This tag makes the UMS server put the client into the specified thin client directory.
- **UMS Registering:** This button opens the *UMS Registering* (page 117) utility from the System menu.

➡ Find more information about using structural tags in the *Best Practice "Using Structure Tags"* (<http://edocs.igel.com/index.htm#10202089.htm>).

13.4.1. Legacy 'setup.ini' transfer

Menu path: **Setup > System > Remote management > Legacy 'setup.ini' transfer**

You can also set up the thin client by directly transferring the `setup.ini` configuration file:

1. In **System > Remote Administration**, disable the **Allow remote management** option in order to disable the IGEL remote management service.
2. Click on **Transfer the setup.ini configuration file** to load the configuration needed for the thin client directly via DHCP.

The `setup.ini` file will then be administered manually without the graphical setup, e.g. of the IGEL UMS.

Two transfer protocols are available – TFTP and FTP. The corresponding DHCP tags are:

TFTP (disabled by default)	
ID 66	Name or IP of the server
ID 67	File path on the server The <code>setup.ini</code> file will be searched for in <File path>/.

FTP (enabled by default)	
ID 161	Name or IP of the server
ID 162	File path on the server The <code>setup.ini</code> file will be searched for in <File path>/igel/ud/.
ID 184	User name
ID 185	Password



It is recommended that you set the **Disable when updating** option at the same time. This will ensure that the `setup.ini` and the update data are transferred separately.

13.5. Shadow

Menu path: **Setup > System > Shadow**

For helpdesk purposes, you can observe the client through shadowing. This is possible via the IGEL Remote Manager or another VNC client (e.g. TightVNC). The options for the VNC functions are as follows:

Ask user for permission	In a number of countries, unannounced mirroring is prohibited by law. Do not disable this option if you are in one of these countries!
Allow entries from remote computer	If this option is enabled, the remote user may make keyboard and mouse entries as if they were the local user.
Use password	Enable this option to set up a password which the remote user must enter before they can begin mirroring.

13.5.1. Secure shadowing (VNC with SSL)

Menu path: **Setup > System > Shadow**

The **Secure Shadowing** function improves security when remote maintaining a client via VNC at a number of locations:

- **Encryption:** The connection between the shadowing computer and the shadowed client is encrypted. This is independent of the VNC viewer used.

- Integrity: Only clients in the UMS database can be shadowed.
- Authorization: Only authorized persons (UMS administrators with adequate authorizations) can shadow clients.

Direct shadowing without logging on to the UMS is not possible.

- Limiting: Only the VNC viewer program configured in the UMS (internal or external VNC viewer) can be used for shadowing.

Direct shadowing of a client by another client is likewise not permitted.

- Logging: Connections established via secure shadowing are recorded in the UMS server log.

In addition to the connection data, the associated user data (shadowing UMS administrator, optional) can be recorded in the log too.



Of course, this is only relevant to clients which meet the requirements for secure shadowing and have enabled the corresponding option. Other clients can be "freely" shadowed in the familiar manner and, if necessary, secured by requesting a password. If you would like to allow secure shadowing only, you can specify this in Misc Settings in the UMS Administration area.

Basic principles and requirements

Menu path: **Setup > System > Shadow**

The **Secure Shadowing** option can be enabled subject to the following requirements being met:

- IGEL Universal Desktop Linux or IGEL Universal Desktop OS 2, each from Version 5.03.190 or IGEL Universal Desktop Windows Embedded Standard 7 from Version 3.09.100
- IGEL Universal Management Suite from Version 4.07.100 onwards
- The client is registered on the UMS server
- The client can communicate with UMS console and UMS server (see below)

Basic technical principles:

Unlike with "normal" shadowing, the connection between the VNC viewer and the VNC server (on the client) is not established directly during secure shadowing. Instead, it runs via two proxies – one for the UMS console and one for the VNC server on the client. These proxies communicate via an SSL-encrypted channel, while the local communication, e.g. between the VNC viewer application and the UMS proxy, takes place in the conventional unencrypted manner. As a result, a secure connection can also be established with external VNC programs that do not support SSL connections.

The two proxies (UMS console and client) communicate with SSL encryption via the same port as the "normal" VNC connection: 5900. As a result, no special rules for firewalls need to be configured in order to perform secure shadowing.

If secure shadowing is active for a client (**Setup>System>Shadowing>Secure Shadowing**), the client generates a certificate in accordance with the X.509 standard and transfers it to the UMS Server when the system is next started. The UMS server checks subsequent requests for a secure VNC connection using the certificate. The certificate in PEM format can be found in the `/wfs/ca-certs/tc_ca.crt` directory on the client. The validity of the certificate can be checked on the (Linux) client using the command:

```
x11vnc -sslCertInfo /wfs/ca-certs/tc_ca.crt
```

Figure 80: Thin client certificate for secure shadowing

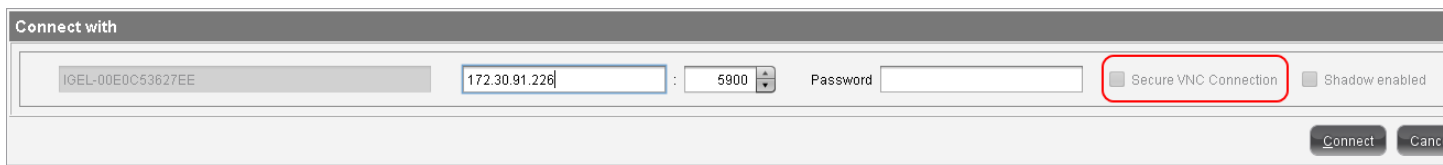


Figure 81: Secure shadowing connection dialog

When a VNC connection has been established, the symbol in the connection tab indicates secure shadowing:



Figure 82: Secure VNC connection

VNC logging

Menu path: **Setup > System > Shadow**

Connections via secure shadowing are always logged in the UMS. Via **UMS Administration>Misc Settings>Secure VNC**, you can configure whether the user name of the person shadowing is to be recorded in the log (the default is inactive).

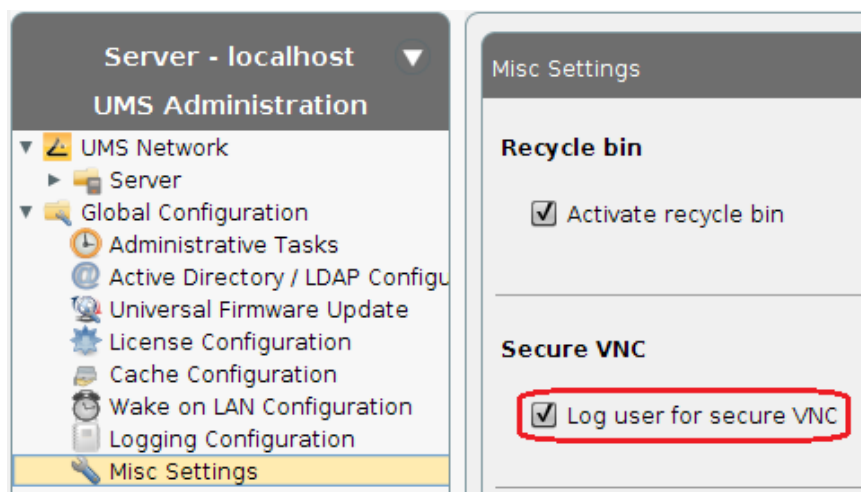


Figure 83: Options for VNC logging

The VNC log can be called up via the **context menu** of a client or folder (for several clients, **Logging>Secure VNC Logs**). The name, MAC address and IP address of the shadowed client, the time and duration of the procedure and, if configured accordingly, the user name of the shadowing UMS administrator are logged.

Secure VNC Logs					
Filter: <input type="text" value="00E0C56133A9"/>					
Thin Client Name	MAC Address	Thin Client IP	User	VNC Starttime	Duration in sec
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:01:17 PM	98
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:06:10 PM	32
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:06:26 PM	19
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:07:09 PM	44
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:07:18 PM	39
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:08:06 PM	48
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:08:38 PM	20
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:09:24 PM	26

Figure 84: Log entries for secure VNC connections

- To sort the list (e.g. according to user names), click on the relevant column header or filter the content shown by making entries in the **Filter** field.

13.6. Remote Access (SSH / RSH)

In order to allow central administration, the thin client can be configured in such a way that it can be accessed via the WAN.

Remote access to the local setup is permitted by default. However, you can restrict remote access to a specific user from a specific host. To enable restriction, give the full name of the host (e.g. `xterm.igel.de`) and the permitted user.

The Users for SSH Access to the thin Client are configured under **System > Remote Access > SSH Access** in the setup.

In the default setting, two users are already configured:

- **user**: The regular thin client user account. It has full shell access, but SSH access is disabled in the default configuration.
- **ruser** A special remote user whose access to applications can be restricted in **Applications access for remote user 'ruser'**



Pick **user** or **ruser** depending on your use case for SSH access. If in doubt, pick the more restricted **ruser**.

13.7. Power Options

Menu path: **Setup > System > Power Options**

Under **System > Power Options**, you will find numerous settings for energy management.

System 201

Battery 203

Display 204

Shutdown 204

13.7.1. System

SsyMenu path: **Setup > System > Power Options > System**

The screenshot shows the 'System' settings window. At the top, 'System standby' is set to 'Never'. Below this, there are two sections: 'On battery' and 'Plugged in'. Under 'On battery', the 'CPU power plan' is set to 'Balanced (recommended)'. Under 'Plugged in', the 'CPU power plan' is set to 'High Performance'. At the bottom, there is a checkbox labeled 'Tray icon' which is currently unchecked.

Figure 85: Energy Options System

System standby	Specify how long the user can be inactive before the system switches to standby mode – from Never or 10 Mins to 24 Hours .
CPU power plan	<p>Specify here which CPU power plan (CPU Governor) the device is to use in AC mode.</p> <p>Explanation of the settings:</p> <ul style="list-style-type: none"> • 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 (recommended). • Power Saver - lowest processor speed <p>The standard settings are High Performance in AC mode and Balanced (recommended) in battery mode.</p>
Tray icon	Enable this setting in order to display a CPU tray icon which allows you to switch quickly between the power plans.

13.7.2. Battery

Menu path: **Setup > System > Power Options > Battery**

The screenshot shows the 'Battery' configuration window. It is divided into two main sections: 'Battery Notification' and 'Battery Tray Icon'.
Battery Notification
 - 'Critical battery level (percentage)': A text input field containing the value '5'.
 - 'Critical battery action': A dropdown menu with 'Show warning' selected.
 - 'Critical command': A dropdown menu with 'Shutdown' selected.
 - 'Low battery level (percentage)': A text input field containing the value '10'.
 - 'Low battery action': A dropdown menu with 'Show warning' selected.
 - 'Low command': A dropdown menu with 'Shutdown' selected.
Battery Tray Icon
 - 'Display percentage': A checkbox that is checked.
 - 'Display time': An unchecked checkbox.

Figure 86: Energy Options Battery

Critical battery level (percentage)	Here you can configure the battery level percentage below which the battery level is regarded as critical. You can configure two different scenarios.
Critical battery action	Here you can specify what action is to be taken in the event of a critical battery level: No Action , Warning , Execute Command or Execute Command in Console .
Critical command	Enter a valid command here. The standard command <code>user_shutdown -f</code> shuts down the system in the proper manner.
Display percentage	Shows the battery level percentage in the tray.
Display time	Shows the remaining battery running time / charging time in the tray.

13.7.3. Display

Menu path: **Setup > System > Power Options > Display**

Display power management settings

☒ Handle display power management

	On battery	Plugged in
Standby Time	6 Minutes	10 Minutes
Suspend Time	8 Minutes	12 Minutes
Off Time	10 Minutes	15 Minutes

Brightness reduction

	On battery	Plugged in
On inactivity reduce to	20 %	80 %
Reduce after	Never	Never

Figure 87: Energy Options Display

Set the screen energy options

Handle display power management	Enable this checkbox in order to be able to make the following settings. In older firmware versions, this option was called DPMS (Display Power Management Signaling).
Standby time	Specify how many minutes the user can be inactive before the screen switches to standby mode.
Suspend time	Specify the number of minutes before the screen switches to suspend mode.
Off time	Specify the number of minutes before the screen switches off.

Brightness reduction

On inactivity, reduce to	Specify to how many percent the screen brightness should be reduced if you are not using the device.
Reduce after	Specify a time between 10 and 120 seconds after which the screen brightness will be reduced.

13.7.4. Shutdown

Menu path: **Setup > System > Power Options > Shutdown**

This setup page contains settings for shutting down.

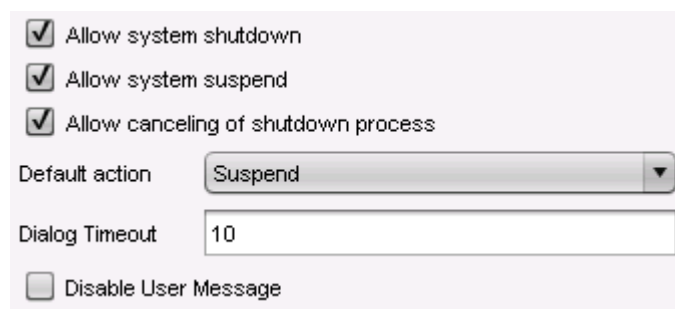


Figure 88: Shutdown

Allow system shutdown	Allows the user to shut down the device.
Allow standby suspend	Allows the user to place the device in standby mode.
Allow canceling of shutdown process	Allows the user to cancel the shutdown or standby process.
Default action	Defines which action is pre-selected in the dialog shown.
Dialog Timeout	Time span in seconds after which the option pre-selected in the dialog is executed.
Disable User Message	When shutting down the device, no dialog which with the user can interact is shown.

13.8. Firmware Customization

Menu path: **Setup > System > Firmware Customization**

Configure the firmware to create your own personal workstation.

13.8.1. Custom partition

Menu path: **Setup > System > Firmware Customization > Custom Partition**

IGEL Linux offers users a data partition on the storage medium. A download/update function which loads data from a server and, where appropriate, updates them can be set up for this dedicated storage area.



If the thin client is reset to the default settings, the custom partition and all data stored on it will be deleted

Enabling the partition

Menu path: **Setup > System > Firmware Customization > Custom Partition > Partition**

The custom partition is disabled by default.

- Click on **System > Firmware Customization > Custom Partition**, in the setup to enable the custom partition in the IGEL setup for the thin client (or with the IGEL Universal Management Suite) via the setup path.

The size of the partition is shown in the form of a numerical value (bytes) followed by a multiplier.

Sensible figures are for example 100 K (for 100 KiB = 100 * 1024 bytes) or 100 M (for 100 MiB = 100 * 1024 * 1024 bytes).

The screenshot shows a software configuration window titled 'Partition'. At the top, there are two icons: a hard drive and a download arrow. Below the icons, the text 'Partition' is followed by 'Download'. A horizontal scrollbar is visible. Below the scrollbar, there is a section with a checked checkbox labeled 'Enable Partition'. Underneath this, there are two input fields: 'Size' with the value '92m' and 'Mount Point' with the value '/custom'.

Figure 89: Enable Partition



The size of the partition should be set to at least 100 KiB. However, no more than 300 MiB should be reserved for the custom 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.



Figure 90: Creating Partition

- Click **Apply** or **OK** in order to confirm your settings.

The partition will be created and mounted at the specified location.

A status window provides information on the process and gives details of any errors when creating the partition. If for example there is insufficient space on the storage medium, it will not be possible to create the partition.



Figure 91: Error Message

If you attempt to change the size of a previously created custom partition, you may find that you are unable to do so if a process is still accessing the partition, e.g. if its content is still being shown in the terminal window.

Defining download source

Menu path: **Setup > System > Firmware Customization > Custom Partition > Download**

In order to load data onto the custom partition, at least one source for partition data must be specified in the Download area.

- Click on **Add**.

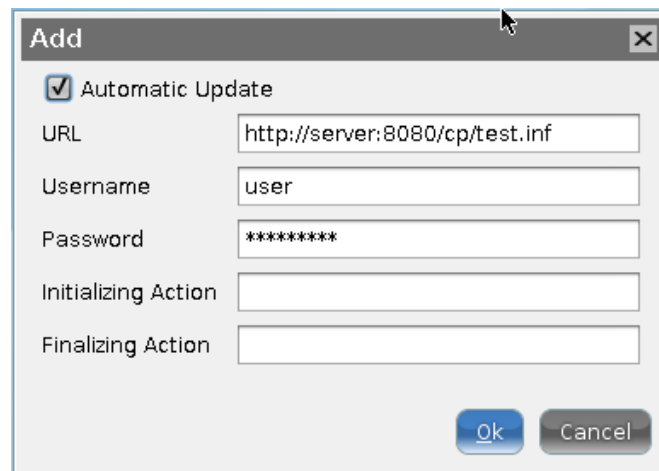


Figure 92: Setting the Download URL.

The transfer protocols are the same as the ones for updating the firmware, e.g. HTTP, HTTPS, FTP. An `INF` file which in turn references a tar archive zipped using `bzip2` must be given as the target.

The structure of the `INF` file is as follows:

[INFO], [PART]	Header informationen
file="test.tar.bz2"	Zipped tar archive
version="1"	Version of the file

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.org). This program also allows `bzip2` compression. Under Linux, `tar`- and `bz2`- files can often 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.

Carrying out actions

Menu path: **Setup > System > Firmware Customization > Custom Partition > Download**

Once the custom partition has been mounted or unmounted, commands (Shellscript) can automatically be executed. For example, a program loaded to the partition can be launched or closed upon shutdown (the partition will be unmounted again in the process).

Example

A custom background image is to be used. The image named `igel.jpg` is zipped into the referenced `test.tar.bz2` file using 7-Zip (see `INF` file above).

The `INF` file and the zipped archive are moved to an IGEL UMS web resource. This can be accessed from the thin client via HTTP.

Make the following settings in the UMS thin client configuration:

1. Enable **Customr Partition** (size e.g. 1 M) and have it mounted on `/custom`.

Under **Download**, a new URL whose target is the `test.inf` file on the UMS server is created:
`http://[ums-server:9080]/web-ressource/test.inf`

2. Enter the access data for the web server and enable **Automatic Updates** if the image is to be replaced later on.
3. Enter the following copy command as an initialization action in order to copy the unzipped image to the correct location:

```
cp /custom/igel.jpg /usr/share/pixmaps/IGEL_UD_4x3_blue.jpg
```

4. Under **User Interface > Screen > Desktop**, select the entry **Igel blue (4x3)** as the background image.

The associated file will be replaced by your own file.

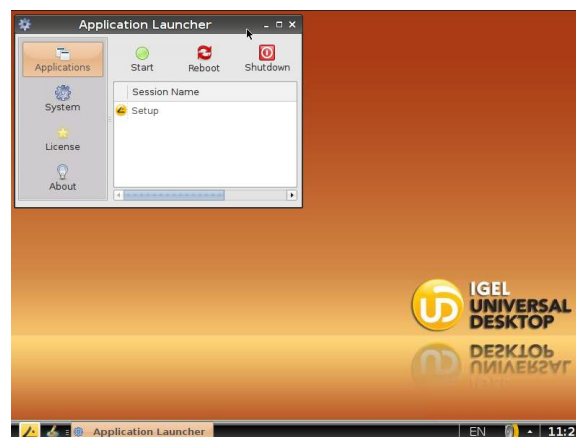


Figure 93: Original background image

5. Save your changes in the IGEL setup and restart the thin client so that it takes the modified settings from the UMS Server.

The custom partition is created and mounted.

The zipped file is transferred, unzipped and copied to the target directory.

The new background image is loaded and displayed:

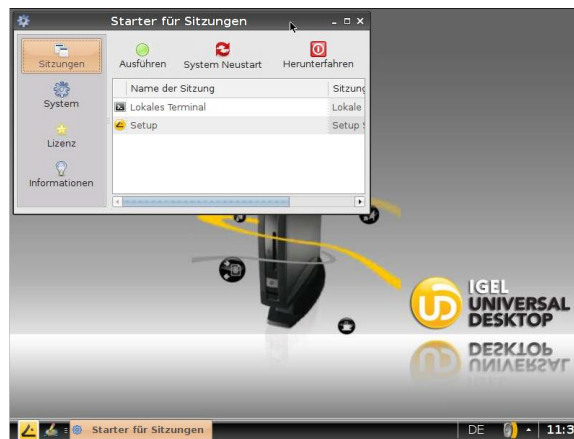


Figure 94: New background image

To replace this image with a new one:

1. Change the JPG in the `test.tar.bz2` file.
2. Increase the version number in the `test.inf` file.

The new version will be downloaded and used then next time you restart the client.



Executable files can also be loaded to the custom partition and called after mounting.

13.8.2. Custom Application

Menu path: **Setup > System > Firmware Customization > Custom Application**

Applications which were loaded onto a custom partition for example can be launched via the **Application Launcher** or an icon on the desktop once they have been defined as own applications. In order for this to be possible, a command to call up the application must be entered under **Settings**.

13.8.3. Custom Commands

Menu path: **Setup > System > Firmware Configuration > Custom Commands**

Custom commands can be executed at various points in time during the system start. These commands can use *predefined environment variables* (page 216).

Base commands (page 211)

Network commands (page 211)

Desktop commands (page 212)

Reconfiguration commands (page 213)

Base commands

Menu path: **Setup > System > Firmware Configuration > Custom Commands > Base Commands**

Base commands run once during the boot procedure. The commands are executed at the following times:

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 effective

Final initialization command

- All partitions available
- All system daemons launched
- UMS settings effective

Network commands

Menu path: **Setup > System > Firmware Configuration > Custom Commands > Network Commands**

Network commands run each time the relevant interface (standard `eth0`) starts within the network. The interface can be selected with the `$INTERFACE` environment variables (`eth0`, `eth1`, `wlan0`). The commands are executed at the following times:

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

Desktop commands

Menu path: **Setup > System > Firmware Configuration > Custom Commands > Desktop Commands**

Desktop commands run each time the X server starts. The commands are executed at the following times:

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 commands

Menu path: **Setup > System > Firmware Configuration > Custom Commands > Reconfiguration Commands**

Reconfiguration commands run when settings are changed via the local setup or the UMS. The commands are executed at the following times:

After reconfiguration changes

- Runs after an effective change in the thin client settings (local setup, UMS)

13.8.4. Corporate design

Menu path: **Setup > System > Firmware Customization > Corporate Design**

In this area, settings allowing you to adapt the user interface to your corporate design are grouped together.

You can place your own logo in the following places:

- *In the bootsplash* (page 213)
- *As a background image* (page 214)
- *As a screensaver* (page 214)
- *As a start button icon* (page 214)
- *As a company logo in the start menu* (page 214)
- *In the taskbar* (page 143)

Custom bootsplash

Menu path: **Setup > System > Firmware Customization > Corporate Design > Custom Bootsplash**

With a bootsplash, you can show your company logo or a specific image during the boot procedure in order to hide the console output from the user.

Requirements: You need to provide an image file for your custom bootsplash on a download server.

Information regarding the image: The file types BMP, JPG, GIF, TIF, PNG and SVG are supported for a **bootsplash**. A total storage area of 25 MB is available for all user-specific images.

The image is 800 x 600 pixels in size (aspect ratio remains unchanged). It can be positioned vertically and horizontally by changing the position values.

To set up a custom bootsplash, proceed as follows:

1. Enable **Custom Bootsplash**.
2. Specify your download server.



If you have already defined a server for the system update files, you can use the same server settings for downloading the boot image.

3. Configure the following further settings:

- **Custom Bootsplash file:** Give the name of the file that you want to display here.
- **Horizontal/Vertical Position of the bootsplash image:** Give the horizontal and vertical position of the displayed image.
- **Horizontal/Vertical Position of the progress indicator:** Give the horizontal and vertical position of the progress bar.

0 means left-justified, 50 centered and 100 right-justified.

The user-specific bootsplash will be downloaded from the given server if you

- enable **Custom Bootsplash** - see Step 1
or
- click on **Bootsplash update** if you previously assigned and saved another image during the setup
or
- you execute a **scheduled Job** in the IGEL Universal Management Suite with the command **Update Desktop Customization**.

Background

Menu path: **Setup > System > Firmware Customization > Corporate Design > Background**

Decorate the desktop background with pre-defined IGEL backgrounds, a fill color or a color gradient, or define your own background image.



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

Requirements: You need to provide your own background image on a download server.

Information regarding the image: The file types BMP, JPG, GIF, TIF, PNG and SVG are supported for a custom background image. A total storage area of 25 MB is available for all user-specific images.

To set up a custom background image, proceed as follows:

1. Go to Corporate Design > Background (1st Monitor):
2. Enable Custom Wallpaper Download.
3. Give a name for the background image file.
4. Go to Corporate Design > Background (1st Monitor) > Background Image Server.
5. Specify the download server.



If you have already defined a server for the system update files, you can use the same server settings for downloading the background image.

6. Click on Wallpaper Update to download the user-specific background image from the given server.

Company logos

Menu path: **Setup > System > Firmware Customization > Corporate Design > Company Logos**

Other areas where you can show your company logo in the firmware are the **screensaver** and the **start menu**.

To define an image for the **screensaver**, proceed as follows:

1. Activate **Enable Image display**.
2. Under **Image File/Directory**, give the full path for an image file or a directory containing a number of image files.



If you enter a folder instead of a single image file as the source, all images in the folder will be displayed as a slide show, the **display time** for the images can be configured.

If you do not specify a file of your own, the IGEL logo will be used.

3. Enable **One Image per Monitor** if you would like to see the image (the images) on each individual monitor rather than one image across all monitors.
4. Specify the **image duration** in seconds.
5. Select the **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** - image is shown in full, with black edge where the format does not match that of the screen.

To define logos for the **start menu**, proceed as follows:

- Under **Start Button Icon**, give the file name of the logo with a full path in order to select your logo as a symbol for the start menu at the bottom left of the taskbar.
- Under **Company logo in start menu**, give the file name of the logo with a full path in order to display your company logo in the start menu window.



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**.



Figure 95: Start menu

13.8.5. Environment variables

Menu path: **Setup > System > Firmware Customization > Environment Variables**

Environment variables allow you to use dynamic parameter content for a number of session types, e.g. so as not to have to enter ICA or RDP servers for every session. Within the IGEL Setup, the variables can be found under: **System→Firmware Configuration→Environment Variables**

Predefined variables can also be supplied and distributed via the IGEL UMS. Additional defined variables can only be used locally and may be overwritten by a UMS configuration.

The environment variables are available in *Custom Commands* (page 210).

In addition, the following session parameters can be updated with variables:

- ICA - User name (ICA sessions→[Session name]→Logon)
- ICA - Citrix server or Published Application (ICA sessions→[Session name] -> Server)
- XenApp - User name (Citrix XenApp/Program Neighborhood→Logon)
- RDP - User name (RDP sessions→[Session name]→Logon)
- RDP - Server (RDP sessions→[Session name]→Server)

Use in sessions

1. Enable environment variables under **Enable variable substitution in session**.
2. Specify the variable name and content (e.g. Variable Name = SERVER NAME | Value = test server)
3. Enter the variable name in the session parameter field. The name is preceded by a \$ sign (e.g. \$SERVERNAME)

In the case of RDP and ICA sessions, the setting is implemented after being saved and is entered into the session file. With XenApp, the setting is not implemented until a session starts and is running.

13.8.6. Features

Menu path: **Setup > System > Firmware Customization > Features**

Using this list of available services, you can quickly enable or disable firmware components such as Powerterm, Media Player etc. If a service was disabled, the associated session type will no longer be available when the system is restarted. Existing sessions will not be shown but will not be deleted either. A disabled session type will not be updated during a firmware update. You should therefore disable unused services in order to speed up update processes.

13.9. IGEL System Registry

Menu path: **Setup > System > Firmware Customization > Custom Commands**

You can change virtually every firmware parameter in the Registry. You will find information on the individual items in the tool tips.



However, changes to the thin client configuration via 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 thin client is to reset it to the factory defaults!

You can search for setup parameters within the IGEL Registry by clicking on the **Parameter Search** button. 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:

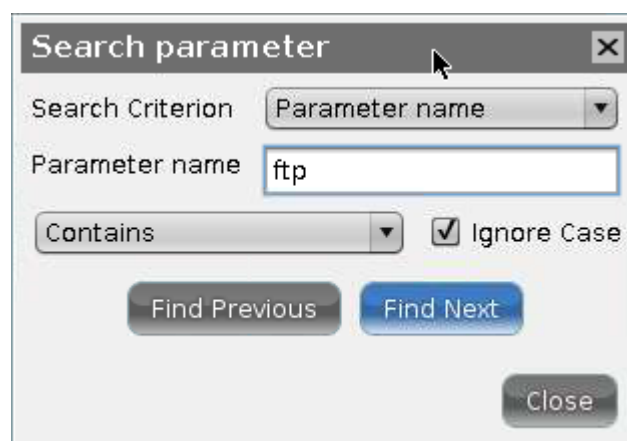


Figure 96: Parameter search in the IGEL Registry

14. Index

A

About this document.....	6
Access control.....	135
Accessories	111
AD/Kerberos	190
AD/Kerberos Configuration	192
Administrator Session.....	174
Advanced	89, 95
Advanced Options	139
Advanced settings	113
Appearance.....	38, 58
Appliance Mode.....	67
Application Launcher.....	12, 115
Ask User	54
Audio	47, 102, 107
Authentication.....	57, 162
Auto Logoff	191
Automount Devices	183

B

Background.....	140, 214
Base commands.....	211
Basic principles and requirements	197
Battery	203
Boot Menu.....	14
Boot Procedure.....	14
Browser Global	83
Browser Plugin.....	103
Browser Plug-ins	99
Browser Sessions	93
Buddy Update	195

C

Call Options	109
Caradigm.....	70
Carrying out actions.....	208

Certificate	175
Certification Authority	175
Change Smartcard Password	111
Checking the Client Certificate	176
Citrix Access Gateway.....	41
Citrix Receiver Selection	22
Citrix Self-Service	40, 68
Citrix StoreFront / Web Interface	36
Citrix XenDesktop	68
Codec	31
COM Ports.....	45
Commands.....	91, 125
Company Key	189
Company logos	215
Configuration	139
Configure Access to RD Connection	53
Configure Connections in the Setup.....	168
Connection settings	62
Connections	56
Content	84, 94
Context menu	99
Corporate design	213
CUPS - Common UNIX Printing System	179
Custom Application	210
Custom bootsplash	213
Custom Commands.....	210
Custom partition.....	206

D

Data Protection.....	95
Defining download source.....	207
Desktop.....	140
Desktop commands	212
Desktop integration	35
Desktop Integration.....	21, 40, 110
Device Information	125
Device Support	27, 46

Devices.....	179
DHCP Options	170
DigitalPersona authentication	28
Disk Utility.....	127
Display	204
Display switch	112
Display, Keyboard and Mapping.....	52
Domain-Realm Mapping.....	192
Drive Mapping	25, 45
DriveLock	28, 46

E

Emergency Boot	15
Enable setup pages for users.....	19
Enabling the partition	206
Encryption.....	92, 95
Ending the Setup	17
Energy options.....	133
Enlarged View	114
Environment variables.....	216
Evidian AuthMgr	73
Example	176, 208
Example configuration for the screen saver.....	148

F

Failsafe Boot - CRC check.....	15
Features	217
Firefox browser.....	83
Firewall	29, 33
Firmware Customization	206
Firmware Update.....	128
Flash Player.....	100
Font Services.....	157
Formatting and meanings.....	6

G

Gamma correction.....	136
Gateway.....	42
GeNUCard.....	171

H

H.323.....	109
Hardware and Network Requirements	139
HDX / ICA Global	22
HDX Flash.....	31
HDX Multimedia Redirection.....	30
Horizon Client Global	59
Horizon Client session.....	62
Hosts	177
Hotkeys	99, 156
Hotplug storage devices	182

I

IBM iSeries Access	76
ICA Connection Center	111
Identify Monitors.....	129
IGEL Linux user manual.....	6
IGEL Smartcard	188
IGEL System Registry	217
IGEL Universal Desktop Firmware	8
Image viewer	131
Important Information	2
Imprivata.....	69
Individual interface.....	161
Information.....	12
Input.....	150

J

Java Control Panel	124
Java Web Start	105
Java Web Start Session	104

K

Keyboard.....	24, 44
Keyboard and additional keyboard	150

L

LAN interfaces.....	160
Language.....	146
Legacy ICA Sessions	32

Legacy 'setup.ini' transfer.....	195
Leostream Connection Broker.....	72
License	13
Local Logon	23, 43, 59
Local Terminal	111
Log off.....	39
Login Options.....	187
Logoff / Desktop Integration	58
Logon	32, 36
Look-up.....	127
LPD - Line Printer Daemon	180

M

Mapping.....	25, 45, 64
Media Player.....	101
Media Player Global	101
Media Player Sessions	103
Menus and symbol bars	96
Mobile broadband network	159
Monitor Calibration	125
Mouse.....	151
Mouse and keyboard.....	63
Multimedia	50, 61, 65

N

Native USB Redirection	30, 49
NCP	171
Netstat.....	126
Network.....	159
Network commands	211
Network Diagnostics.....	125
Network Drives.....	177
Network Information.....	13
Network Integration	16
NFS.....	177
NFS Font Service	158
NoMachine NX.....	73
Nuance channel for dictation	29

O

OpenVPN	170
Optimization	78, 81
Options	29, 34, 37, 41, 48, 65, 77, 80, 102, 104, 137, 173

P

Pager	144
Parallels 2X client session	74
Password.....	187
Password Change.....	39
PDF viewer	100
Performance	47, 62, 64
Performance and Options	53
Ping	125
Playback.....	102, 103
Power Options	201
PowerTerm selection.....	75
PowerTerm terminal emulation	75
PowerTerm WebConnect	74
PPTP	170
Pre-defined configuration	54
Print	85
Printer	27
Printers	46, 179
Printing	94
Privacy.....	87
Proxy	65, 85, 94, 178

Q

Quick Installation	9
Quick Settings Session	112
Quick setup	19
Quiet Boot.....	14

R

RDP Global	42
RDP Multipoint Server	70
RDP Session.....	51
Realm 1-4.....	192

Reconfiguration commands	213	Signature pad.....	155
Reconnect.....	34, 39	Simple Certificate Enrollment Protocol - SCEP	174
RedHat Spice.....	100	SIP	108
Remote Access (SSH / RSH)	201	Smartcard	37, 62, 184
Remote Desktop Web Access.....	53	Smartcard login	71
Remote management.....	195	Smartcard Personalization.....	128
RemoteFX Support.....	47	Soft keyboard.....	124
Reset to factory defaults	15	Softpro SPVC Channel.....	29
Restarting	95	Software Requirements.....	138
RHEV/Spice	69	Sound Mixer.....	116
Routing	176	SSH Session	82
S		Start menu	145
Save Sessions	190	Starting the Setup.....	17
Save User and Password.....	189	Supported formats and codecs.....	8
SCEP	175	Systancia AppliDis Client.....	73
SCIM (Input Methods)	155	System	13, 202
Screen	132	System Information	127
Screen Saver and Screen Lock	147	System Log Viewer.....	117
Screenshot tool.....	121	System Settings.....	193
Secure shadowing (VNC with SSL)	196	T	
Security	89, 95, 187	Tabs.....	84, 94
Serial Connections - COM Ports.....	26	Taking a screenshot	123
Server.....	32, 36, 41, 51, 76, 80	Task Manager	119
Server Location	23	Taskbar.....	141
Server Options	59	Taskbar background	143
Session Control Bar.....	146	Taskbar items.....	143
Sessions	12, 21	TCP/IP	180
Settings	94, 110	Telephone Book.....	110
Setup Application	17	Test Smartcard.....	190
Setup Areas.....	18	The IGEL Linux desktop.....	10
Setup Search	20	ThinLinc.....	76
Setup Session.....	111	ThinLinc Global	76
Shadow	196	ThinLinc Sessions	79
Shadow clients securely	198	ThinPrint	181
Shutdown.....	204	Time and Date.....	193
Shutting Down and Restarting a Device	14	Touchpad	152

Touchpad Advanced	154	Window settings	96
Touchpad General	153	Windows Drive - SMB	178
Touchpad scrolling.....	154	Wireless	163
Touchscreen	151	Wireless Manager.....	165
Touchscreen calibration	118	Wireless regulatory domain	169
Traceroute	126		
U		X	
UMS Registration.....	117	X Session	74
Universal MultiDisplay.....	138	XC Font Service	157
Update	194	XDMCP	134
Upgrade License	129	X-Server	16
Usage	140		
USB access control.....	185		
USB redirection.....	60		
USB Storage Devices.....	182		
User Account	107		
User Interface	81, 132		
Using the Task Manager	120		
V			
Verbose Boot	14		
VERDE session.....	83		
Via Browser.....	55		
Video.....	102		
Virtual Private Network - VPN	170		
VMware Horizon.....	67		
VNC logging	199		
VNC Optimization	78, 81		
VNC Viewer.....	83		
VoIP Client	105		
vWorkspace Client and AppPortal.....	66		
W			
Wake-on-LAN.....	163		
Webcam Information	130		
What is new in 5.09.100?	7		
WiFi Configuration.....	172		
Window	24, 33, 44, 63, 77, 80, 101		