

Windows Embedded Standard 7

User manual



IGEL[®]
**UNIVERSAL
DESKTOP**

Important Information

Please note some important information before reading this documentation.

Copyright

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

Copyright © 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.

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 *IGEL Support Portal*
<https://www.igel.com/en/members-area/login-logout.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/otrs-igel/public.pl?Action=PublicFAQExplorer;CategoryID=3>.

Contents

1.	Introduction	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	12
6.	Sessions.....	13
	6.1. Citrix ICA.....	13
	6.2. Remote Desktop Protocol - RDP	17
	6.3. VMware Horizon client	18
	6.4. vWorkspace Client and AppPortal	19
	6.5. Leostream Connection Broker	20
	6.6. Nomachine NX	21
	6.7. PowerTerm WebConnect.....	21
	6.8. PowerTerm terminal emulation.....	22
	6.9. Microsoft Internet Explorer browser session	23
	6.10. Windows Media Player	24
	6.11. Voice over IP (VoIP) client.....	25
7.	Accessories	26
	7.1. Setup Session	26
	7.2. Sound control.....	26
	7.3. Windows Services	27
8.	User interface.....	28
	8.1. Screen.....	28
	8.2. Language	29
	8.3. Desktop and start menu	29
	8.4. Entry.....	30
9.	Network	30
	9.1. LAN and WLAN (wireless)	30
	9.2. VPN connection.....	31
	9.3. Routing.....	31
	9.4. Network drives.....	31
10.	Devices	32
	10.1. Thin Print.....	32
	10.2. USB devices	32
11.	Security.....	33
	11.1. Password.....	33
	11.2. Active Directory	33

11.3. Network.....	34
11.4. Windows Firewall.....	34
12. System.....	35
12.1. Date and time	35
12.2. Remote administration	35
12.3. Update.....	35
12.4. VNC (Shadowing)	37
12.5. File Based Write Filter	41
12.6. Energy options	43
12.7. Firmware customization	44
12.8. Registry	45
12.9. System restoration.....	46
13. Index.....	47

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 28)</i>	Screen, desktop, start menu, language, entry
<i>Network (page 30)</i>	LAN/WLAN, VPN, routing, network drives
<i>Devices (page 32)</i>	ThinPrint, USB
<i>Security (page 33)</i>	User accounts, password, Active Directory, Password Manager Agent
<i>System settings (page 35)</i>	Date/time, remote management, shadowing, energy options, registry, write filters, update, firmware functions

Formatting and meanings

The following formatting is used in the document:

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

Note regarding operation

Warning: Important note which must be observed

What is new in 3.10.100 ?

You will find the release notes for the IGEL Universal Desktop W7 3.10.100 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/) and in our *Knowledge Base* (<http://edocs.igel.com/>).

The updated Version 4.2 of Citrix Receiver provides *Launch Options* (page 17) for sessions in the start menu and on the desktop. The *RDP client* (page 17) now supports protocol version 8.1. The system also includes *Microsoft Internet Explorer 11* (page 22).

This version also allows customers who would like to manage Windows Embedded Standard with Microsoft SCCM for example rather than via IGEL UMS to uninstall the IGEL system. Further details can be found in a best practice document.

Please note the licensing information for Windows Embedded Standard, especially when using Microsoft Office 365.

1. 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 firmware included with every IGEL Universal Desktop product is multi-functional and contains a wide range of protocols allowing access to server-based services. The IGEL Universal Desktop Firmware is available with two possible operating systems and with the following options:

Operating system	Options
Windows Embedded Standard 7	<ul style="list-style-type: none">• Ericom PowerTerm Terminalemulation
IGEL Linux	<ul style="list-style-type: none">• IGEL Shared Workplace• IGEL Universal MultiDisplay (LX only)• Codec package (LX only)

The structure of the IGEL setup is almost identical on all thin clients and in the Universal Management Suite (UMS) management software. This means that 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.

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 on the IGEL symbol.
A pop-up menu opens.
2. Change the
 - Network settings
 - Display settings
 - Keyboard settings
3. Click on **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 on the yellow IGEL symbol in the Windows taskbar in order to bring up the device information.

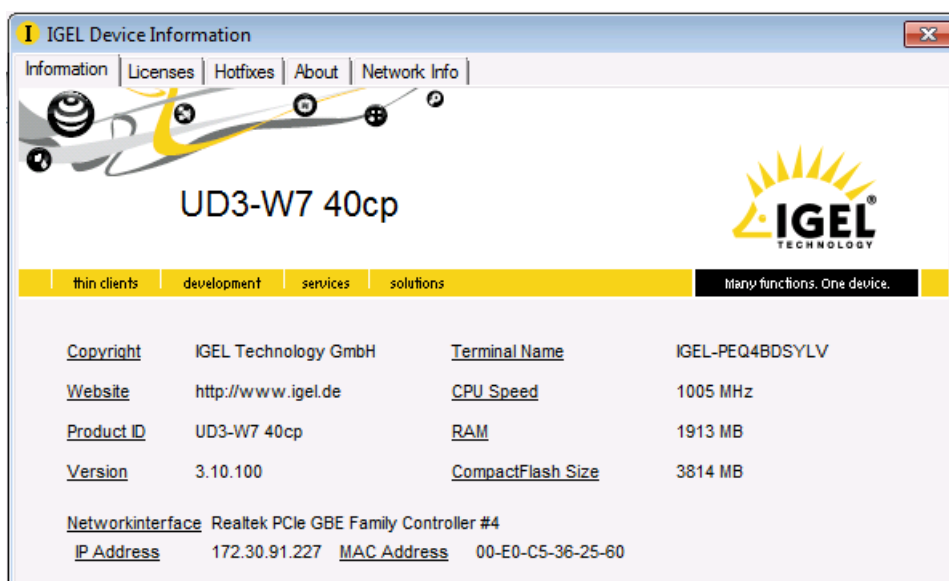


Figure 2: IGEL device information

Information	Details of the product, the firmware version, the IP address and a number of hardware details such as CPU and RAM are shown.
Licenses	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 Next and Back .
Hotfixes	Shows all Microsoft Windows system patches, e.g. security updates.
About	Provides a detailed overview of your thin client hardware and software. In particular, the licensed functions included in the firmware are shown here.
Network information	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 on the **Setup** symbol in the taskbar or
- Click on 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 on **Apply** to save the changes you have made.
- Click on **OK** to save your changes and close the application.
- Click on **Cancel** to close the application without saving your changes.

5.1. Setup areas

The setup application comprises the following main areas:

Sessions	In this area, you can create and configure application sessions such as ICA, RDP, terminal emulation, browser and others.
Accessories	The IGEL setup application can be restricted for users (not the administrator). A number of Windows services can be enabled or disabled.
User interface	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).
Network	In this area, you can configure all the network settings for LAN / WLAN interfaces. Network drives are also configured here.
Devices	The options for using various USB devices (e.g. memory sticks, WLAN or Bluetooth devices) as well as printers are enabled or configured here.
Security	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.
System	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 on 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.

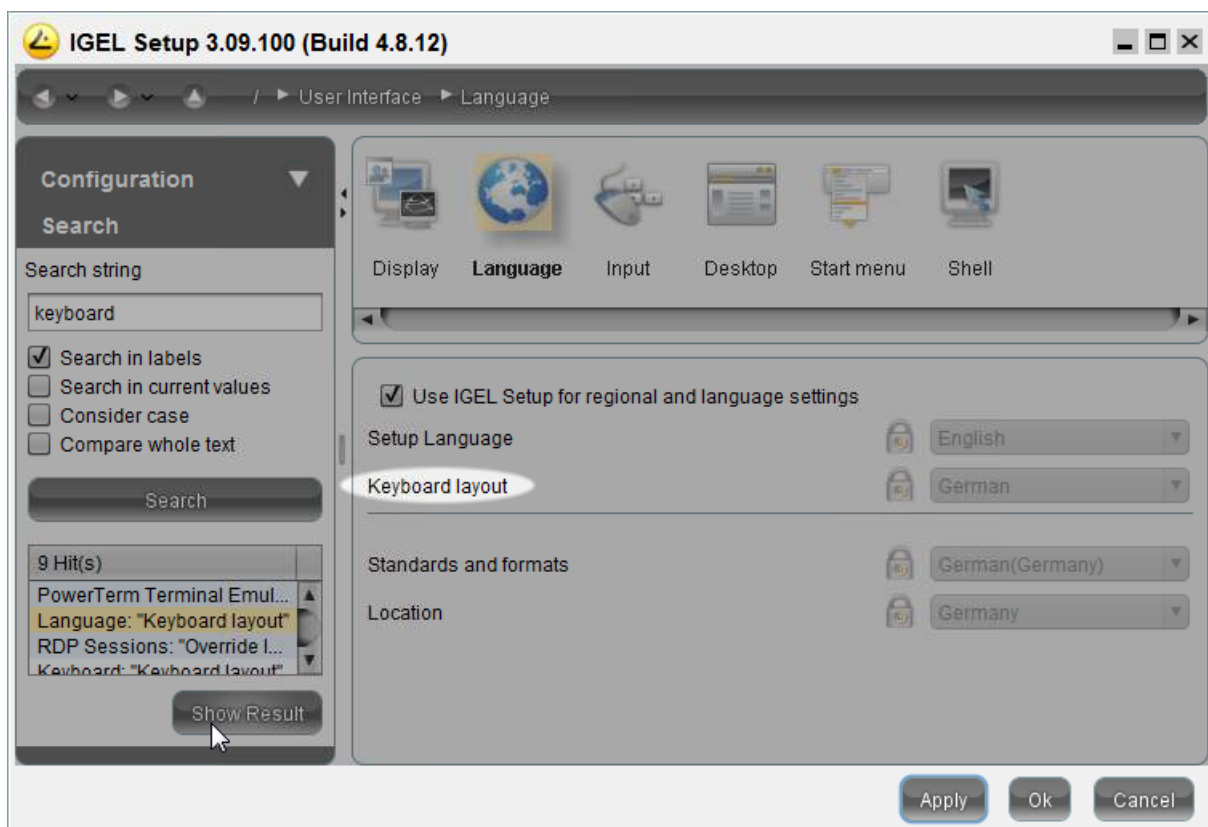


Figure 4: Searching Setup Pages

6. Sessions

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.

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 ICA

6.1.1. Global settings

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://support.citrix.com/proddocs/index.jsp>.

Server location (master browser)	Allows you to define the HTTP master browser for ICA connections
Window settings	Allows you to define the standard window size and color depth
Keyboard	Allows you to change the keyboard layout – hotkeys for the server system can be set up on function keys or key combinations on the local keyboard.
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 alternative address	<p>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. (You will find more information on server configuration if you look for the command <code>altaddr</code> in your Citrix administration manual.)</p> <p>Once the alternative address is enabled, the server must be added to the address list under Server Location.</p>
Options	Allows you to set globally effective options, e.g. automatic reconnection or the size of the cache
USB redirection	Allows you to create rules for the use of local USB devices during the XenDesktop session. Depending on the device class or sub-class, use during the session can be allowed or refused. Combinations of rules are also possible. If the devices in question have been specified exactly, a rule can also be created on the basis of the manufacturer and product ID. In this case, no classification is necessary.
HDX	Allows you to enable flash redirection, file access, microphone and webcam access as well as access to USB and other devices.

6.1.2. ICA settings

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.

Connections	Allows you to specify the Citrix server or the published application with which the connection is to be established and to determine the browser protocol for application browsing
Logon	Allows you to specify the user logon information for the server logon process. Alternatively, the user can enter the logon data when the connection to the session is established.
Window settings	Allows you to specify the window size and color depth for the session. The Seamless Window mode can be enabled for published applications.
Firewall	Allows you to configure ICA connections which run via a firewall, a SOCKS proxy server or a Citrix Secure Gateway (in relay mode).
Reconnection	Allows you to enable automatic reconnection to the session and limit the number of attempts.

Options	Allows you to optimize performance and behavior:
Compression	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.
Caching image data	Allows you to enable caching in the cache memory (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 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 transmission	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.
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	Allows you to set up the start options via the desktop or start menu / autostart.

SpeedScreen only works if the function was enabled and configured on the Citrix server beforehand.

6.1.3. Self-Service-Plugin

Under **Connections**, 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

here.

Specify options for authentication under **Logon**, for menus under **Appearance** and for links on the desktop and in the start menu under **Desktop Integration**.

6.2. Remote Desktop Protocol – 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>.

6.2.1. RDP global

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. Exception: The **Clipboard** and **Hotkeys** keyboard parameters. These can only be set globally for all sessions.

6.2.2. RDP sessions

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

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

6.3. VMware 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).

Server URL	<input type="text"/>
<input type="checkbox"/> Use SSL encryption	
Username	<input type="text"/>
User password	<input type="text"/>
Domain	<input type="text"/>
Session type	Desktop ▼
Desktopname	<input type="text"/>
Application Name	<input type="text"/>
hide client after launch session	off ▼
Protocol	Server default ▼
<input type="checkbox"/> Log in as current user	
Kiosk mode	off ▼

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.

Note regarding the use of ThinPrint within the Horizon session (page 32)

6.4. vWorkspace Client and 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.

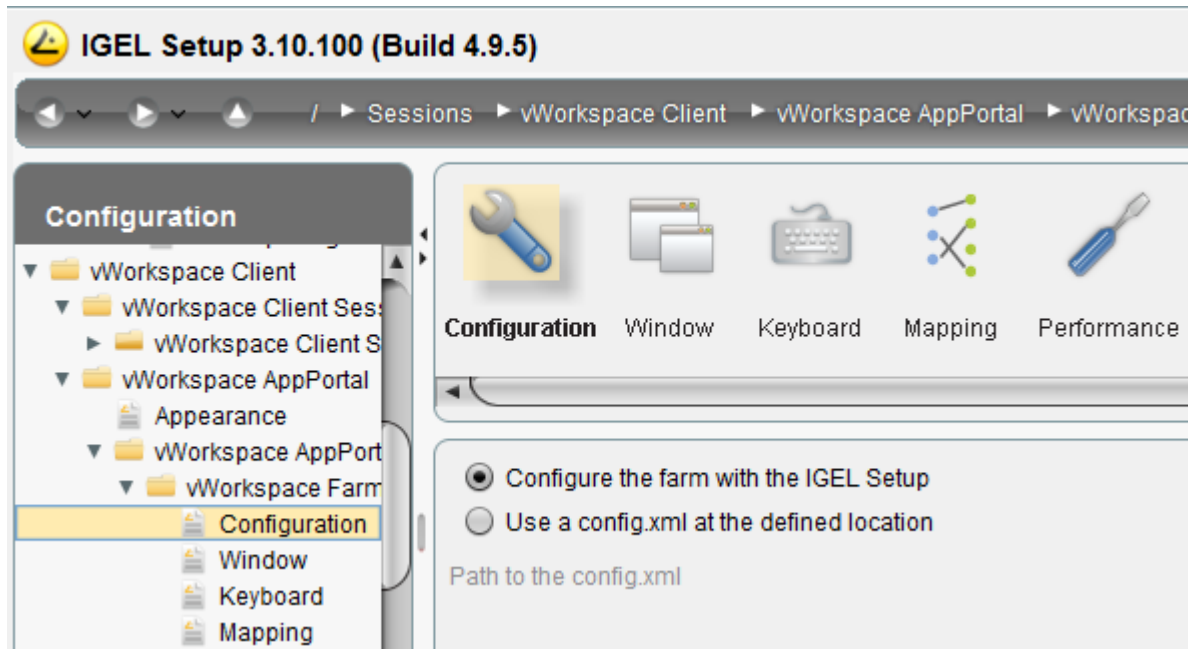


Figure 6: Configuration in the IGEL setup

6.5. Leostream Connection Broker

- 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.

Actions	Name	Leostream API Protocols	iTap Protocols
Edit	Default	rdesktop, RDP, NoMachine NX	RDP
Edit	"Default" policy	rdesktop	RDP, VNC

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. Nomachine NX

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.

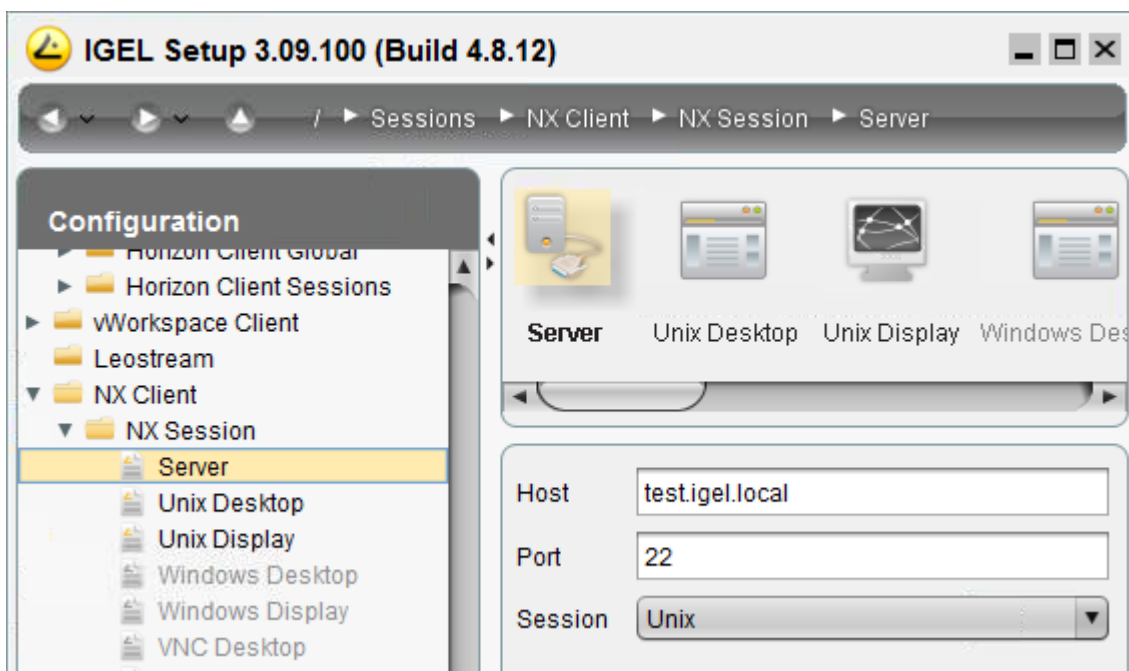


Figure 8: Nomachine NX configuration parameters

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

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

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 **Power Term Emulation Setup**, proceed as follows:

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

The **PowerTerm Emulation Setup** window opens.

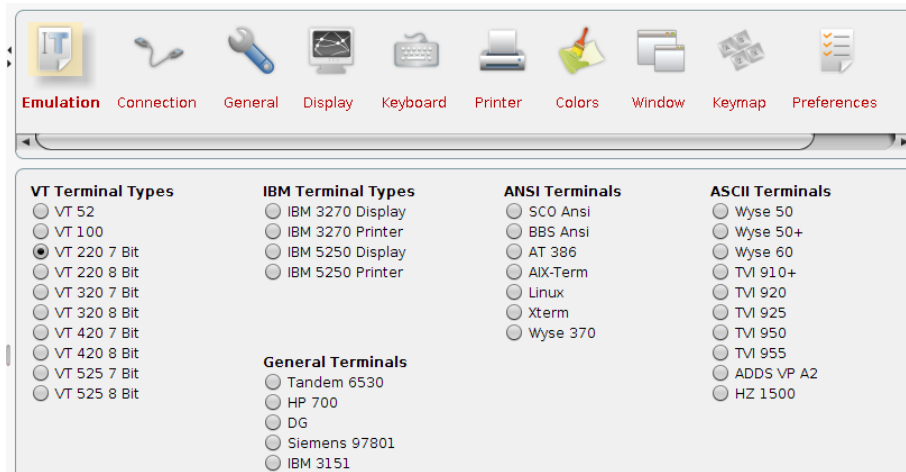


Figure 9: PowerTerm emulation setup

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. Microsoft Internet Explorer browser session

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

- Disable the IGEL settings for the MSIE in order to enable the original settings (in the IE menu).

The following setup pages are available:

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

In the IGELsetup for the browser session, you can configure most Internet Explorer settings in order to distribute this configuration via the IGEL UMS to other IGEL thin clients.

6.10. 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/de-de/windows/music-photos-video-help>.

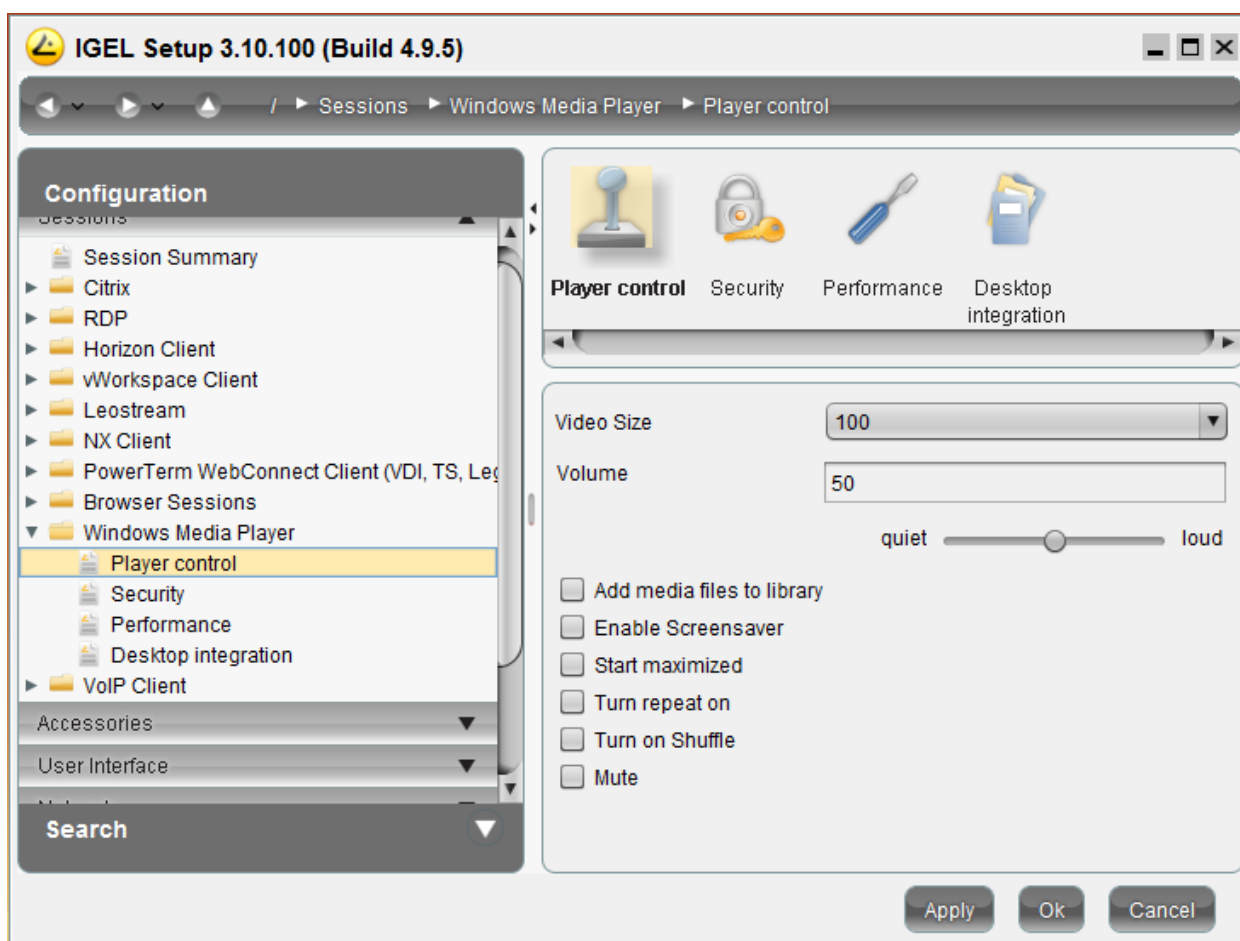


Figure 10: Player control in the IGEL setup

6.11. Voice over IP (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>.

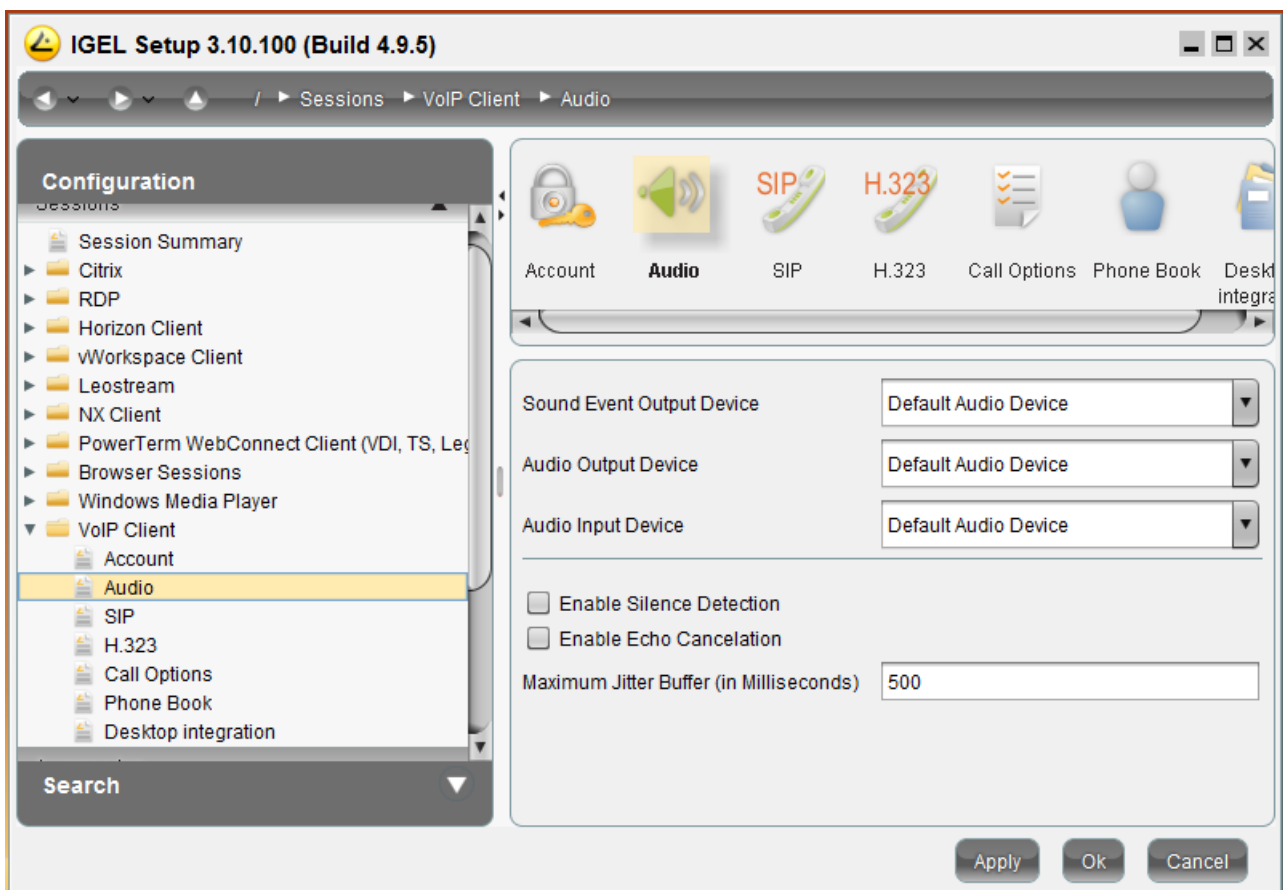


Figure 11: Configuration for IP telephony

7. Accessories

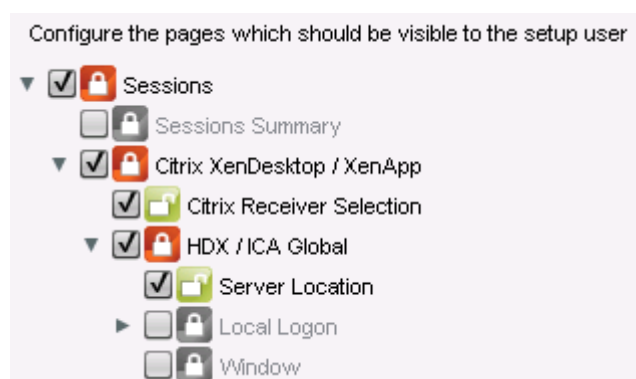
7.1. Setup Session

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 33)). 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**.

If users are to be allowed to edit parts of the setup even without a password, create a *quick setup* (page 8) session, the password for the **Setup user** will not be enabled in this case.

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 (open lock) indicates that the user is able to edit the parameters on this setup page.



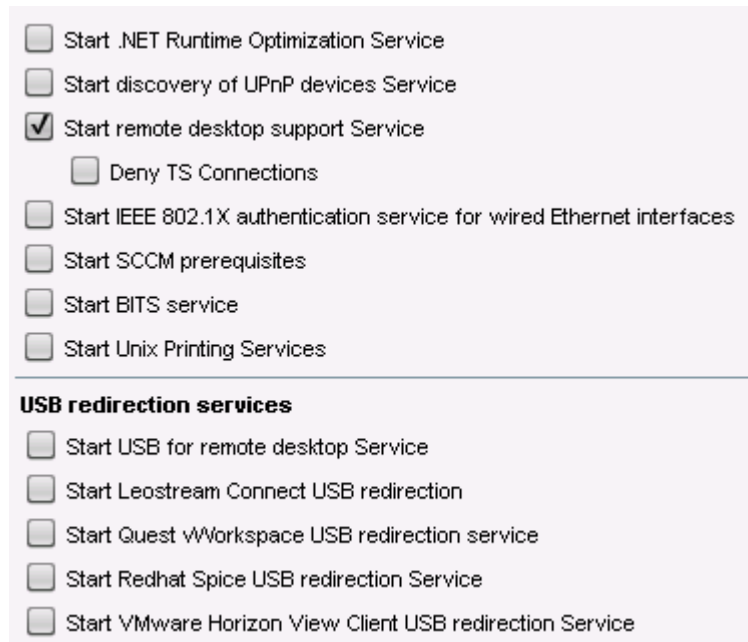
If you enable a setup page on the lower levels, the node points required for access will automatically be marked as visible (but blocked for editing purposes)

7.2. Sound control

Here, you can set the **system volume** or **mute the sound**.

7.3. Windows Services

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



The screenshot shows a list of Windows services with checkboxes. The 'Start remote desktop support Service' checkbox is checked. Below it, the 'Deny TS Connections' checkbox is unchecked. The 'USB redirection services' section is highlighted in bold and contains five unchecked checkboxes.

- Start .NET Runtime Optimization Service
- Start discovery of UPnP devices Service
- Start remote desktop support Service
 - Deny TS Connections
- Start IEEE 802.1X authentication service for wired Ethernet interfaces
- Start SCCM prerequisites
- Start BITS service
- Start Unix Printing Services

USB redirection services

- Start USB for remote desktop Service
- Start Leostream Connect USB redirection
- Start Quest vWorkspace USB redirection service
- Start Redhat Spice USB redirection Service
- Start VMware Horizon View Client USB redirection Service

Figure 12: Windows Services

8. User interface

8.1. Screen

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

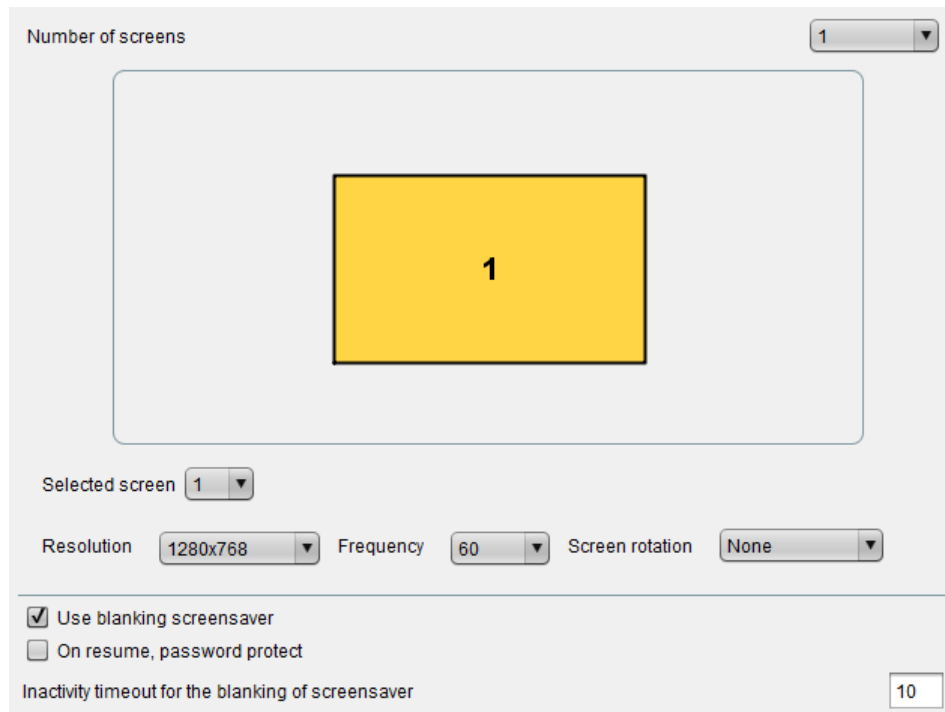


Figure 13: Advanced screen settings

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:

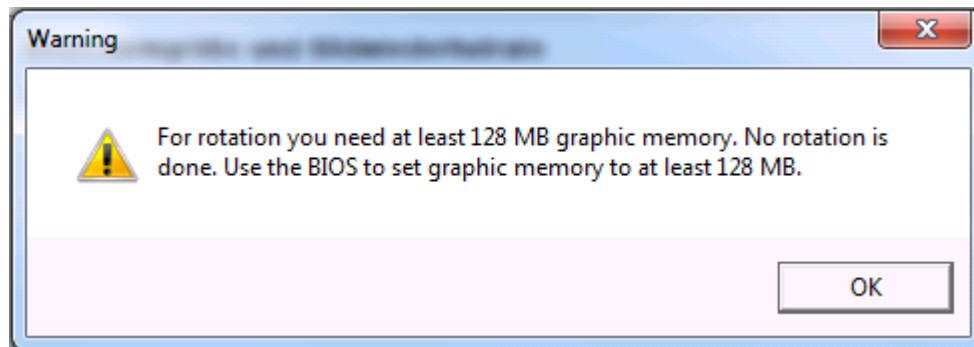


Figure 14: Warning notice for insufficient video memory

8.2. 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.

Warning: 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. Desktop and start menu

The following options are available:

Show recycle bin	The recycle bin is hidden as standard.
Fix taskbar	The taskbar can be fixed in the current position.
Prevent computer being locked	Disables the option for locking the desktop via Win+L or Ctrl+Alt+Del .
W7	Enables Aero Glass effects (transparent windows, miniature view).
Always show message symbols in the taskbar	
Arrange start menu alphabetically	This allows you to arrange all entries in the start menu in alphabetical order.

8.4. Entry

In the **Entry** 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.

9. Network

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

9.1. LAN and WLAN (wireless)

Here you will find the configuration parameters for the available interfaces (integrated LAN, LAN via PCI card and WLAN). The internal LAN interface is pre-configured for DHCP as standard.

The screenshot shows a network configuration interface with the following settings:

- Encryption options: Disable Encryption, Enable WEP Encryption, Enable WPA Encryption
- Wireless Network Name (SSID): WLAN
- Network authentication: WPA Enterprise
- Data encryption: TKIP
- Network key: [Empty field]
- EAP Type: PEAP
- Auth Method: MSCHAPV2
- How to authenticate on Network: User
- Connect if this network is in range:
- Automatically use Windows logon name and password:
- Do not prompt user to authorize new servers:
- Enable Fast Reconnect:
- Enable Quarantine checks:
- Disconnect if server does not respond cryptobinding TLV:
- Use a different user name for the connection:

Figure 15: Configuration parameters for interfaces

In the **WLAN** area, you will find all parameters for the wireless network including the options for encrypting the connection. You can also 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

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

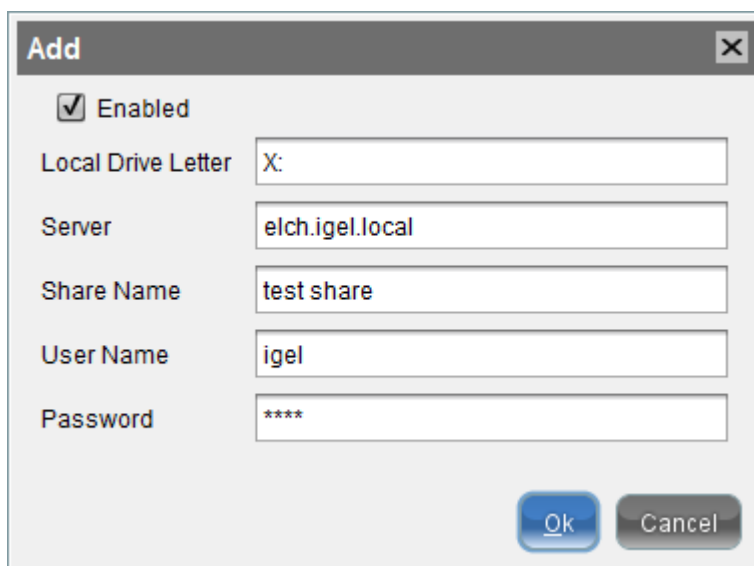
In order to use a specific network route, define the gateway for forwarding on this page. Specifying the network interface is optional. The route affects all network devices used.

9.4. Network drives

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 dialog box titled "Add" with a close button (X) in the top right corner. Inside the dialog, there is a checked checkbox labeled "Enabled". Below this, there are five text input fields arranged vertically:

- "Local Drive Letter" with the value "X:"
- "Server" with the value "elch.igel.local"
- "Share Name" with the value "test share"
- "User Name" with the value "igel"
- "Password" with the value "****"

At the bottom right of the dialog, there are two buttons: "Ok" and "Cancel".

Figure 16: Add network drives

10. Devices

10.1. Thin Print

The ThinPrint client is launched automatically when an ICA or RDP session is executed. Once the ThinPrint client has been launched, you can access the printer configuration menu via the ThinPrint symbol in the taskbar. No configuration parameters are available in the IGEL setup.

If you use ThinPrint within VMware Horizon, please disable the system's ThinPrint client in the setup under **Firmware Configuration > Features**. The Horizon client comes with its own ThinPrint implementation which only functions correctly if no other ThinPrint client is active.

10.2. USB devices

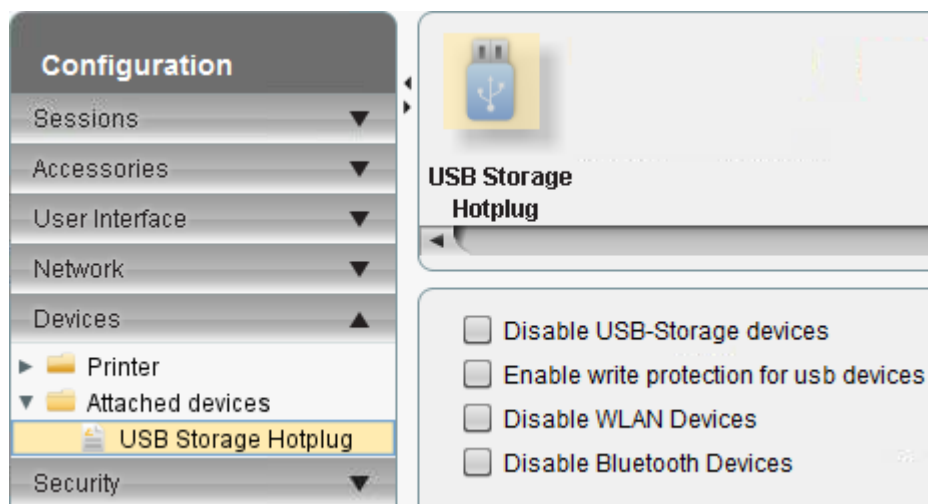


Figure 17: Device configuration

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

11.1. Password

You can set up an administrator password in order to protect the IGELsetup 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

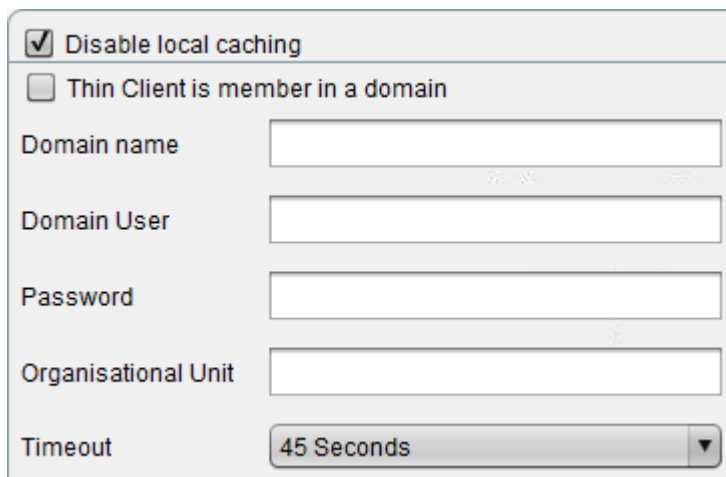
Specify a user who is automatically logged on when the system starts.
The `User` user is logged on as standard.

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

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.



The screenshot shows a configuration dialog box for Active Directory. It contains the following elements:

- Disable local caching**
- Thin Client is member in a domain**
- Domain name**: A text input field.
- Domain User**: A text input field.
- Password**: A text input field.
- Organisational Unit**: A text input field.
- Timeout**: A dropdown menu currently set to **45 Seconds**.

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

Here, you can **Deactivate administrative shares** or specify that the thin client should not be shown in the network.

11.4. Windows Firewall

Here, you can manage the rules for the **Windows Firewall**. These can be linked to a program or a network port.

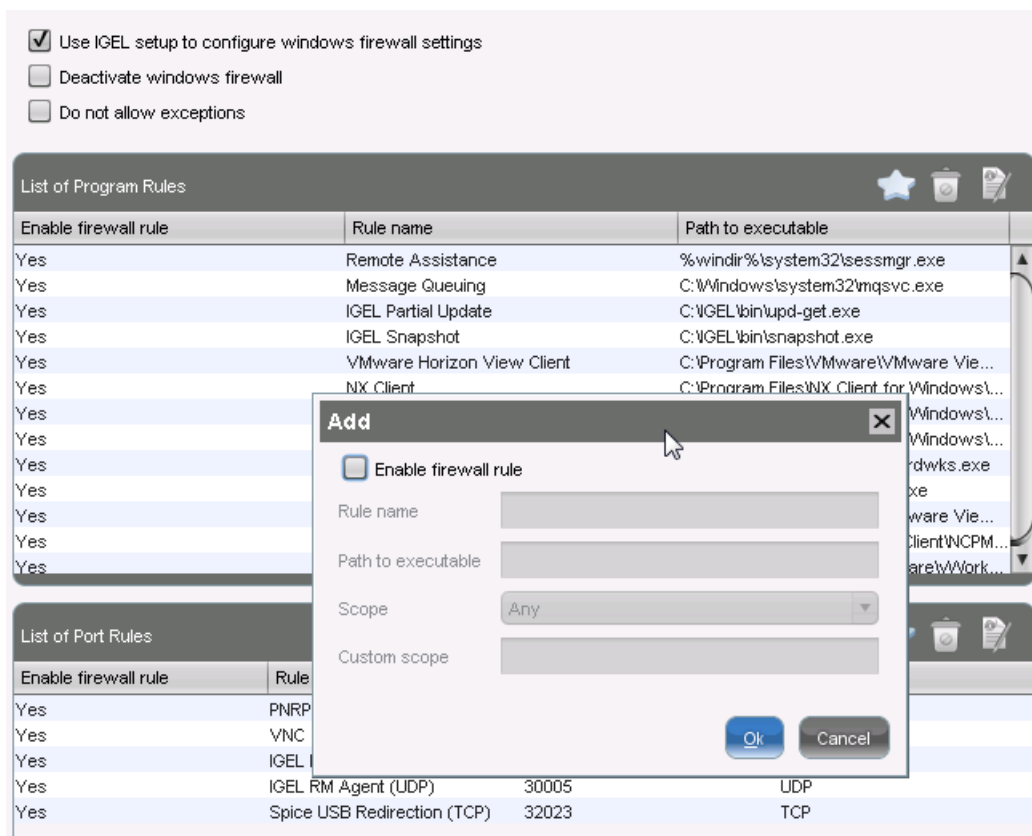


Figure 19: Windows Firewall

12. System

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

12.1. 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. Remote administration

Define the remote management server (IGEL UMS server) on which the device is to register. Via the **Allow Remote Management** checkbox, you can disable the option of administration via the UMS server:

Setup→**System**→**Registry**→**Path**: `system.remotemanager.allow_remote_management`.

If the IGEL UMS server sends new settings to the thin client or if the thin client is shut down by the UMS, the user can receive corresponding information. The message display time can be configured via **Enable User Information**.

12.3. 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

12.3.1. 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.com>.

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.

Warning: 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.

12.3.2. 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 the executed through a scripting engine on the basis of the script 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.

12.3.3. 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.

12.4. 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.

12.4.1. 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.

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`

```
VNC Certificate file:
  /wfs/ca-certs/tc_ca.crt

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1572055243 (0x5db3a8cb)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=DE, L=Bremen, O=IGEL
    Validity
      Not Before: Jun  6 06:04:50 2014 GMT
      Not After : Jun  6 06:04:50 2037 GMT
    Subject: C=DE, L=Bremen, O=IGEL
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (1024 bit)
      Modulus:
        00:a4:e4:67:f3:cf:23:90:06:c3:d6
        5e:0e:00:b8:43:14:6d:61:c5:65:ca
```

Figure 20: Thin Client Zertifikat für sicheres Spiegeln

If a UMS administrator calls up the **Shadowing** function in the UMS Console for the thin client, the console receives a signed request from the UMS Server which is then passed on to the thin client to be shadowed. This in turn passes on the request to the UMS server which checks the validity of the request using the original certificate. If this check is successful, the console reports that the channel for the connection between the proxies can be established. The UMS proxy on the console connects to the server proxy on the thin client, and the server proxy in turn establishes on the thin client the connection to its VNC server.

Only when these connections have been established does the console call up the VNC viewer which then connects to the console proxy. The VNC client and VNC server are now connected via the two proxies which transfer data with SSL encryption.

Secure shadowing can be enforced independently of the thin client configuration for all thin clients that support this function: **UMS Administration > Misc Settings > Activate Global Secure VNC.**

Shadow thin clients securely

In order to shadow a thin client securely (with encryption), the administrator must log on to the server via the UMS console. When doing so, it is irrelevant whether a purely local UMS administrator account is used or the user was adopted via an Active Directory for example. As always, however, the UMS administrator must have the right to shadow the object, see.

The thin client to be shadowed is called up in the navigation tree and, as usual, can be executed via **Shadow** in the context menu. The connection window however differs from the dialog for normal VNC shadowing. The IP and port of the thin client to be shadowed cannot be changed, and a password for the connection is not requested – this is superfluous after logging on to the console beforehand.



Figure 21: Verbindungsdialog Sicheres Spiegeln

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



Figure 22: Secure VNC connection

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).

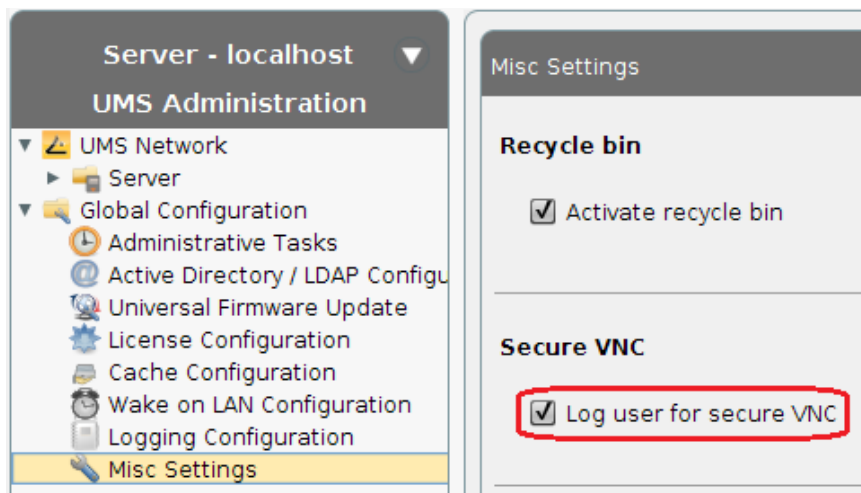


Figure 23: Options for VNC logging

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 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

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.

Warning: 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.

Excluded directory
\RegfData
WINDOWS\system32\config\SYSTEM
WINDOWS\system32\config\SYSTEM.LOG
IGEL\upd
\Program Files\NCP\SecureClient\ncpphone.sav
\Program Files\NCP\SecureClient\ncpphone.cfg
\Program Files\NCP\SecureClient\ncpphone.bak
\Program Files\NCP\SecureClient\ncp.db
\Program Files\NCP\SecureClient\MedStat.dat
\Users\Administrator\AppData\Roaming\Microsoft\Protect
\Users\User\AppData\Local\Citrix\AuthManager\Data
\Users\User\AppData\Local\Citrix\SelfService\stores
\Users\User\AppData\Roaming\Microsoft\Protect
\Users\Administrator\AppData\Local\Citrix\AuthManager\Data
\Users\Administrator\AppData\Local\Citrix\SelfService\stores

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

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

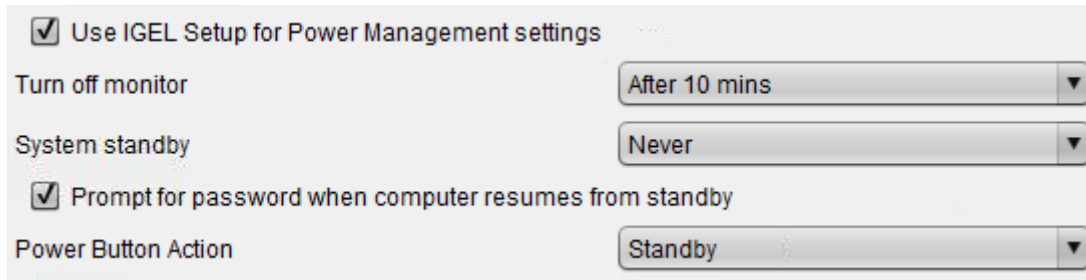


Figure 26: Energy Options

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

- Switch off monitor
- Standby
- Ask for password when ending standby mode
- Pressing the power switch

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

12.7. 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.

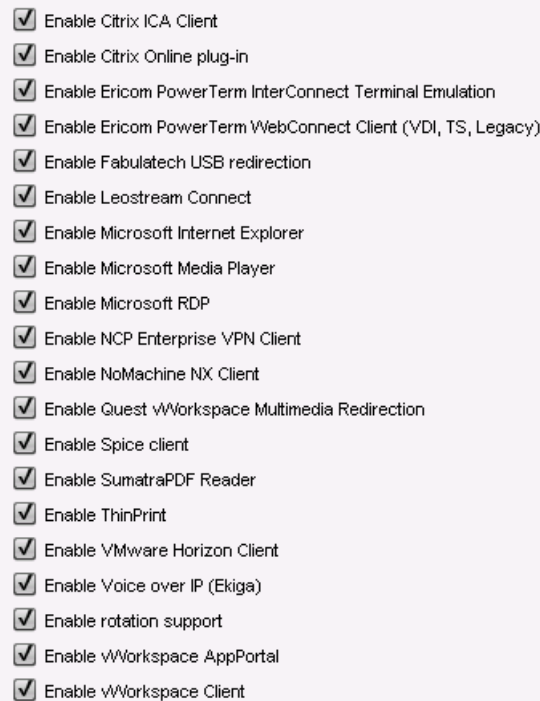
- 
- Enable Citrix ICA Client
 - Enable Citrix Online plug-in
 - Enable Ericom PowerTerm InterConnect Terminal Emulation
 - Enable Ericom PowerTerm WebConnect Client (VDI, TS, Legacy)
 - Enable Fabulatech USB redirection
 - Enable Leostream Connect
 - Enable Microsoft Internet Explorer
 - Enable Microsoft Media Player
 - Enable Microsoft RDP
 - Enable NCP Enterprise VPN Client
 - Enable NoMachine NX Client
 - Enable Guest vWorkspace Multimedia Redirection
 - Enable Spice client
 - Enable SumatraPDF Reader
 - Enable ThinPrint
 - Enable VMware Horizon Client
 - Enable Voice over IP (Ekiga)
 - Enable rotation support
 - Enable vWorkspace AppPortal
 - Enable vWorkspace Client

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

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.

- Click on **Parameter Search...** in order to search for specific parameters in the **IGEL Registry**.
- Search for the parameter name `wpa` if you require WPA encryption settings for securing your WLAN. The parameter found in the structure is highlighted:

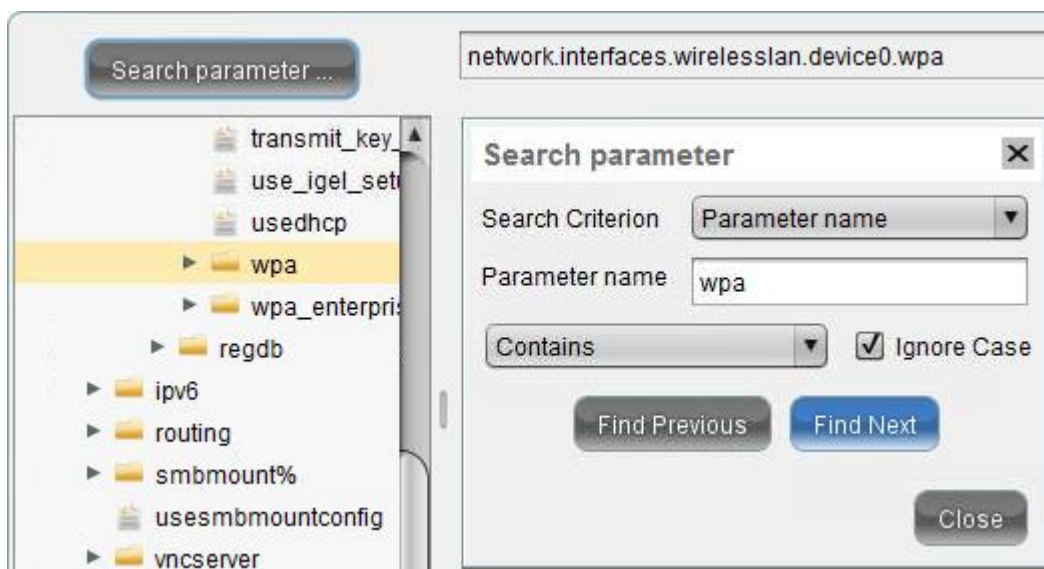


Figure 28: Search Parameter

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	26
Active Directory	34
Available options	38
B	
Basic principles and requirements	39
Boot options	9
C	
Citrix ICA	13
Creating a snapshot.....	36
D	
Date and time	36
Desktop and start menu	29
Devices.....	33
Downloading a snapshot	37
E	
Energy options.....	44
Entry	30
F	
File Based Write Filter	42
Firmware customization	44
Firmware update via snapshot.....	37
Formatting and meanings.....	5
G	
Global settings	13
I	
ICA settings	14
IGEL device information	9
IGEL setup.....	10
Important Information	2
Installing partial updates	38
Introduction.....	7
L	
LAN and WLAN (wireless)	31
Language.....	29
Leostream Connection Broker.....	20
M	
Microsoft Internet Explorer browser session	22
N	
Network	31
Network drives	32
Netzwerk.....	35
Nomachine NX.....	21
P	
Partial update	37
Password.....	34
PowerTerm terminal emulation	22
PowerTerm WebConnect	21
Q	
Quick installation	8
R	
RDP global.....	17
RDP sessions	17
Registry	45
Remote administration.....	36
Remote Desktop Protocol - RDP.....	17
Routing.....	32
S	
Screen	28
Searching setup pages	11
Secure shadowing (VNC with SSL)	39
Security	34
Self-Service-Plugin	17
Sessions.....	13
Setup areas	11
Setup Session.....	26
Shadow thin clients securely	41
Snapshots.....	36

Sound control	26
System	36
System restoration	47
T	
Thin Print	33
U	
Update	36
USB devices.....	33
User interface	28
V	
VMware Horizon client.....	18
VNC (Shadowing).....	38
VNC logging	41
Voice over IP (VoIP) client	24
VPN connection	31
vWorkspace Client and AppPortal.....	19
W	
What is new in 3.10.100 ?	6
Windows Firewall	35
Windows Media Player.....	24
Windows Services.....	27