

IGEL Zero HDX

Manual



Contents

1.	Quick Installation	6
1.1.	The IGEL Linux Desktop.....	6
2.	Boot Procedure.....	8
2.1.	Boot Menu	8
2.2.	Network Integration	9
2.3.	X-Server.....	9
3.	Application Launcher	10
3.1.	General System Information.....	11
3.2.	Sessions.....	11
3.3.	System Tools	12
3.4.	License.....	13
3.5.	Network Information	14
3.6.	Shutdown and Restart	14
4.	Setup Application.....	15
4.1.	Starting the Setup	15
4.2.	Completing the Setup	15
4.3.	Setup Areas	16
4.4.	Setup Search	18
5.	Sessions	20
5.1.	Citrix Receiver selection.....	20
5.2.	Citrix ICA - global settings	21
5.3.	Citrix ICA - Sessions	31
5.4.	Citrix StoreFront / Web Interface	35
5.5.	Citrix Access Gateway	38
5.6.	Appliance mode	38
5.7.	SSH Session	39
5.8.	Firefox browser	41
5.9.	Media Player	54
5.10.	Java Web Start Session	57
5.11.	VNC Viewer	57
6.	Accessories	58
6.1.	ICA Connection Center.....	58
6.2.	Local Terminal	58
6.3.	Change Smartcard Password	58
6.4.	Smartcard Personalization	58
6.5.	Setup Session	58
6.6.	Quick Settings Session.....	58
6.7.	Display switch	59
6.8.	Application Launcher	59
6.9.	Sound Mixer.....	60

6.10.	System Log Viewer	60
6.11.	UMS Registration	61
6.12.	Touchscreen Calibration	61
6.13.	Soft Keyboard (On-screen Keyboard)	62
6.14.	Java Control Panel	62
6.15.	Calibration Pattern	62
6.16.	Commands	62
6.17.	Network Diagnostics	63
6.18.	System Information	64
6.19.	Drive Management	66
6.20.	Firmware Update	66
6.21.	Identify Monitors	67
6.22.	Upgrade License	67
6.23.	Webcam Information	68
6.24.	Image Viewer	69
7.	User Interface	70
7.1.	Screen	71
7.2.	Language	84
7.3.	Screen Saver and Screen Lock	84
7.4.	Input	88
7.5.	Keyboard Commands - Hotkeys	90
7.6.	Font Services	90
8.	Network	92
8.1.	LAN interfaces	92
8.2.	Wireless	98
8.3.	DHCP Options	104
8.4.	Virtual Private Network - VPN	104
8.5.	Simple Certificate Enrollment Protocol - SCEP	107
8.6.	Routing	109
8.7.	Hosts	109
8.8.	Network Drives	110
8.9.	Proxy	111
9.	Devices	111
9.1.	Printers	111
9.2.	USB Storage Devices	114
9.3.	USB Access Control	116
9.4.	PC/SC Interface	117
10.	Security	118
10.1.	Password	118
10.2.	Login Options	118
10.3.	AD/Kerberos Configuration	122
11.	System Settings	124
11.1.	Time and Date	124

11.2. Update	125
11.3. Remote Management	126
11.4. VNC (Shadowing)	127
11.5. Secure shadowing (VNC with SSL).....	127
11.6. Remote Access (SSH / RSH).....	131
11.7. Energy	132
11.8. Firmware Customization.....	142
11.9. IGEL System Registry.....	144
12. Index.....	146

Introduction

IGEL Thin Clients comprise the very latest hardware and an embedded operating system. Depending on the product concerned, this operating system may be based on IGEL Linux or Microsoft Windows Embedded Standard*. We have done our utmost to provide you with an excellent overall solution and promise to provide the very same level of quality service and support.

The IGEL Linux Firmware

The new IGEL zero clients for Citrix HDX, Microsoft RDS/ RemoteFX or VMware Horizon provide a genuine zero client experience at a low price yet avoid the restrictions that are typical of zero clients from other manufacturers, e.g. the lack of an update facility, management and support.

IGEL supplies specialized zero clients without compromises, i.e. optimized for one of the three leading virtualization solutions and with free support. Thanks to the Appliance Mode, the zero clients boot quickly and directly into the relevant VDI session such as Citrix XenDesktop or VMware Horizon View.

Experience "zero touch deployment" thanks to rule-based configuration during rollout. Reduce your management outlay to virtually zero thanks to profile-based, automatic remote-management of all settings. This means "zero" local management for you.

The structure of the IGEL setup is virtually identical on all zero clients and in the Universal Management Suite (UMS) management software. As a result, the configuration parameters in the local device setup can be found in the same location in the tree structure as a profile used in the management software for example. The IGEL Universal Management Suite is available to all customers on the IGEL download site. It allows management of an unlimited number of IGEL thin clients.

IGEL zero clients are future-proof. Free updates allow access to new functions if necessary. And if you decide to change the VDI solution later on, this is no problem either. With an IGEL Universal Desktop upgrade license, you can get your existing IGEL zero client hardware ready for access to other VDI solutions.

1. Quick Installation

If you follow the procedure below, you can install the thin client within your network environment in just a few minutes:

1. Connect the thin client to a monitor (VGA, DVI, DisplayPort), an AT-compatible keyboard with a PS/2 or USB connection, a USB mouse and the LAN using an RJ45 connector.
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 the **Setup** symbol in the taskbar, or launch the IGEL Setup using the key combination **Ctrl+Alt+S**.
5. Select the system language and keyboard layout under **User Interface→Language**.
6. Select the display resolution under **User Interface→Display**.
7. Enter a local IP address in the **Network** section of the setup or retain the default DHCP mode for automatic network configuration.
8. Click on **OK** to save and apply your changes.

The device will now 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 tool tips under **User Interface→Screen→Desktop**.

1.1. The IGEL Linux Desktop

After the system starts, you will see the IGEL Linux desktop.



Figure 1: IGEL Linux desktop

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

- **Start menu** (also IGEL menu)
- **Quick launch bar** with symbols for the **Application Launcher**, **setup** and sessions
- **Info area** with symbols for the **volume**, **network**, **time** and **desktop** (show/hide window)

The Start menu offers the following areas and functions:

- **Application area** for launching sessions
- **System area** for access to system programs
- **Info area (About)** for displaying all relevant system information
- **Search** for finding functions in the Start menu
- Buttons for **shutting down** and **restarting** the system

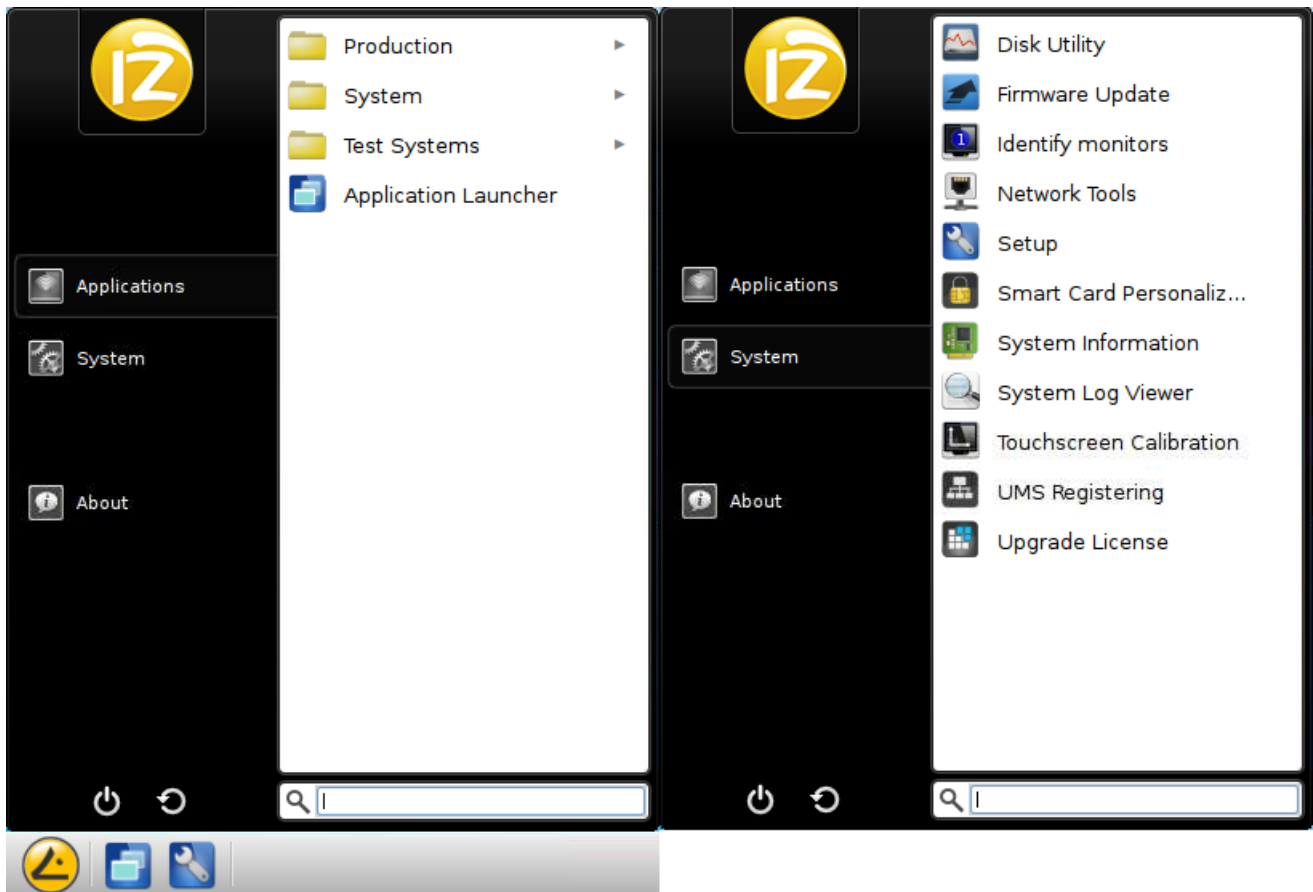


Figure 2: IGEL Start menu with application and system area

2. Boot Procedure

The quick installation procedure is complete.

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

2.1. 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 8)	Normal boot
Verbose Boot (page 8)	Boot with system messages
Emergency Boot (page 8)	Setup only
Failsafe Boot (page 9)	With CRC check
Reset to Factory Defaults (page 9)	Resets the thin client to the default factory settings

2.1.1. Quiet Boot

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

2.1.2. 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.

2.1.3. 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.

2.1.4. 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**.

2.1.5. 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.

➤ You must then confirm your decision.

If the device is protected by an administrator password, you will be prompted to enter this password. You have three attempts to do so.

Do you not know the password?

1. When you are prompted to enter the password, press the **Enter key** three times.
2. Press **Ctrl** to bring up the **Terminal Key**, the individual key for the thin client.
3. Contact us using an RMA form:
<https://www.igel.com/en/service-support/rma-request.html>
(<https://www.igel.com/en/service-support/rma-request.html>)
4. 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.

2.2. Network Integration

Is the kernel loaded?

If it is, the next step is the network configuration.

There are three possible ways of integrating the terminal into the network environment. Depending on the terminal's settings, you can choose between **DHCP**, **BOOTP** or a **manually configured IP address**.

2.3. X-Server

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

3. Application Launcher

- To launch the tool, click on the **Application Launcher** symbol in the quick launch bar or in the Start menu.

The various Launcher sub-areas allow access to configured sessions/system programs or show information relating to licenses, the system and network connections.

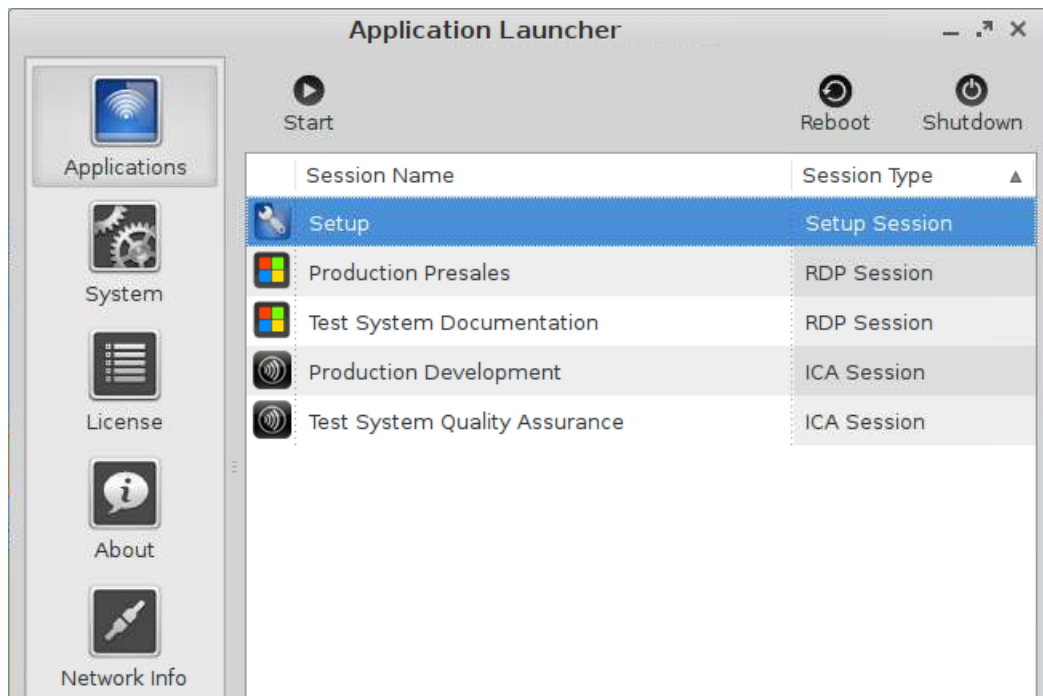


Figure 3: Application Launcher

Because the setup program is the central configuration tool for all thin client settings, a setup session is already pre-defined under **Sessions** and **System**.

Sessions (page 20)

System (page 12)

License (page 13)

Network information (page 14)

Shutting down and restarting a device (page 14)

3.1. General System Information

Within the **Application Launcher** you will find the **Information** page with important system data such as the firmware version, licensed services and hardware specifications.

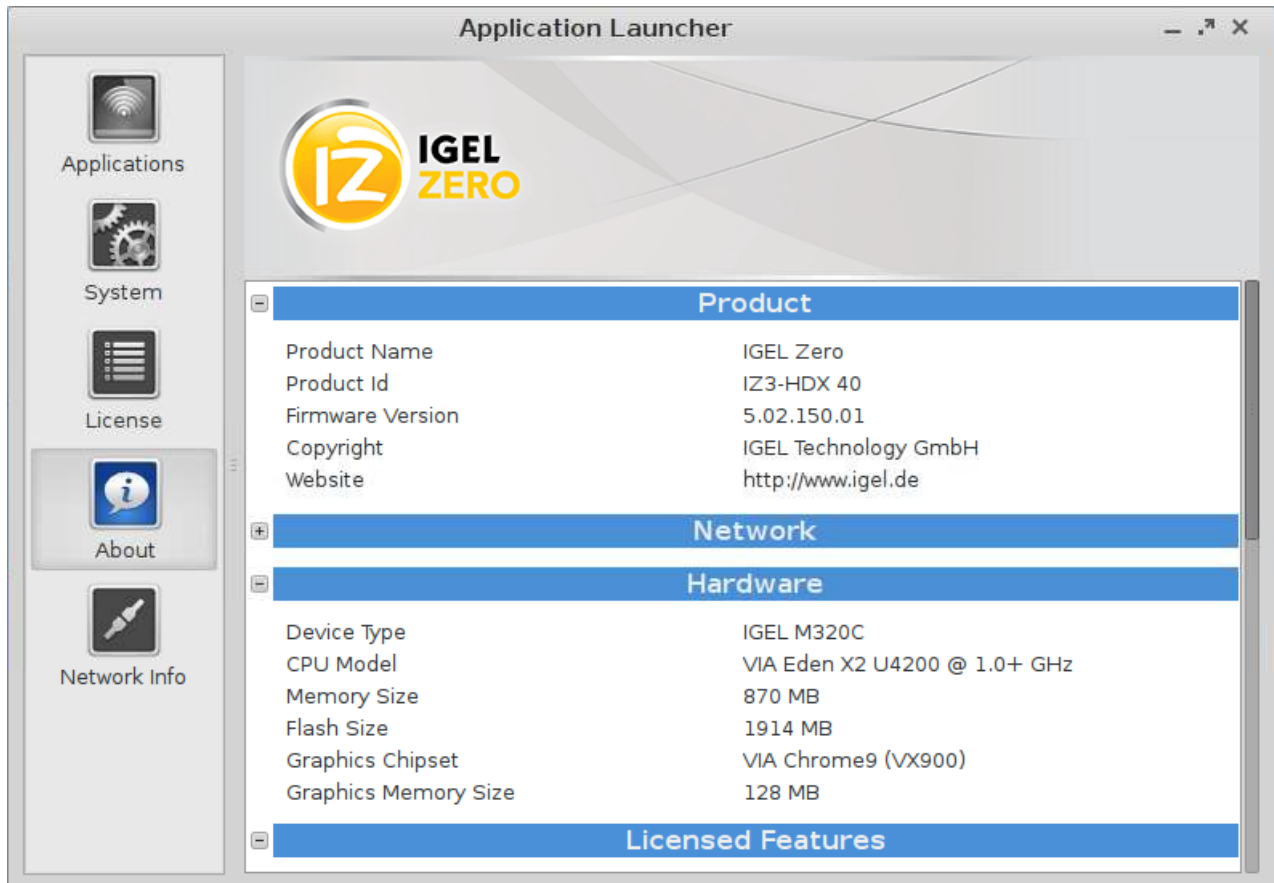


Figure 4: Application Launcher - system information

Details of the current network configuration with the IP address and device name are also given here.

3.2. Sessions

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

- To open an application, double-click on it or click on **Run**.
- Alternatively, you can launch sessions via icons on the desktop, in the quick launch bar or from the Start menu and context menu.
- Applications can also be launched automatically and a key combination (hotkey) can be defined.

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

3.3. System Tools

On the **System** page, you can run various tools including the firmware updating tool with the pre-set update information.



Figure 5: Application Launcher - system tools

The following tools are available:

Identify monitors	Shows the screen's number and manufacturer details.
Firmware update	Carries out the update with the settings made during the setup.
Disk utility	Shows information regarding connected USB drives.
Upgrade license	Reads a new license file from the USB stick and modifies the functions of the firmware accordingly.
Network tools	Provides detailed information on the network connection and offers a number of problem analysis tools such as Ping or Traceroute.
Setup	Launches the IGEL Setup.
Smart Card 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.
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).
Webcam Information	Shows video data of a detected webcam and allows to test the cam.

3.4. 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

3.5. 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:

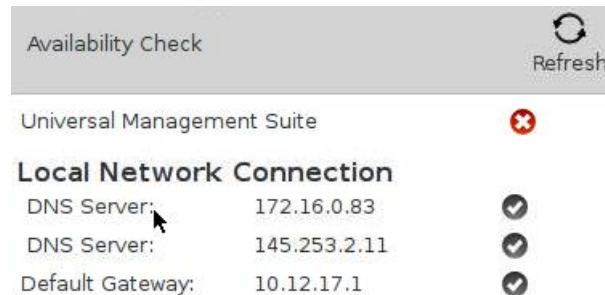


Figure 6: Network information

3.6. Shutdown and Restart

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

You can change the standard 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**→**Energy**→**Shut Down**.

4. Setup Application

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

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

Starting the setup (page 15)

Completing the setup (page 15)

Setup areas (page 15)

Setup search (page 18)

4.1. Starting the Setup

You can open the setup in the following ways:

- Double-click on **Setup** in the **Application Launcher** or click on **Run**.
- Double-click on **Setup** on the desktop (if available based on the settings).
- Select **Setup** in the context menu on the desktop (if available based on the settings).
- Select **System→Setup** in the Start menu.
- Click on **Setup** in the quick launch bar.
- 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.

4.2. Completing the Setup

The buttons **OK**, **Cancel** and **Apply** are usually available on every individual setup page.

- 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.

4.3. Setup Areas

The setup application comprises the following main areas:

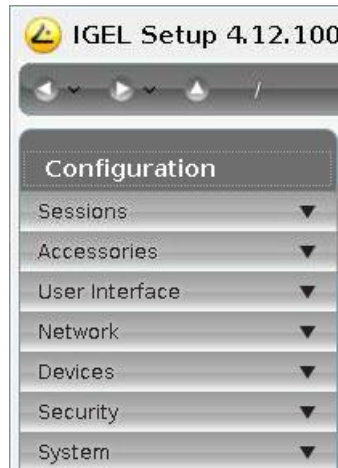


Figure 7: Setup areas

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.

4.3.1. 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 118)). 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.

1. Under **Security**→**Password**, enable the password for the **administrator** and the **setup user**.
2. Under **Accessories**→**Setup Session**→**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 indicates that the user can edit the parameters on this setup page.

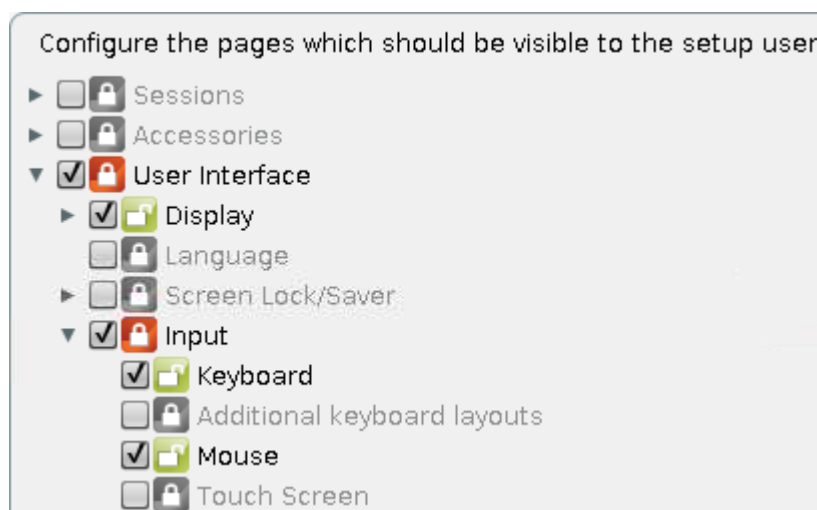


Figure 8: Restricted access to the setup

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).

4.3.2. Quick Settings

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 118)). 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.

1. Under **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 **Accessories**→**Quick Settings**, define the name and the options for bringing up the quick setup.

3. Under **Accessories**→**Quick Settings**→ **Page Authorizations**, 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.

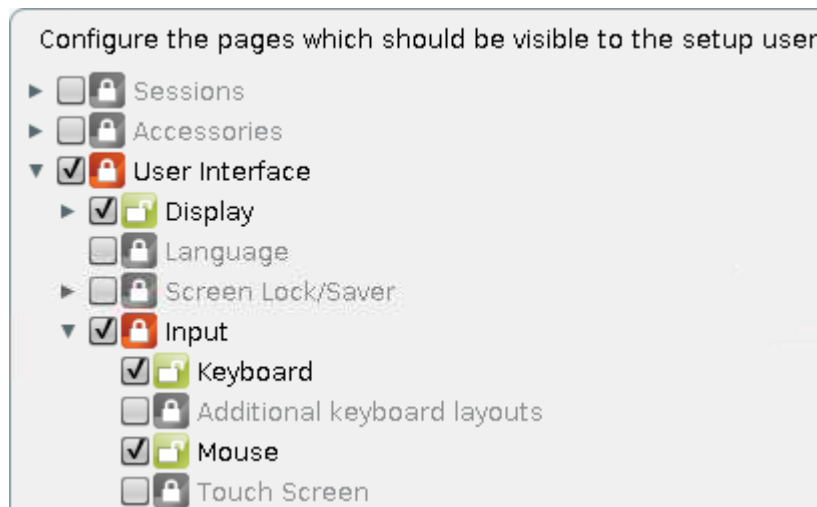


Figure 9: Restricted access to the setup

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).

4.4. Setup Search

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

1. To start a search, click on the button below the tree structure.
2. Enter the text you wish to search for.
3. Specify the details for your search – narrow it down to field headers for example.
4. Select one of the hits.
5. 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.

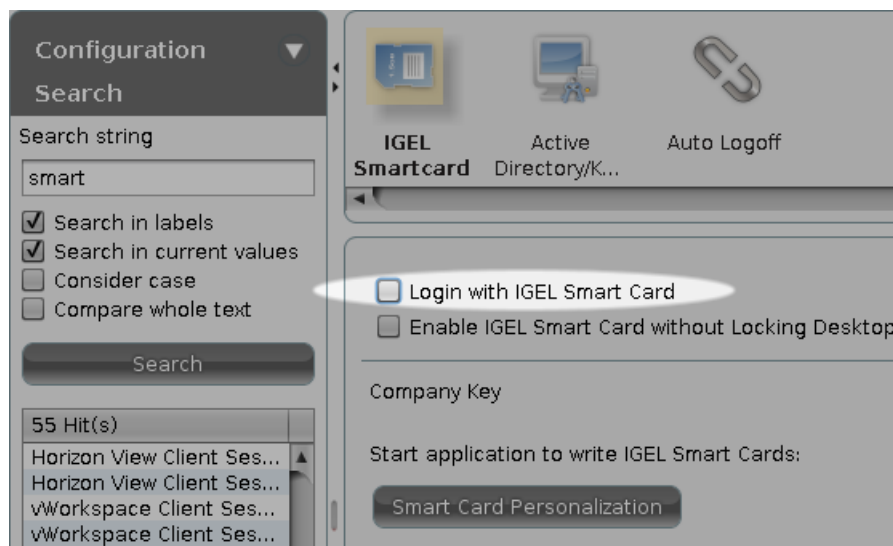


Figure 10: Setup search

5. 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.

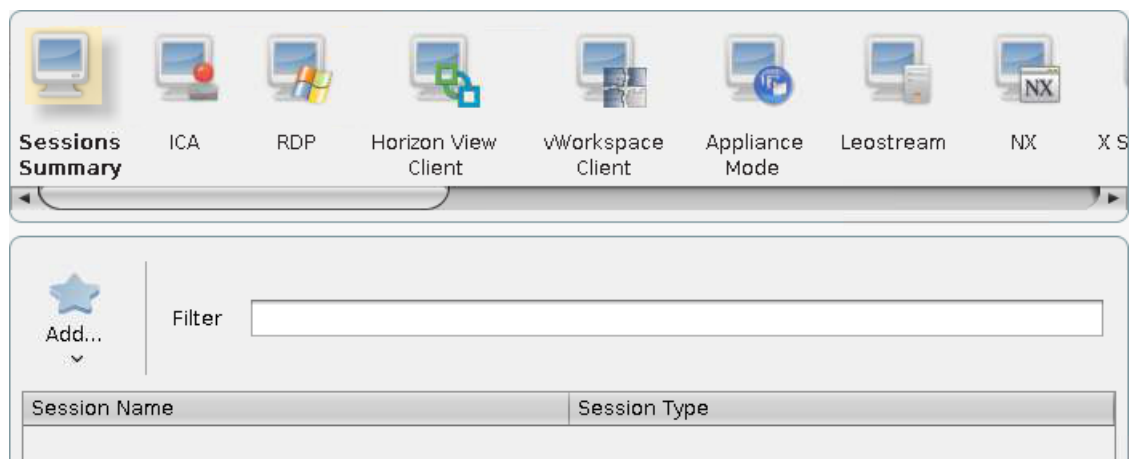


Figure 11: Session overview

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

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

For each session there is a configuration page entitled **Desktop Integration** on which the following actions can be performed:

- Determining the look of the session on the local desktop
- Setting up the name of the session

Note: None of these characters can be used in the session name: \ / : * ? " < > | [] { } ()

- Selecting the session start options (autostart, restart)
- Enabling hotkey use

5.1. Citrix Receiver selection

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

The preset **Standard** setting now corresponds to Citrix Receiver 13.1.3. Previously, Version 12 was preset.

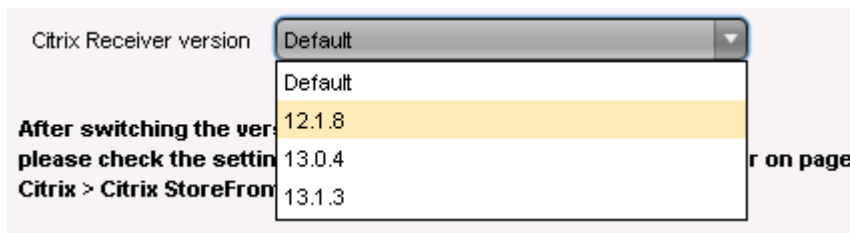


Figure 12: Citrix Receiver selection

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

5.2. Citrix ICA - global settings

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

These are the standard values for all Citrix sessions. Most of these properties, in particular the color depth, resolution and the server IP or server name, can be changed separately for each session.

Both versions of Citrix Receiver client are available - Citrix Receiver 12 and Citrix Receiver 13. As default the client version 12 will be used and you can activate version 13 in **IGEL Setup→Sessions→Citrix→Citrix Receiver Selection→Use Citrix Receiver 13**.



Figure 13: Citrix Receiver 13 Activation

Please note that there are a lot dependencies when changing the version of Citrix Receiver. There are some hints in the IGEL Setup application and a feature comparison of both versions can be found in our FAQ: *Citrix Receiver Feature Matrix* <http://faq.igel.com/otrs-igel/public.pl?Action=PublicFAQZoom;ItemID=619>

IMPORTANT: Citrix Receiver 13 does currently not support Kerberos authentication!

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

5.2.1. Server location

The **Server Location** option - also referred to as server browsing - allows you to bring up via the Citrix ICA client connected to the network a list of all Citrix servers and all published applications which are accessible via the network and use the selected browsing protocol.

The standard functionality for this option is **Auto-Locate** (Broadcast). With this function, the ICA client sends a "Get nearest Citrix server" package. The address of the first Citrix server to reply then functions as the master ICA browser.

You can also 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 does not support 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.

5.2.2. Local logon

Use Kerberos pass-through authentication in all ICA sessions	<p>This option enables single sign-on for all ICA sessions if Log on to the thin client with AD/Kerberos is configured.</p> <p>The server too must be configured for pass-through 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.</p> <p>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.</p>
Use local logon window	If this option is enabled, you will need to enter the password again when logging on.
Restart 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.
Pre-populate logon information	The logon window is pre-populated with the user name and domain.
Show domain	Shows the domain entry in the logon window.
Use client name as user name	This setting may help to resolve reconnection problems during load balancing.
Allow logging on with smartcard	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.
smartcard	Allows local access to smartcards and tokens from various manufacturers.

5.2.3. 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.

5.2.4. Keyboard / hotkey assignment

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. It 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 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**.

5.2.5. Mapping

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

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. On this page, you can specify which folders or drives are mapped during the logon. This then applies for all ICA connection sessions.

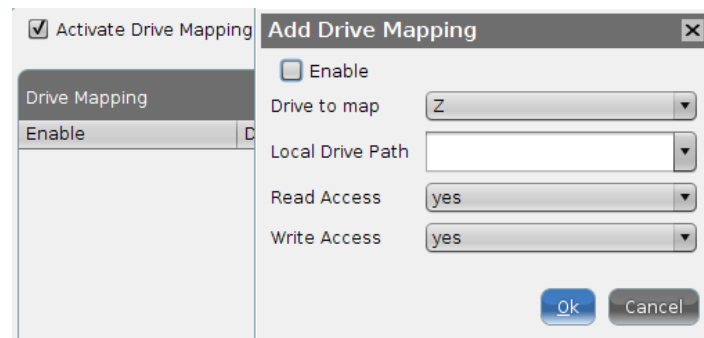


Figure 14: Drive mapping

The **Enable 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.

The procedure for setting up drive mappings is as follows:

1. Click on **Add** to bring up the mapping window.
2. Select a **target drive** 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 path name of the local directory to which the mapping is to refer.

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

COM ports - serial connections

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 **Add** under **COM Port Device**.

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

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

Printers

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 printer jobs in a queue, you need to install the printer on the server.

Device support / virtual communication channels

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.

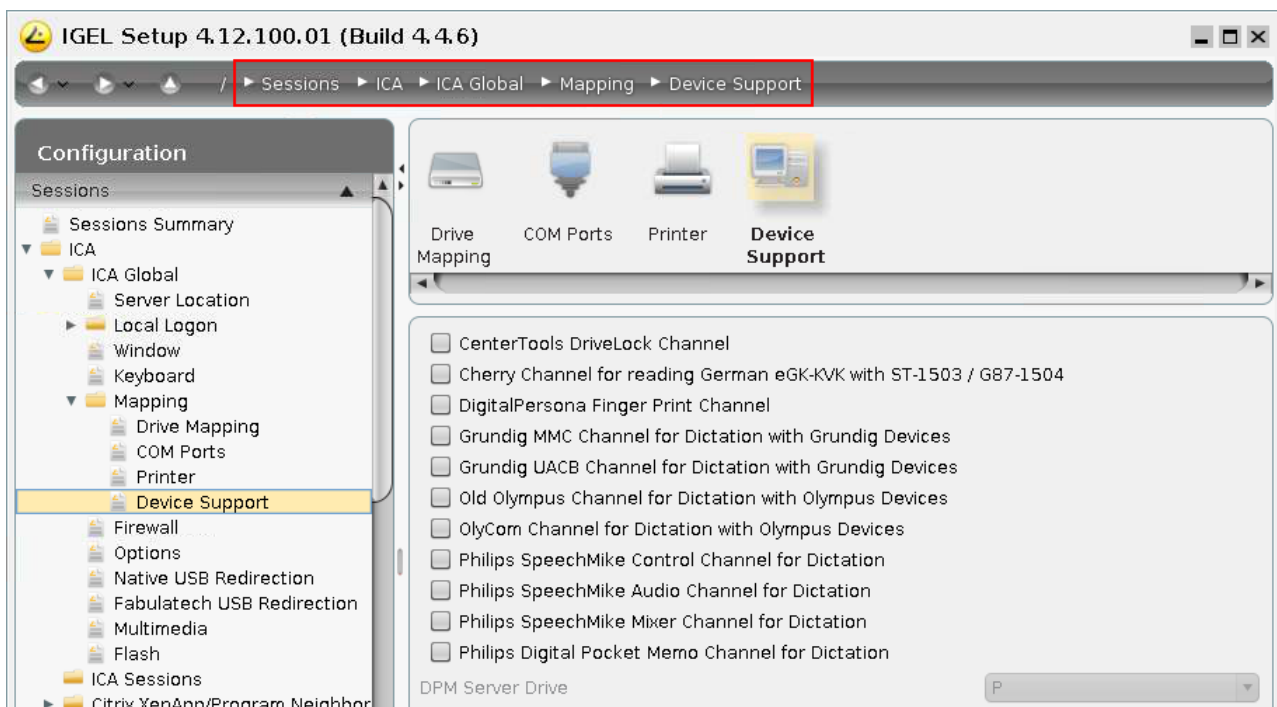


Figure 15: Supported devices

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

DriveLock

The virtual DriveLock channel (ICA protocol) is included in the UDLX from Version 4.11.100 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.

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 device settings **Devices→Storage Devices→USB Storage Hotplug**, as they can influence the USB devices during the Citrix session.
- Install and enable the DriveLock channel in the Universal Desktop setup under **Sessions→ICA→ICA 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](#)

DigitalPersona authentication

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).

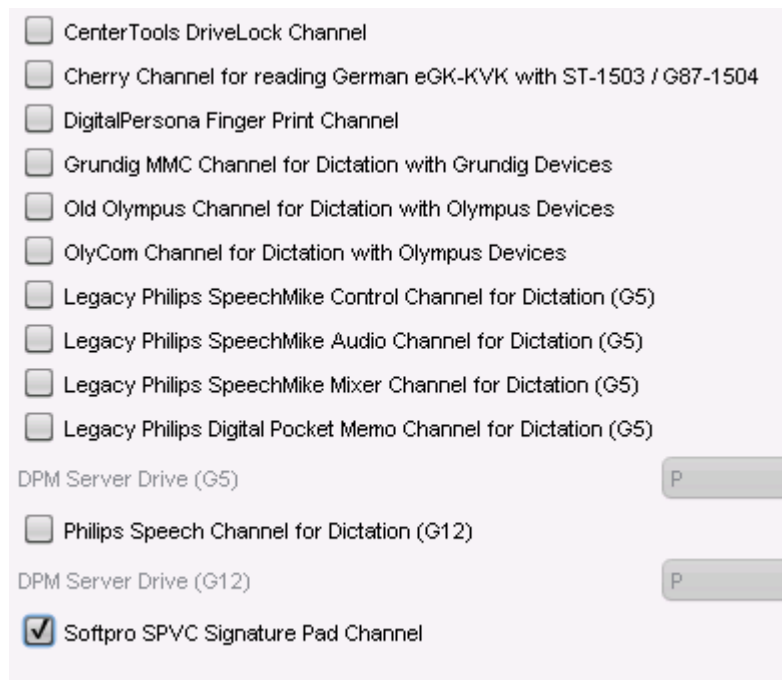
When used in conjunction with the DigitalPersona U.are.U 4500 fingerprint readers which are connected to IGEL thin clients via USB, the software provides a secure and quick means of authentication on virtual desktops.

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

Softpro SPVC Channel

- 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.



☐ CenterTools DriveLock Channel
☐ Cherry Channel for reading German eGK-KVK with ST-1503 / G87-1504
☐ DigitalPersona Finger Print Channel
☐ Grundig MMC Channel for Dictation with Grundig Devices
☐ Old Olympus Channel for Dictation with Olympus Devices
☐ OlyCom Channel for Dictation with Olympus Devices
☐ Legacy Philips SpeechMike Control Channel for Dictation (G5)
☐ Legacy Philips SpeechMike Audio Channel for Dictation (G5)
☐ Legacy Philips SpeechMike Mixer Channel for Dictation (G5)
☐ Legacy Philips Digital Pocket Memo Channel for Dictation (G5)
 DPM Server Drive (G5) P
☐ Philips Speech Channel for Dictation (G12)
 DPM Server Drive (G12) P
☒ Softpro SPVC Signature Pad Channel

Figure 16: Softpro SPVC channel

5.2.6. Firewall

Use alternative 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.
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 in the **Server Location** field in **Global Settings for ICA**.

5.2.7. ICA global options

On this page, 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 warning sounds	This option allows you to disable Windows warning sounds.
Use backing store	The X Server temporarily stores hidden desktop 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.
Caching	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 also specify the minimum size of bitmap files which are to be stored in the cache as well as the directory in which the files can be stored locally.

An excessively high setting can mean that the thin client has too little storage space for its own system and other applications. If in doubt, you can 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 pass-through in Program Neighborhood sessions	Allows the use of Kerberos pass-through authentication in the Citrix Program Neighborhood session.

5.2.8. 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.

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/> (<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 27).

5.2.9. Multimedia redirection

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.

☒ Enable Multimedia Redirection

☒ HDX Realtime WebCam Redirection

HDX WebCam frame rate: 5

HDX WebCam quality: 16

HDX WebCam width: 352

HDX WebCam height: 288

HDX WebCam delay time: 2000

HDX WebCam delay type: 1

☐ Enable HDX Realtime Media Engine

☐ Enable Content Redirection

Figure 17: Multimedia redirection

To improve multimedia playback on the remote desktop, follow the procedure below:

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.

5.2.10. Flash redirection

Depending on the performance of the thin client, Citrix HDX Mediastream 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→Flash Player**.

5.2.11. Codec

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

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

If Version 12.x of the Citrix Receiver is selected, this setup page cannot be edited.

5.3. Citrix ICA - Sessions

If a session is created or edited, you can change the ICA session settings if they differ from the global settings.

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

5.3.1. Server

Browser protocol	Allows you to select the protocol needed for transmission or the global standard setting
Do not use standard server location	Lifts the standard server requirement – for each protocol separately
Server	<p>By clicking on the Search button, you send a transmission signal which queries all available servers and published applications.</p> <ul style="list-style-type: none"> • 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 one of the published applications is selected, 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.
Work directory	Details of the path name of the work directory for the application

5.3.2. Logon

Use Kerberos pass-through 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 pass-through authentication. When launching the ICA session, it is no longer necessary to enter a user name and password again.
Use pass-through 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 they no longer need to be entered again when launching a session.
User, password, domain	A user name, password and domain for the ICA session can be entered here. These details are automatically forwarded to the server and no longer need to be entered on the logon screen.
Hide password protection before logging on	This option switches the Windows splash screen on and off. This option must be disabled when logging on to Windows using a smartcard!

5.3.3. Window settings

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 standard setting for color table	The color table is preset on a global basis. You can approximate it for this session.
Window size	By disabling the full-screen mode , you can choose between the global default setting and a session-specific setting.
Start monitor (Dualview)	Specifies which monitor in an environment with several monitors is to be used for the session.
Enable seamless window mode	The seamless window 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.

5.3.4. Firewall

Use alternative 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.
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 in the **Server Location** field in **Global Settings for ICA**.

5.3.5. Reconnect

You can edit **Global Settings for ICA** for the **Reconnect** option.

5.3.6. Options

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

Compression	Reduces the amount of data transmitted via the ICA session. This results in a reduction in network traffic to the detriment of CPU performance. If you connect your server(s) via WAN, you should use compression. If you use a relatively low-performance server and only work in one LAN, you should disable this option.
Caching image data	Enables caching in the cache memory (configured in the global ICA settings) for each session. This makes sense if you use a number of ICA sessions but only one or two sessions are critical from a network bandwidth point of view or are intensively used during the day. In this case, you should reserve the cache memory for these settings.
Encryption method	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.
Audio transfer	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.
HDX latency reduction	Improves the performance of connections with a high level of latency by immediately reacting to keyboard entries or mouse clicks. This makes the thin client feel more like a normal PC.
Mouse click feedback	The mouse pointer immediately turns into an hourglass symbol, thus providing visual feedback in response to a mouse click.
Local text echo	Displays text entered more quickly and avoids latency within the network. Select a mode from the drop-down list: <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 AUTO if you are not sure how fast the connection is.

HDX must be enabled and configured on the Citrix server for it to work.

5.3.7. 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.

5.4. Citrix StoreFront / Web Interface

Some of the settings are already configured under Global settings for ICA and in the *ICA session setup* (page 31).

- Select the start options for the Citrix XenApp session, see **Desktop integration**.

5.4.1. Connections

- Under **Server Location**, specify the master browsers in which published applications can be searched for.

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.

- Click on **Use Citrix XenApp Service Page** to obtain settings from the server and configure published applications via the Citrix XenApp service page.

5.4.2. Options

Specify audio, keyboard and display options if they differ from the global settings.

☒ Use server settings for all Options (Citrix XenApp)

☒ Client Audio

☐ Overwrite local Client Audio setting with server setting

Audio Bandwidth Limit: medium

Color Depth: Global setting

Window Size: Seamless|Desktop

☐ Restrict full screen sessions to workarea

Handling of keyboard shortcuts: Server setting

Figure 18: Citrix Storefront Options

5.4.3. Logging on and off

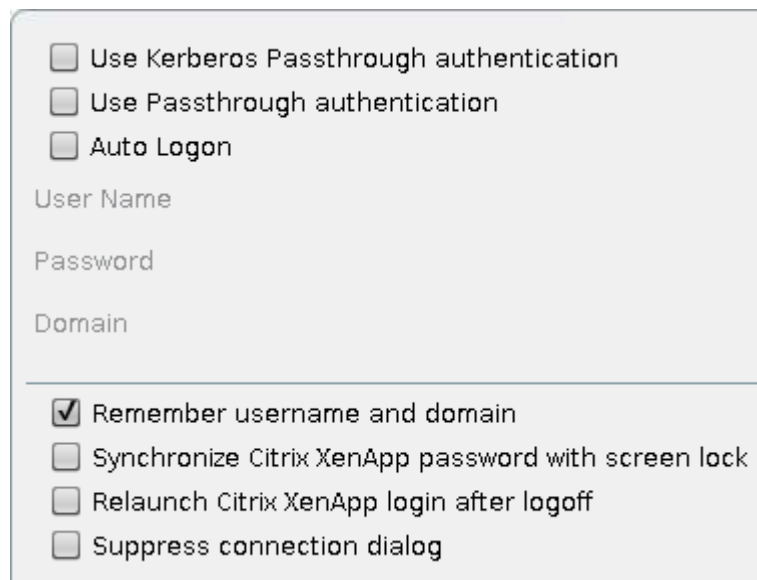


Figure 19: Citrix Storefront logon

- Enable **Use Kerberos Pass-Through Authentication** in order to use 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.
- Enable **Use Pass-Through Authentication** in order to use temporarily stored logon data for listing and launching applications.
- Enable **Log On Automatically** in order to use the pre-set logon data when connecting to the server.

You can synchronize the password for the lock screen application (xlock) with the PN password.

The logoff option generates a **PN Logoff** button allowing you to log off from PN via a hotkey.

5.4.4. Appearance

You can configure the XenApp/Program Neighborhood applications in such a way that they are displayed in various areas of the local system, e.g. on the local desktop or in the Start menu.

- Enable **Scale Symbols for the Start Menu** to automatically adjust the size of the application symbol.

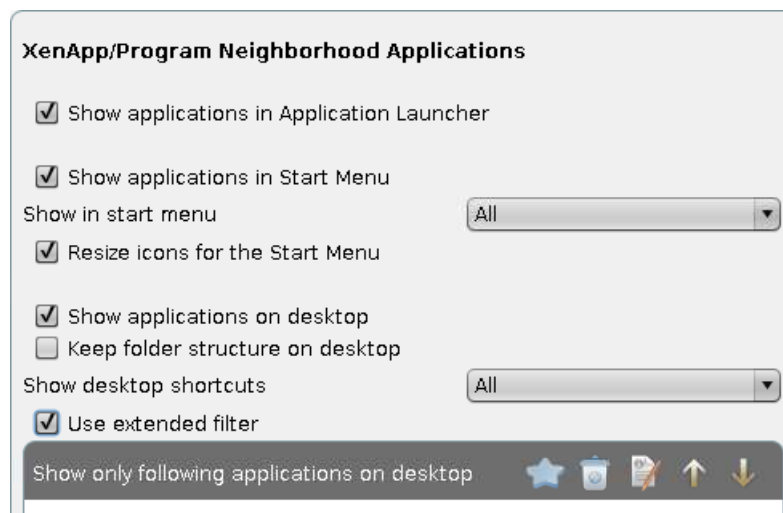


Figure 20: Citrix Storefront layout

5.4.5. Change password

Specify how a connection for changing a password is to be established.

Generic session	Searches for servers/applications and subsequently establishes a connection
Pre-configured 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.

5.4.6. Reconnecting and updating

➤ Select the required option when reconnecting with 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.

5.4.7. Log off

If the **Use hotkey** option is enabled, you can log off from a session using a key combination. The combination consists of **modifier** keys such as **Ctrl** (Control), **Alt** and **Shift** and a number or a letter as a **hotkey**.

5.4.8. 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.

5.5. Citrix Access Gateway

With the **Citrix Access Gateway (CAG)** client, you can establish a VPN connection to a CAG standard server 4.6. The VPN connection is an SSL tunnel. A certificate is transferred from the server to the client in the process. 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.

5.6. Appliance mode

The **appliance mode** can be enabled for the following session types (provided that they are available on your system):

- VMware Horizon
- Citrix XenDesktop
- RHEV/Spice
- Imprivata
- RDP Multipoint Server

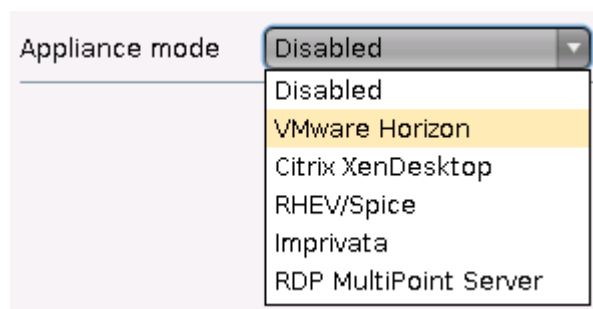


Figure 21: Session Types in Appliance Mode

If you run an appliance mode, no other application access is possible. Only the server session for the specified virtualization server will be shown.

The system hotkey **Ctrl+Alt+S** for launching the IGEL setup application does not work in the appliance mode. Please use **Ctrl+Alt+F2** instead.

1. Enable one of the appliance options.

2. Further configuration:

- For VMware Horizon, Citrix XenDesktop and RHEV/Spice:

Configure access to the relevant server, i.e. to the VMware Horizon server, XenDesktop delivery server or RHEV/Spice on the current setup page as well as in the global settings for the relevant session type.

- For Imprivata:

Configure the **URL of the server**, the **path to the application** and further settings on the current setup page.

- For RDP Multipoint Server:

IGEL Linux will find one or more RDP Multipoint Servers itself if they are in the same network. In addition, they must obtain their IP address from the same DHCP server as the thin client. In the appliance mode, you will see a selection list with servers to which you can connect:

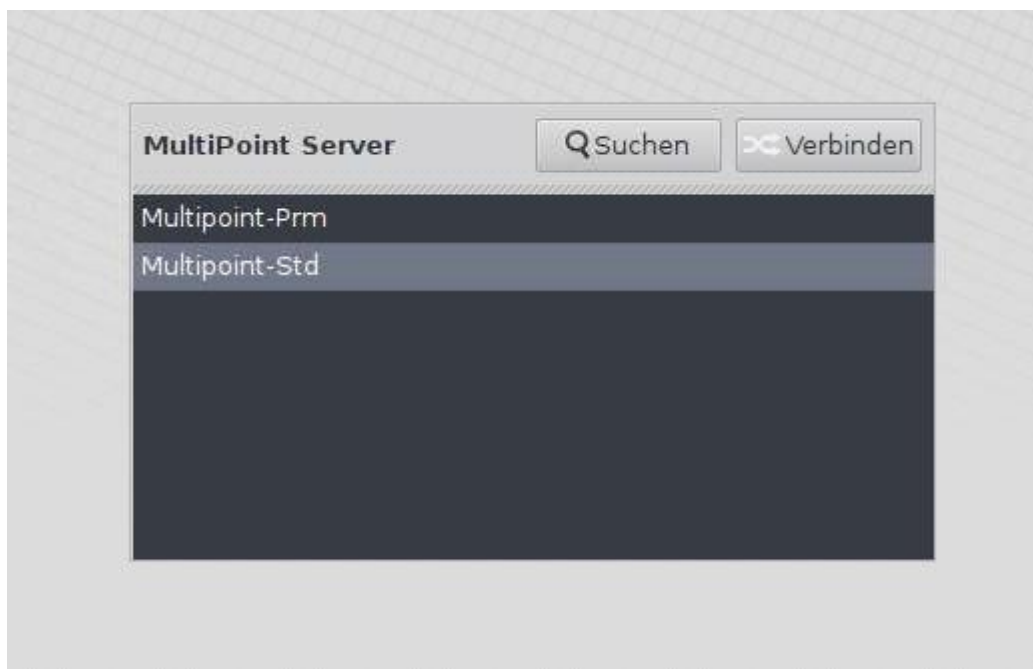


Figure 22: List of RDP Multipoint Servers

5.7. SSH Session

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.

5.8. Firefox browser

In order to allow central configuration via the IGEL UMS, the original configuration parameters for the Firefox 38.1.0 ESR web browser are assigned to the IGEL setup. These global settings can be changed for each browser session.

5.8.1. Browser Global

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

When Firefox starts	Show my home page ▼
Startuppage	http://www.igel.com
Display resolution	System setting ▼
Minimum font size	None ▼
<input checked="" type="checkbox"/> Show browser splash screen	

Figure 23: Settings under Browser Global

- Select an appropriate start screen from the following options:
 - Start with a blank page
 - Show my home page
 - Resume previous session
 - Load the last visited page
- Under **Start Page**, specify the URL if you would like to launch Firefox with the start page.
- Select the desired **display resolution** in DPI - e.g. 72 for medium-sized screens or 96 for large screens.
- Optionally, specify a **minimum font size**.
- If necessary, disable the **browser splash screen** – it is enabled by default.

Tabs

In this area, you determine the settings which affect the individual tabs in the browser.

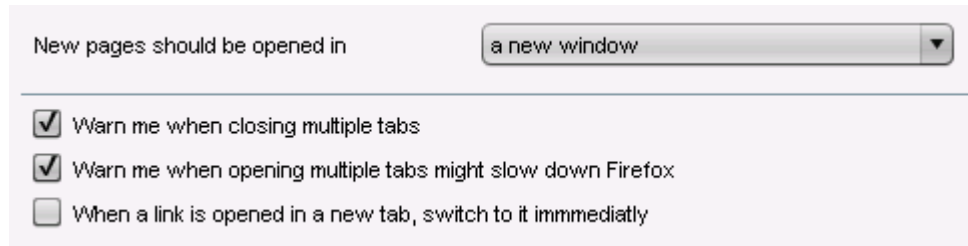


Figure 24: Tabs settings

- Select whether a new **browser page** is to be opened in the current browser window, in a new browser window or in a new tab.

By default, you are warned if you close a number of tabs at the same time or if too many tabs are open and this is slowing down browser performance.

- Uncheck the relevant checkboxes to disable the warnings.

By default, tabs which are opened from the left open in the foreground.

- Uncheck the **When a link is opened in a new tab, switch to it immediately** checkbox in order to open these tabs in the background.

Contents

In this area, you can define all settings which affect pop-up windows and downloads.

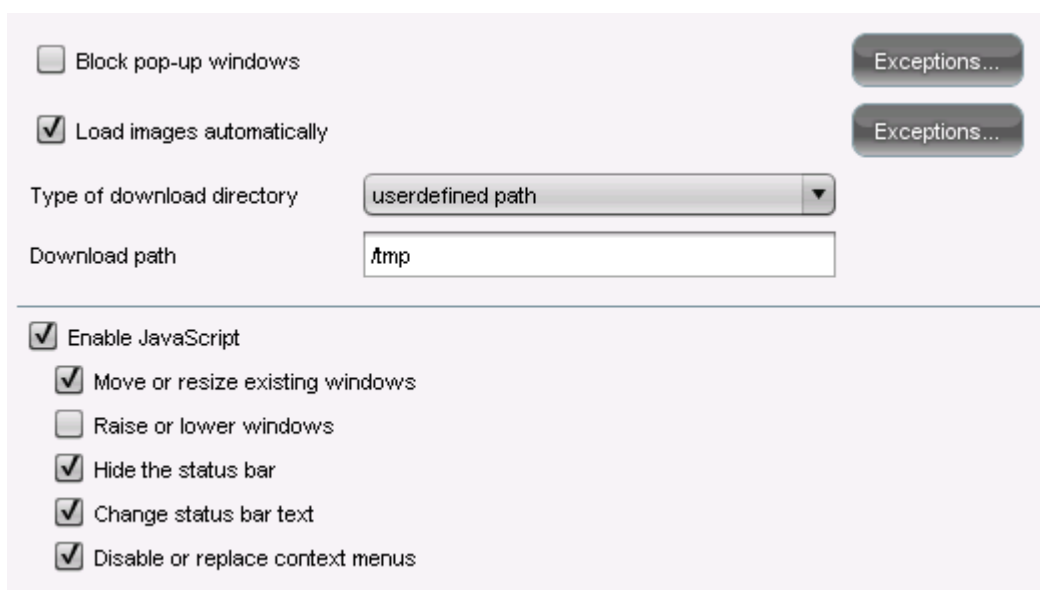


Figure 25: Browser content settings

Block pop-up windows is enabled by default.

- Uncheck the checkbox in order to allow pop-ups when loading pages.
- Specify **exceptions** in order to exclude specific pop-ups from the setting.

Load images automatically is enabled by default.

- Uncheck the checkbox in order to prevent images being loaded automatically. This will allow browser pages to load more quickly. Here too, you can define **exceptions**.

The **download directory** can be defined here. If you select **User-defined path**, the exact path must be given.

For reasons of space, you should not use a local path.

Enable JavaScript is enabled by default. The exact settings can be defined here.

- Uncheck the checkbox in order to disable JavaScript.

Print

In this area, you can set the **default paper size** for the printer.

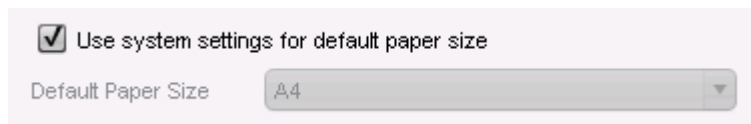


Figure 26: Paper size setting

Proxy

In this area, you can select the proxy configuration. You have four options:

Direct connection to the Internet	Enable this option if you do not wish to use a proxy.
Manual proxy configuration	Configure the proxy individually. Under No proxy for , you can list entries for which no proxy will be used, e.g. <code>.mozilla.org</code> , <code>.net.de</code> , <code>.net.nz</code> . Under Proxy realm , give details of the area for which the proxy is responsible. This information must be provided in order for automatic logon to work. Leave the Proxy realm , User name and Password boxes empty in order to allow manual entries when logging on.
Automatic proxy configuration	Specify the URL for automatic proxy configuration.
System-wide proxy configuration	Use the network/proxy settings from the IGEL setup.

Figure 27: Proxy settings

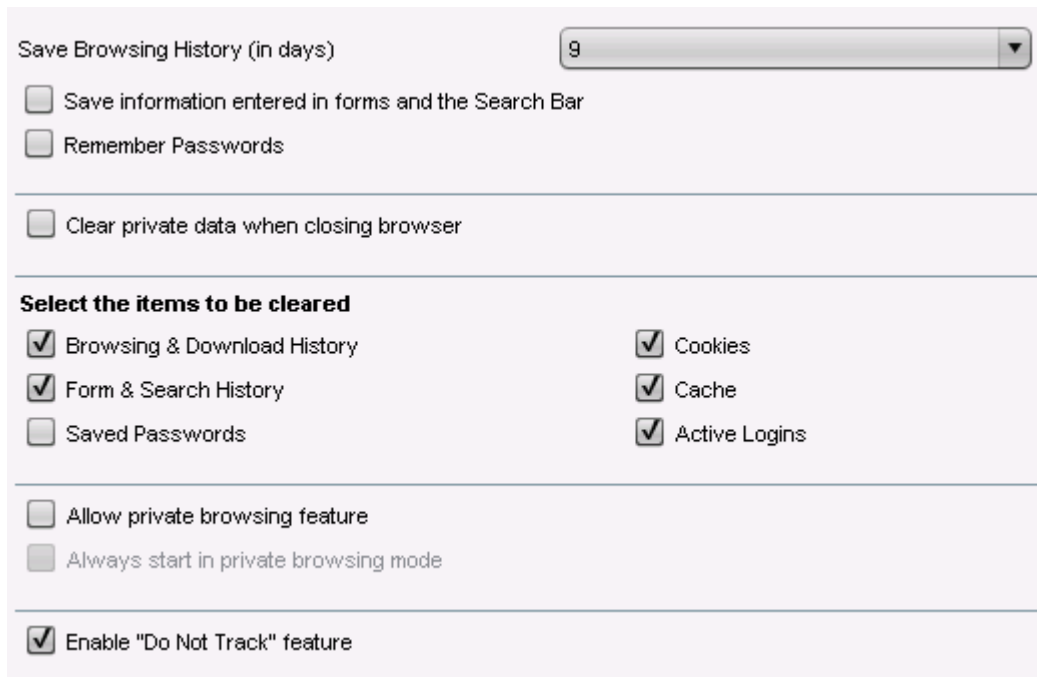
Data protection

Here, you can configure data protection settings for the following areas:

- *Private data* (page 45)
- *Protection against tracking* (page 45)
- *Browser address bar* (page 46)

Private data

In this area, you can define settings for your browsing history and private data.



The screenshot shows the 'Data Protection' settings in a browser. At the top, there is a dropdown menu for 'Save Browsing History (in days)' set to '9'. Below this are three checkboxes: 'Save information entered in forms and the Search Bar' (unchecked), 'Remember Passwords' (unchecked), and 'Clear private data when closing browser' (unchecked). A section titled 'Select the items to be cleared' contains two columns of checkboxes: 'Browsing & Download History' (checked), 'Form & Search History' (checked), 'Saved Passwords' (unchecked), 'Cookies' (checked), 'Cache' (checked), and 'Active Logins' (checked). Below this section are two more checkboxes: 'Allow private browsing feature' (unchecked) and 'Always start in private browsing mode' (unchecked). At the bottom, the 'Enable "Do Not Track" feature' checkbox is checked.

Figure 28: Data protection settings

- Define whether, and if so, in how many days you would like to save your **browsing history**.

Any history created before the defined date will be lost when you restart your browser.

- Define whether you would also like to save **entries in forms and search bars** or **passwords** in your history.
- Enable **Clear private data when closing browser** if you would like to delete at the end of the browser session the data created when surfing.
- Specify exactly which private data you would like to delete.
- Enable **Allow private browsing feature** in order to use Firefox in private mode where no data are stored.
- Enable **Launch browser in private mode as standard** if Firefox should always start in private mode.

Protection against tracking

In this area, you can specify how you would like to protect yourself against tracking on the Internet.

- ☒ Enable "Do Not Track" feature
- ☒ Enable built-in tracking protection

Figure 29: Do not track

- Disable the **Do not track feature** if you would like to allow websites to track your activities.

The **Do not track (DNT) feature** is enabled by default. With this function, you tell a website that you do not want to be tracked by third parties, e.g. for behavioral advertising. Do not track transfers an HTTP header every time that you request data from the Internet. In this case, the site visited decides what it will do with the privacy request.

- Disable **tracking protection** if you do not wish to use the tracking protection provided by Firefox.

With protection against the tracking of activities, you can control your online privacy. Even if Firefox includes a **do not track feature** which tells websites that you do not want your surfing habits to be recorded, companies do not have to adhere to it. The protection against tracking in Firefox puts you in control by blocking domains and websites which are known for tracking users. In this case, Firefox actively blocks content which records the user's surfing habits.

Address bar

Here, you can specify further rules in order to tailor the behavior of the address bar to your needs:

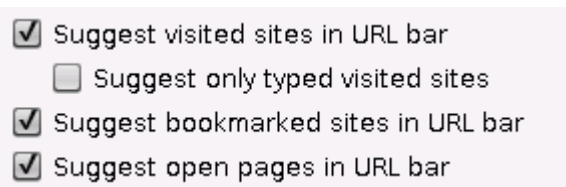


Figure 30: Further data security settings

- When typing in a URL, would you like to be given suggestions from **history entries**? Or only from entries that you actually typed in?
- Or would you like to be given suggestions from your **bookmarks**?
- Should **tabs that were previously opened** be suggested as a destination?

Security

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

Safe browsing is disabled by default.

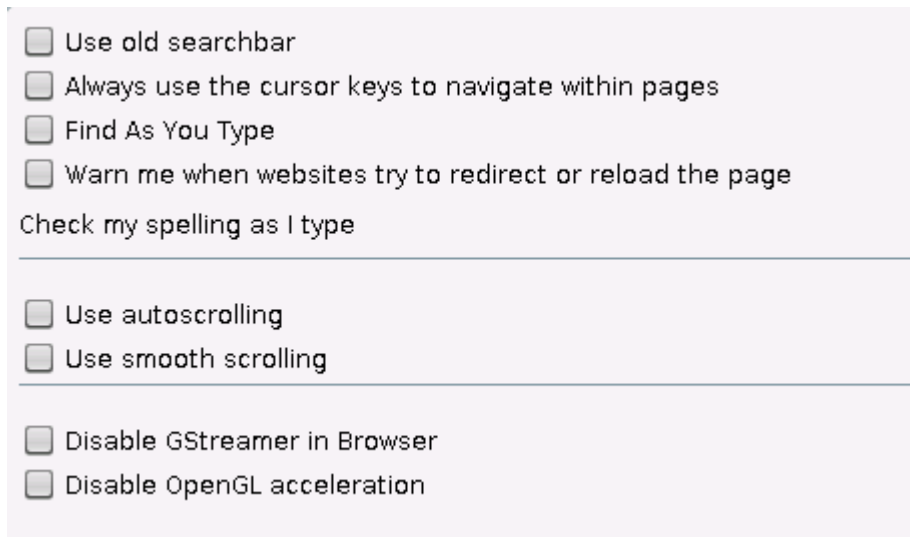
- Check the checkbox in order to enable integrated phishing protection.

Malware protection is disabled by default.

- Check this checkbox in order to download malware blacklists and check downloads for malware.

Advanced

In this area, you can define settings for entry options, scrolling and websites.



The screenshot shows a settings window with a light purple background. It contains several checkboxes grouped into three sections by horizontal lines. The first section includes 'Use old searchbar', 'Always use the cursor keys to navigate within pages', 'Find As You Type', and 'Warn me when websites try to redirect or reload the page'. Below these is a text input field labeled 'Check my spelling as I type'. The second section includes 'Use autoscrolling' and 'Use smooth scrolling'. The third section includes 'Disable GStreamer in Browser' and 'Disable OpenGL acceleration'.

- ☐ Use old searchbar
- ☐ Always use the cursor keys to navigate within pages
- ☐ Find As You Type
- ☐ Warn me when websites try to redirect or reload the page
- Check my spelling as I type

- ☐ Use autoscrolling
- ☐ Use smooth scrolling

- ☐ Disable GStreamer in Browser
- ☐ Disable OpenGL acceleration

Figure 31: Advanced settings

- Enable **Always use the cursor keys to navigate within pages** if you would like to use this function.
- Enable **Find as you type** if you would like to see search suggestions while typing.
- Enable **Warn me when websites try to redirect or reload the page** if you would like to use this function.
- Select **Check spelling as I type** and specify whether you would like this to apply to text fields only or to text fields and text lines.
- If you select **Use autoscrolling**, you can move the view of a website in the display area vertically by pressing the middle mouse button and moving the mouse.
- Select **Use smooth scrolling** in order to scroll line by line or pixel by pixel.
- Enable **Disable GStreamer support for the browser** if you have problems when playing back videos on HTML5 websites.
- Enable **Disable OpenGL acceleration** if your client has problems with OpenGL applications.

Encryption

In this area, you can determine the settings for encryption protocols, certificate validation and authentication solutions.

Encryption



Minimum required encryption protocol	SSL3
Maximum supported encryption protocol	TLS 1.2
When a website requires a certificate	Select one automatically

Figure 32: Encryption settings

- Select a minimum and maximum **encryption protocol**. The following are available to choose from
 - **SSL3**
 - **TLS 1.0**
 - **TLS 1.1**
 - **TLS 1.2**
- Determine what is to be done **if a website asks for a security certificate**.
- Click on **Show certificates** in order to manage the certificates used by Firefox.

Certificate validation



Certificate Validation (Online Certificate Status Protocol)	Validate a certificate if it specifies an OCSP server
Response Signer	Builtin Object Token:IPS CLASE1 root
Service URL	http://ocsp.ips.es/
<input type="checkbox"/> When an OCSP server connection fails, treat the certificate as invalid	

Figure 33: Certificate settings

- Define the **Certificate validation**. The following are available to choose from:
 - **Validate a certificate if it specifies an OCSP server**
 - **Do not use OCSP for certificate validation**
 - **Validate all certificates using the following OCSP server**

In this case, you will need to give details of the **response signer** and the **service URL**.

If you have selected validation with OCSP, you can enable the **When an OCSP server connection fails, treat the certificate as invalid** option.

Authentication

- Select an authentication solution from the following products in order to protect your network:



A list of authentication solutions, each preceded by an unchecked checkbox:

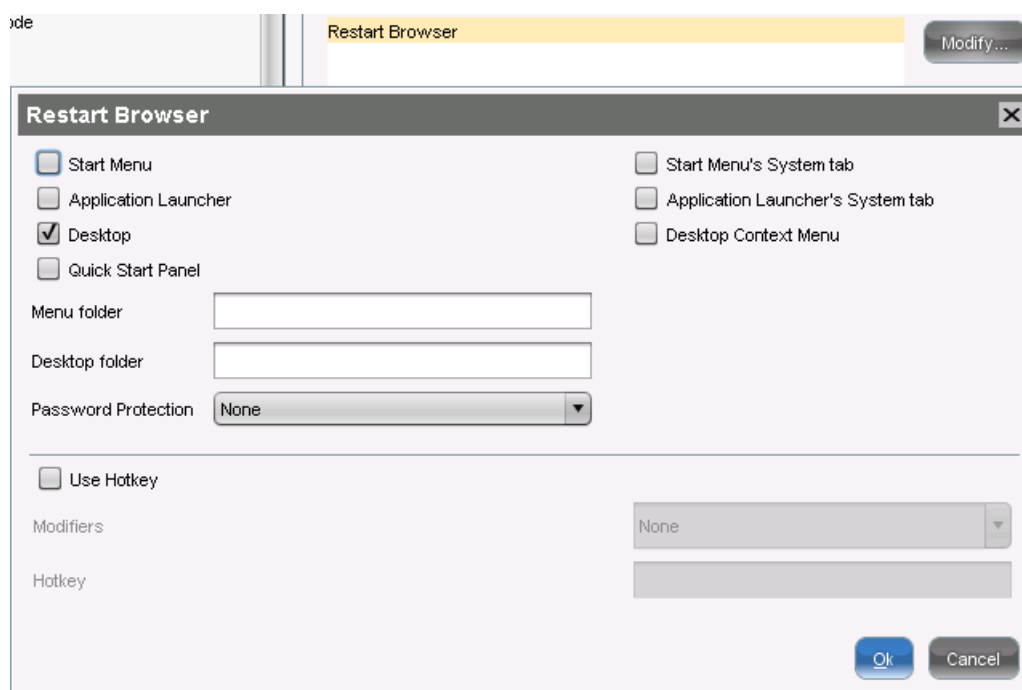
- ☐ Use "Aladdin eToken" Security Device
- ☐ Use "Gemalto" Security Device
- ☐ Use "IDProtect" Security Device
- ☐ Use "SafeSign" Security Device
- ☐ Use "SecMaker" Security Device
- ☐ Use TCOS 3 NetKey Security Device
- ☐ Use TCOS 3 SigG Security Device
- ☐ Use TCOS 3 Elster Security Device
- ☐ Use TCOS 3 SD Security Device

Figure 34: Authentication solutions

Commands

In this area, you can specify the settings for certain commands.

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



The screenshot shows a window titled "Restart Browser" with a "Modify..." button in the top right. The window contains the following settings:

- ☐ Start Menu
- ☐ Application Launcher
- ☒ Desktop
- ☐ Quick Start Panel
- Menu folder:
- Desktop folder:
- Password Protection:
- ☐ Start Menu's System tab
- ☐ Application Launcher's System tab
- ☐ Desktop Context Menu
- ☐ Use Hotkey
- Modifiers:
- Hotkey:

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

Figure 35: Commands setting

5.8.2. Firefox Browser Session

The original Firefox parameters are pre-set under **Settings**. The standard settings are carried over from the **Browser Global** setup.

The following settings for the browser session can also be configured:

Window	Allows you to specify the full-screen mode and multi-monitor options as well as the Firefox language / prevent users making changes to the browser / hide the configuration page (about:config) and the printer dialog
Symbol bars and toolbar	Allows you to hide/show toolbar items or complete toolbars in a session / configure a kiosk mode (browser in full-screen mode, restricted access to toolbars and autostart/restart configuration)
Hotkeys	Allows you to enable/disable hotkeys used in the Firefox browser.
Context menu	Allows you to enable/disable items in the browser context menu.

Window settings

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

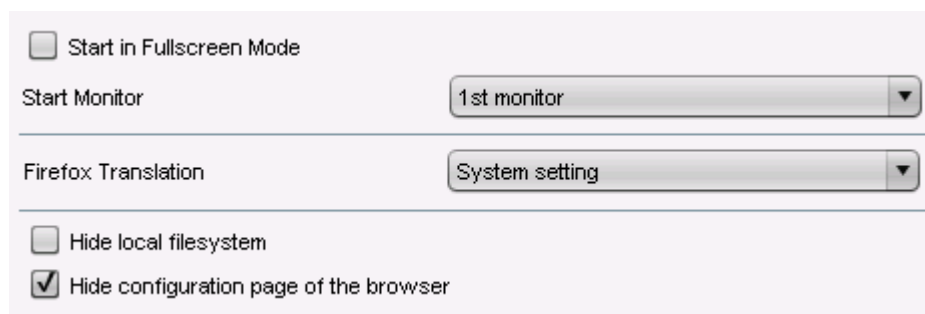


Figure 36: Window settings

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

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:

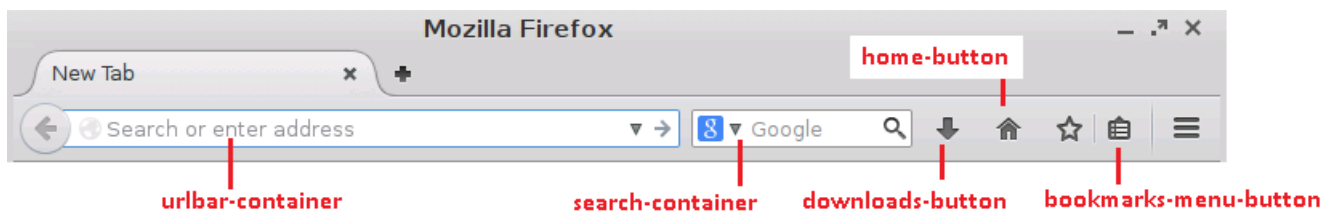


Figure 37: Navigation symbol bar

- Configure the **Application menu**:

The following items are pre-set:

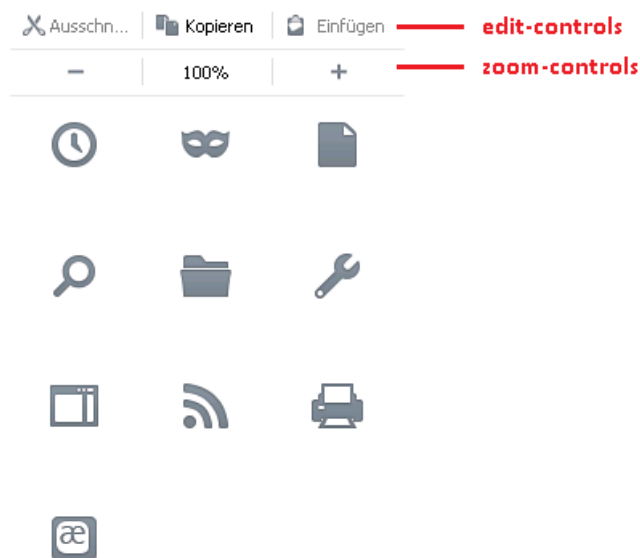


Figure 38: Application menu

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

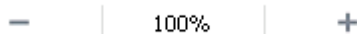
➤ Configure the **Application menu**:

➤ **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



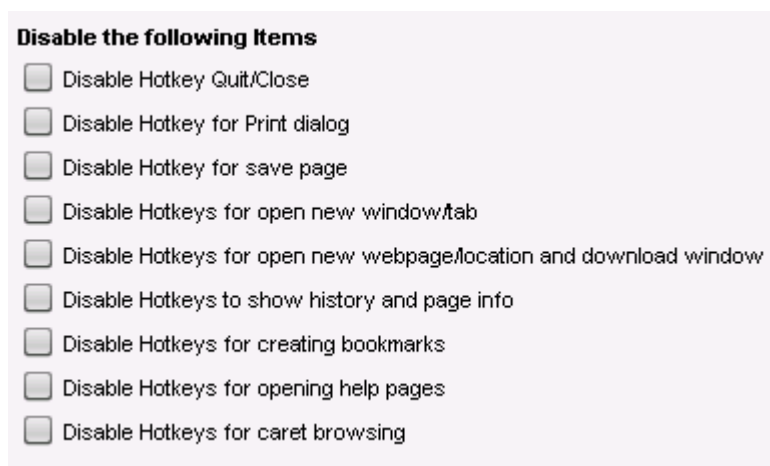
Downloads button



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

Hotkeys

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



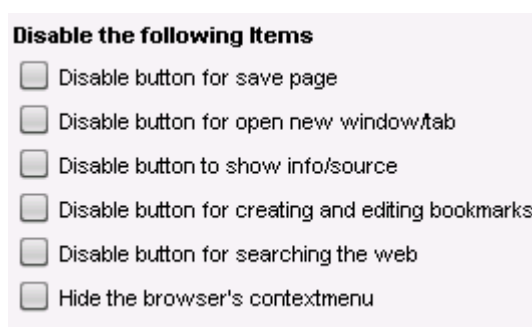
Disable the following Items

- ☐ Disable Hotkey Quit/Close
- ☐ Disable Hotkey for Print dialog
- ☐ Disable Hotkey for save page
- ☐ Disable Hotkeys for open new window/tab
- ☐ Disable Hotkeys for open new webpage/location and download window
- ☐ Disable Hotkeys to show history and page info
- ☐ Disable Hotkeys for creating bookmarks
- ☐ Disable Hotkeys for opening help pages
- ☐ Disable Hotkeys for caret browsing

Figure 39: Hotkeys settings

Context menu

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



Disable the following Items

- ☐ Disable button for save page
- ☐ Disable button for open new window/tab
- ☐ Disable button to show info/source
- ☐ Disable button for creating and editing bookmarks
- ☐ Disable button for searching the web
- ☐ Hide the browser's contextmenu

Figure 40: Context menu settings

5.8.3. Browser Plug-ins

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

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.

The external link for downloading the Flash Player is up to date at the time of release of this software. However, it may change over time.

In addition to the official download source, you can specify your own source in the company network or the pre-configured firmware update source.

If the Flash Player fails to download via the external link, check the current path and file name in the browser as these may have changed in the meantime.

PDF viewer

Here, you can specify whether PDF documents are to be embedded in the browser or displayed in a separate window.

RedHat 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**.

5.9. Media Player

Set up the Media Player for your multimedia applications here.

The following codecs are licensed via either the Fluendo Codec Pack or the MPEG LA Advanced Feature Pack:

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

AC3 is not licensed.

5.9.1. Media Player Global

- Configure universal settings which will apply by default during all Media Player sessions.

If need be, the settings can be changed in the individual sessions.

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

- 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

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

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

- 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 Plug-in

If you would like to use the Media Player as a **browser plug-in**, you can change the configuration values here.

This will affect manually configured Media Player sessions.

5.9.2. 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

- 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

If necessary, you can change the pre-configured settings for the operating components here.

5.10. Java Web Start Session

In order to be able to access Java web applications, you must enter the address of the necessary JNLP file. For example, this may be an IGEL UMS console which can also be run as a Java Web Start application.

5.11. 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.

6. Accessories

Information on other accessories provided by the Universal Desktop can be found [here](#).

6.1. 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.

6.2. Local Terminal

With a terminal session, you can execute local commands via a shell. In this case, the shell is similar to the Windows DOS command prompt.

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`.

6.3. 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**.

6.4. Smartcard Personalization

Configure the options to start the **Smart Card Personalization** (page 119).

6.5. Setup Session

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 17).

6.6. Quick Settings Session

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* (page 17).

6.7. Display switch

In this area, you can define settings for switching displays.

Display selection is disabled by default.

- Enable display selection by enabling one of the **session launching options** under **Accessories→Display Switch**.
- Enable **Use hotkeys** in order to determine a hotkey or an icon for this session.
- If necessary, specify autostart options.
- Define the following settings under **Accessories→Display Switch→Options**:

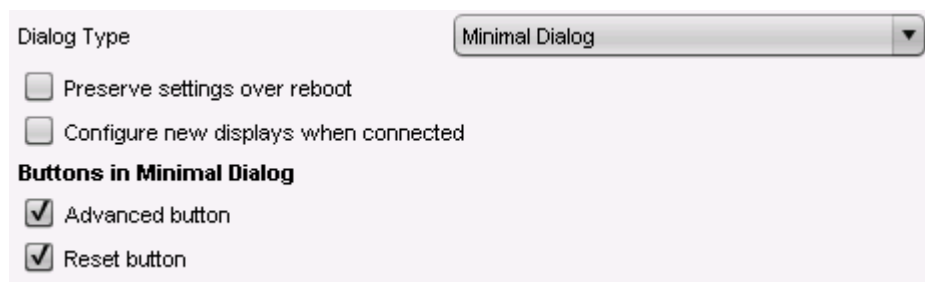


Figure 41: Settings for switching displays

- Under **Dialog type**, specify how the display selection dialog is to look:

Minimal dialog	Works with two displays only.
Advanced dialog	The user themselves can change the resolution or rotation outside the setup.
- Enable **Configure new displays when connected** in order to be able to define settings for newly connected devices which are connected during operation.
- Enable **Preserve settings over reboot** in order to save the display settings so that they can be reused in the event of a reboot.
- Specify the buttons for the minimal dialog:

Advanced	Allows you to jump to the advanced dialog in the minimal dialog.
Reset	Allows you to reset the configuration to the setup settings.

6.8. Application Launcher

- Show the **Setup** and **Application Launcher** on the local desktop or in the start menu, or define hotkeys and the autostart option.

You can hide various items, e.g. buttons for shutting down or restarting the device, from the user.

6.9. Sound Mixer

Use the sound control to adjust the output volume and the input level as well as the balance between the input and output.

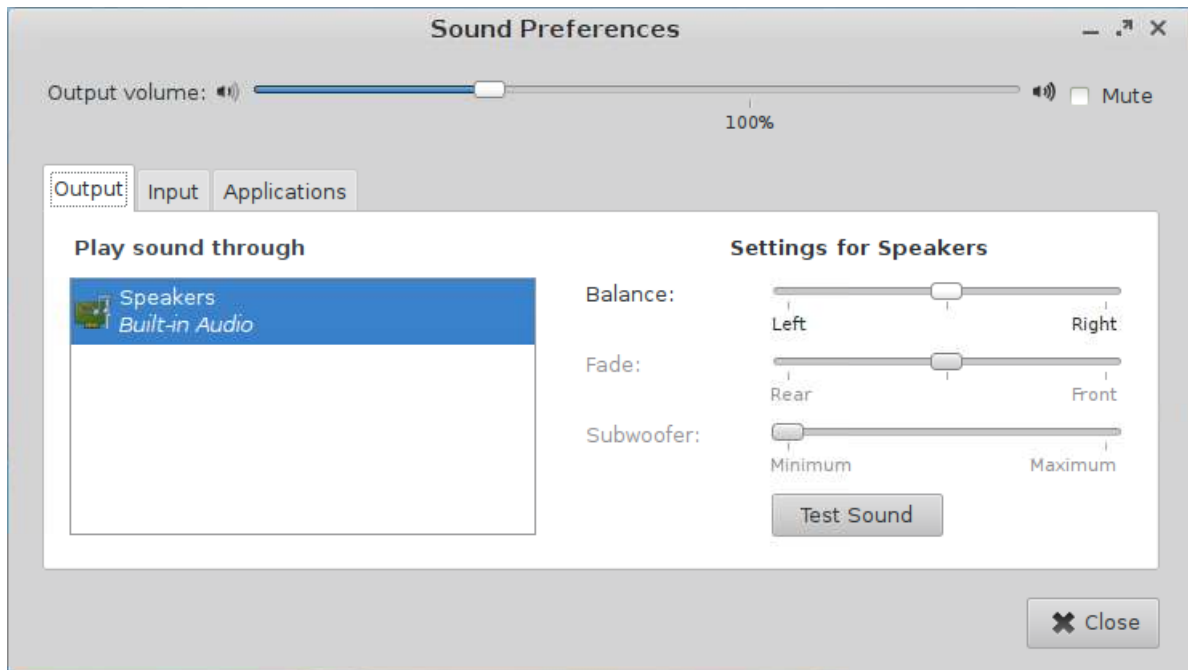


Figure 42: Sound control

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.

6.10. 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).

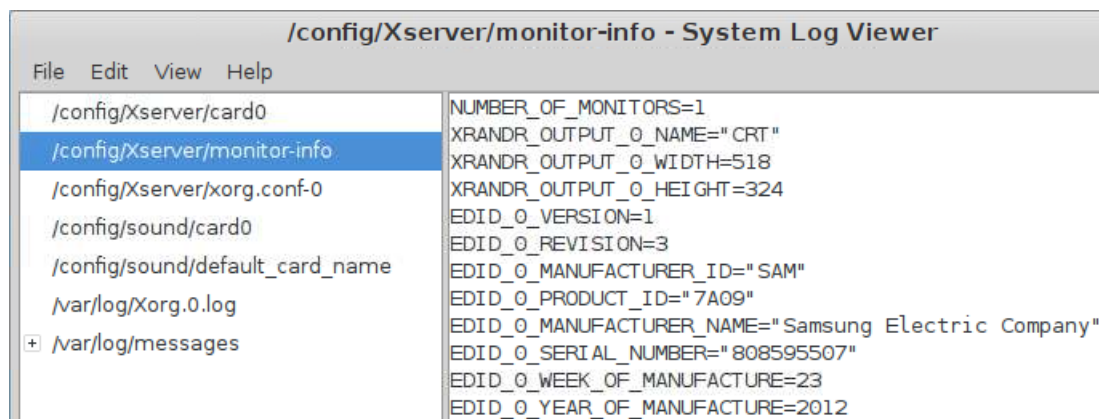


Figure 43: System logs

6.11. UMS Registration

Registration of the thin client in the IGEL Universal Management Suite can also be performed locally. To do this, enter the server address (with port) and the necessary access data. Directories already on the server can be selected directly.

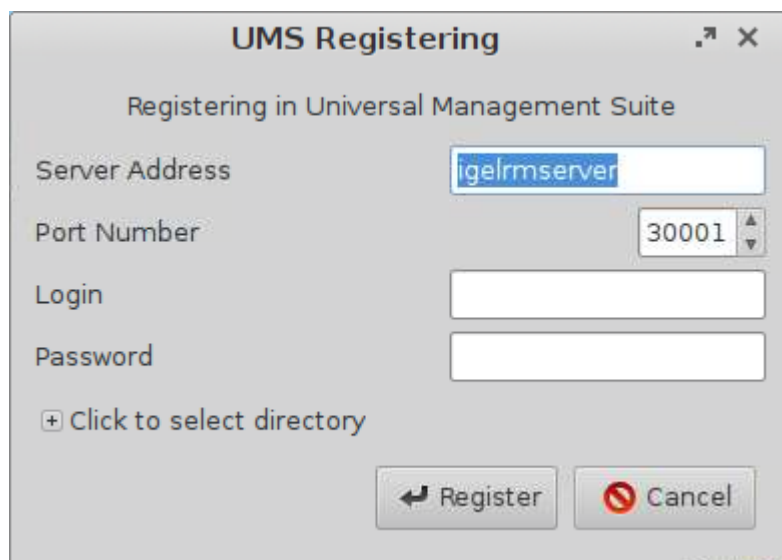


Figure 44: Register thin client on the UMS Server

6.12. Touchscreen Calibration

After launching the calibration program, you will see a pattern with calibration points which must be touched one after another.

6.13. Soft Keyboard (On-screen Keyboard)

Enable the soft keyboard (on-screen keyboard) for use with a touchscreen, e.g. IGEL UD9.

6.14. 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 run 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 run 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>.

6.15. Calibration Pattern

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.

6.16. Commands

The following system commands can be made accessible to the user:

- Log out
- Sort symbols
- Switch off terminal
- Restart terminal
- Restart window manager

6.17. Network Diagnostics

The IGEL Universal Desktop Linux firmware features a number of tools for network analysis. These include:

- *Device information* (page 63)
- *Ping* (page 63)
- *Netstat* (page 64)
- *Traceroute* (page 64)
- *Look-up* (page 64)

6.17.1. 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.)

6.17.2. 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.

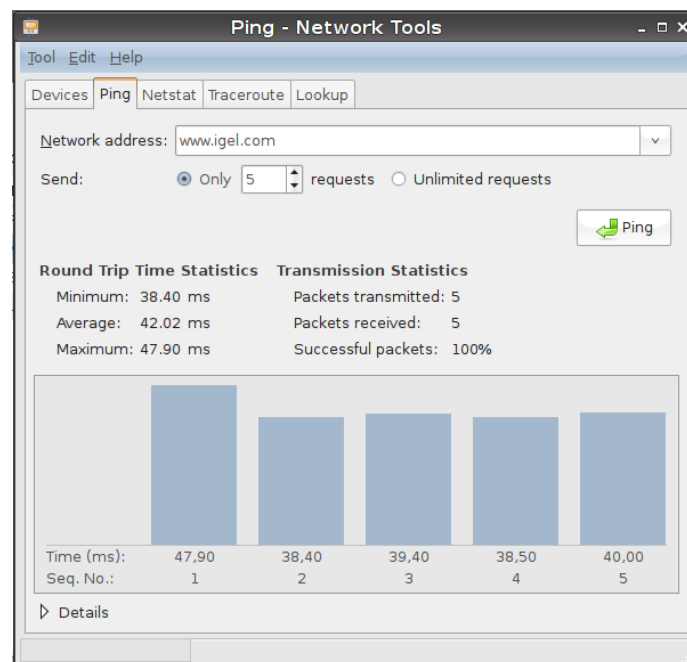


Figure 45: Ping network tools

- Enable **Program→Signal Tone for Ping** to configure the thin client to output an audible signal each time a Ping is sent.

6.17.3. 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.

6.17.4. Traceroute

With **Traceroute**, you can trace the route to a network address.

6.17.5. Look-up

The **Look-up** tool shows various information regarding your network address. The available information types are shown in this screenshot.

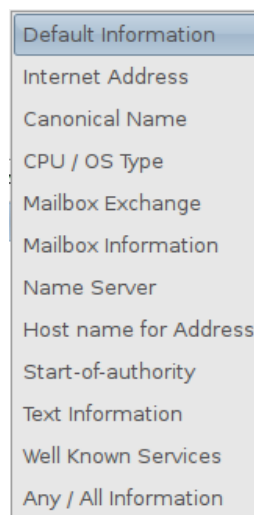


Figure 46: Information types for network address

6.18. 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.

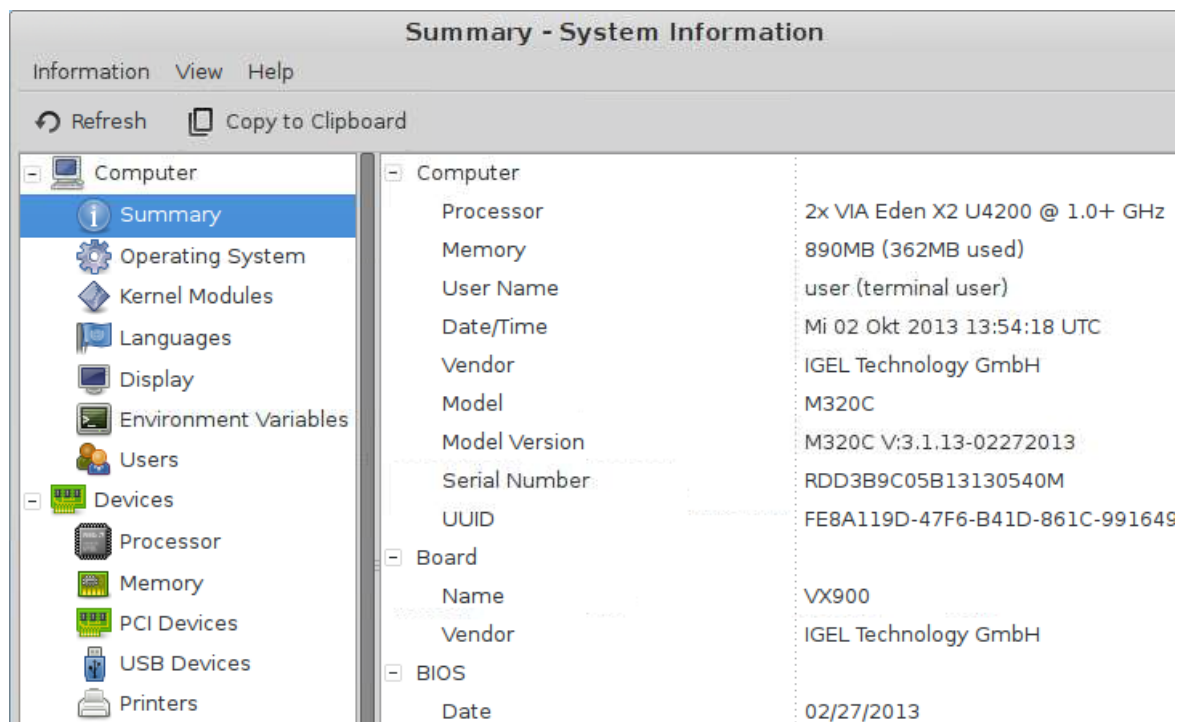


Figure 47: System information

6.19. Drive Management

Drive management shows all recognized USB drives along with their respective properties (device name, mount point etc.).

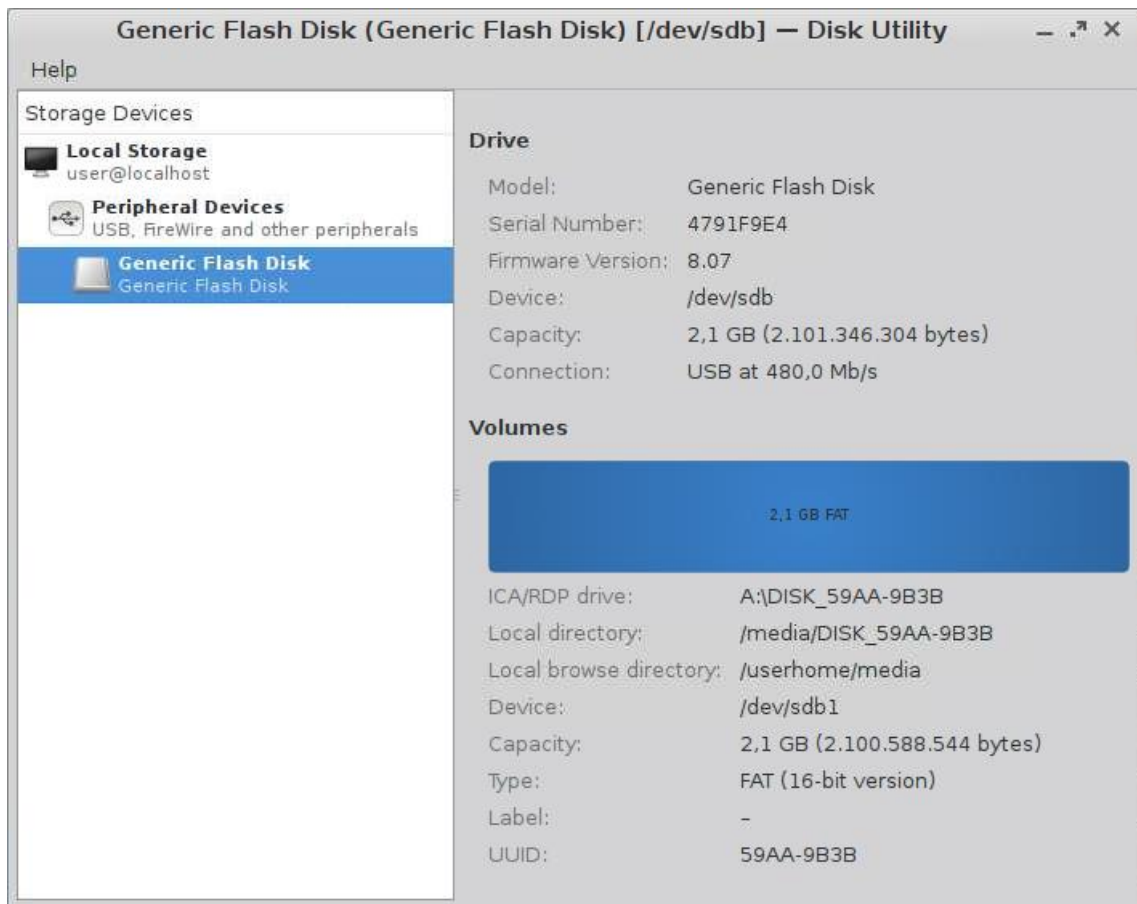


Figure 48: Drive management

6.20. Firmware Update

This session updates the firmware with the settings saved in **System→Update→Firmware Update**.

6.21. Identify Monitors

Shows the screen number from the IGEL setup and hardware information on every connected screen.



Figure 49: Identify screens

6.22. 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.

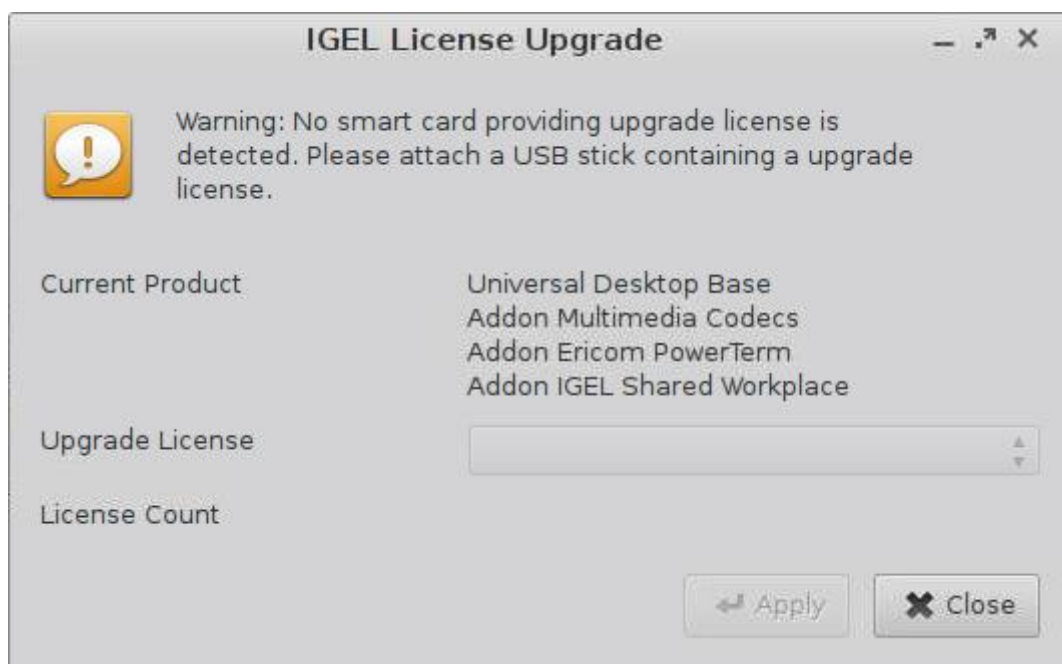


Figure 50: Firmware license upgrade

6.23. 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.

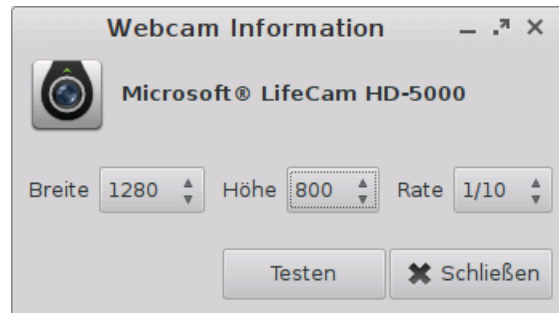


Figure 51: Webcam information

A list with all supported video formats can be created in the Linux Console using the command:
`webcam-info -l`.

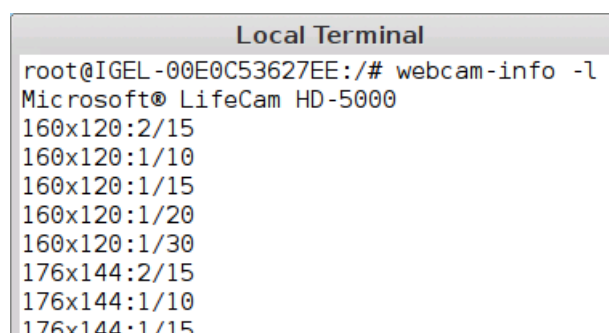


Figure 52: Command webcam-info -l

- 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* (*Webcam Testseite cameroid.com*) in your browser within the session (Adobe Flash must be installed).

6.24. Image Viewer

From IGEL Universal Desktop Linux 5.06.100, the GPicview image viewer can be used to view a variety 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 FAQs (<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 *this Ubuntu users' website*. (<http://wiki.ubuntuusers.de/GPicview>)

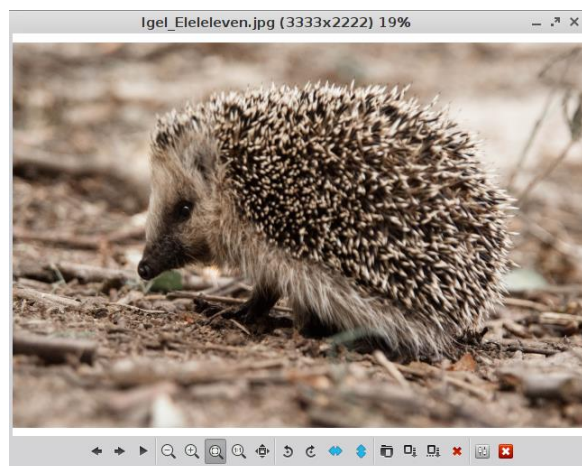


Figure 53: Image Viewer

7. User Interface

Configure the user interface exactly as you want it:

- Define *General Display Settings* (page 71)
- Set the *system language* (page 84).
- Define your *entry options* (page 87).
- Expand the *character sets* (page 90).

7.1. Screen

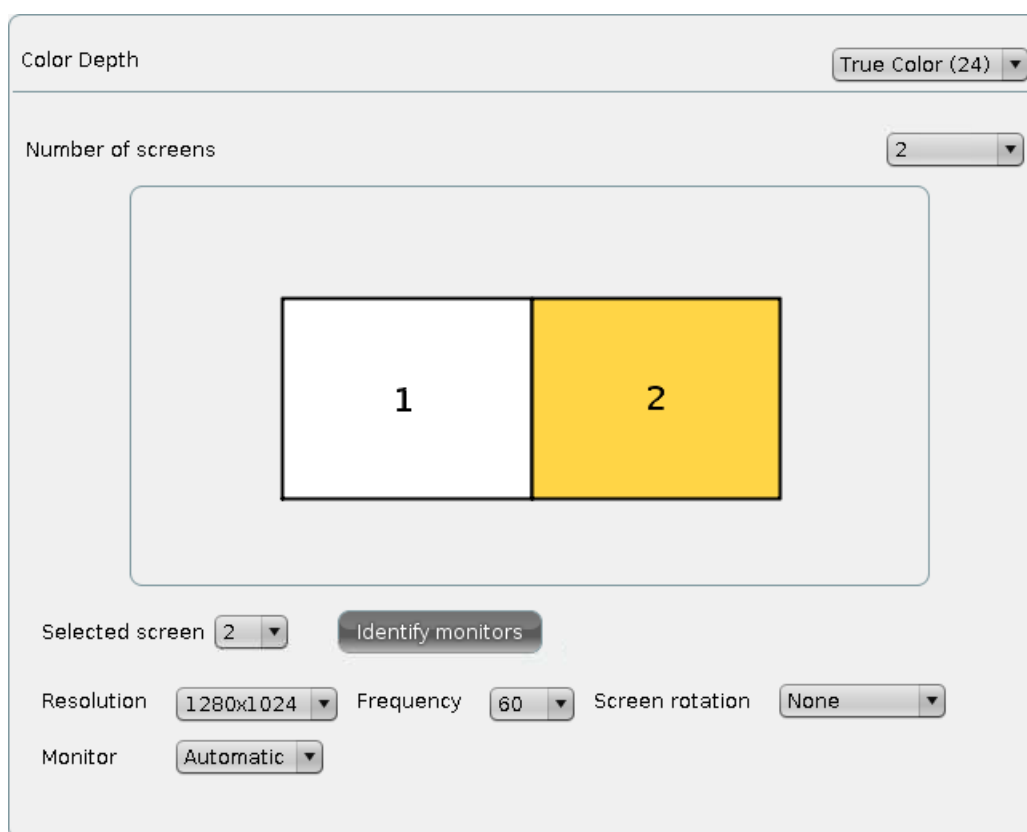


Figure 54: Screen settings

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	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.
Screen configuration	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.

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

7.1.1. Energy options

In this area, you can handle display power management. Your screen must support Display power management signaling.

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 55: 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.

7.1.2. 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**).

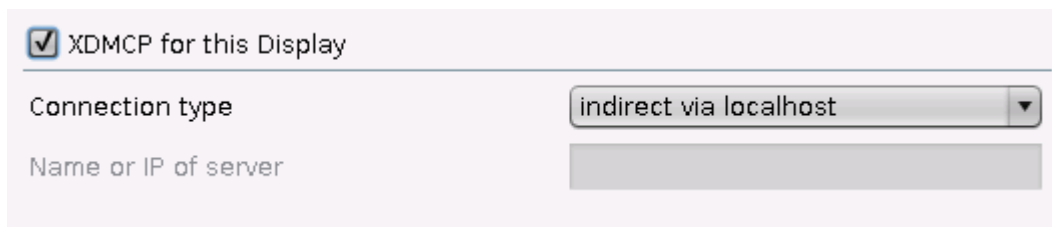


Figure 56: Display XDMCP

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 XDMCP 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.

7.1.3. 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

Calculate

List of Trusted X Hosts

★ 🗑️ 📄

Figure 57: 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 .

7.1.4. 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.

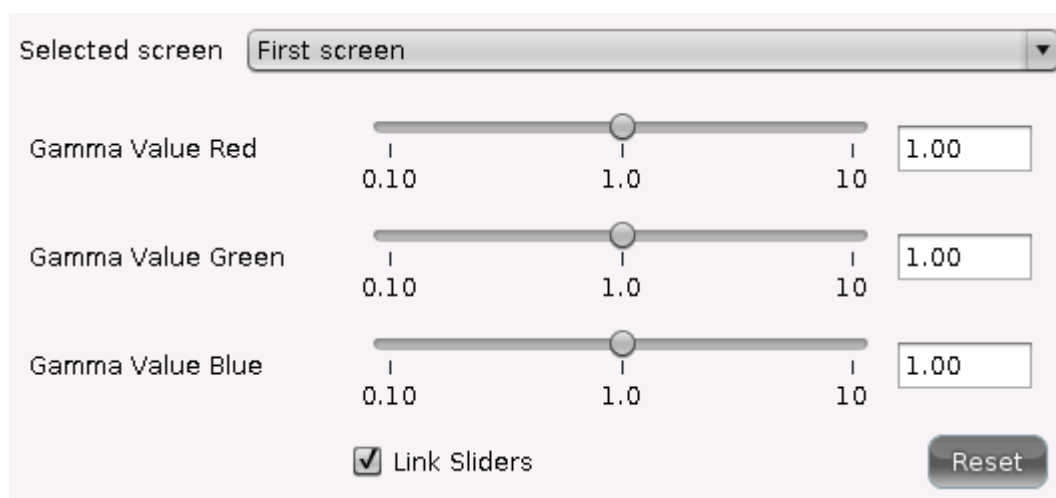


Figure 58: Gamma correction

7.1.5. Desktop

With the help of the following five dialog fields, you can configure the appearance and behavior of the desktop, windows, task bar, paggers (virtual screens) and start menu.

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

- Change the **user interface themes**,
- Specify **fonts**
- Change the **desktop icon size**

- Configure the display and delay time for **tool tips**.

<input checked="" type="checkbox"/> Local Window Manager for this Display	
Tooltip Delay Time	<input type="text" value="500"/>
Tooltip Display Time	<input type="text" value="600"/>
Userinterface Theme	<input type="text" value="IGEL-light"/>
Desktop Icon Size	<input type="text" value="64"/>
Desktop Fonts	
Default Font	<input type="text" value="Sans"/>
Default Font Size	<input type="text" value="10"/>
Desktop Icon Font Size	<input type="text" value="11"/>
Titlebar Font	<input type="text" value="Sans Bold"/>
Titlebar Font Size	<input type="text" value="11"/>

Figure 59: 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 of your own.

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

Wallpaper (1st Monitor) Igel blue (4x3)

Wallpaper Style (1st Monitor) Stretched

Color Style (1st Monitor) Solid Color

Desktop Color (1st Monitor) Choose color

2nd Desktop Color (1st Monitor) Choose color

☒ Enable Custom Wallpaper Download (1st Monitor)

Custom Wallpaper file (1st Monitor)

Figure 60: Wallpaper

Own background image - server configuration

Wallpaper	Here, you can set up the desktop background with pre-defined IGEL backgrounds, a fill color or a color gradient. You can also use a background image of your own. You can set up a separate background image for each monitor that is connected to the thin client.
Custom Wallpaper Download	<p>A user-specific background image can be provided on a download server. In the Desktop→Background window, enable the option Enable Custom Wallpaper Download and give the name of the background image file. You can specify the download server in the Desktop→Background→Custom Wallpaper window. If you have already defined a server for the system update files, you can use the same server setting for downloading the background image.</p> <p>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.</p>

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.

For further instructions on how to customize your IGEL Linux desktop see our best practice.

Task bar

In this area, you can enable and configure the task bar.

☒ Use Taskbar
☒ Taskbar clock
 Taskbar Position: Bottom
☐ Taskbar on top of all windows
☐ Taskbar Auto Hide
 Dualview taskbar size: Restrict taskbar onto one monitor
 Taskbar Button Height: 40
 Window button sorting order: Window title

Figure 61: Desktop Task Bar

Under **Window button sorting order**, you can specify how the opened windows are to be sorted in the task bar:

Time stamp:	The buttons are not sorted – they remain in chronological order according to when they were created.
Window title:	The buttons are listed alphabetically.
Drag and drop:	You can arrange the buttons in any order using drag and drop. You must drag a button far enough – at least over half of the button to be skipped.
Groups:	You can also sort the applications in group form according to time stamp and window title. All setup applications for example would then be together and sorted accordingly.

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 task bar. 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

Horizontal Number of Screens

Vertical Number of Screens

[Names of the workspaces](#)

Paging Resistance

☐ Wrap Workspaces while dragging a window

☐ Wrap Workspaces with pointer

Figure 62: Desktop Pager

Start menu

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

Start Menu Type

☒ Enable Lock Display Button

☒ Enable Logout Button

☒ Enable Restart Button

☒ Enable Shutdown Button

☒ Enable System Tab

☒ Enable About Button

Figure 63: 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.

7.1.6. Options

Configure the options for the display here:

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

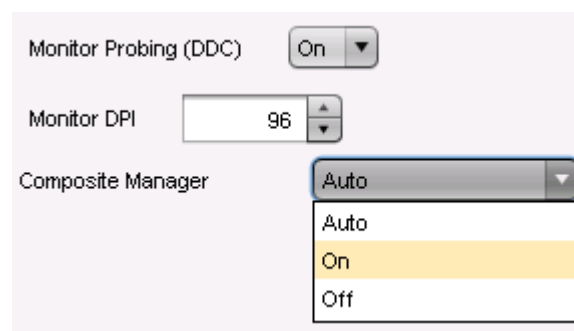


Figure 64: Display options

7.1.7. 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.

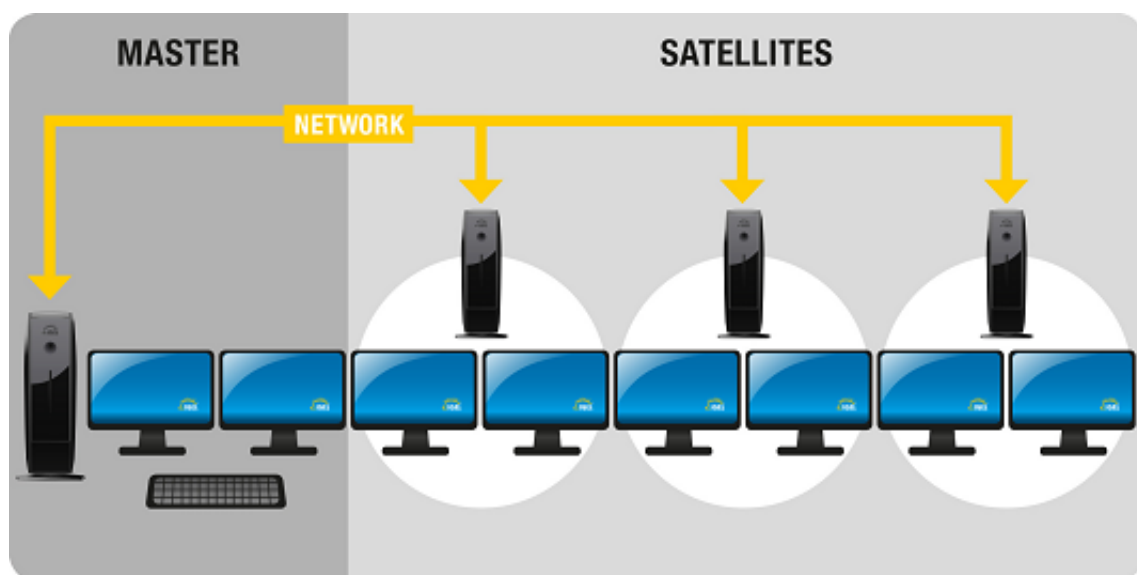


Figure 65: IGEL Universal MultiDisplay Setup

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**.

```
style="max-width:200px;"
```

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.

7.2. Language

Select the system language from the list. You can also set the keyboard layout and the entry language depending on the system language.

The chosen language is the language for the user interface and therefore applies for all local applications.

7.3. Screen Saver and Screen Lock

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 66: 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 118)).

Figure 67: 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.

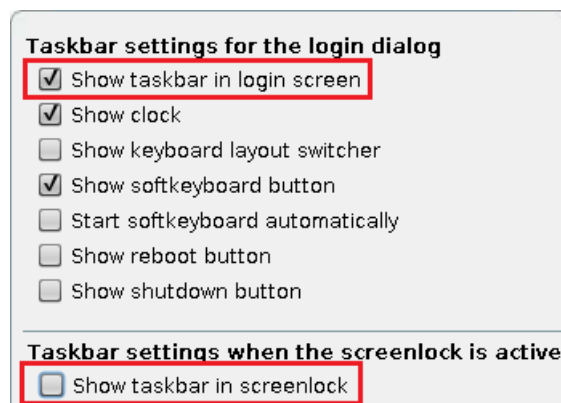


Figure 68: Taskbar on Login Dialog

7.3.1. Example configuration for the screen saver

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 69: 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 70: Clock configuration

7.4. Input

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

The following parameters can be configured:

- *Keyboard* (page 88)
- *Mouse* (page 89)
- Touchscreen

7.4.1. Keyboard and additional 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: <ul style="list-style-type: none"> • Initial key repeat delay – Determines the delay (in milliseconds) before automatic repetition begins. • Key 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.
Boot with NumLock enabled	Stipulates that NumLock is to be automatically enabled during the boot procedure.

- You can define additional keyboard layouts which can be selected by the user. The layout can be selected in the taskbar.

7.4.2. Mouse

Mouse type and mouse connection	Determines the type of mouse used and how it is connected
Left-handed mode	Changes the orientation of the mouse by switching the mouse buttons to left-handed mode.
3-button mouse emulation (no support for serial 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.
Mouse speed	Determines the mouse resolution in counts per inch
Mouse double-click interval	Changes the maximum interval (in milliseconds) between two consecutive mouse clicks which are to be recognized as a double-click.

7.4.3. SCIM (Input Methods)

The **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.

7.4.4. Signature Pad

Enable use of the SOFTPRO Virtual Serial SignPad (VSSP) signature pad in sessions (COM port mapping).
USB signature pads are made available in the sessions via COM port mapping.

1. To do this, enable **support** under **User Interface→Entry→Signature Pad**.
2. Apply this change by selecting **Apply** or **OK**.
3. Enable **COM port mapping** for the device `/dev/ttyVSSP0` in the session configuration.

7.5. Keyboard Commands - Hotkeys

You will find a list of existing keyboard commands for window management here. A keyboard combination can be defined for each function.

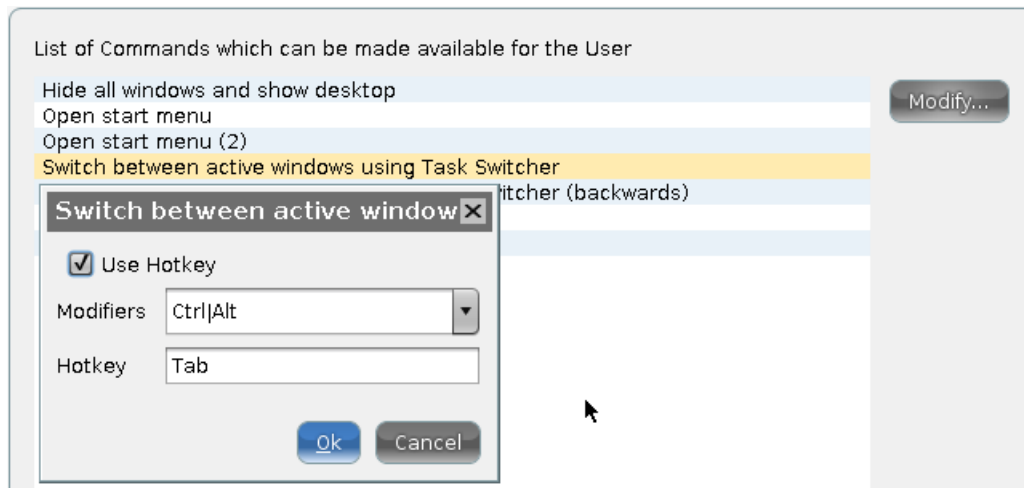


Figure 71: Keyboard commands

7.6. Font Services

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

- *XC font service* (page 90)
- *NFS font service* (page 91)

7.6.1. XC Font Service

If you need other fonts in addition to the ones offered by the thin client, you can use the XC font service.

This service must be installed on the 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.

7.6.2. 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.

8. Network

LAN interfaces (page 92)

Authentication (page 95)

Wireless (Wi-Fi) Connections (page 98)

VPN (page 104)

SCEP (page 108)

Routing (page 109)

Hosts (page 109)

Network drives (page 110)

8.1. 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.

Figure 72: 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 will find instructions for dynamic DNS registration via DNS in an *FAQ document* <http://edocs.igel.com/index.htm#10203508.htm>.

8.1.1. Individual 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 <i>best practice document</i> http://edocs.igel.com/index.htm#10203497.htm .
Network link type	Specify the network link type for the interface. The default is Automatic Recognition .

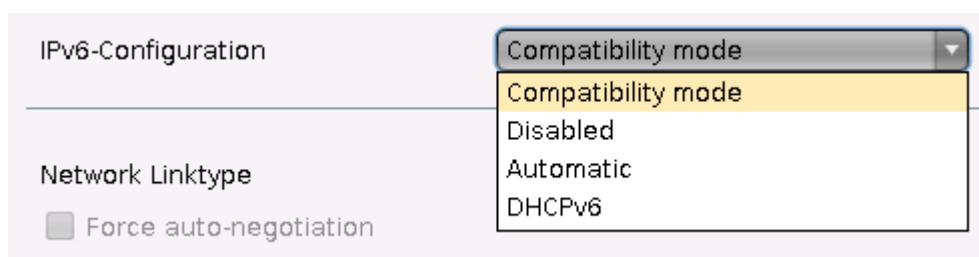


Figure 73: Configuration of an individual interface

Authentication

Enables IEEE 802.1x authentication
(Wired 802.1x only)

Enables network port authentication in accordance with the 802.1x standard. The following authentication methods are currently supported:

- EAP-PEAP/MSCHAPv2
- EAP-PEAP/TLS
- EAP-TLS

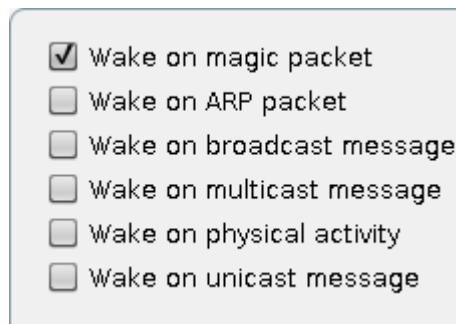
The entry options in the **Authentication** menu vary depending on the authentication method chosen. If the fields **User Name** and **Password** are not already populated, an entry mask for authentication purposes will be shown.

EAP type	Selects the authentication method: <ul style="list-style-type: none"> • PEAP for EAP-PEAP/MSCHAPv2 and EAP-PEAP/TLS • TLS for EAP-TLS
Check server certificate	Checks the authentication server
CA root certificate	Path name of the file with root certificate(s) for server authentication. The file may be in PEM or DER format.
PEAP/Auth method	Select the Phase 2 authentication method <ul style="list-style-type: none"> • MSCHAPv2 for EAP-PEAP/MSCHAPv2 • TLS for EAP-PEAP/TLS.
EAP-PEAP/MSCHAPv2/User name	Retains the user name for logging in for MSCHAPv2 authentication.
EAP-PEAP/MSCHAPv2/Password	Retains the password for MSCHAPv2 authentication.
EAP-PEAP/TLS/Client certificate	Path name of the file with the certificate for client authentication in the PEM (base64) or DER format. Leave empty if a private key in the PKCS12 format is used.
EAP-PEAP/TLS/Private key	Allows you to enter the path name of the file with the private key for the client certificate in the PEM (base64), DER or PFX format
EAP-PEAP/TLS/User name	User name for logging in for TLS authentication
EAP-PEAP/TLS/Password for private key	Password for accessing the encrypted private key in the private key file
EAP-TLS/Client certificate	Path name of the file with the certificate for client authentication in the PEM (base64) or DER format; leave empty if a private key in the PKCS12 format is used.
EAP-TLS/Private key	Path name of the file with the private key for the client certificate in the PEM (base64), DER or PFX format
EAP-TLS/User name	User name for logging in for TLS authentication
EAP-TLS/Password for private key	Password for accessing the encrypted private key in the private key file.

For IEEE 802.1x authentication purposes, the client certificate can also be requested and administered via SCEP. See *Network/SCEP* (page 108).

Wake-on-LAN

Select the packages or messages with which the thin client can be started via the network.

A screenshot of a dialog box titled "Wake-on-LAN" with a list of six options, each preceded by a checkbox. The first option, "Wake on magic packet", has its checkbox checked. The other five options have unchecked checkboxes.

- ☒ Wake on magic packet
- ☐ Wake on ARP packet
- ☐ Wake on broadcast message
- ☐ Wake on multicast message
- ☐ Wake on physical activity
- ☐ Wake on unicast message

Figure 74: Wake-on-LAN options

8.2. Wireless

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

You will find details of compatible WIFI modules in our *IGEL Linux 3rd Party Hardware Database* (<https://www.igel.com/en/service/linux-3rd-party-hardware-database.html>).

If you use mobile devices and regularly spend time in different WIFI zones, you will benefit from our new function: IGEL Café Wireless. This means that you can

- easily connect to new, previously unknown WIFI networks
- save connections that you have set up and then reuse them later on

straight from the user interface via the **Wireless Manager** 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 WIFI interface, proceed as follows:

1. Open the **IGEL Setup** and click on **Network→LAN Interfaces→Wireless**.

Figure 75: Enable user-defined connections

2. Enable the **Wireless Interface**.
3. Select the configuration for your **IP-Addresses** (DHCP or manuel).
4. Select a configuration type for operation with **IPv6**.
5. Enable at least the **Tray Icon**, **Context Menu** und **Wireless Manager**. Via the **Wireless Manager** 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 WiFi network** (page 102), if you do not select it via the .

Additional connections can be configured in the **Additional WiFi networks** (page 102)

7. Configure your location in the **WiFi frequency range** (page 103).

Once these settings become active on the thin client, a new symbol for wireless connections will appear in the system tray:



Figure 76: WiFi symbol

8.2.1. Wireless Manager

You can bring up the **Wireless Manager** from the tray icon:

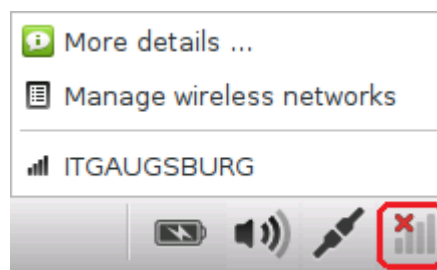


Figure 77: Symbol bar with WiFi context menu

You will need to have switched on the **Wireless Manager** under **Network→LAN Interface→Wireless**.

1. Click on the **Wireless** tray icon in the taskbar and then on **Manage wireless networks** in order to bring up **Wireless Manager**:

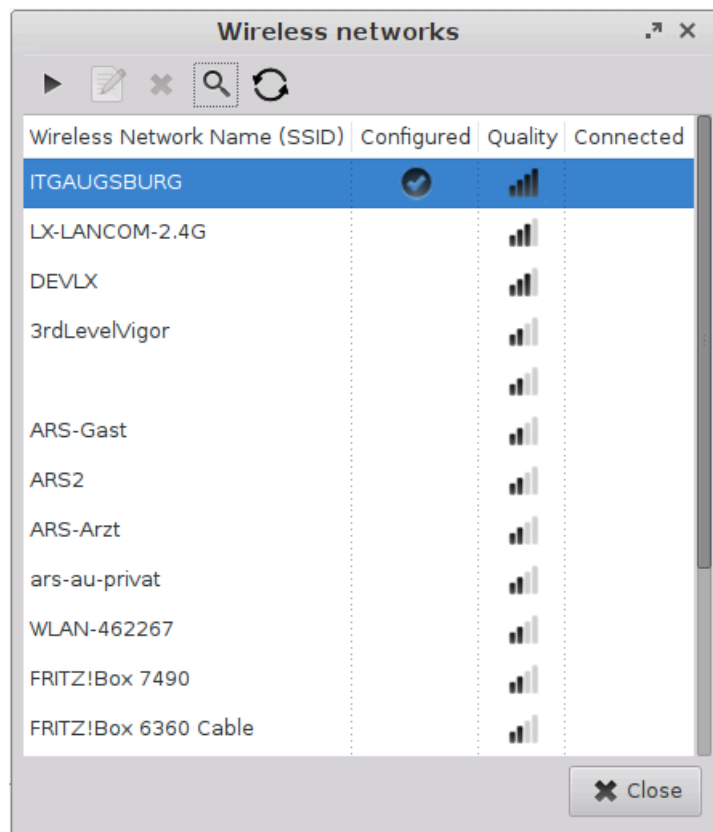


Figure 78: Wireless Manager

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 79: Configure WiFi connection

You can either **permanently store** 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.

- Click on the **Connect Network** button in order to establish the previously configured connection:

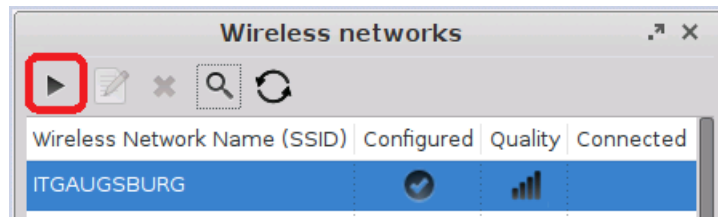


Figure 80: Establish connection to WiFi

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:

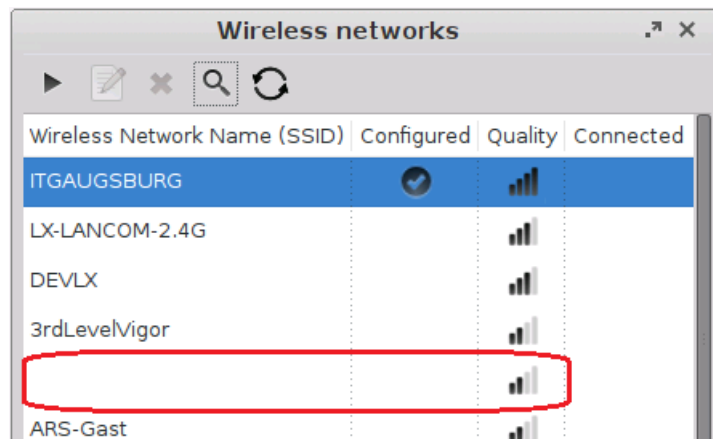


Figure 81: Hidden network

In order to connect to a previously unknown hidden network, you must first enter the SSID before the access data are retrieved:

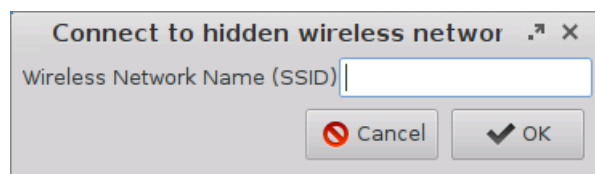


Figure 82: Name of the hidden network

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

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

5. The IGEL Setup shows all connections configured by the local user locally and in the UMS under **Network→LAN Network→Wireless→Additional WiFi networks**:

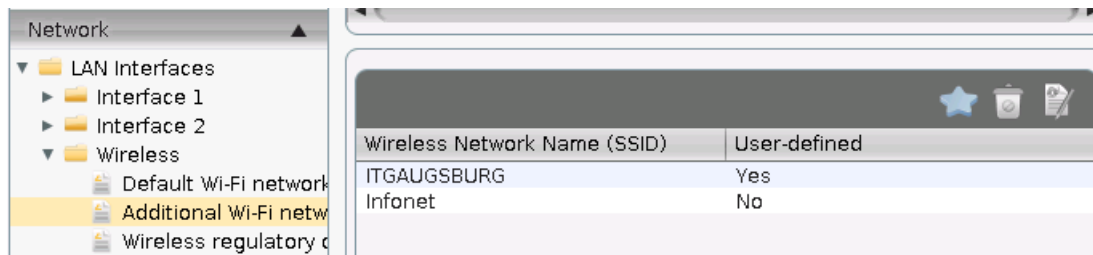


Figure 83: User-defined WiFi connections in the IGEL Setup

A **Yes** in the **User-defined** column means that you can change or delete this connection in the **WiFi Manager**. A connection that you have set up in the **WiFi 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.

8.2.2. Configure connections in the setup

In the **Default WiFi network** and **Additional WiFi networks** areas, you can configure wireless network connections:

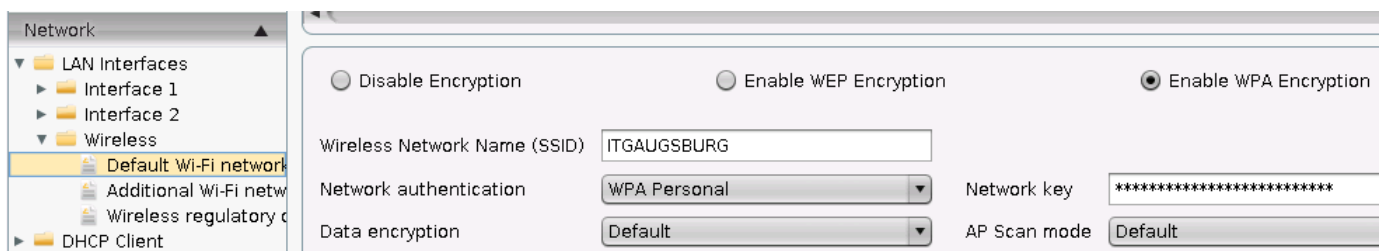


Figure 84: WiFi configuration

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 *Netzwerk/SCEP* (page 108) and our Certificate Enrollment and Renewal with SCEP (NDES) best practice.

The connections defined under **Additional WiFi networks** have the same value as the connection entered under **Default WiFi network**. Here, you can pre-configure WIFI connections which are available for selection by the user in the *Wireless Manager* (page 99).

The connections configured in the **Wireless Manager** are likewise shown in the **Additional WiFi networks** list and are automatically flagged as **User-defined**.

Connections to hidden networks

Hidden wireless networks (WIFI 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 interface→Wireless→Default WiFi network** and set the **AP-Scan mode** parameter to **No broadcast**.

Figure 85: Connection configuration for hidden networks

Additional connections can be configured in the **Additional WiFi networks** dialog.

8.2.3. WiFi frequency range

In this area, you can configure your location:

Channel No.	Center frequency (GHz)	Channel flags

Figure 86: WiFi frequency ranges

Ensure that the WiFi frequency range is configured correctly in order to prevent your device making illegal transmissions.

8.3. DHCP 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.

8.4. Virtual Private Network - VPN

Remote users securely access company networks via virtual private network protocols (VPN). You can set up your client accordingly for this purpose.

8.4.1. 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).

8.4.2. 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 <http://edocs.igel.com/index.htm#10203430.htm> describes how you can set up OpenVPN connections.

8.4.3. GeNUCard

The dedicated VPN device GeNUCard offers preconfigured Internet and VPN connections.

After starting a GeNUCard session the connection dialog opens. Various start options can be configured under **Desktop integration**.

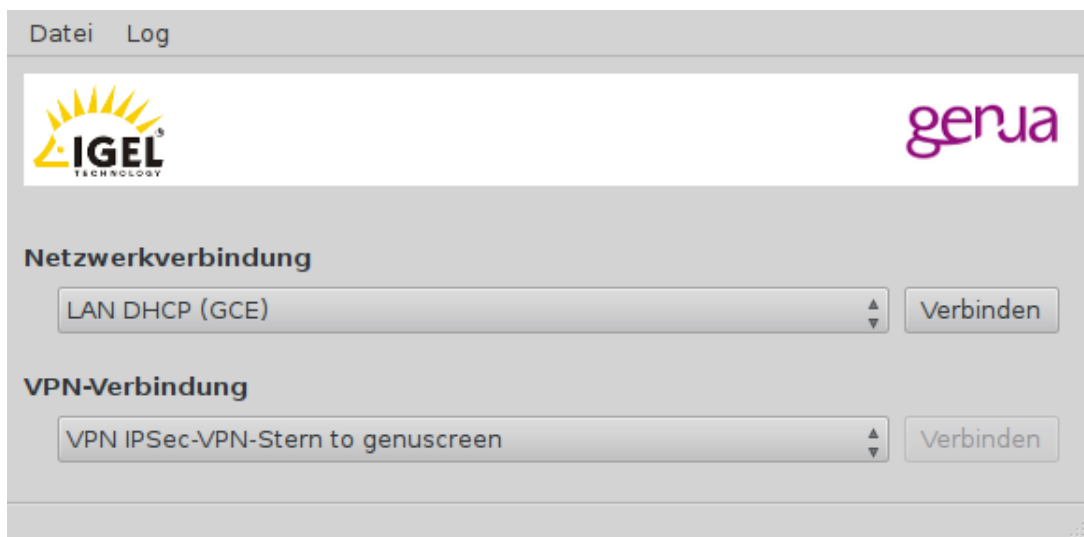
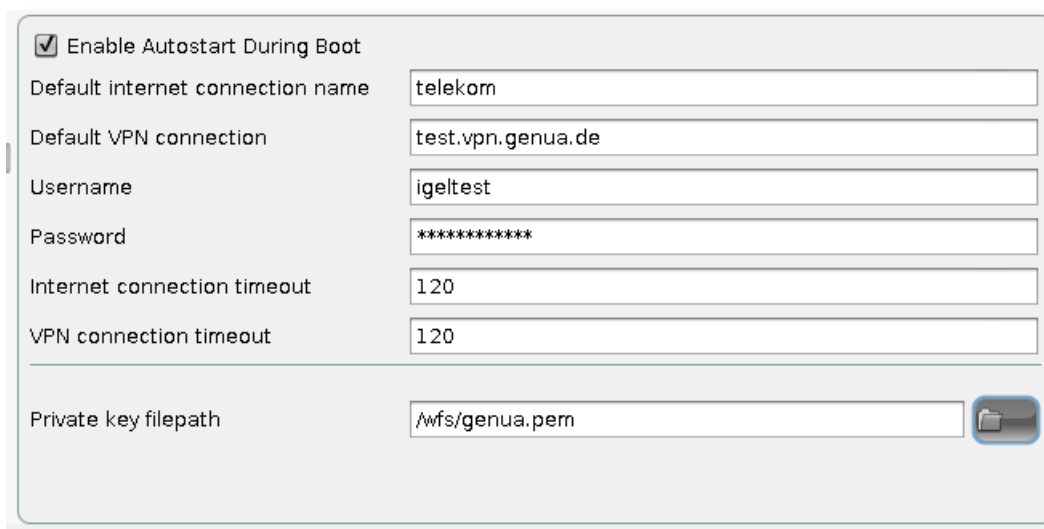


Figure 87: GeNUCard configuration

The **File** menu lists entries to **Change PIN** and for **Rekeying**.

GeNUCard Options

A valid combination of connection and user data can per entered in Setup under **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	igetest
Password	*****
Internet connection timeout	120
VPN connection timeout	120
Private key filepath	/wfs/genua.pem

Figure 88: Automatically establishing connections

There is also an option for autostarting the connection during boot, which is required for updating the IGEL firmware over VPN.

GeNUCard Administrator Session

Use the genucenter software to configure and manage your GeNUCard. For further information refer to www.genua.de.

Optionally you can set up an administrator session for configuring the Internet connection for GeNUCard:

1. Click **Add Instance** under **System→Registry→genucard%**.
A GeNUCard icon appears on the Desktop.
2. Click the GeNUCard icon.
The GeNUCard login window opens.
3. Enter **Username** and **Password**.
4. Click **OK**.

The Internet/VPN window opens..

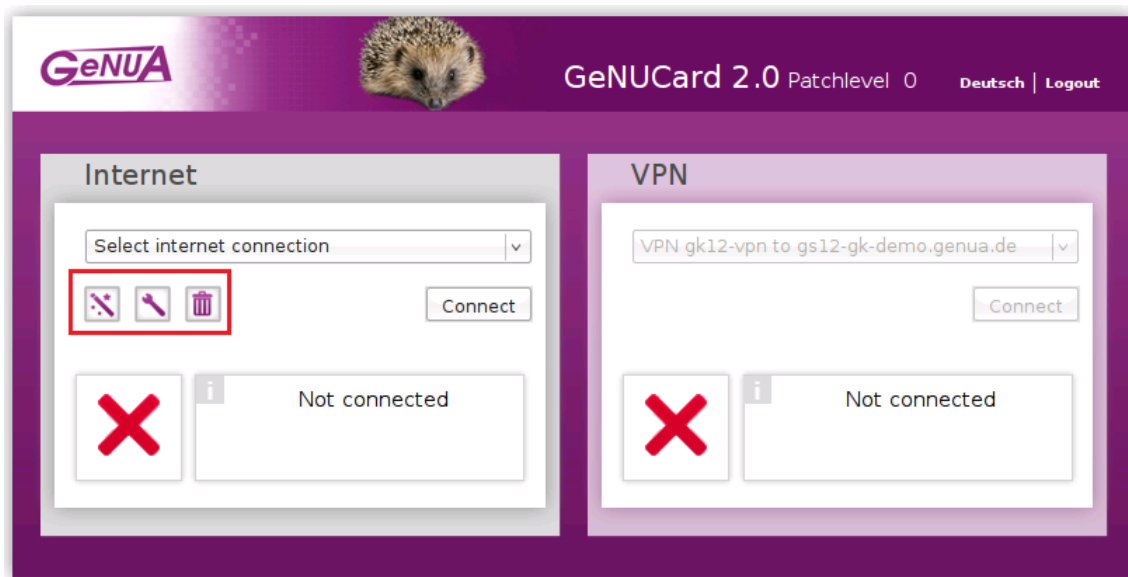


Figure 89: Internet/VPN window

5. Under **Internet** use the **New**, **Modify** and **Delete** buttons to configure the Internet connection.

8.4.4. 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>

8.5. Simple Certificate Enrollment Protocol - SCEP

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

A Microsoft Windows 2008 Server (MSCEP, NDES) for example can serve as a queried counterpart (SCEP server and certification 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.

8.5.1. 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.

8.5.2. 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.

8.5.3. 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.

8.5.4. 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`.

8.5.5. 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.

8.6. 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.

8.7. 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.

8.8. 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.

8.8.1. 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.

8.8.2. Windows Drive - SMB

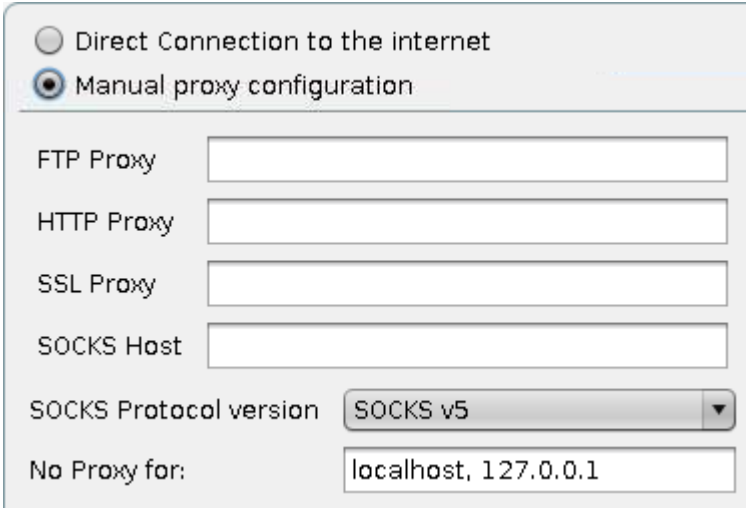
SMB is used by Microsoft Windows NT, Windows 95/98, Windows 2000 and Windows XP etc. to share hard drives and printers. As Unix (including Linux) can process this protocol with Samba Suite tools, hard drives and printers can be used along with Windows hosts. Consequently, items shared via SMB can be 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.

8.9. Proxy

Select the communication protocols for which a system-wide proxy is to be used.



The screenshot shows a configuration window for system-wide proxy settings. At the top, there are two radio buttons: 'Direct Connection to the internet' (unselected) and 'Manual proxy configuration' (selected). Below these are several input fields: 'FTP Proxy', 'HTTP Proxy', 'SSL Proxy', and 'SOCKS Host'. A dropdown menu for 'SOCKS Protocol version' is set to 'SOCKS v5'. At the bottom, there is a 'No Proxy for:' field containing the text 'localhost, 127.0.0.1'.

Figure 90: System-wide proxy

9. Devices

➤ Click on **Hardware Information** for an overview of your IGEL thin client device.

9.1. Printers

Various printing systems can be used with the thin client.

9.1.1. CUPS - Common UNIX Printing System

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. ➤ 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: Map printer in ICA sessions: Map printer in RDP sessions:	Makes the printer available in NX sessions. Makes the printer available in ICA 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
(Citrix Universal Printer Driver 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.

9.1.2. LPD - Line Printer Daemon

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.

9.1.3. 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.

9.1.4. 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 **Printers** 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.

9.2. USB Storage Devices

USB storage devices can be configured here.

9.2.1. Storage Device Hotplug

➤ Specify how USB devices are set up here.

The most important details are

- the number of possible devices,
- the allocation of drive letters,
- the access type available to users in ICA sessions (read and/or write access).

Newly connected devices are automatically recognized by default. The terminal gives an audible signal and a pop-up window informing you that a new device has been found and will be started appears.

USB Storage Hotplug Automount

Number of USB storage hotplug devices

☐ Private drive letter for each USB storage drive

Start USB storage drives with this driveletter.

ICA Read Access for USB storage hotplug devices

ICA Write Access for USB storage hotplug devices

☒ Use USB storage hotplug beep

☒ Show USB storage hotplug message

Message timeout

☒ Show device description ☒ Show errors

☒ Show local directory ☒ Show server drive

Figure 91: USB storage hotplug

9.2.2. Automount Devices

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.

9.3. USB Access Control

USB devices can be permitted or prohibited for use on the thin client on the basis of rules. Sub-rules for specific devices or device classes are also possible.

1. Enable USB access control under **Devices→USB Access Control**.
2. Select a **set rule** (default behavior) which will either allow or prohibit the use of USB devices.
3. Expand the general rule by adding class rules and device rules where you specify the procedure for handling specific classes or devices.

Device classes can be for example entry devices, printers or mass storage devices, while device rules relate to the manufacturer, the product or the actual device (identified via its Universally Unique Identifier UUID).

Example:

- The set rule prohibits the use of USB devices on the thin client.
- However, the use of all Human Interface Devices (HID) is permitted.
- The USB storage device with the UUID `67FC-FDC6` is also permitted.

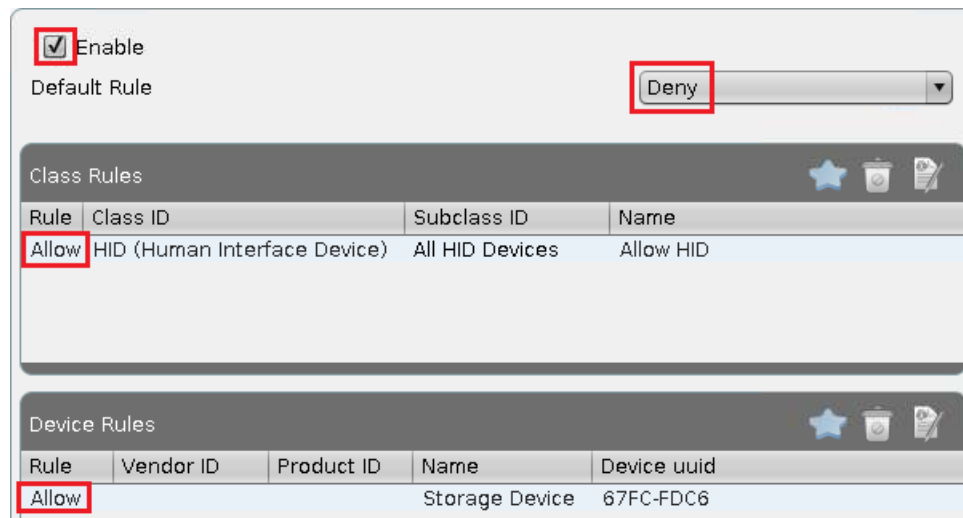


Figure 92: USB access control

Other USB storage devices, printers etc. cannot be used on the thin client with this setting.

9.4. PC/SC Interface

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.

10. 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 variable options for permitting restricted configuration by users.

10.1. 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 17)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.

10.2. Login Options

- 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.

10.2.1. 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 58).

You can use the optional IGEL smartcard for local authentication and personalized session configuration ("Flying Doctor Scenario").



Figure 93: 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.

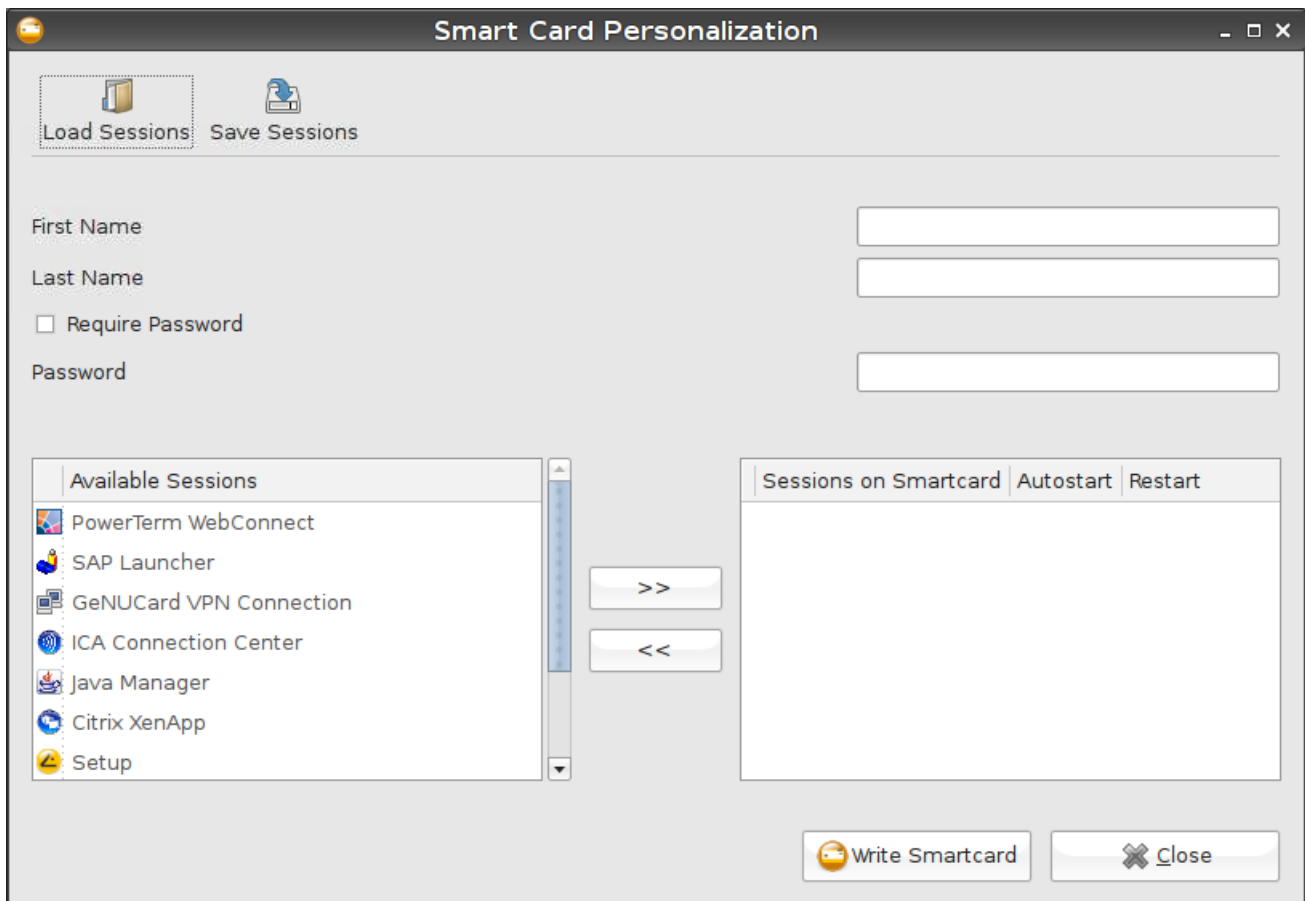


Figure 94: Smartcard personalization

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).

In 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.

10.2.2. AD/Kerberos

Logging in with Kerberos	Enables local login to the thin client via the Kerberos protocol. AD/Kerberos must also be <i>configured</i> (page 122) for this purpose. The login can be used for single sign-on in a number of session types (ICA, RDP).
Link for logging off	Allows you to configure the way(s) in which the user can log off.

10.2.3. Auto logout

Define an **Auto Logout** action which is carried out when you end the last instance of a session type:

1. Bring up the **Security→Login→Auto Logout** setup page.
2. Choose a **Session Type**.
3. Choose a **command (Auto Logout 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 **Logout** 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.

10.3. AD/Kerberos Configuration

- 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).

10.3.1. 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.

10.3.2. 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

11. System Settings

As previously explained under *Quick installation* (page 6), various basic system settings can be configured in the sub-structure.

Date and time (page 124)

Update (page 125)

Remote management (page 126)

VNC (mirroring) (page 127)

Remote access (SSH / RSH) (page 131)

Energy (page 132)

Firmware configuration (page 142)

IGEL System Registry (page 144)

11.1. Time and Date

1. Go to **System**→**Time and Date**

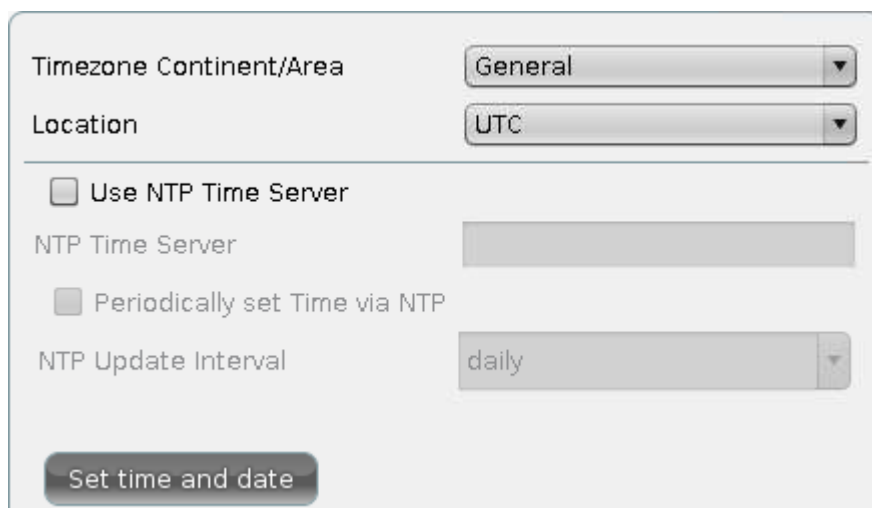


Figure 95: Set time and date

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 .

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)

11.2. 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

11.2.1. 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.

11.3. Remote Management

If the thin client is registered by an IGEL UMS server, the server address and the port number will be shown under **Remote Management**.

You can also register to a UMS Server directly:

1. Open the **Application Launcher**.
2. Start the application **System > UMS Registering**.
3. Enter the UMS Server's **Address** and **User Credentials**.

If a valid entry exists in DNS for the UMS Server you can keep the default value `igelrmserver` for the server's address.

4. Optional: Choose a target **Directory** on the server.
5. Optional: Define a **Structure Tag** to register the thin client according to the UMS default directory rules.

Structure Tags can also be deployed to thin clients via DHCP option 226 to support the automatic registration and sorting in the UMS database. A Structure Tag received via DHCP overrides a manually configured tag when the client gets registered to the UMS.

6. Click **Register**.

11.3.1. Directly transferring the configuration file

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.

11.4. VNC (Shadowing)

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.

11.5. Secure shadowing (VNC with SSL)

The **Secure Shadowing** function improves security when remote maintaining a thin client via VNC at a number of locations:

- **Encryption:** The connection between the shadowing computer and the shadowed thin client is encrypted.

This is independent of the VNC viewer used.

- Integrity: Only thin clients in the UMS database can be shadowed.
- Authorization: Only authorized persons (UMS administrators with adequate authorizations) can shadow thin 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 thin client by another thin 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 thin clients which meet the requirements for secure shadowing and have enabled the corresponding option. Other thin 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.

11.5.1. Basic principles and requirements

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
- Thin client is registered on the UMS server
- Thin 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 thin 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 thin 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 thin 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 thin client (**Setup→System→Shadowing→Secure Shadowing**), the thin 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 thin client. The validity of the certificate can be checked on the (Linux) thin client using the command: `x11vnc -sslCertInfo /wfs/ca-certs/tc_ca.crt`



Figure 97: Secure shadowing connection dialog

When a VNC connection has been established, the symbol in the connection tab indicates secure shadowing:



Figure 98: Secure VNC connection

11.5.3. VNC logging

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).

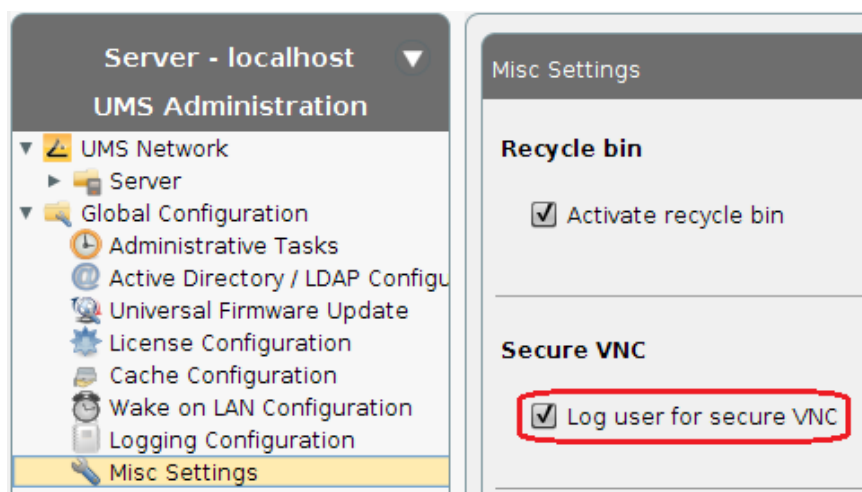


Figure 99: Options for VNC logging

The VNC log can be called up via the **context menu** of a thin client or folder (for several thin clients, **Logging→Secure VNC Logs**). The name, MAC address and IP address of the shadowed thin 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 100: 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.

11.6. 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.

11.7. Energy

Under **System -> Energy**, you will find numerous settings for energy management.

11.7.1. Energy options

The **System-> Energy->Energy Options** setup page offers numerous settings for energy management.

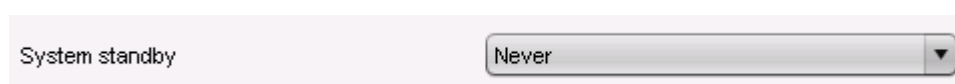


Figure 101: Standby

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 .
----------------	---

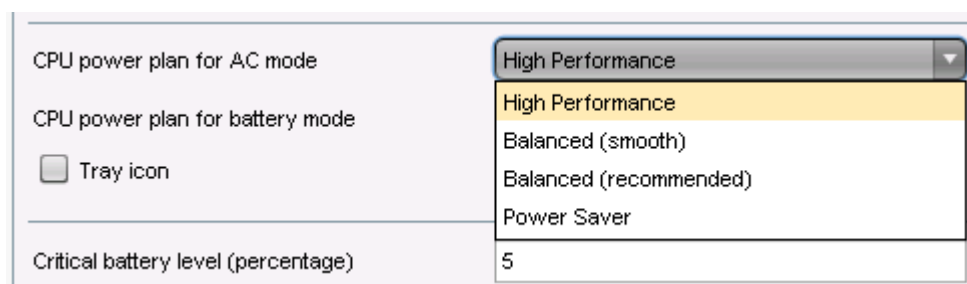


Figure 102: CPU

CPU power plan for AC mode	<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>
CPU power plan for battery mode	<p>Specify here which CPU power plan (CPU Governor) the device is to use in battery mode. For an explanation of the settings, see above.</p>
Tray icon	<p>Enable this setting in order to display a CPU tray icon which allows you to switch quickly between the power plans.</p>

Critical battery level (percentage)	<input type="text" value="5"/>
Critical battery action	<input type="text" value="Show warning"/>
Critical command	<input type="text" value="Shutdown"/>

Figure 103: Critical charge level

Critical battery level (percentage)	Here you can configure the battery level percentage below which the battery level is regarded as critical.
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.




Figure 104: Low charge level

Low battery level (percentage)	Here you can configure the battery level percentage below which the battery level is regarded as low.
Low battery action	Here you can specify what action is to be taken in the event of a low battery level: No Action , Warning , Execute Command or Execute Command in Console .
Low command	Enter a valid command here. The standard command <code>user_shutdown -f</code> shuts down the system in the proper manner.

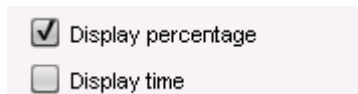


Figure 105: Options

Display percentage	Shows the battery level percentage in the tray.
Display time	Shows the remaining battery running time / charging time in the tray.

11.7.2. Energy system

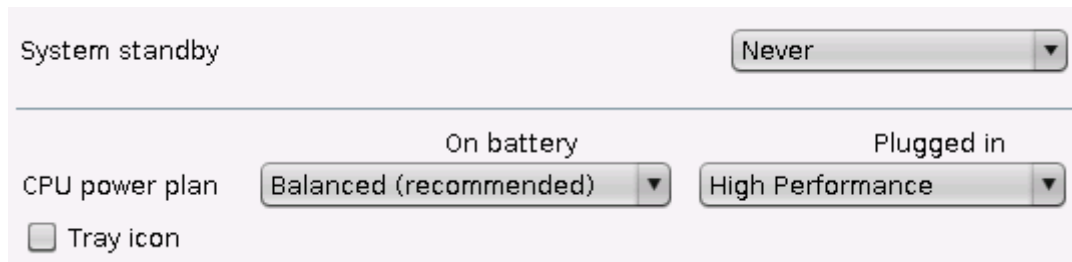


Figure 106: Energy Options System

Standby time	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.

11.7.3. Rechargeable battery

Battery Notification

Critical battery level (percentage)

Critical battery action Show warning ▼

Critical command Shutdown ▼

Low battery level (percentage)

Low battery action Show warning ▼

Low command Shutdown ▼

Battery Tray Icon

☒ Display percentage

☐ Display time

Figure 107: 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.

11.7.4. Screen

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 108: 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.

11.7.5. Shut down

This setup page contains settings for shutting down.

Figure 109: 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.

11.7.6. Energy options

The **System-> Energy->Energy Options** setup page offers numerous settings for energy management.

Figure 110: Standby

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 .
----------------	---

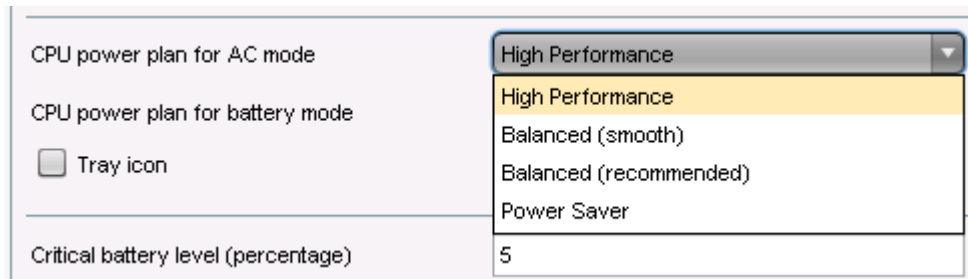


Figure 111: CPU

CPU power plan for AC mode	<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>
CPU power plan for battery mode	Specify here which CPU power plan (CPU Governor) the device is to use in battery mode. For an explanation of the settings, see above.
Tray icon	Enable this setting in order to display a CPU tray icon which allows you to switch quickly between the power plans.

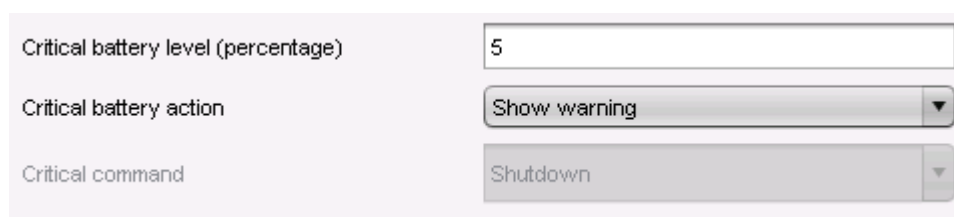


Figure 112: Critical charge level

Critical battery level (percentage)	Here you can configure the battery level percentage below which the battery level is regarded as critical.
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.

Figure 113: Low charge level

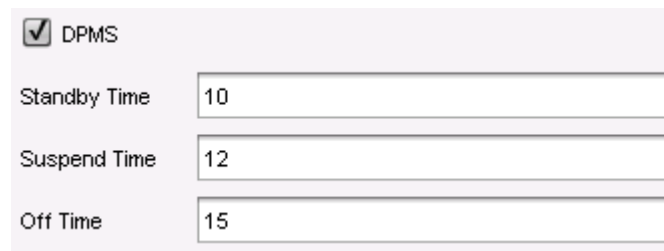
Low battery level (percentage)	Here you can configure the battery level percentage below which the battery level is regarded as low.
Low battery action	Here you can specify what action is to be taken in the event of a low battery level: No Action , Warning , Execute Command or Execute Command in Console .
Low command	Enter a valid command here. The standard command <code>user_shutdown -f</code> shuts down the system in the proper manner.

Figure 114: Options

Display percentage	Shows the battery level percentage in the tray.
Display time	Shows the remaining battery running time / charging time in the tray.

11.7.7. DPMS

With DPMS (Display Power Management Signaling), you can send signals for power management to your monitor if it supports this function.



☒ DPMS

Standby Time

Suspend Time

Off Time

Figure 115: DPMS

DPMS	Enable DPMS.
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.

11.8. Firmware Customization

Configure the firmware to create your own personal workstation.

11.8.1. Custom Application

Applications which were loaded onto a customer partition for example can be launched via the **Application Launcher** or an icon on the desktop once they have been defined as own applications. In order for this to be possible, a command to call up the application must be entered under **Settings**.

11.8.2. Custom commands

Custom commands can be mounted at various points in time during the system start. These commands can use *configured environment variables* (page 144).

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 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 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 run when settings are changed via the local setup or the UMS.

The commands are executed at the following times:

After reconfiguration	Runs after an effective change in the thin client settings (local setup, UMS)
------------------------------	---

11.8.3. Custom Bootsplash

See the description in the chapter *User Interface* (page 70).

11.8.4. 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**

Pre-defined 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 142).

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.

11.8.5. 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.

11.9. IGEL System Registry

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:

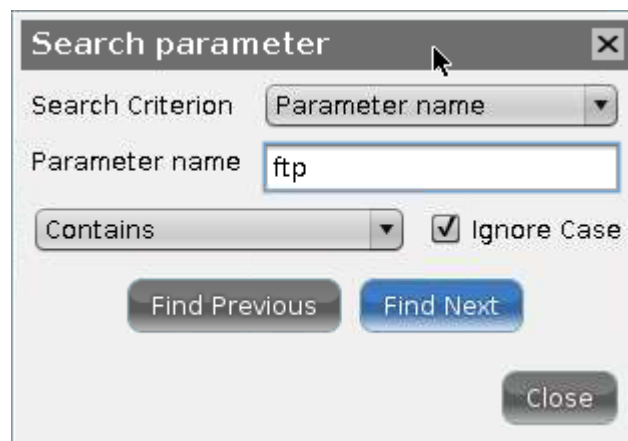


Figure 116: Parameter search in the IGEL Registry

12. Index

A

Access control.....	74
Accessories	58
AD/Kerberos	121
AD/Kerberos Configuration	122
Address bar.....	46
Advanced	47
Advanced Options	83
Appearance.....	36
Appliance mode.....	38
Application Launcher.....	10, 59
Audio	56
Authentication.....	95
Auto logout.....	121
Automount Devices	116

B

Background.....	76
Basic principles and requirements	128
Boot Menu.....	8
Boot Procedure.....	8
Browser Global	41
Browser Plug-in	56
Browser Plug-ins	53
Buddy Update.....	126

C

Calibration Pattern	62
Certificate	108
Certification Authority.....	108
Change password	37
Change Smartcard Password.....	58
Checking the Client Certificate	109
Citrix Access Gateway.....	38
Citrix ICA - global settings.....	21
Citrix ICA - Sessions.....	31

Citrix Receiver selection	20
Citrix StoreFront / Web Interface	35
Codec	31
COM ports - serial connections	25
Commands.....	49, 62
Company Key	120
Completing the Setup.....	15
Configuration	84
Configure connections in the setup.....	102
Connections	35
Contents.....	42
Context menu	53
CUPS - Common UNIX Printing System	112
Custom Application	142
Custom Bootsplash	143
Custom commands	142

D

Data protection.....	44
Desktop.....	75
Desktop integration	34, 38
Device Information	63
Device support / virtual communication channels	26
Devices.....	111
DHCP Options	104
DigitalPersona authentication	27
Directly transferring the configuration file.....	126
Display switch	59
Domain-Realm Mapping.....	123
DPMS	140
Drive Management.....	66
Drive mapping.....	25
DriveLock	27

E

Emergency Boot.....	8
Enable Setup Pages for Users	17
Encryption.....	47

Energy	132
Energy options.....	72, 132, 138
Energy system.....	135
Environment variables.....	144
Example	109
Example configuration for the screen saver.....	86

F

Failsafe Boot - CRC check.....	9
Features	144
Firefox browser.....	41
Firefox Browser Session.....	50
Firewall	28, 33
Firmware Customization	142
Firmware Update.....	66
Flash Player.....	54
Flash redirection	30
Font Services.....	90

G

Gamma correction.....	75
General System Information	11
GeNUCard.....	105
GeNUCard Administrator Session	106
GeNUCard Options	106

H

Hardware and Network Requirements	82
Hosts	109
Hotkeys.....	53

I

ICA Connection Center	58
ICA global options.....	28
Identify Monitors.....	67
IGEL Smartcard	119
IGEL System Registry	144
Image Viewer.....	69
Individual interface.....	94
Input	88

Introduction.....	5
-------------------	---

J

Java Control Panel	62
Java Web Start Session	57

K

Keyboard / hotkey assignment.....	24
Keyboard and additional Keyboard	88
Keyboard Commands - Hotkeys	90

L

LAN interfaces.....	92
Language.....	84
License	13
Local logon.....	23
Local Terminal.....	58
Log off	38
Logging on and off	36
Login Options.....	118
Logon	32
Look-up	64
LPD - Line Printer Daemon.....	113

M

Mapping.....	24
Media Player.....	54
Media Player Global.....	55
Media Player Sessions	56
Menus and symbol bars.....	50
Mouse	89
Multimedia redirection.....	30

N

NCP	107
Netstat	64
Network	92
Network Diagnostics.....	63
Network Drives	110
Network Information.....	14
Network Integration	9

NFS.....	110	SCEP	108
NFS Font Service	91	SCIM (Input Methods)	89
O		Screen	71, 137
OpenVPN	104	Screen Saver and Screen Lock	84
Options	34, 35, 56, 57, 80	Secure shadowing (VNC with SSL)	127
P		Security	46, 118
Pager	78	Server	31
Password	118	Server location	22
PC/SC Interface	117	Sessions.....	11, 20
PDF viewer	54	Setup Application.....	15
Ping	63	Setup Areas.....	16
Playback.....	55, 57	Setup Search	18
PPTP	104	Setup Session.....	58
Print	43	Shadow thin clients securely	129
Printers	26, 111	Shut down.....	137
Private data	45	Shutdown and Restart	14
Protection against tracking.....	45	Signature Pad.....	89
Proxy	44, 111	Simple Certificate Enrollment Protocol - SCEP	107
Q		Smartcard Personalization.....	58
Quick Installation.....	6	Soft Keyboard (On-screen Keyboard)	62
Quick Settings	17	Softpro SPVC Channel.....	27
Quick Settings Session	58	Software Requirements.....	81
Quiet Boot	8	Sound Mixer.....	60
R		SSH Session	39
Realm 1-4.....	122	Start menu	79
Rechargeable battery	136	Starting the Setup.....	15
Reconnect.....	33	Storage Device Hotplug	114
Reconnecting and updating.....	37	System Information	64
RedHat Spice.....	54	System Log Viewer.....	60
Remote Access (SSH / RSH)	131	System Settings.....	124
Remote Management.....	126	System Tools.....	12
Reset to Factory Defaults	9	T	
Routing	109	Tabs.....	42
S		Task bar.....	78
Save Sessions	121	TCP/IP	113
Save User and Password.....	120	Test Smartcard.....	121

The IGEL Linux Desktop	6
The IGEL Linux Firmware	5
ThinPrint	113
Time and Date	124
Touchscreen Calibration.....	61
Traceroute	64

U

UMS Registration.....	61
Universal MultiDisplay.....	81
Update	125
Upgrade License	67
Usage	84
USB Access Control.....	116
USB redirection.....	29
USB Storage Devices.....	114
User Interface	70

V

Verbose Boot	8
Video.....	55
Virtual Private Network - VPN	104
VNC (Shadowing).....	127
VNC logging	130
VNC Viewer.....	57

W

Wake-on-LAN.....	97
Webcam Information	68
WiFi frequency range	103
Window	24, 55
Window settings.....	32, 50
Windows Drive - SMB.....	110
Wireless	98
Wireless Manager.....	99

X

XC Font Service	90
XDMCP	73
X-Server	9