

# Windows Embedded Standard 7



**IGEL<sup>®</sup>**  
**UNIVERSAL  
DESKTOP**

# Important Information

Please note some important information before reading this documentation.

## Copyright

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

Copyright © 2015 IGEL Technology GmbH. All rights reserved.

## Trademarks

IGEL is a registered trademark of IGEL Technology GmbH.

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

## Disclaimer

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

## IGEL Support and Knowledge Base

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

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

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

# Contents

Important Information .....	2
1. IGEL Universal Desktop Firmware .....	7
2. Quick installation .....	8
3. Boot options .....	9
4. IGEL device information .....	9
5. IGEL setup .....	10
5.1. Setup Areas .....	11
5.2. Searching Setup Pages .....	11
6. Sessions .....	13
6.1. Citrix .....	13
6.2. Remote Desktop Protocol - RDP .....	21
6.3. Horizon Client .....	27
6.4. vWorkspace Client and AppPortal .....	29
6.5. Leostream .....	30
6.6. NX Client .....	31
6.7. PowerTerm WebConnect .....	31
6.8. PowerTerm Terminal Emulation .....	32
6.9. Browser Sessions .....	33
6.10. Windows Media Player .....	34
6.11. VoIP Client .....	35
7. Accessories .....	36
7.1. Setup Session .....	36
7.2. Sound Mixer .....	37
7.3. Windows Services .....	37
8. User interface .....	38
8.1. Display .....	38
8.2. Language .....	39
8.3. Input .....	39
8.4. Desktop and Start Menu .....	40
8.5. Shell .....	40
9. Network .....	41
9.1. LAN and Wireless .....	41
9.2. VPN Connection .....	41
9.3. Routing .....	41
9.4. Network Drives .....	42
10. Devices .....	43
10.1. Printer .....	43
10.2. Attached Devices .....	43

11.	Security .....	44
11.1.	Password .....	44
11.2.	Active Directory .....	45
11.3.	Network .....	45
11.4.	Windows Firewall .....	45
12.	System .....	47
12.1.	Date and Time .....	47
12.2.	Update .....	47
12.3.	Remote Management .....	49
12.4.	Shadow .....	50
12.5.	File Based Write Filter .....	55
12.6.	Energy Options .....	56
12.7.	Firmware Customization .....	57
12.8.	Registry .....	58
12.9.	System Restoration .....	59
13.	Index .....	60

## About this document

All illustrations and descriptions in this document relate to the IGEL Universal Desktop W7 firmware in version 3.10.100.

This manual is divided into the following sections:

<i>Quick installation (page 8)</i>	Setting up the thin client for the first time
<i>Boot options (page 9)</i>	Information about the client boot process
<i>IGEL device information (page 9)</i>	Device and setup information
<i>IGEL setup (page 10)</i>	Configuring, launching and ending setup
<i>Sessions (page 13)</i>	Creating and configuring application sessions
<i>User interface (page 38)</i>	Screen, desktop, start menu, language, entry
<i>Network (page 41)</i>	LAN/WLAN, VPN, routing, network drives
<i>Devices (page 43)</i>	ThinPrint, USB
<i>Security (page 44)</i>	User accounts, password, Active Directory, Password Manager Agent
<i>System settings (page 47)</i>	Date/time, remote management, shadowing, energy options, registry, write filters, update, firmware functions

## What is new in 3.11.100?

You will find the release notes for the IGEL Universal Desktop W7 3.11.100 both as a text file next to the installation programs on our *download server* ([http://myigel.biz/index.php?dir=IGEL\\_UNIVERSAL\\_DESKTOP\\_FIRMWARE/W7/](http://myigel.biz/index.php?dir=IGEL_UNIVERSAL_DESKTOP_FIRMWARE/W7/)) and in our *Knowledge Base* (<http://edocs.igel.com/>).

- **Universal Management Suite Structure Tag:** Sort thin clients automatically into Universal Management Suite (UMS) directories by giving them a *Structure Tag* (page 49).
- **Redirect Ctrl-Alt-Delete to session:** If *this option* (page 14) is enabled, this key combination will not be processed by the local thin client. It will be forwarded to the Citrix, RDP or Horizon session instead.
- **Newly installed add-ons** can be enabled automatically without prompting the user:


Further information can be found under *Advanced* (page 33).



Please note the *licensing information for Windows Embedded Standard* (<http://edocs.igel.com/#10203297.htm>), especially when using Microsoft Office 365.

## Formatting and meanings

The following formatting is used in the document:

<i>Hyperlink</i>	Internal or external links
Proprietary names	Proprietary names of products, firms etc.
<b>GUI text</b>	Items of text from the user interface
<b>Menu &gt; Path</b>	Menu paths in systems and programs
Entry	Program code or system entries
<span style="border: 1px solid black;">Keyboard</span>	Commands that are entered using the keyboard
 Reference to other parts of the manual or other eDocs articles.	



Note regarding operation



**Warning:** Important note which must be observed

# 1. IGEL Universal Desktop Firmware

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

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

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

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

## Management software: Universal Management Suite

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



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

## 2. Quick installation

By following the procedure below, you can install the end device in your network environment in just a few minutes:

1. Connect the end device to a VGA or DVI monitor, an AT-compatible keyboard with a PS/2 or USB connection, a USB mouse and the LAN using an RJ45 connector.
2. Connect the end device to the power supply.
3. Switch on the end device and wait until the graphic desktop is launched.  
You are now logged on as a user with the name user (password is user).

To log on as an administrator, proceed as follows:

1. Select **Start > Log Off**.  
- with W7, holding down the **Shift** key -
2. Hold down the **Shift** key and click on Log Off.
3. Hold down the **Shift** key until the logon window is shown.
4. Log on as an administrator user with the password administrator.



Change the administrator password after logging on for the first time!

A yellow IGEL symbol is shown in the Windows taskbar:



Figure 1: IGEL symbol in the taskbar

You can configure basic system settings here.

1. Right-click the IGEL symbol.

A pop-up menu opens.

2. Change the
  - Network settings
  - Display settings
  - Keyboard settings

3. Click **OK** to save your changes.

The device will now restart and will use the new settings thereafter.

These basic settings can also be configured in the IGEL setup application. A handy tool tip is available for virtually every setting. If you would like to know more about a setting or option, simply move your mouse pointer over it and wait a moment.



## 3. Boot options

To select your desired boot options, proceed as follows:

1. Wait until the message `Booting, please wait` appears during the boot process.
2. Press the `Esc` key.  
A selection menu opens.
3. Select one of the three boot options:

**Windows Embedded Standard** The system boots normally.

**Download firmware image** The firmware download menu is shown.  
In order to download a snapshot file from your server or a connected USB stick, you will need to provide the necessary connection details.

**Start rescue shell** In this case, you access the underlying Linux system, e.g. in order to restore the system or reset the IGEL setup data.

## 4. IGEL device information

The IGEL device information provides a quick overview of the basic properties of your device.

- Double click the yellow IGEL symbol in the Windows taskbar in order to bring up the device information.

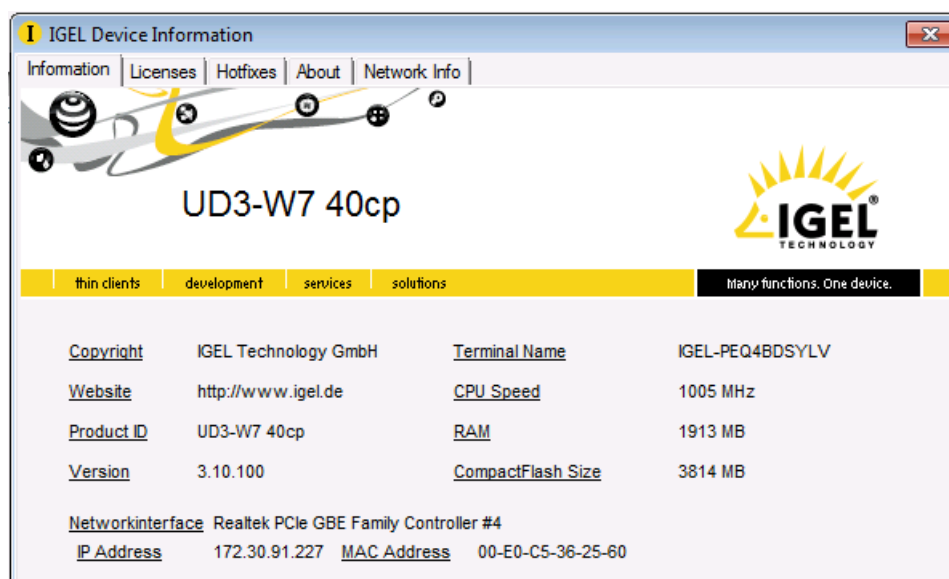


Figure 2: IGEL device information

<b>Information</b>	Details of the product, the firmware version, the IP address and a number of hardware details such as CPU and RAM are shown.
<b>Licenses</b>	All software licenses contained in the firmware, e.g. the GNU General Public License are shown. The individual licenses can be brought up by selecting <b>Next</b> and <b>Back</b> .
<b>Hotfixes</b>	Shows all Microsoft Windows system patches, e.g. security updates.
<b>About</b>	Provides a detailed overview of your thin client hardware and software. In particular, the licensed functions included in the firmware are shown here.
<b>Network information</b>	Shows various information regarding the current network as well as the availability of a UMS server.

## 5. IGEL setup

There are various ways in which you can set up the IGEL thin client to meet your needs:

- via the Windows Embedded System system management
- with the local IGEL setup
- with the IGEL Universal Management Suite
- via a VNC connection to the device (shadowing)
- and/or through combinations of the above ways.

We assume that you are familiar with Windows system management and have not dealt with it in this manual. A separate set of documentation for this is available from Microsoft. We do not recommend that you configure the thin client via Windows system management because the settings cannot be saved in a profile and will not be retained during an update with a snapshot.

If you are logged on as an administrator, you can open the IGEL setup applications from the Windows start menu. The setup structure is similar to that on the IGEL Linux thin clients and in the IGEL Universal Management Suite (IGEL UMS). An icon for launching the setup application can be placed on the desktop.



The setup is blocked for `user` as standard. However, parts of the setup can be made available to the restricted user so that they can for example select the keyboard layout or system language themselves

To launch the setup (after logging on as an administrator or if setup pages are available for the user), proceed as follows:

- Click the **Setup** symbol in the taskbar or
- Click the **Setup** application in the start menu or
- Place a symbol for the **Setup** on the desktop (**Setup > Accessories > Setup Session > Start Options**).

To end the setup, proceed as follows:

- Click **Apply** to save the changes you have made.
- Click **OK** to save your changes and close the application.
- Click **Cancel** to close the application without saving your changes.

## 5.1. Setup Areas

The setup application comprises the following main areas:

<b>Sessions</b>	In this area, you can create and configure application sessions such as ICA, RDP, terminal emulation, browser and others.
<b>Accessories</b>	The IGEL setup application can be restricted for users (not the administrator). A number of Windows services can be enabled or disabled.
<b>User interface</b>	The system language, display settings, entry devices as well as the behavior of the desktop and start menu can be configured here. These settings apply to all users in a group (user / administrator).
<b>Network</b>	In this area, you can configure all the network settings for LAN / WLAN interfaces. Network drives are also configured here.
<b>Devices</b>	The options for using various USB devices (e.g. memory sticks, WLAN or Bluetooth devices) as well as printers are enabled or configured here.
<b>Security</b>	Passwords for the administrator and the user are set up, a user is specified for the automatic logon procedure and domain information for a used Active Directory is entered here. The Windows firewall can also be configured here via the IGEL setup.
<b>System</b>	A number of basic parameters such as time synchronization, firmware update information, write filter configuration (File Based Write Filter, FBWF) etc. can be specified here. Individual IGEL services (features) can also be managed (enabled / disabled) here.

- Click one of these areas to open up the relevant sub-structure.
- Navigate within the tree structure in order to switch between the setup options.
- Use the arrow buttons to move backwards and forwards between the visited setup pages or to reach the next level up.



Figure 3: Arrow buttons

## 5.2. Searching Setup Pages

To search for parameter fields or values in the setup, proceed as follows:

1. Open the **Search** area in the left-hand window.
2. Enter the search parameters.
3. Select one of the hits.
4. Click on **Show Result** and you will be taken to the relevant setup page.

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

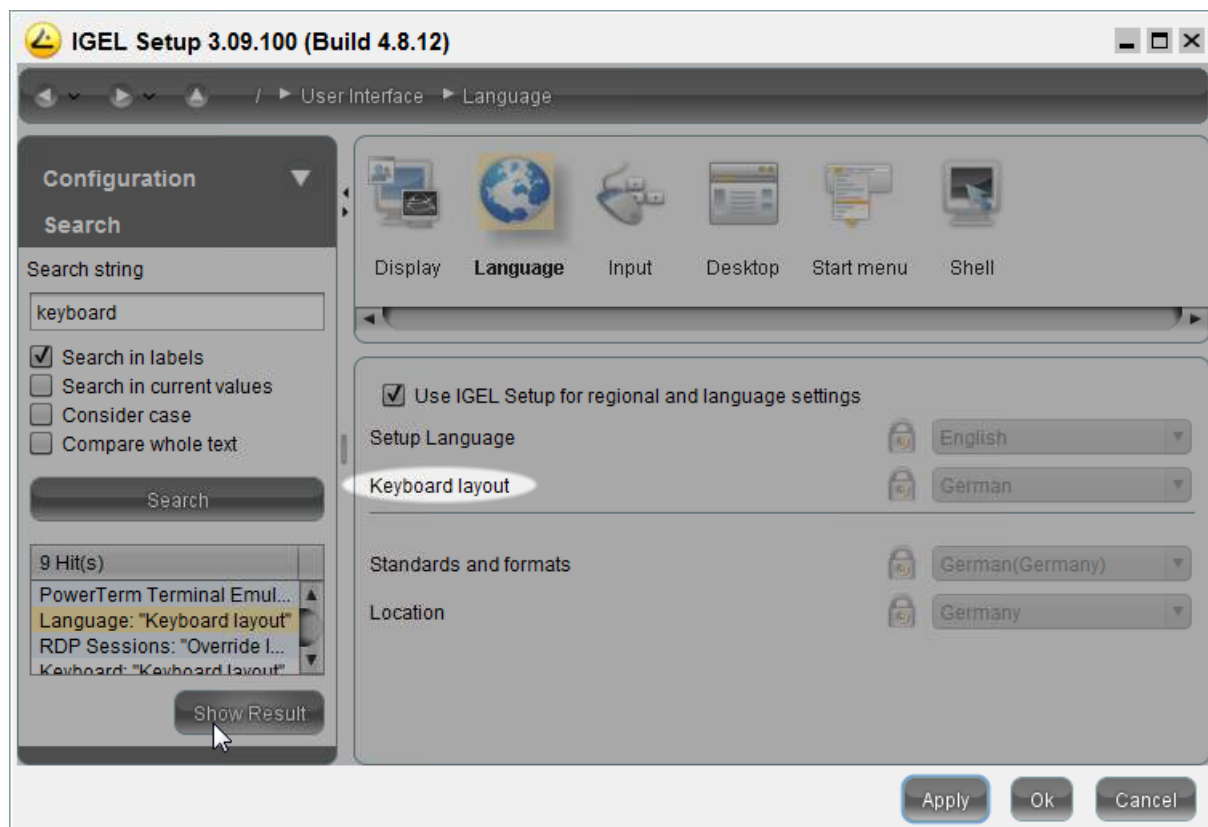


Figure 4: Searching Setup Pages

## 6. Sessions

Menu path: **Setup > Sessions**

The session types which are available for configuration depend on the license for your IGEL thin client. An overview of the functions included with each license level can be found in the product list on the IGEL website [www.igel.de](http://www.igel.de).

The **Session Overview** area in the IGEL setup lists all sessions already configured.

To add a new session, proceed as follows:

➤ Click on **Add**.

or

➤ Navigate to the desired session type in the structure tree and create a new session there.

Each session configuration contains the point **Desktop Integration**. Here, you can define the session name, the appearance of the session in the start menu or on the desktop and the start behavior (automatic / manual).

### 6.1. Citrix

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

- **Use IGEL Setup for configuring Citrix settings:** If this option is enabled, you can configure the Citrix client via the IGEL Setup.
- **Installation root path for Citrix Client:** Specify the path to the directory in which the Citrix client is installed, e.g. `C:\Program Files\Citrix\ICA Client`.
- **Installation root path for Citrix Selfservice Plug-in:** Specify the path to the directory in which the Citrix Self-Service Plugin is installed.

#### 6.1.1. ICA Global

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

The global settings define standard parameters which are used in all sessions or can be overwritten in the relevant session configuration.



Further information regarding the individual parameters can be found in the original documentation from Citrix: <http://docs.citrix.com/>.

## Server Location

Menu path: **Setup > Sessions > Citrix > ICA Global > Server Location**

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

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

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



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

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



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

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



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

## Window

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

- **Default Number of Colors:** Specifies the standard color depth - the default setting is a color depth of 256 colors.
- **Default Horizontal Resolution:** Specifies the window width in pixels.
- **Default Vertical Resolution:** Specifies the window height in pixels.

## Keyboard

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



These settings can only be configured globally here and cannot be overwritten in the sessions.

- **Keyboard Layout:** This is set to **default** but you can also select a country-specific layout. **default** means that the local keyboard setting will be used in ICA too.
- **Redirect Ctrl-Alt-Delete to sessions:** If this option is enabled, this key combination will not be processed by the local thin client. It will be forwarded to the session instead.
- **Hotkeys:** Hotkeys for the server system can be mapped to function keys or key combinations on the local keyboard.

## Firewall

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

Allows you to configure ICA connections which run via a firewall, a SOCKS proxy server or a Citrix Secure Gateway (in relay mode).

- **Use Alternate Address:** This option should be enabled if you use ICA sessions in order to establish a connection with a specific Citrix server behind a firewall. Generally speaking, the Citrix server's IP address within the local network is different from the one used outside. Once the alternate address is enabled, the server must be added to the address list under **Proxy Server**.
- ➡ You will find more information on server configuration if you look for the command `altaddr` in your Citrix administration manual.
- **SOCKS / Secure Proxy:** Select the standard proxy settings here or define the settings yourself.
  - **Proxy Type:** Choose between **None (Direct Connection)**, **SOCKS** and **Secure (HTTPS)**. Enter the address for the **Proxy Server** and the **Proxy Port**, unless you have selected **None**.
- **Secure Gateway (relay mode):** Enter the **Secure Gateway address** and **Port**.

## Options

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

- **Disable Windows Alert Sounds:** If this option is enabled, no Windows alert sounds will be played.
- **Deferred screen update mode:** If this option is enabled, updates from the local video buffer will be delayed on the screen. The local video buffer is used if the seamless Windows mode or HDX latency reduction is used.



If you work with images that are displayed over and over again, you can significantly improve the performance of your ICA session(s) with the following three settings.

- **Cache Size in kB:** Specify the maximum amount of local system storage capacity (in kilobytes) used for temporary storage purposes.
- **Minimum Bitmap Size in Bytes:** Specify the minimum size of the bitmap files that are to be stored in the cache.
- **Persistent Cache Path:** Specify the directory where the files are to be stored locally.



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

- **Enable Auto Reconnect:** If this option is enabled, the Citrix client will automatically reconnect if the connection was terminated.
- **Maximum Retries:** Number of reconnection attempts
- **Enable Single Sign On through ICA file:** If this option is enabled, you only need to log on once.

## USB Redirection

Menu path: **Setup > Sessions > Citrix > ICA Global > USB Redirection**

- **Enable USB redirection (XenDesktop and Citrix VM Hosted):** If this option is enabled, you can use the local computer's USB devices in sessions.
- **Default Rule:** Choose between **Deny** and **Allow** to set a rule for all devices to which no more specific rule applies.
- **Class Rules:** Define rules by selecting a **Class ID** and **Subclass ID** for USB devices.
- **Device Rules:** Define rules for individual devices by entering a **vendor ID** and **Product ID**.

How to work with rules:

- To create a rule, click .
- To remove a rule, click .
- To edit a rule, click .

## HDX

Menu path: **Setup > Sessions > Citrix > ICA Global > HDX**

- **Flash acceleration/redirection:** Specify whether Flash content should **Always** or **Never** be redirected or the system should **Ask** the user.



Redirecting Flash content can improve playback.




- **File access:** Specify what access to local client files is allowed.
- **Microphone and webcam access:** Specify what access to local microphones and webcams is allowed.
- **PDA access:** Specify what access to personal digital assistants (PDAs) is allowed.
- **USB and other devices access:** Specify what access to USB devices, scanners, digital cameras and the like is allowed.

### 6.1.2. ICA Sessions

Menu path: **Setup > Sessions > ICA > ICA Sessions**

Many of the session parameters can be pre-defined through the global settings. However, a number of them can only be set in the session configuration, e.g. login data or desktop integration.

How to work with sessions:

- To create a session, click .
- To remove a session, click .
- To edit a session, click .

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



## Server

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

- **Browser Protocol:** The protocol that is to be used when searching for servers and published applications.
- **Don't use default server location:** If this option is enabled, the default server stipulation will be lifted. You can then enter one or more HTTP server locations.
- **Citrix Server:** If this option is selected, the user is connected to the entire desktop as if logging on at the server itself. As a result, all applications, permissions and settings contained in the user's profile (local server profile) are available.
- **Published Application:** If you select a published application, the session is opened in a window which contains just one application. The session is ended if you close this application.
- **Server:** You can manually enter the IP address or the host name of the server in this field.
- **Application:** If you have entered the server manually, you can specify a published application here. These fields are automatically filled in if you have selected one of the recognized published applications.
- **Working directory:** Path of the working directory for the application

## Logon

Menu path: **Setup > Sessions > Citrix > ICA Sessions > [Session Name] > Logon**

- **User Name:** Allows you to specify the user name for the session
- **Password:** Allows you to specify the password for the session
- **Domain:** Allows you to specify the domain for the session



If you save a **user name**, **password** and **domain** in the session configuration, the user no longer needs to give these when launching a session. If you leave these fields empty, the user will have to enter them in a mask before the session is launched.

- **Do not show Password Protection Window (Ctrl-Alt-Delete) before Logon:** This option switches the Windows splash screen on and off.

## Window

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

- **Number of Colors:** The color depth is specified in *ICA Global* (page 14). You can change it for this session.
- **Use full screen mode:** By disabling full screen mode, you can choose between the global default setting and a session-specific setting.
- **Window size:** Choose between the default and a range of other sizes.
- **Enable Seamless Window Mode:** Seamless mode can only be used with published applications or with a specified start program for the server connection.

## Firewall

Menu path: **Setup > Sessions > Citrix > ICA Sessions > [Session Name] > Firewall**

Allows you to configure ICA connections which run via a firewall, a SOCKS proxy server or a Citrix Secure Gateway (in relay mode).

- **Use alternate address through firewalls:** This option should be enabled if you use ICA sessions in order to establish a connection with a specific Citrix server behind a firewall. Generally speaking, the Citrix server's IP address within the local network is different from the one used outside. Once the alternative address is enabled, the server must be added to the address list under **Proxy Server**.
- ➔ You will find more information on server configuration if you look for the command `altaddr` in your Citrix administration manual.
- **SOCKS / Secure Proxy:** Select the standard proxy settings here or define the settings yourself.
  - **Proxy Type:** Choose between **None (Direct Connection)**, **SOCKS** and **Secure (HTTPS)**. Enter the address for the **Proxy Server** and the **Proxy Port**, unless you have selected **None**.
- **Secure Gateway (relay mode):** Enter the **SSL Proxy Server** and **SSL Proxy Port**.

## Options

Menu path: **Setup > Sessions > Citrix > ICA Sessions > [Session Name] > Options**

- **Compress:** Data compression reduces the amount of data transferred via the ICA session. This in turn reduces network traffic to the detriment of CPU performance. Compression should be used when connecting the server via WAN. No compression is necessary for low-performance servers and when working in a LAN.
- **Persistent Cache Enabled:** Allows you to enable caching (configured in the global ICA settings)  
This makes sense when using a number of ICA sessions if only one or two sessions are critical with regards to network bandwidth or are used heavily during the day. In this case, you should reserve the cache memory for these sessions.
- **Encryption Level:** Encryption increases the security of your ICA connection. **Basic** encryption is enabled by default. You should ensure that the Citrix server supports RC5 encryption before you select a higher degree of encryption.
- **Client Audio:** If this option is enabled, system sounds and audio output from your applications will be transferred to the thin client and played back via the connected loudspeakers. The higher the level of audio quality you select, the more bandwidth is needed for transferring audio data.
- **Speedscreen Latency Reduction:** Improves the performance of high-latency connections by allowing the client to react immediately to keyboard entries or mouse clicks. This gives users the feeling that they are using a normal PC.



SpeedScreen only works if the function has been enabled and configured on the Citrix server.

- **Mouse click feedback:** Visual feedback in response to a mouse click – an hourglass symbol appears immediately.
- **Local Text Echo:** Displays the text entered more quickly. This avoids latencies within the network. Select a mode from the drop-down list:
  - **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.
  - **Off:** For faster connections (connection via a LAN)
  - **Automatic:** If you are not sure how fast the connection is.

## Desktop integration

Menu path: **Setup > Sessions > Citrix > ICA Sessions > [Session Name] > Desktop Integration**

- **Session Name:** Give the name of the session which is to be shown.
- **Starting Methods for Session:**
  - **Start Menu:** If this option is enabled, an entry will be created in the start menu.
  - **Desktop:** If this option is enabled, an entry will be created in the start menu.
  - **Autostart:** If this option is enabled, the session will start automatically when the user logs on to the device.

### 6.1.3. Self-Service Plugin

Menu path: **Setup > Sessions > Citrix > Self-Service Plug-In**

With the Self-Service Plug-In, the user can find and launch published applications and desktops.

## Server

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

- **Use IGEL Setup for Citrix Self-Service Plug-in:** If this option is enabled, you can configure the Self-Service Plug-In on this and the following setup pages.

Here, you can set up sessions for

- Citrix XenApp 6.x or older,
- Citrix XenApp/XenDesktop 7.x Store,
- Citrix XenApp/XenDesktop 7.x Legacy Mode.

## Logon

Menu path: **Setup > Sessions > Citrix > Self-Service Plugin > Logon**

- **Allow user to save password:** Select from the following options:
  - Do not allow user saving password
  - Allow user saving password for https stores only
  - Allow user saving password for http and https stores
- **Allow user to add stores:** Select from the following options:
  - Do not allow user to add stores
  - Allow user to add https stores only
  - Allow user to add http and https stores
- **Allow the use of http stores:** If this option is enabled, the client can connect to stores even without encryption (via HTTP).
- **Logon mode:** Select from the following options:
  - Prompt user
  - Smart card logon
  - Pass-through authentication
  - Pass-through with smart card authentication

## Appearance

Menu path: **Setup > Sessions > Citrix > Self-Service Plugin > Appearance**

- **Use categories from published applications as submenu path:** If this option is enabled, the applications will be sorted according to categories in the start menu.
- **Additional submenu in Startmenu:** Here, you can specify a directory which contains the applications in the start menu.
- **Additional submenu on Desktop:** Here, you can specify a directory which contains the applications on the desktop.
- **Enable Citrix Receiver Selfservice Mode:** If this option is enabled, you will find the applications in a custom self-service GUI.
- **Give users the option to add or remove accounts in Non-Self-Service Mode:** If this option is enabled and Selfservice Mode is not active, the user can edit accounts via the Citrix Receiver context menu in the Accounts system tray.

## Desktop integration

Menu path: **Setup > Sessions > Citrix > Self-Service Plugin > Desktop Integration**

- **Login Session Name:** Give the name of the session which is to be shown.
- **Starting Methods for Session:**
  - **Put shortcuts in Startmenu:** If this option is enabled, an entry will be created in the start menu.
  - **Put shortcuts on Desktop:** If this option is enabled, a link will be placed on the desktop.
  - **Autostart:** If this option is enabled, the session will start automatically when the user logs on to the device.

## 6.2. Remote Desktop Protocol – RDP

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

The Microsoft RDP client is used for connections via the Remote Desktop Protocol (RDP). The configuration of the client was ported to the IGEL Setup.

➡ You will find detailed information regarding Microsoft RDP on the website <http://technet.microsoft.com>.

- **Use IGEL Setup for configuring RDP settings:** If this option is enabled, you can configure RDP via the IGEL Setup.

### 6.2.1. RDP (global settings)

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

A number of settings that are effective in RDP sessions can be pre-set globally and can be used as standard in newly created sessions or overwritten in the session configuration.

- **Window:** Allows you to set the number of colors, display via several monitors, multi-monitor support and the window size
- **Mapping:** Allows you to assign audio, keyboard hotkeys, printers, COM ports, smartcards and drives to the session
- **Performance:** Performance-relevant settings such as desktop background, font smoothing, video redirection, bitmap cache and compression
- **Options:** Allows you to set the application, work directory, options for authentication and configuration for an RD Gateway server
- **USB Redirection:** Allows you to prohibit and enable RemoteFX USB redirection for individual USB devices

### Logon

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

- **Server:** Allows you to specify the server to connect to.
- **User Name:** Allows you to specify the user name.
- **Domain:** Allows you to specify the domain.
- **Reconnect:** If this option is enabled, the client will automatically reconnect if the connection was terminated.

### Window

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

- **Number of Colors:** Allows you to specify the standard color depth.
- **Span desktop:** If this option is enabled, the RDP session will use all available monitors as a desktop.
- **True Multimonitor support:** If this option is enabled, the user can connect with multi-monitor configurations.
- **Window size:** Choose between **fullscreen** and a range of fixed sizes.
- **Display the Connection Bar:** If this option is enabled, a symbol bar for minimizing and closing a full-screen session will be shown.

## Keyboard

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



These settings can only be configured globally here and cannot be overwritten in the sessions.

- **Enable Clipboard Mapping:** If this option is enabled, content can be shared between the local system and the session via the clipboard.
- **Overwrite local window manager keyboard shortcuts:** If this option is enabled, the session shortcuts will override equivalent local ones.
- **Redirect Ctrl-Alt-Del to sessions:** If this option is enabled, this key combination will not be processed by the local thin client. It will be forwarded to the session instead.

## Mapping

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

- **Enable Client Audio:** Select one of the following options:
  - On - local
  - On - remote
  - Off
- **Audio Recording Redirection**
- **Overwrite local window manager keyboard shortcuts:** If this option is enabled, the session shortcuts will override equivalent local ones.
- **Enable Printer Mapping**
- **Enable COM Port Mapping:** If this option is enabled, local COM ports will be available in the session.
- **Enable Smart Card Mapping:** Redirect smartcards.
- **Enable Clipboard Mapping:** If this option is enabled, content can be shared between the local system and the session via the clipboard.
- **Enable Drive Mapping:** Provide local drives during a session:
  - Map all Drives
  - Specific drives (select)
  - Drives that I connect to later

## Performance

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

- **Detect connection quality automatically:**

If you disable this option, you can manually configure the following settings for reducing visual effects in order to conserve resources:

- **Disable Wallpaper**
- **Don't show contents of window while dragging**
- **Disable Menu and Window animation**
- **Disable Themes**
- **Disable Cursor Settings**
- **Disable Font Smoothing**
- **Disable Desktop Composition**

- **Video Redirection:** If this option is enabled, videos will be played back locally.
- **Redirect DirectX commands:** Graphics functions are executed locally.
- **Disable Bitmap cache:** Images are not cached locally.
- **Compression:** If this option is enabled, the data transferred will be compressed.



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

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

## Options

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

- **Application:** Specify a start-up application for the terminal server session.
- **Working Directory:** Specify the working directory.
- **Authentication Options:** Select from the following options to check whether the server authenticates itself correctly:
  - **Always connect, even if authentication fails**
  - **Do not connect if authentication fails**
  - **Warn me if authentication fails**

Select from the following options for the RD Gateway:




- **Automatically detect RD Gateway server settings**
- **Do not use a RD Gateway server:** Direct connection to the RDP server
- **Use these Gateway server settings:** If you choose this option, edit the following settings:
  - **Server name**
  - **Login method:** Choose from **Allow me to select later**, **Ask for password (NTLM)** and **Smart Card**.
  - **Bypass RD Gateway server for local addresses:** If this option is enabled, no gateway will be used for connections within the local network.
  - **Use my RD Gateway credentials for the remote computer**

## USB Redirection

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

- **Enable RemoteFX USB redirection:** If this option is enabled, you can allow or prohibit redirection.

### 6.2.2. RDP sessions

- Click  to create a new session..
- Click  to delete the session.
- Click  to edit the session.

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

<b>Server</b>	Allows you to specify a server and a start-up application for the terminal server session.
<b>Logon</b>	The necessary logon information is configured here. Otherwise, the terminal server logon window for entering the user and the password will be displayed.
<b>Window</b>	Allows you to specify the size of the session window and the color mode. The local taskbar can be configured so that it remains visible during a full-screen session.
<b>Performance</b>	Allows you to disable non-essential graphical functions such as skin styles, window animation etc. This is useful in the event of performance problems.
<b>Mapping</b>	<p>Allows you to specify the audio output device (local/remote) and determine how key strokes and clipboard content are handled. The mapping of serial connections and local drives can be enabled for a session.</p> <p>You can make connected mass storage devices available to the user using the appropriate mapping: Select <b>Enable</b>, choose the drive letter and the device to be mapped.</p>
<b>Options</b>	Allows you to specify the start application and the work directory for use during the session (how authentication errors are handled during the logon procedure). If, when connecting to the server, a terminal server gateway is to be used, you can configure the relevant settings here (No Gateway is pre-set).
<b>Desktop integration</b>	Allows you to set up the start options via the desktop or start menu / autostart.



## Server

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

Choose between the following modes:

- **Server:** If this option is selected, you only need to enter the **Server**.
- **Enable RemoteApps mode:** If this option is selected, fill in the following fields:
  - **RemoteApp Server Port:** Network port via which the application is offered, the default setting is 3389.
  - **Program to execute**
  - **Name for the executed program**
  - **Commandline Parameters for the executed program**

## Logon

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

- **User Name:** Allows you to specify the user name
- **Domain:** Allows you to specify the domain
- **Reconnect:** If this option is enabled, the client will automatically reconnect if the connection was terminated.

## Window

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

- **Window Size:** Choose between **default**, **fullscreen** and a range of fixed sizes.
- **Number of Colors:** Allows you to specify the standard color depth
- **Span desktop over all displays:** If this option is enabled, the RDP session will use all available monitors as a desktop.
- **True Multimonitor support:** If this option is enabled, the user can connect with multimonitor configurations.
- **Display the Connection Bar:** If this option is enabled, a symbol bar for minimizing and closing a fullscreen session will be shown.

## Performance

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

- **Detect connection quality automatically:**

If you disable this option, you can manually configure the following settings for reducing visual effects in order to conserve resources:

- Disable Wallpaper
- Don't show contents of window while dragging
- Disable Menu and Window animation
- Disable Themes
- Disable Cursor Ssettings
- Disable Font Smoothing
- Disable Desktop Composition
- **Video Redirection:** If this option is enabled, videos will be played back locally.
- **Redirect DirectX Commands:** Graphics functions are executed locally.
- **Disable Bitmap cache:** Images are not cached locally.
- **Compression:** If this option is enabled, the data transferred will be compressed.



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

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

## Mapping

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

- **Enable Client Audio:** Select one of the following options:
  - On - local
  - On - remote
  - Off
- **Audio Recording Redirection**
- **Overwrite local window manager keyboard shortcuts:** If this option is enabled, the session shortcuts will override equivalent local ones.
- **Enable Printer Mapping**
- **Enable COM Port Mapping:** If this option is enabled, local COM ports will be available in the session.
- **Enable Smart Card Mapping:** Redirect smartcards.
- **Enable Clipboard Mapping:** If this option is enabled, content can be shared between the local system and the session via the clipboard.
- **Map all Drives**
- **Specific drives (select)**
- **Drives that I connect later to**

## Options

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

- **Application:** Specify a start-up application for the terminal server session.
- **Working directory:** Specify the working directory.
- **Authentication Options:** Select from the following options to check whether the server authenticates itself correctly:
  - Always connect, even if authentication fails
  - Do not connect if authentication fails
  - Warn me if authentication fails

Select from the following options for the RD Gateway:

- **Automatically detect RD Gateway server settings**
- **Do not use a RD Gateway server:** Direct connection to the RDP server
- **Use these Gateway server settings:** If you choose this option, edit the following settings:
  - **Server name**
  - **Login method:** Choose from **Allow me to select later**, **Ask for password (NTLM)** and **Smart Card**.
  - **Bypass RD Gateway server for local addresses:** If this option is enabled, no gateway will be used for connections within the local network.
  - **Use my RD Gateway credentials for the remote computer**

## Desktop integration

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

- **Session Name:** Give the name of the session which is to be shown.
- **Starting Methods for Session:**
  - **Start Menu:** If this option is enabled, an entry will be created in the start menu.
  - **Desktop:** If this option is enabled, a link will be placed on the desktop.
  - **Autostart:** If this option is enabled, the session will start automatically when the user logs on to the device.

## 6.3. Horizon Client

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

To create a new Horizon client session, proceed as follows:

1. Click on **Add** in the **Session** menu.  
The **Connection Settings** page appears.
2. Select the necessary server data and advanced options, e.g. **kiosk mode**.
3. Configure the display settings (window size) and the integration of local USB devices (mapping).

Figure 5: Connection settings

- ➡ You will find a detailed description of the client parameters in the original documentation for Horizon at [http://www.vmware.com/support/pubs/view\\_pubs.html](http://www.vmware.com/support/pubs/view_pubs.html).
- ➡ *Note regarding the use of ThinPrint within the Horizon session (page 43)*

### 6.3.1. Horizon Client Global

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

- **Keyboard** (cannot be overwritten in the sessions):
  - **Redirect Ctrl-Alt-Delete to sessions:** If this option is enabled, this key combination will not be processed by the local thin client. It will be forwarded to the session instead.

## 6.4. vWorkspace Client and AppPortal

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

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

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

- ➔ All configuration parameters for the vWorkspace Client and the vWorkspace AppPortal farm are described in detail in the original documentation for the relevant client version. See <https://support.software.dell.com/vworkspace/8.0.1>.



In the IGEL setup, parameter settings can be configured for each farm. Alternatively, details of a configuration file (XML) which is saved at a different location are given there. Direct configuration of the client outside the IGEL setup is not possible.

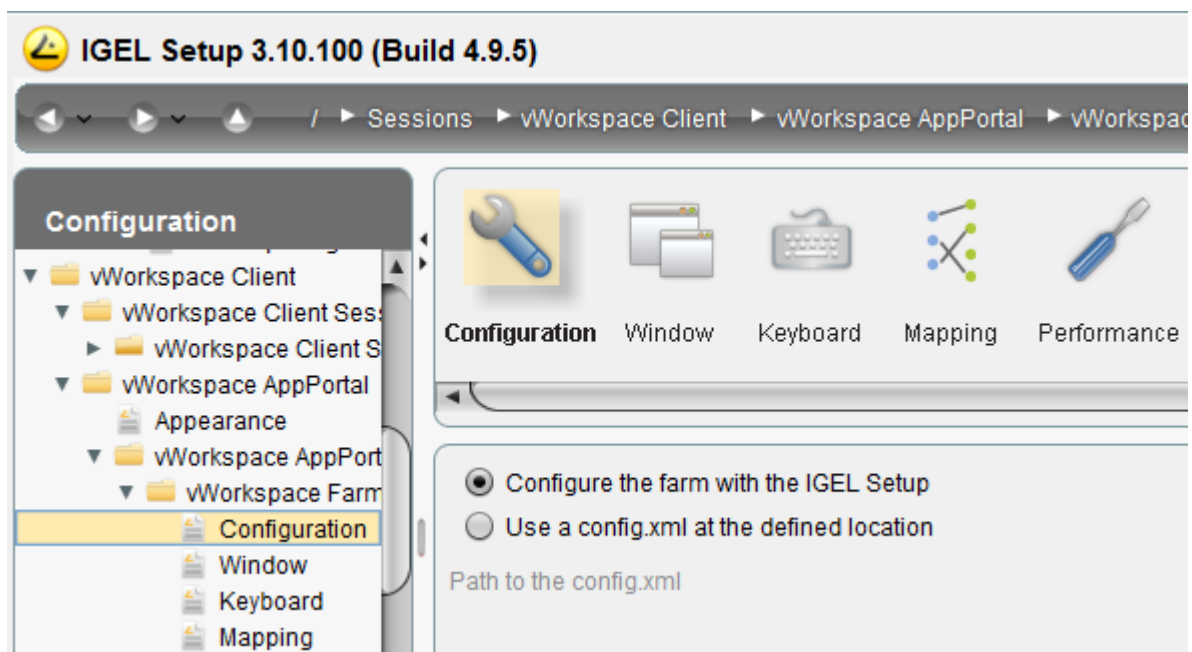


Figure 6: Configuration in the IGEL setup

## 6.5. Leostream

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

- Specify the **server**, **user** and **domain** for logging on with Leostream Connection Broker and enter details of the desktop you would like to connect.

If you do not specify a desktop, you will be given a list of available desktops when you log on.

In the administration for the Leostream Connection Broker, you need to configure the connection plan so that RDP is used on a priority basis for the connection. The three protocols RDP, rdesktop and Ericom Blaze use the same port 3389. The priority for RDP must therefore be higher than that for the other two protocols.

This screenshot shows the use of rdesktop with preference over RDP, e.g. for connecting to IGEL UD Linux thin clients.

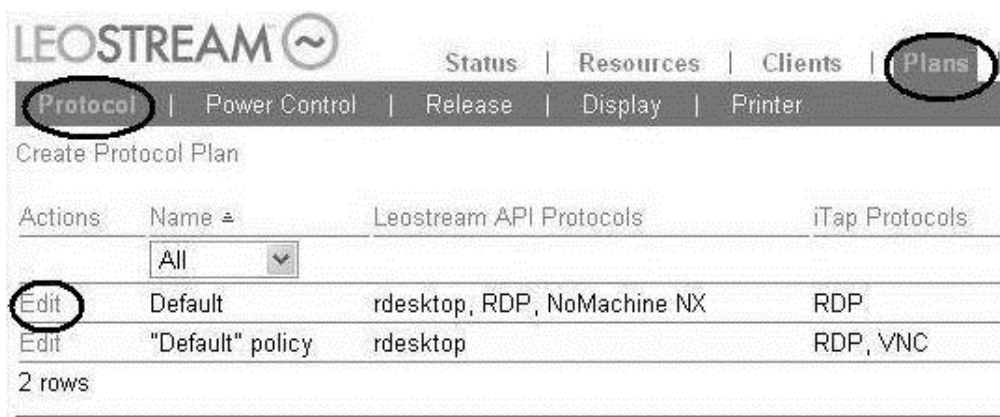


Figure 7: Leostream protocol

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

## 6.6. NX Client

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

The configuration parameters available depend on the server setting. Depending on what session type (Unix, Windows, VNC or Shadow) is being used, the irrelevant setup pages will be grayed out.

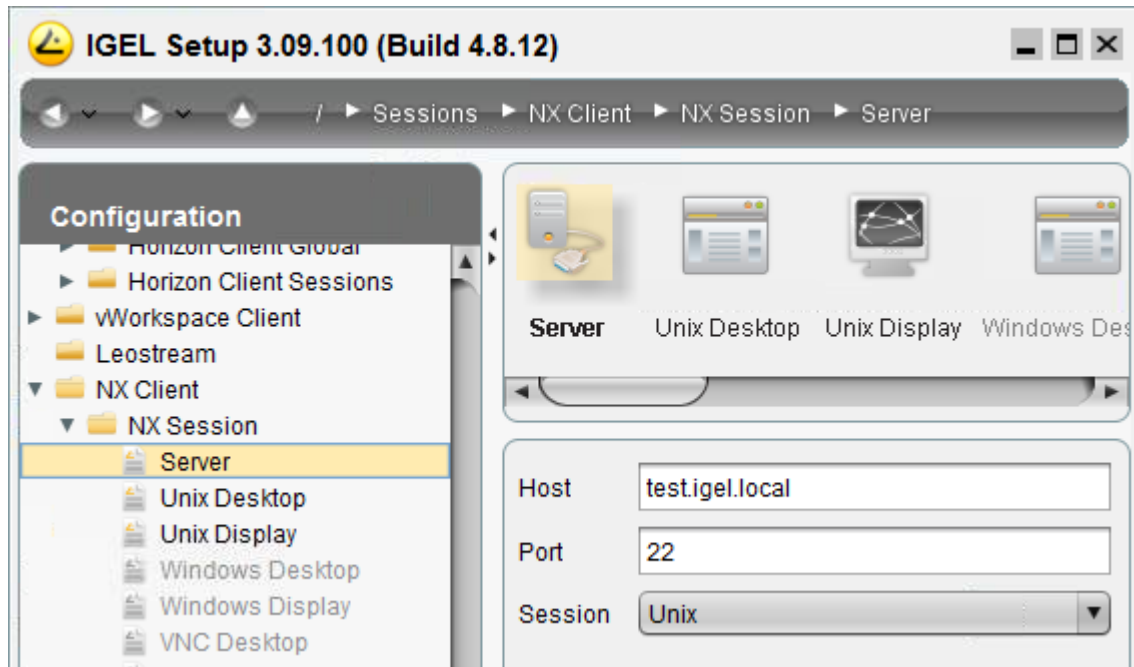


Figure 8: Nomachine NX configuration parameters

- ➡ Further information regarding configuration details such as server settings, performance, services etc. can be found in the original documentation from Nomachine at <http://www.nomachine.com/documents.php>.

## 6.7. PowerTerm WebConnect

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

With **PowerTerm WebConnect**, you have both local and remote access to applications on Windows terminal servers, virtual desktops, hypervisors such as VMware, Microsoft, Xen and Virtual Iron, blade PCs and legacy hosts.

- Enter the **host name** of the WebConnect server you would like to establish a connection to.
- ➡ The server configuration is described in the WebConnect documentation from Ericom: <http://www.ericom.com/doc/QRG/WebConnectGettingStarted.pdf>.

## 6.8. PowerTerm Terminal Emulation

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

On IGEL thin clients with Windows Embedded Standard, PowerTerm InterConnect software from ERICOM Software Ltd. is used for interaction with legacy host systems.

To open the **PowerTerm Emulation Setup**, proceed as follows:

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

The **PowerTerm Emulation Setup** window opens.

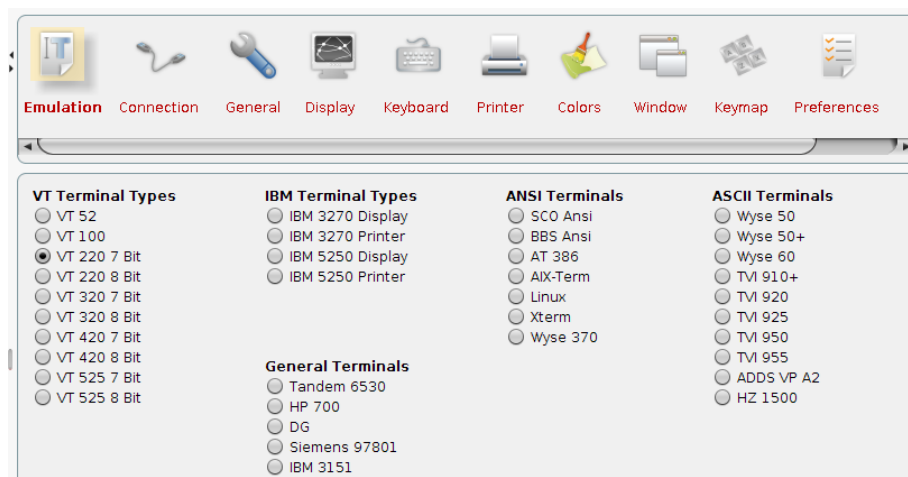


Figure 9: PowerTerm emulation setup

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

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

➡ You will find detailed information on configuring the PowerTerm software on the Ericom documentation website <http://www.ericom.com/help.asp?cat=support>.



## 6.9. Browser Sessions

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

Under **Browser Sessions**, you can configure the **Microsoft Internet Explorer** in the IGEL setup.

The following setup pages are available:

<b>Global</b>	Allows you to set up the global browser data such as start page or download directory etc.
<b>Security</b>	Allows you to permit SSL/TSL-encrypted connections and set up warnings in the event of zone changes
<b>Advanced</b>	Allows you to specify how images and sounds embedded in websites are handled.
<b>Start</b>	Allows you to specify the locations from which access to the browser application is possible.
<b>Window</b>	Allows you to set the full-screen or theater mode
<b>Proxy</b>	Allows you to configure proxy settings.
<b>Toolbar Items</b>	Allows you to disable/enable various menu parameters such as the print dialog or the <b>Close</b> button.
<b>Toolbars</b>	Allows you to configure symbol bars shown in the browser application.



To enable the original settings (in the IE menu), disable the IGEL settings for the MSIE.

### 6.9.1. Browser sessions

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

In this area, you can change various settings for the Microsoft Internet Explorer.

- **Show pictures:** If this option is enabled, images on websites will be shown.
- **Play sounds in webpages:** If this option is enabled, the background sound of a website will be played. Playback will begin as soon as the page is opened.
- **Show friendly HTTP error messages:** If this option is enabled, a user friendly error message without details will be shown in the event of a problem with HTTP communication. If the option is disabled, the error message will contain details to help rectify the error.
- **Automatically enable newly installed add-ons:** If this option is enabled, newly installed add-ons will be enabled automatically. If the option is not enabled, a user prompt asking whether the add-on is to be enabled will appear the first time the browser starts following installation.

## 6.10. Windows Media Player

Menu path: **Setup > Sessions > Windows Media Player**

Under **Windows Media Player**, you will find parameters for controlling the Windows Media Player (Version 12).

- ➔ Help for using the current Media Player is available from Microsoft:  
<http://windows.microsoft.com/en-us/windows/music-photos-video-help>.

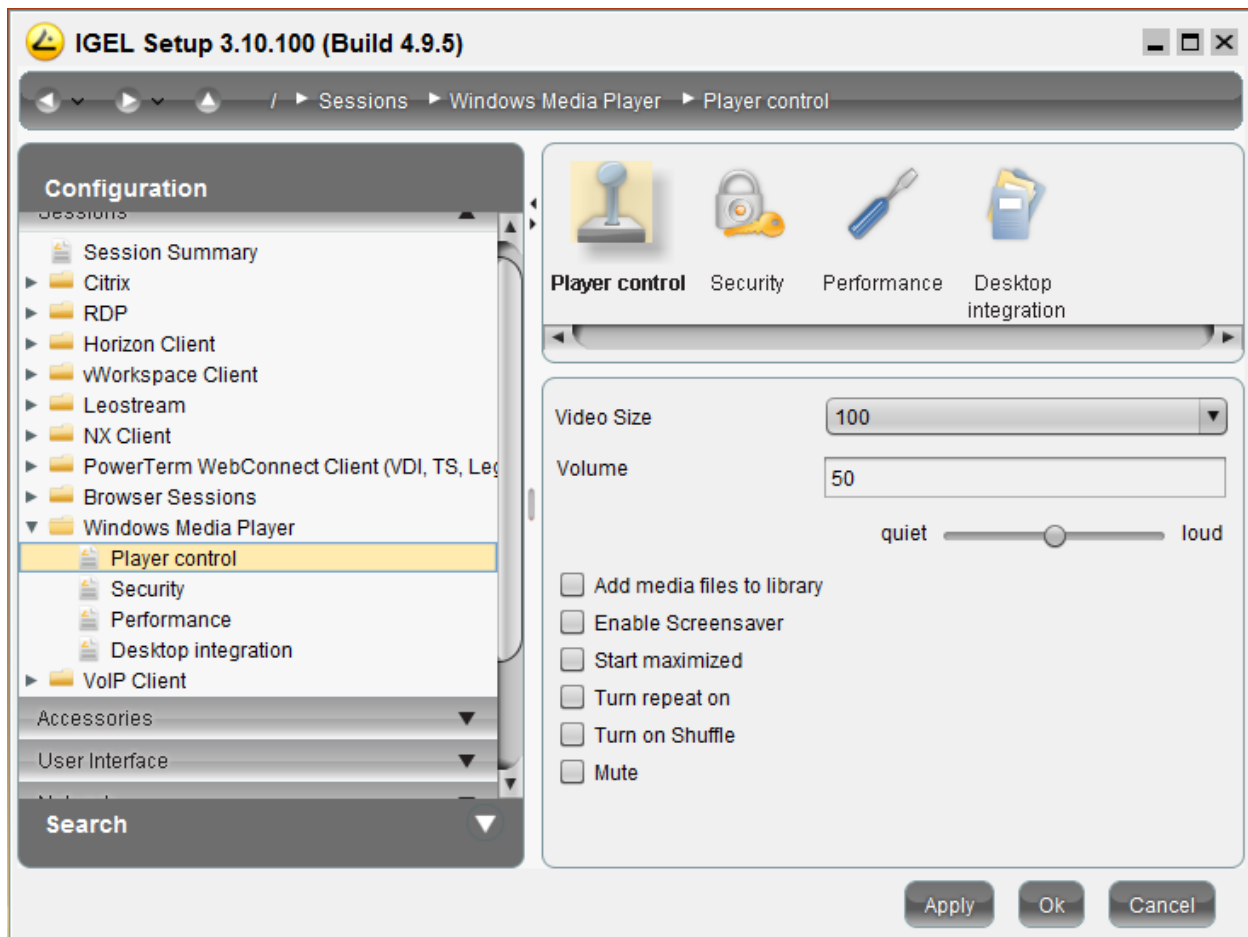


Figure 10: Player control in the IGEL setup

## 6.11. VoIP Client

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

In the **VoIP Client** section, you can configure the client for IP telephony. IGEL Universal Desktop provides the VoIP client Ekiga (<http://ekiga.org>). The client allows the use of SIP and H.323. In addition to local contacts, LDAP address books can be used too.

➔ You will find a detailed description of the configuration options in the original documentation for the Ekiga client at <http://wiki.ekiga.org/index.php/Manual>.

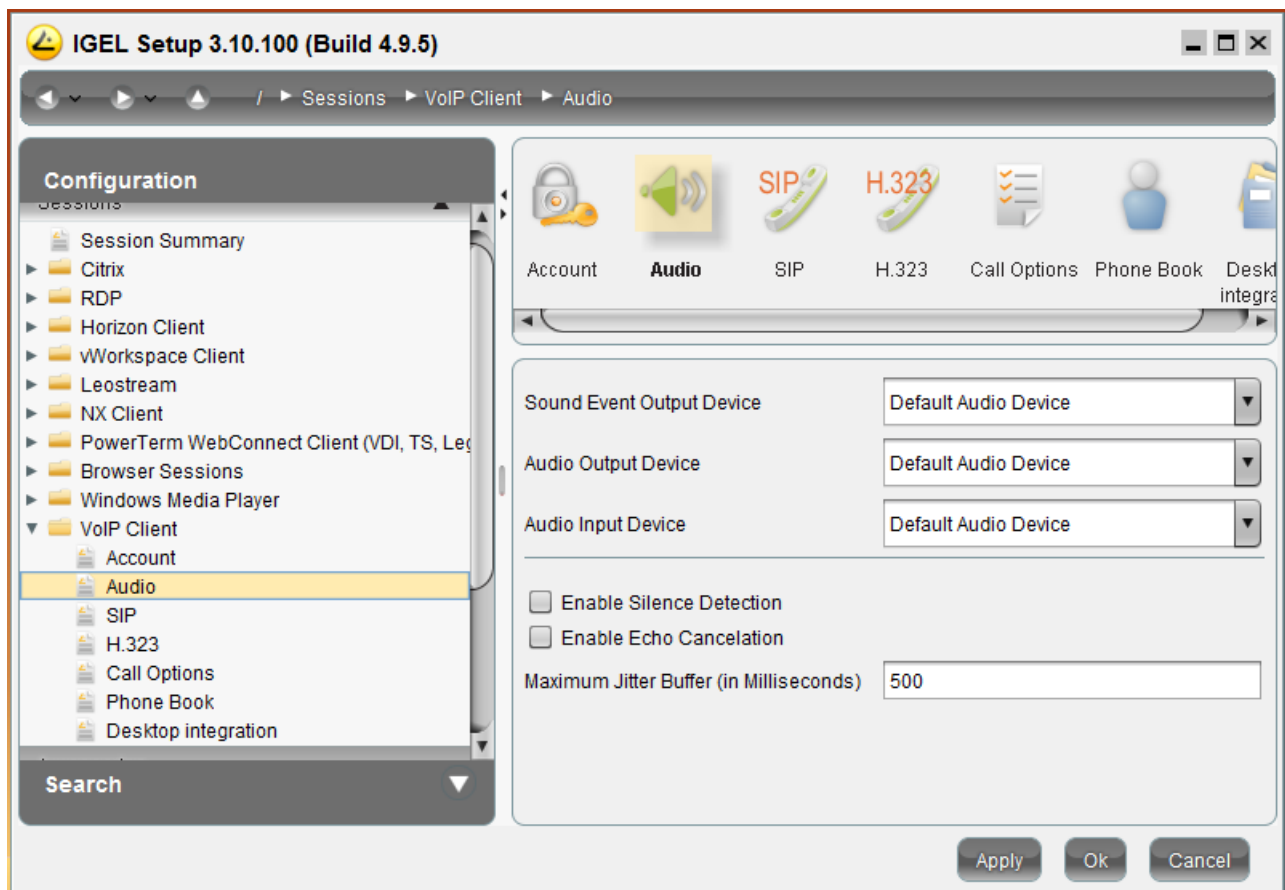


Figure 11: Configuration for IP telephony

## 7. Accessories

Menu path: **Setup > Accessories**

### 7.1. Setup Session

Menu path: **Setup > Accessories > Setup Session**

If an Administrator password has been set, IGEL Setup can only be opened by an Administrator after entering the password (see *password* (page 44)). However, selected Setup Sections can be made available to users, e.g. to let them change the language or configure a lefthand mode for the mouse.

1. Activate the Administrator and Setup user passwords under **Security > Password**.
2. Under **Accessories > Setup Sessions > User Page Permissions**, unlock the items you want to make available to users.
  - A checked checkbox means that an item is visible in Setup,
  - a green symbol (open padlock) means, that a user can change the parameter.

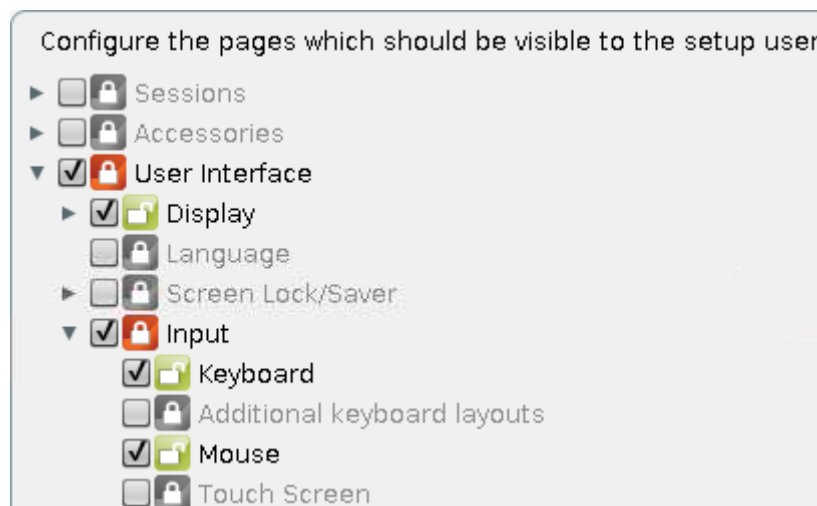


Figure 12: Restricted access to the setup



If you unlock a Setup item at a low hierarchy level, the levels required to access it are made visible automatically, but remain read-only.

## 7.2. Sound Mixer

Menu path: **Setup > Accessories > Sound Mixer**

Set the **Master volume** or **Mute** the device here.

## 7.3. Windows Services

Menu path: **Setup > Accessories > Windows Services**

Here, you can launch or disable Windows services. These include **USB redirection**.

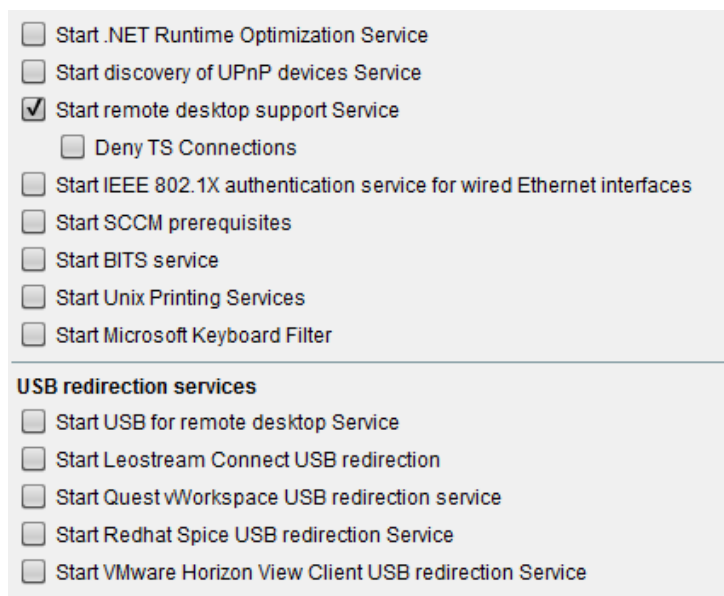


Figure 13: Windows services

## 8. User interface

Menu path: **Setup > User Interface**

### 8.1. Display

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

The basic and advanced screen settings can be configured as standard in the IGEL setup or via the Windows system options.

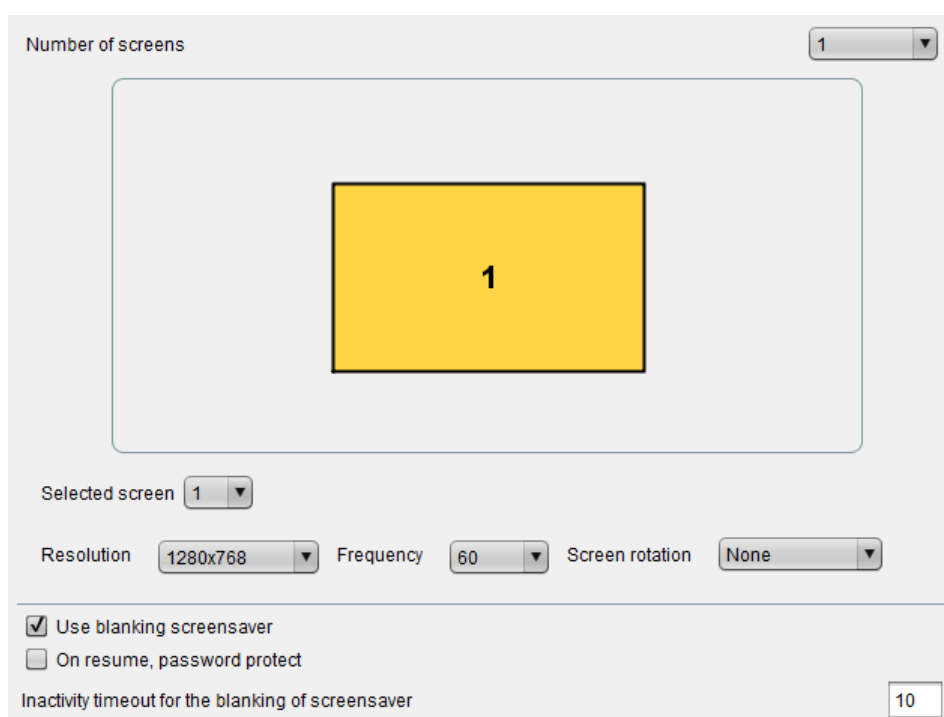


Figure 14: Advanced screen settings

To configure multiscreen environments in the IGEL setup, proceed as follows:

1. Increase the **Number of Screens** parameter.
2. Select the associated resolutions.
3. Specify the position of the screens in relation to each other.

For details of the maximum resolutions supported by IGEL models, please see the data sheet for the relevant device.

W7 – For the rotation (pivot), at least 128 MB as video memory must be configured in the client's BIOS (default is 64 MB). You will find the setting under **Integrated Peripherals>VGA Shared Memory Size** in the BIOS. If a screen rotation is configured and less than 128 MB of video memory is set, a corresponding message will appear:

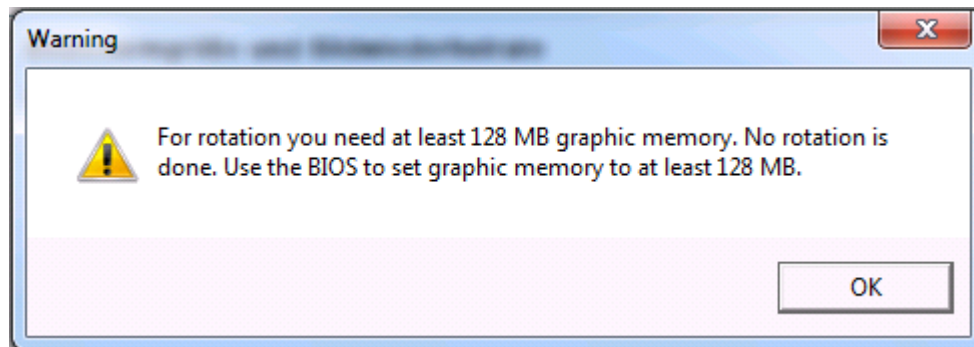


Figure 15: Warning notice for insufficient video memory

## 8.2. Language

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

Select the setup language and the keyboard layout, and configure your local settings (format for time, numbers etc.).

For UD W7 systems, language packages are available as partial updates on the <http://myigel.biz> website. These allow you to change the system language too.



Installing language packages for UD-W7 can take up to 45 mins! Do not cancel the procedure prematurely as this could result in system inconsistencies!

## 8.3. Input

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

In the **Input** area, you can define the keyboard and mouse specifications such as keyboard layout, left-hand mode for the mouse or double-click settings. These settings override the Windows system settings.

## 8.4. Desktop and Start Menu

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

Selected options:

- **Show recycle bin on the desktop:** The recycle bin is hidden as standard.
- **Set Taskbar Changeable:** The taskbar can be changed.
- **Disable Lock workstation:** Disables the option for locking the desktop via **Win+L** or **Ctrl+Alt+Del**.
- **Sort Start Menu Item Alphabetically:** This allows you to arrange all entries in the start menu in alphabetical order.

## 8.5. Shell

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

In this area, you can specify which configuration dialogs are to be available for users and/or administrators via the Control Panel.



## 9. Network

Menu path: **Setup > Network**

Configure the network parameters for each available interface (LAN / WLAN) and connect network drives.

### 9.1. LAN and Wireless

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

Here you will find the configuration parameters for the available LAN and WLAN interfaces.

The internal **LAN** interface is pre-configured for DHCP as standard.

In the **WLAN** area, you will find all parameters for the wireless network including the options for encrypting the connection. Configure hidden networks by entering the WLAN name (SSID).



Please note that the settings for the Windows system are initially active when configuring the wireless connection. Enable the use of the IGEL setup for WLAN in the setup.

### 9.2. VPN Connection

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

Create a session for using the NCP Secure Enterprise Client. The VPN connection is configured exclusively via the GUI of the VPN client. NCP provides its own management software for remote administration of the clients.

➡ Further information regarding configuration and use is available from NCP:  
<https://www.ncp-e.com/en/resources/library/manuals.html>



Please note that the NCP Secure Enterprise Client must be licensed separately with NCP in order to be able to use it on a permanent basis.

### 9.3. Routing

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

In order to use a specific network route, define the **Gateway** for forwarding on this page. Specifying the network interface is optional. The route affects all network devices used.

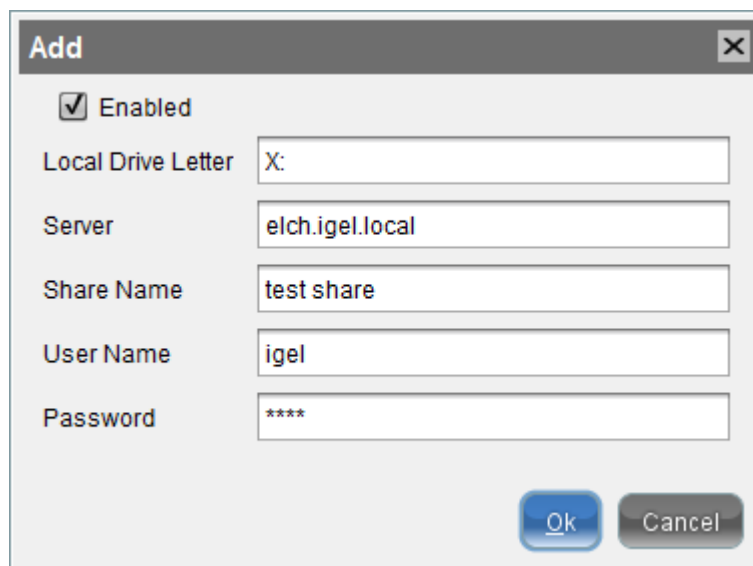
## 9.4. Network Drives

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

Under **Network Drives**, you determine both the drives that are to be connected during booting and the associated logon data.

You can allocate a drive letter for each drive.

- If no letter is entered, the drive will need to be connected manually later on.
- If the logon data for the relevant server were saved in the IGEL setup, no further logon data will be requested.
- If the letter allocated is already reserved, only the drive connected first will be shown. An error entry for the second will appear in the event log.

The image shows a 'Add' dialog box with a close button (X) in the top right corner. It contains several fields: a checked 'Enabled' checkbox, 'Local Drive Letter' with 'X:' entered, 'Server' with 'elch.igel.local' entered, 'Share Name' with 'test share' entered, 'User Name' with 'igel' entered, and 'Password' with '\*\*\*\*' entered. At the bottom right are 'Ok' and 'Cancel' buttons.

<input checked="" type="checkbox"/> Enabled	
Local Drive Letter	X:
Server	elch.igel.local
Share Name	test share
User Name	igel
Password	****
<input type="button" value="Ok"/> <input type="button" value="Cancel"/>	

Figure 16: Add network drives

# 10. Devices

Menu path: **Setup > Devices**

## 10.1. Printer

Menu path: **Setup > Devices > Printer**

In this area, you can set up your local printers. Decide whether you would like to configure a printer in the IGEL Setup or via the configuration file.

➡ Please note our FAQs regarding *Thin Print* <http://edocs.igel.com/index.htm#10203398.htm>.

## 10.2. Attached Devices

Menu path: **Setup > Devices > Attached devices**

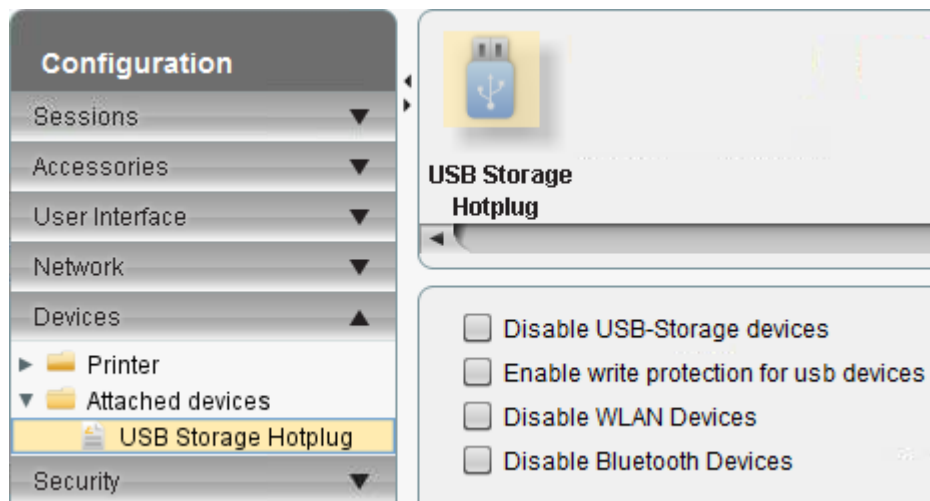


Figure 17: Device configuration

On this setup page, you can enable or disable the use of various USB device types. A distinction is made between three types.

- USB storage devices
- WLAN devices
- Bluetooth devices

Each of these types can be disabled. USB devices can also be connected in a read-only manner (with write protection).

# 11. Security

Menu path: **Setup > Security**

## 11.1. Password

Menu path: **Setup > Security > Password**

You can set up an administrator password in order to protect the IGEL Setup application. Access to the setup is then only possible with this password.

The password allowing the administrator to log on to the system and the setup password can be different. Changes to passwords are only saved if you click on the **OK** or **Apply** button.

You can also allocate a password for the `User` user. If the setup user is enabled too, `User` can also access approved setup pages. You can configure these under **Accessories > Setup Session**.

**Automatic logon:** Specify a user who is automatically logged on when the system starts. The `User` user is logged on as standard.

The administrator password for the setup application is also queried if you call up the boot menu by pressing **ESC** when starting the rescue shell or firmware update.



It is strongly recommended that you change the administrator password after starting the thin client for the first time. Only the administrator can change passwords.

## 11.2. Active Directory

Menu path: **Setup > Security > Active Directory**

On this page, you can configure access to your Active Directory domain. Add the necessary domain and the user information for access to the Active Directory domain.

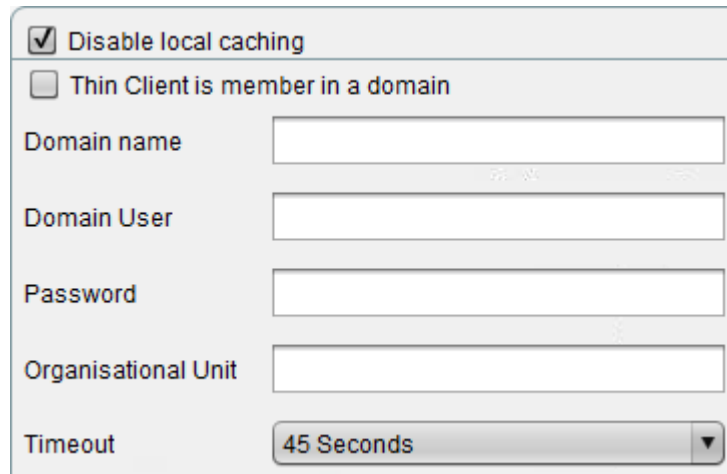


Figure 18: Configuration for Active Directory domain



When taking a snapshot of the system, it often makes sense to leave the domain beforehand. A corresponding option can be set in the **Snapshot** menu.

## 11.3. Network

Menu path: **Setup > Security > Network**

Deactivate administrative shares here or hide the device by activating **Do not show Thin Client in network**.

## 11.4. Windows Firewall

Menu path: **Setup > Security > Windows Firewall**

Set rules for **Windows Firewall** here, Program Rules and Port Rules are available.

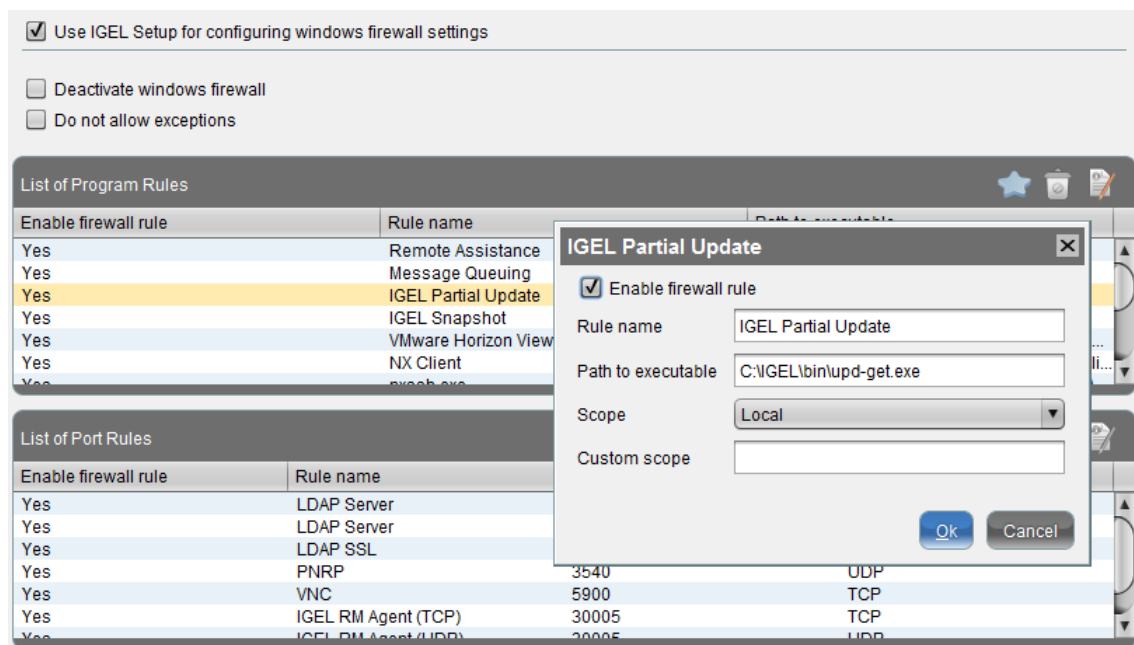


Figure 19: Firewall Rules

# 12. System

Menu path: **Setup > System**

In the sub-structure, you can configure a number of basic system settings:

## 12.1. Date and Time

Menu path: **Setup > System > Date and Time**

Set the correct time zone for the location of your device. If necessary, enable time synchronization and select the time server and the update interval.

## 12.2. Update

Menu path: **Setup > System > Update**

Two procedures for updating the system are available:

- **Snapshots** for updating the Windows Embedded System, including the IGEL firmware functions.
- **Partial updates** for adding new functions or language packages.

### 12.2.1. Snapshots

A **snapshot** is an image of the first partition (Volume C:) which contains the Windows Embedded Standard operating system. You can use this image either for system restoration or for distribution to other IGEL Windows Embedded devices which are equipped with the same hardware. Firmware updates from IGEL too are made available as a snapshot file (.snp).

The web server of the IGEL Universal Management Suite can be used to create and install snapshots. Further information can be found in the IGEL UMS manual.

### Creating a snapshot

To create a snapshot of the current system, proceed as follows:

- Define the transmission protocol for the target server used (HTTP or HTTPS and FTP)  
or select `file` in order to save the snapshot locally, e.g. on a connected USB storage device.



In order to use `file`, at least 4 GB of free storage space must be available on the storage device. Create the path `\igel\snapshots` beforehand. To create the snapshot, specify the file name only.

You can also prepare a USB storage device for use as a snapshot storage device. In this case, the selected drive will be formatted and the path mentioned above will be created.

- Click on **Prepare USB Device**.

All data on the selected drive will be deleted!

If the snapshot file is to be ported to other devices, specify in advance that the domain to which the device was added is left.

## Firmware update via snapshot

Firmware updates are made available as snapshots on the IGEL download server <http://myigel.biz>.

1. Download the zipped `.snp` file.
2. Make the file available to the thin clients: either on your own FTP or HTTP server in the network or locally on a USB storage device.
3. Using this snapshot, execute the thin client's **Download Snapshot** function.

The alternative method using the Universal Firmware update mechanism of the Universal Management Suite is described in more detail in the UMS manual.

## Downloading a snapshot

An existing snapshot can also be installed via HTTP(S), FTP or directly via a connected storage device. In the latter case, the snapshot will be searched for in the path `\igel\snapshots`. Specify only the file name without a path here.



Do not interrupt the download or the use of the snapshot. This could result in system inconsistencies.

The option **Reset Terminal Settings** deletes the configuration performed in the setup and the UMS registration with the client-side certificate. All parameters are reset to their defaults. The data on the user's partition (Volume F:) are also deleted. The firmware licenses, however, are retained.

### 12.2.2. Partial update

The IGEL mechanism for partial updates allows you to make changes to IGEL thin clients with Windows Embedded Standard without transferring the complete system via snapshot. The changes are made with the help of scripts which are downloaded to the clients and then executed through a scripting engine on the basis of the scripting language Lua.

This mechanism distributes scripts from a server to clients. IGEL has supplemented the script language with modules. As a result, you can access system services such as:

- Windows registry
- File system operations
- IGEL setup data interface
- Executing a process
- Rebooting
- Shutting down the operating system
- HTTP and FTP access

The extensions with the name Luna and the complete reference can be found in the Luna reference.

The Tomcat Web Server in the IGEL Universal Management Suite can be used to install partial updates. It can also be used to distribute updates via profile to a number of clients. More detailed information can be found in the IGEL UMS manual.



## Installing partial updates

To install partial updates on the system, proceed as follows:

1. Bring up the update configurations in the setup via **System > Updates > Partial Update**.
2. Check the **Partial Update** checkbox.
3. Select a transmission protocol.
4. Specify the source server/path on the drive.
5. Click on **Apply** to save the settings.
6. Click on **Search for Updates** to search the source for updates.

Available updates can then be installed directly. The device will reboot for this purpose. It will also reboot after the update has been installed.

### 12.2.3. Available options

#### Update when booting

Partial updates of the source will be installed automatically the next time the client is rebooted. This option is particularly recommended for configuration via the IGEL UMS.

#### Show installed packages

Update packages already installed are registered in the system and are listed here.



If Microsoft IIS (Internet Information Services) is used as the HTTP server in order to provide files for the partial update, you must configure the server in such a way that it accepts download inquiries for all files regardless of the MIME type. If FTP is used for file transmission, no such restrictions apply.

## 12.3. Remote Management

Menu path: **Setup > System > Remote Management**

Here, you can configure settings relating to the remote administration of the client using the Universal Management Suite (UMS).

- **Enable Remote Management:** If this option is enabled, you can administer the client using the UMS.
- **Universal Management Suite Server:** If the client is already registered on a UMS, the UMS will be in this list. Otherwise, enter the host name or IP address and the port number of the UMS on which the client is to register.



The list can contain more than one UMS instance. If the client cannot contact a UMS under the host name `igelrmserver`, and the DHCP option 244 is not set, the client will go through the entries in the list until it can contact a UMS successfully.

- **Enable User information:** If this option is enabled, a message window will inform the user that the client is receiving new settings from the UMS or is being shut down.
  - **User Information Message Timeout:** Number of seconds for which the message window is shown.
  - **Universal Management Suite Structure Tag:** Give a Structure Tag indicating into which directory the client is automatically sorted in the UMS.
- ➡ Further information regarding the use of Structure Tags can be found in the *"Using Structure Tags" Best Practice* (<http://edocs.igel.com/index.htm#10202089.htm>)

## 12.4. Shadow

Menu path: **Setup > System > Shadow**

For helpdesk purposes, you can observe the client through shadowing. This is possible via the IGEL Remote Manager or another VNC client (e.g. TightVNC). The options for the VNC functions are as follows:

Ask user for permission	In a number of countries, unannounced mirroring is prohibited by law. Do not disable this option if you are in one of these countries!
Allow entries from remote computer	If this option is enabled, the remote user may make keyboard and mouse entries as if they were the local user.
Use password	Enable this option to set up a password which the remote user must enter before they can begin mirroring.

### 12.4.1. Secure shadowing (VNC with SSL)

Menu path: **Setup > System > Shadow**

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

- **Encryption:** The connection between the shadowing computer and the shadowed client is encrypted. This is independent of the VNC viewer used.
- **Integrity:** Only clients in the UMS database can be shadowed.
- **Authorization:** Only authorized persons (UMS administrators with adequate authorizations) can shadow clients.

Direct shadowing without logging on to the UMS is not possible.

- **Limiting:** Only the VNC viewer program configured in the UMS (internal or external VNC viewer) can be used for shadowing.

Direct shadowing of a client by another client is likewise not permitted.

- **Logging:** Connections established via secure shadowing are recorded in the UMS server log.

In addition to the connection data, the associated user data (shadowing UMS administrator, optional) can be recorded in the log too.



Of course, this is only relevant to clients which meet the requirements for secure shadowing and have enabled the corresponding option. Other clients can be "freely" shadowed in the familiar manner and, if necessary, secured by requesting a password. If you would like to allow secure shadowing only, you can specify this in Misc Settings in the UMS Administration area.

## Basic principles and requirements

Menu path: **Setup > System > Shadow**

The **Secure Shadowing** option can be enabled subject to the following requirements being met:

- IGEL Universal Desktop Linux or IGEL Universal Desktop OS 2, each from Version 5.03.190 or IGEL Universal Desktop Windows Embedded Standard 7 from Version 3.09.100
- IGEL Universal Management Suite from Version 4.07.100 onwards
- The client is registered on the UMS server
- The client can communicate with UMS console and UMS server (see below)

Basic technical principles:

Unlike with "normal" shadowing, the connection between the VNC viewer and the VNC server (on the client) is not established directly during secure shadowing. Instead, it runs via two proxies – one for the UMS console and one for the VNC server on the client. These proxies communicate via an SSL-encrypted channel, while the local communication, e.g. between the VNC viewer application and the UMS proxy, takes place in the conventional unencrypted manner. As a result, a secure connection can also be established with external VNC programs that do not support SSL connections.

The two proxies (UMS console and client) communicate with SSL encryption via the same port as the "normal" VNC connection: 5900. As a result, no special rules for firewalls need to be configured in order to perform secure shadowing.

If secure shadowing is active for a client (**Setup>System>Shadowing>Secure Shadowing**), the client generates a certificate in accordance with the X.509 standard and transfers it to the UMS Server when the system is next started. The UMS server checks subsequent requests for a secure VNC connection using the certificate. The certificate in PEM format can be found in the `/wfs/ca-certs/tc_ca.crt` directory on the client. The validity of the certificate can be checked on the (Linux) client using the command:

```
x11vnc -sslCertInfo /wfs/ca-certs/tc_ca.crt
```



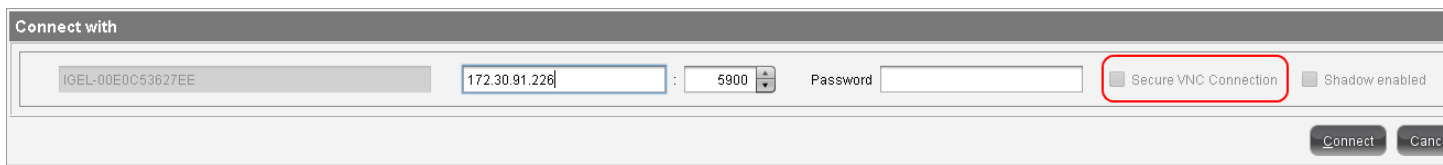


Figure 21: Secure shadowing connection dialog

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



Figure 22: Secure VNC connection

## VNC logging

Menu path: **Setup > System > Shadow**

Connections via secure shadowing are always logged in the UMS. Via **UMS Administration>Misc Settings>Secure VNC**, you can configure whether the user name of the person shadowing is to be recorded in the log (the default is inactive).

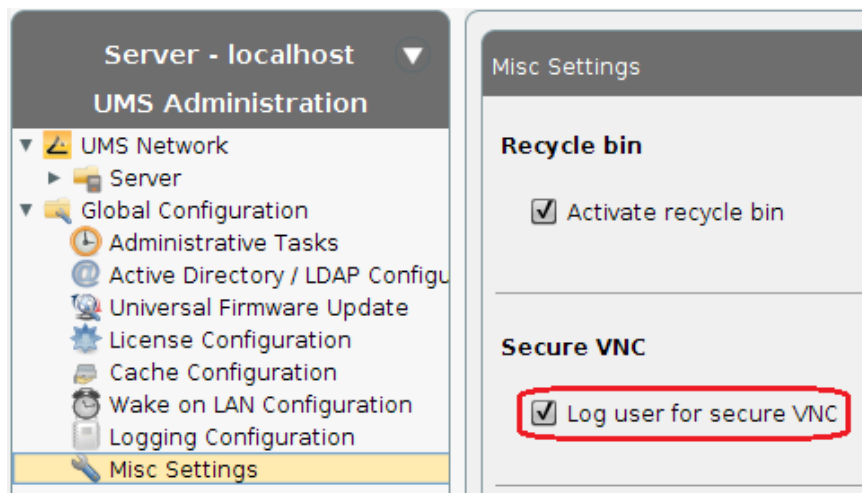


Figure 23: Options for VNC logging

The VNC log can be called up via the **context menu** of a client or folder (for several clients, **Logging>Secure VNC Logs**). The name, MAC address and IP address of the shadowed client, the time and duration of the procedure and, if configured accordingly, the user name of the shadowing UMS administrator are logged.

Secure VNC Logs					
Filter: <input type="text" value="00E0C56133A9"/>					
Thin Client Name	MAC Address	Thin Client IP	User	VNC Starttime	Duration in sec
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:01:17 PM	98
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:06:10 PM	32
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:06:26 PM	19
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:07:09 PM	44
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:07:18 PM	39
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:08:06 PM	48
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:08:38 PM	20
IGEL-00E0C56133A9	00:E0:C5:61:33:A9	10.201.1.123	igel	Jul 9, 2014 1:09:24 PM	26

Figure 24: 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.

## 12.5. File Based Write Filter

Menu path: **Setup > System > Data Based File Writer**

The **File Based Write Filter (FBWF)** is the system's own write filter for Windows Embedded Standard. A detailed description of the FBWF function can be found at <http://msdn.microsoft.com/en-us/library/aa940926.aspx>.

The write filter protects the system against accidental changes or deletions and harmful software. You should (re)activate the filter after setting up the system, e.g. after installing your own applications or making changes to the Windows system outside the IGEL setup. Changes in the IGEL setup or via the IGEL UMS management are not blocked by the write filter.

The FBWF status is shown in the taskbar:

Red symbol: FBWF disabled

Green symbol: FBWF enabled (standard setting)

In the IGEL setup, you can

- enable or disable the write filter,
- define the filter storage space (in MB, max. 1024 MB, the standard setting is 64 MB),
- exclude directories from the write filter (e.g. for the signatures of a virus scanner).

Data can then be written to these directories, even if the filter is enabled.



Do not change or delete the entries initially present in the list (see below). Otherwise, the system will no longer run in a stable manner.

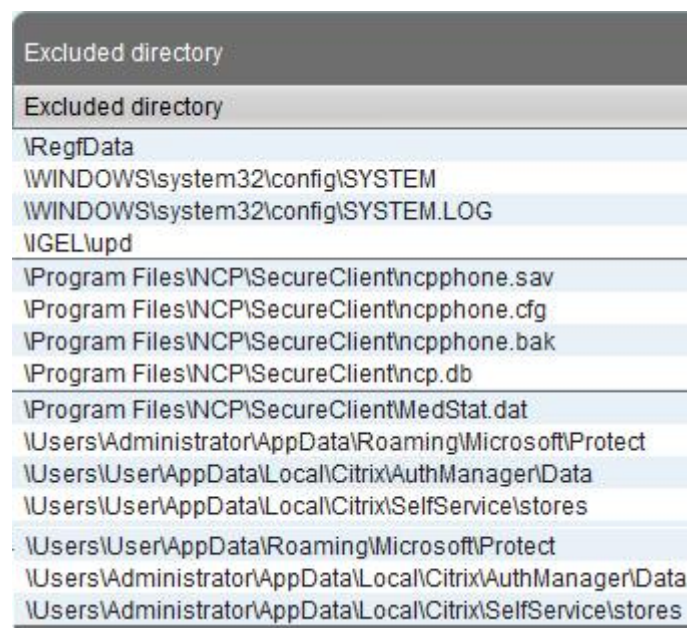


Figure 25: Excluded Directory

If no more FBWF storage space is available, the error message **There is not enough disk space on the disk** will be displayed. After this error message, the system may not run in a stable manner and data may be lost.

- Restart the system in order to restore the device.

The FBWF must be enabled during regular system operation! Disable the write filter only temporarily, e.g. for administrative duties. IGEL does not support permanent operation with the write filter disabled. Directory exceptions must be defined as specifically as possible in order to ensure the greatest possible protection for the system in spite of the exceptions.

## 12.6. Energy Options

Menu path: **Setup > System > Power Management**

The usual energy saving options found in Windows have been carried over to the IGEL setup too.

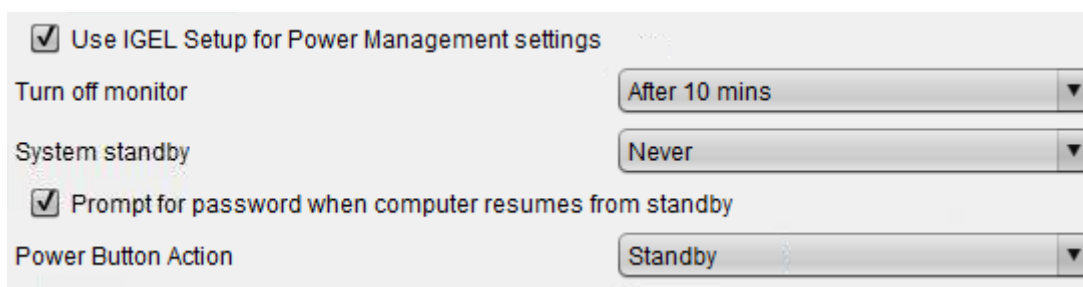


Figure 26: Energy Options

You can set the following parameters on the IGEL thin client:

- Turn off monitor
- System Standby
- Prompt for password when computer resumes from standby
- Power Button Action

You can configure the system behavior here in order to enable the standby mode for example.



## 12.7. Firmware Customization

Menu path: **Setup > System > Firmware Customization**

With the help of the list of available **Features**, you can easily enable or disable firmware functions (e.g. session types).

If a function was disabled, the associated session type will no longer be available when the system is restarted. Existing sessions of this type will no longer be shown but will not be deleted either.

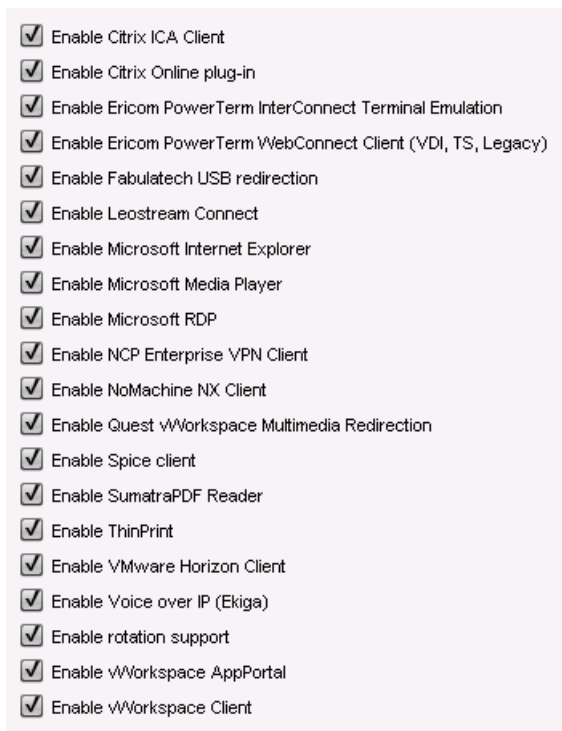


Figure 27: List of available functions



Disable the **ThinPrint** function in this list if you want to use ThinPrint within a VMware Horizon session. The VMware Horizon client features its own ThinPrint component which may be disturbed by the ThinPrint service running in parallel.

You can also create and configure your **Custom Applications**. Give details of the start options for a custom application as well as the application to be launched and, where applicable, the parameters to be transferred.

## 12.8. Registry

Menu path: **Setup > System > Registry**

The **IGEL Registry** is a structured collection of all configurable parameters, a number of which cannot be found on setup pages. You can change many firmware parameters 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 original factory defaults via a snapshot.

1. Click on **Parameter Search...** in order to search for specific parameters in the **IGEL Registry**.
2. Search for the parameter name `wpa` if you require WPA encryption settings for securing your WLAN.

The parameter found in the structure is highlighted:

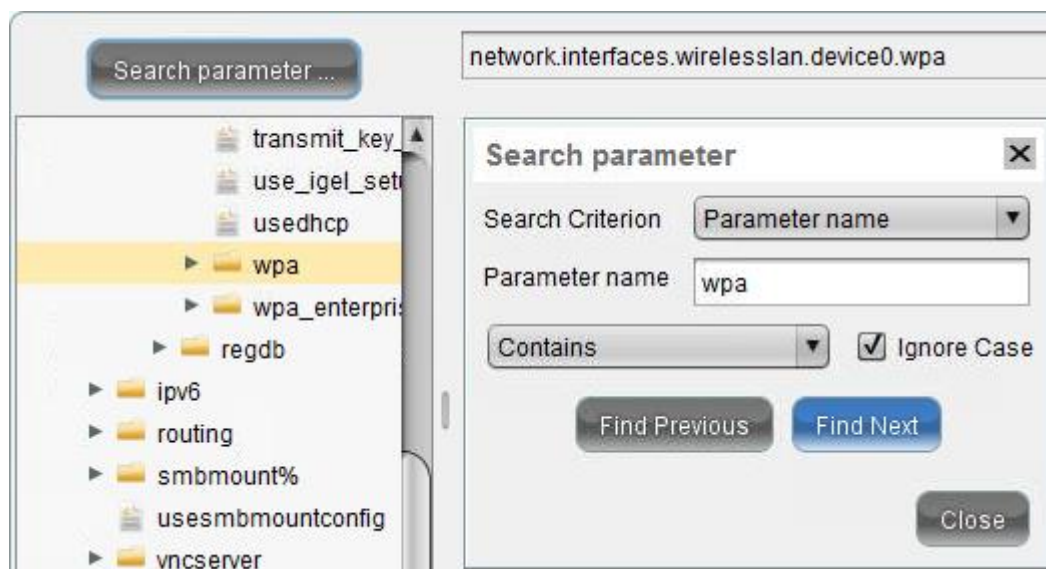


Figure 28: Search Parameter

## 12.9. System Restoration

If the system no longer functions correctly, you can simply restore it via the hidden boot menu.

To access the boot menu, proceed as follows:

- Press the **ESC** key briefly after switching on the device.
- Download a previously created firmware snapshot and set the parameter **Reset Terminal Settings** to `true` in order to reset all system configuration parameters.

The download settings correspond to the above described procedure for the system update (snapshot mechanism).



If you have set a password to protect the local IGEL setup application, this will affect the boot menu. Without the setup password, you will not be able to access this restoration tool. System restoration will then only be possible with the IGEL Universal Management Suite!

Alternative:

- Press the **ESC** key briefly after switching on the device.
- Select the **Rescue Shell**.
- Delete the local settings using the command `reset_wes`.



Important: Data in the User partition (F:) will be retained both when resetting the local settings and when installing a snapshot. You should therefore delete them separately!

# 13. Index

## A

About this document.....	5
Accessories .....	34
Active Directory .....	42
Appearance.....	19
Attached Devices .....	41
Available options .....	47

## B

Basic principles and requirements .....	49
Boot options .....	9
Browser sessions .....	31
Browser Sessions .....	31

## C

Citrix.....	13
Creating a snapshot.....	45

## D

Date and Time .....	45
Desktop and Start Menu .....	37
Desktop integration.....	18, 20, 26
Devices.....	41
Display .....	36
Downloading a snapshot .....	46

## E

Energy Options .....	54
----------------------	----

## F

File Based Write Filter .....	52
Firewall .....	14, 17
Firmware Customization .....	54
Firmware update via snapshot.....	46
Formatting and meanings.....	5

## H

HDX .....	16
Horizon Client .....	27
Horizon Client Global.....	27

## I

ICA Global .....	13
ICA Sessions .....	16
IGEL device information .....	9
IGEL setup .....	10
IGEL Universal Desktop Firmware .....	7
Important Information .....	2
Input.....	37
Installing partial updates .....	47

## K

Keyboard.....	14, 21
---------------	--------

## L

LAN and Wireless.....	39
Language.....	37
Leostream .....	28
Logon .....	17, 19, 21, 24

## M

Mapping.....	21, 25
--------------	--------

## N

Network .....	39, 43
Network Drives .....	39
NX Client .....	29

## O

Options .....	15, 18, 22, 26
---------------	----------------

## P

Partial update .....	46
Password.....	42
Performance .....	22, 25
PowerTerm Terminal Emulation.....	30
PowerTerm WebConnect .....	30
Printer .....	41

## Q

Quick installation .....	8
--------------------------	---

## R

RDP (global settings).....	20
RDP sessions .....	23

Registry .....	55
Remote Desktop Protocol - RDP .....	20
Remote Management.....	47
Routing .....	39

## S

Searching Setup Pages.....	11
Secure shadowing (VNC with SSL) .....	48
Security .....	42
Self-Service Plugin .....	19
Server.....	16, 19, 24
Server Location .....	13
Sessions .....	13
Setup Areas.....	11
Setup Session.....	34
Shadow .....	48
Shadow clients securely .....	50
Shell .....	38
Snapshots .....	45
Sound Mixer .....	34
System .....	45
System Restoration.....	57

## U

Update .....	45
USB Redirection .....	15, 23
User interface .....	36

## V

VNC logging .....	51
VoIP Client .....	32
VPN Connection.....	39
vWorkspace Client and AppPortal.....	28

## W

What is new in 3.11.100? .....	5
Window .....	14, 17, 21, 25
Windows Firewall .....	43
Windows Media Player.....	32
Windows Services.....	35