



Unified Management Agent (UMA)

- [UMA Manual](#) (see page 3)
- [UMA How-Tos](#) (see page 128)
- [UMA Troubleshooting](#) (see page 133)

UMA Manual

This document describes *IGEL Unified Management Agent (UMA)*.

- [What is new?](#) (see page 4)
- [Overview](#) (see page 5)
- [Installation](#) (see page 6)
- [First Steps](#) (see page 14)
- [IGEL Setup](#) (see page 18)
- [Sessions](#) (see page 22)
- [Accessories](#) (see page 89)
- [User Interface](#) (see page 94)
- [Network](#) (see page 99)
- [Devices](#) (see page 103)
- [Security](#) (see page 105)
- [System](#) (see page 111)

What is new?

Find the release notes for *IGEL Unified Management Agent 2.03.100* (for Windows 7 and Windows 10) as a plaintext file alongside the installers on the [IGEL¹download server²](#).

- The unified write filter (UWF) is supported if Windows 10 is in use. For further information, see [Unified Write Filter \(UWF\)](#) (see page 124).

¹ http://myigel.biz/index.php?dir=IGEL_UNIVERSAL_DESKTOP_FIRMWARE/W7/

² http://myigel.biz/index.php?dir=IGEL_UNIVERSAL_DESKTOP_FIRMWARE/W7/



Overview

IGEL Unified Management Agent (UMA) enables you to manage *Windows 7* as well as *Windows 10* systems and selected applications via *IGEL Universal Management Suite (UMS)*. Optionally, a local setup application is available.

Installation


- [Prerequisites](#) (see page 7)
- [Installing Manually](#) (see page 8)
- [Installing via Group Policies \(GPO\)](#) (see page 10)
- [Uninstalling Manually](#) (see page 11)
- [Commandline Options](#) (see page 12)

Prerequisites

Supported Windows versions:

- *Windows 7 Professional* (32 and 64 bit)
- *Windows 7 Enterprise* (32 and 64 bit)
- *Windows 7 Embedded Standard* (32 and 64 Bit)

 *Windows Embedded Compact 7* is not supported.

 To be able to install UMA in version *2.03.100* on Windows 7 (64 Bit), the Windows security update KB3033929 must be installed. For further information, see <https://technet.microsoft.com/de-de/library/security/3033929>.

- All commercial Windows 10 versions except Windows 10 Mobile and Windows 10 IoT Core

Unified Write Filter (UWF) and File Based Write Filter (FBWF)

If the unified write filter (UWF, on Windows 10) or the file-based write filter (FBWF, on Windows 7) is to be used, it must be installed before UMA installation.

To install the write filter later, UMA must be deinstalled in the meantime.

Supported management software

- *IGEL Universal Management Suite (UMS) 5.02.100* or higher

Installing Manually

Preparations When Using Windows Embedded Standard 7

Make sure that the write filter (file-based write filter, FBWF) is disabled:

1. Log on to *Windows* as an administrative user.
2. Open the *Windows* command prompt.
3. Execute the `fbwfmgr` command.
4. Check whether the output contains the `disabled` status for the current session.
5. If the File-Based Write Filter is enabled, disable it using `fbwfmgr` or another tool your OEM may have installed.

Find more [Information about fbwfmgr](#)³ on the Microsoft Developer Network.

Preparations When Using Windows 10 IoT

Make sure that the write filter (unified write filter, UWF) is disabled:

1. Log on to *Windows* as an administrative user.
2. Open the *Windows* command prompt.
3. Execute the `uwfmgr` command.
4. Check whether the output contains the `disabled` status for the current session.
5. If the write filter is enabled, disable it using `fbwfmgr` or another tool your OEM may have installed.

Find more information about `fbwfmgr` on the [Microsoft Developer Network](#)⁴.

Installation

1. Log on to Windows as an administrative user.
2. Download the `*.exe` installation file from <https://www.igel.com>⁵ to a local directory.
3. Double-click the installation file.
4. Select the language to be used during the installation procedure.
5. Click **Next**.
6. Accept the license agreement displayed in order to proceed with the installation.
7. Select the **destination location** for the installation or accept the default.
8. Select whether the local setup application is to be installed.
9. Review your settings and click **Install**. Use **Back** to go back in order to adjust your settings. *UMA* will be installed.

³ <https://www.youtube.com/watch?v=pxwOB8IKyU8>

⁴ <https://msdn.microsoft.com/en-us/library/jj979579%28v=winembedded.81%29.aspx>

⁵ <https://www.igel.com/software-downloads/enterprise-management-pack/>

10. *Activate the write filter.*
11. Restart the computer.



Installing via Group Policies (GPO)

Read the how-to [Deploying UMA with Group Policies \(see page 129\)](#) in order to install UMA via Group Policies (GPO).

Uninstalling Manually


1. Go to **Windows Start Menu > Control Panel > All Control Panel Items > Programs and Features**.
2. Right-click the list item **IGEL Unified Management Agent**
3. Click **Uninstall**
4. Confirm that you want to uninstall the software.
5. When prompted, restart the computer in order to complete the removal procedure.

Commandline Options

The stand-alone installer (file extension *.exe) for the IGEL Unified Management Agent (UMA) supports various commandline options.

 The options are not supported by the Windows Installer for UMA (file extension *.msi).

Overview

 Please note that in silent mode (/SILENT and /VERYSILENT), all error messages are suppressed, too.
This means that you will get no feedback as to whether the installation failed or succeeded.

 Make sure to enter the options in uppercase.

Option		Parameter	Meaning
/SILENT	Works only in combination with /ACCEPTTEULA . If /ACCEPTTEULA is missing, the installation is aborted.	None	Shows only the progress bar of the installer GUI and hides everything else.
/VERYSILENT	Works only in combination with /ACCEPTTEULA . If /ACCEPTTEULA is missing, the installation is aborted.	None	Hides the installer GUI completely.
/ACCEPTTEULA		None	Accepts the End User License Agreement (EULA).
/NOLOCALSETUP		None	IGEL Setup will not be installed.



Option		Parameter	Meaning
/ REMOVESETTINGS		None	Deletes the C:\ProgramData\IGEL folder.
/ REGISTERUMS		IP address or hostname of UMS server	Automatically enrolls the device with the UMS server provided.

First Steps

Immediately after installing, no features of *Unified Management Agent* are enabled, apart from remote management via *Universal Management Suite (UMS)*. The first steps when bringing the device into service are:

- [Registering with UMS \(see page 15\)](#)
- [Licensing via UMS \(see page 16\)](#)
- [IGEL Device Information \(see page 17\)](#)


Registering with UMS

1. Use the [Scan for Thin Clients](#)⁶ function of *Universal Management Suite* to find *UMA* devices on the local network.
2. These can be identified by:
 - known MAC address
 - known IP address
 - product *IGEL Unified Management Agent W7* or *IGEL Unified Management Agent W10*
3. Check the **Include** checkbox for all devices you want to register with *UMS*.
4. Click **OK**.

⁶ <https://www.youtube.com/watch?v=pxwOB8IKyU8>

Licensing via UMS

1. Go to **System > License management** in UMS.

 From UMS *Version 5.07.100*, the license management for thin client licenses can be found under **UMS Administration > Global Configuration > Licenses**.

2. Click **+** symbol in order to add a license.
3. Select the license file (with `*.lic` extension).
4. Click **OK**.
The new license shows up in the list.
5. Select the newly added license in order to view the devices licensed by it.
Read more about licensing *UMA* in the Licensing *UMA* how-to.

IGEL Device Information

Right-click the *UMA* icon in System Tray in order to open **IGEL Device Information**.


The individual tabs:

- **Information:** A summary of the most important information such as version, IP address, MAC address, host name and product ID
- **License Information:** License information about software used in the product
- **Hotfixes:** A list of Microsoft Hotfixes applied to this product
- **About:** System properties displayed in a tree structure
- **Network Information:** Availability of the registered *UMS*, availability and IP addresses of DNS servers and default gateway

IGEL Setup

You have several options for configuring a device managed by *UMA*:

- via the local *IGEL* setup application
- via *IGEL Universal Management Suite*
- via a VNC connection to the device (shadowing)
- and/or a combination of these.

 Configuring the device via the Windows System Panel is strongly discouraged, as this would not save the settings in a profile.

The setup structure is similar to that on *IGEL Linux* thin clients and in *IGEL Universal Management Suite (UMS)*.

To start the setup application (when logged in as Administrator or if setup pages have been activated for users):

- ▶ Click the **Setup** symbol in Start menu or
- ▶ Click **Setup** in the programs list or
- ▶ Place an icon for **Setup** on the Desktop (**Setup > Accessories > Setup Session > Starting Methods for Session**).

To exit Setup:

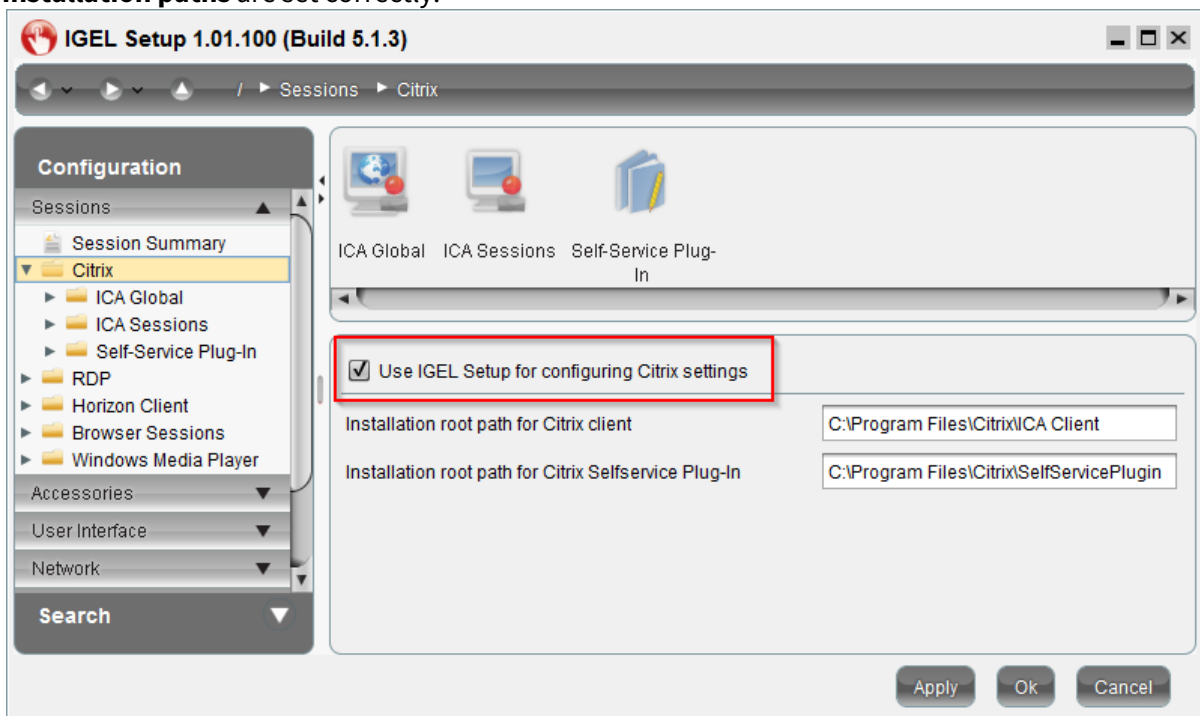
- ▶ Click **Apply** in order to save changed settings.
- ▶ Click **OK** in order to save changed settings and exit Setup.
- ▶ Click **Cancel** in order to exit Setup without saving any changes.

-
- [Activating Setup Sections](#) (see page 19)
 - [Setup Areas](#) (see page 20)
 - [Searching setup pages](#) (see page 21)

Activating Setup Sections

By default *UMA* does not change any settings on the *Windows* system. Only remote management via *UMS* is activated.

- In order to use a Setup section for configuration, check the **Use IGEL Setup for configuring [section] settings** checkbox.
- If you have installed the software managed by a Setup section yourself, please make sure that the **installation paths** are set correctly.



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** (see page 89): The *IGEL* setup application can be restricted for users (not the administrator). A number of Windows services can be enabled or disabled.
- **User interface** (see page 94): 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** (see page 99): In this area, you can configure all the network settings for LAN / WLAN interfaces. Network drives are also configured here.
- **Devices** (see page 103): 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** (see page 105): 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** (see page 111): 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.

To navigate in the setup application:

- ▶ 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.



Searching setup pages

To search for parameter fields or parameter 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.


Sessions

- [Supported Sessions](#) (see page 23)
- [Citrix](#) (see page 24)
- [Remote Desktop Protocol - RDP](#) (see page 47)
- [VMware Horizon Client](#) (see page 64)
- [Browser Sessions](#) (see page 71)
- [Windows Media Player](#) (see page 88)

Supported Sessions

Only specific versions of 3rd-party software are supported by *UMA*:

- *Citrix Receiver 4.4*
- *VMWare Horizon Client for Windows 3.5.2*
- *Windows Media Player 12*
- *Microsoft Internet Explorer 11*

 You need to install these programs yourself. After installation *UMA* can configure and launch them.

Citrix

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


- **Use IGEL Setup for configuring Citrix settings**
 - The *IGEL* Setup will change the *Citrix* settings.
 - The *Citrix* settings will be changed in another way.
- **Install on 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`
- **Install on root path for Citrix Self-Service:** Specify the path to the directory in which the Citrix Self-Service Plugin is installed.

-
- [ICA Global](#) (see page 25)
 - [ICA Sessions](#) (see page 33)
 - [Self-Service Plugin](#) (see page 42)

ICA Global

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

The global settings define default parameters which are used in all sessions or can be overridden 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](#) (see page 26)
 - [Window](#) (see page 27)
 - [Keyboard](#) (see page 28)
 - [Firewall](#) (see page 29)
 - [Options](#) (see page 30)
 - [USB Redirection](#) (see page 31)
 - [HDX](#) (see page 32)


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.

 **TCP/IP + HTTP** 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 default color depth.
Possible values:
 - **16**
 - **256**
 - **Thousands**
 - **Millions**
- **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 overridden in the sessions.

- **Keyboard layout: Default** is pre-populated but you can also select a country-specific layout. **Default** means that the local keyboard setting will be used in ICA too.
- **Redirect Ctrl-Alt-Delete to sessions**
 - The key combination will not be processed by the local thin client. It will be forwarded to the session instead.
 - The key combination will be processed by the thin client.
- **Hotkeys:** You can set up the hotkeys for the server system on function keys or key combinations on the local keyboard.

Firewall

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

Here, you can 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 to 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 [Server Location](#) (see page 26).

- The *Citrix server* has no alternate IP address.

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 default 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**


- The local system's alert sounds will not be used.
- The local system's alert sounds will be used.

- **Deferred screen update mode**

- Updates from the local video buffer will be shown on the screen with a delay. The local video buffer is used if the seamless Windows mode or HDX latency reduction is used.
- Updates from the local video buffer will not be delayed.

 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 memory in kilobytes used for temporary storage purposes.

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

- **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.
- **Enable Auto Reconnect**
 - The *Citrix* client will automatically reconnect if the connection was terminated.
 - The *Citrix* client will not automatically reestablish the connection.
- **Maximum retries:** Number of reconnection retries
- **Enable Single Sign-on through ICA file:**
 - You will only need to log on once.
 - "Single sign-on" will not be used.


USB Redirection

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

- **Enable USB Redirection (XenDesktop and Citrix VM hosted):**
 - 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.
- **Automatically redirect all devices via native USB redirection**
 - All USB devices with native USB redirection will be forwarded.
- **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**.

You can edit the rules using the following icons:

 add

 remove


 edit

 copy

HDX

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

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

 Redirecting Flash content can improve playback.

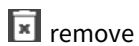
- **File access:** Specify what access to local client files is allowed.
- **Microphone and webcam access:** Specify what access to local microphones and webcams is allowed.
- **PDA access:** Specify what access to personal digital assistants (PDAs) is allowed.
- **USB and other devices access:** Specify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

ICA Sessions

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

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

You can edit sessions using the following icons:



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

-
- [Connections](#) (see page 34)
 - [Logon](#) (see page 35)
 - [Window](#) (see page 36)
 - [Firewall](#) (see page 37)
 - [Wiederverbindung](#) (see page 38)
 - [Options](#) (see page 39)
 - [Desktop Integration](#) (see page 41)

Connections


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

- **Browser Protocol:** The protocol that is to be used when searching for servers and published applications.
- **Don't use default server location**
 - The default server location will not be used. Enter one or more HTTP server locations.
 - The default server location will be used.
- **Citrix Server:** 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.
- **Connections:** 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:** Details of the path name 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 will no longer need to give these details at the start of a session. If you leave these fields empty, the user will have to enter them in a mask before the session start.


- **Do not show Password Protection Window (Ctrl-Alt-Delete) before Logon**
 - The *Windows* Password Protection Window will not be shown.
 - The *Windows* Password Protection Window will be shown.

Window

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

In this area, you can define the window size and color depth for the session. For published applications, the seamless window mode can be enabled.

- **Number of Colors:** The color depth is specified in [ICA Global](#) (see page 27). You can change it for this session.
- **Use full-screen mode**
 - The session will be shown in full-screen mode.
 - You can choose between the global default setting and a session-specific setting.
- **WindowSize:** Choose between the pre-defined default size and a range of other sizes.
- **Enable Seamless Window Mode**
 - Seamless Window Mode will be used.

 Seamless Window Mode can only be used with published applications or with a specified start program for the server connection.

- Seamless Window Mode will not be used.

Firewall

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

Here, you can 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 to 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 **Server Location**.

- No alternate IP address will be used.

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 default 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**.

Wiederverbindung

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

- **Enable Auto Reconnect**

- The *Citrix* client will automatically reconnect if the connection was terminated.
- The *Citrix* client will not automatically reestablish the connection.

- **Maximum Retries:** Number of reconnection retries


Options

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

- **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.
 - The data to be transmitted will not be compressed. This setting is suitable when using relatively low-performance servers and when working in a LAN.
- **Persistent Cache Enabled**
 - The image data will be cached. 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 space for these sessions.
 - The image data will not be cached.
- **Client Drive Mapping**
 - The local drives will be available in the session.
 - The local drives will not be available in the session.
- **Encryption Level:** 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 level of encryption.
- **Client Audio**
 - 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.
 - No system sounds and audio output will be transferred to the thin client.

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 was enabled and configured on the *Citrix* server beforehand.

- **Mouse click feedback:** Visual feedback in response to a mouse click – an hourglass symbol appears immediately.
 - **Off**
 - **On**
 - **Automatic**
- **Local Text Echo:** Displays the text entered more quickly. This avoids latencies within the network. Select a mode from the drop-down list:
 - **Off:** For faster connections (connection via a LAN)
 - **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.

- **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.
- **Start Menu**
 - An entry will be placed in the start menu.
 - No entry will be placed in the start menu.
- **Desktop**
 - A start icon will be placed on the desktop.
 - No start icon will be placed on the desktop.
- **Autostart**
 - The session will start automatically after you log on to the device.
 - The session will not start automatically.

Self-Service Plugin

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

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

- **Login Session Name:** Specify the name of the session to be displayed.
- **Put shortcuts in start menu**
 - Shortcuts are displayed in the start menu.
 - Shortcuts are not displayed in the start menu.
- **Verknüpfungen auf dem Desktop**
 - Shortcuts are displayed on the desktop.
 - Shortcuts are not displayed on the desktop.
- **Autostart**
 - The session starts automatically after logging in to the device.
 - The session will not start automatically.

-
- [Server](#) (see page 43)
 - [Logon](#) (see page 44)
 - [Appearance](#) (see page 45)
 - [Desktop Integration](#) (see page 46)

Server

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

- **Use IGEL Setup for Citrix Self-Service Plugin configuration:**

- The *IGEL* setup will configure the *Citrix Self-Service* plugin.
- The *Citrix Self-Service* plugin will be configured in another way.

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:**

Possible values:

- **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:**

Possible values:

- **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**

The client is allowed to connect to stores without encryption (via HTTP).

The client is not allowed to connect to stores without encryption.

- **Logon mode:**

Possible values:

- **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**
 - The applications will be sorted according to categories in the start menu.
 - The applications will be sorted differently.
- **Additional submenu in start menu:** Here you can specify a directory which contains the applications in the start menu.
- **Additional sub-menu on desktop:** Here you can specify a directory which contains the applications on the desktop.
- **Enable Citrix Receiver Self-Service Mode:**
 - You will find the applications in a custom Self-Service GUI
 - The Self-Service GUI will not be used.
- **Give user the option to add or remove accounts in Non-Self-Service Mode**
 - If the Self-Service Mode is disabled, the user can edit accounts via the *Citrix Receiver* context menu in the system tray.
 - The user cannot edit accounts via the *Citrix Receiver* context menu in the 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.

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

- **Put shortcuts in Start Menu**

- Shortcuts for the published apps and desktops will be set up in the start menu.
- No shortcuts will be set up in the start menu.

- **Put shortcuts on the desktop**

- Shortcuts for the published apps and desktops will be set up on the desktop.
- No shortcuts will be set up on the desktop.

- **Autostart**

- The session will start automatically after you log on to the device.
- The session will not start automatically.

Remote Desktop Protocol - RDP

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

The *Microsoft* RDPclient is used for connections via the Remote Desktop Protocol (RDP). The configuration of the client has been integrated into the *IGEL* setup.

You will find detailed information regarding *Microsoft RDP* on the website <http://technet.microsoft.com>⁷.

- **Use IGEL Setup for configuring Microsoft RDP settings:**

- Configure RDP using the *IGEL* Setup.
- Do not use Setup.

-
- [RDP \(Global Settings\)](#) (see page 48)
 - [RDP Sessions](#) (see page 56)

⁷ <http://technet.microsoft.com/>

RDP (Global Settings)

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

Global settings specify how the RDP client (`mstsc.exe`) behaves if it is launched without a specific session.

- **Window:** Allows you to set the number of colors, display via several monitors, true 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 wallpaper, font smoothing, video redirection, bitmap cache and compression
- **Options:** Allows you to set the application, working directory, authentication options and configuration for an RD Gateway server
- **USB Redirection:** Allows you to prohibit and allow RemoteFX USB redirection for individual USB devices

-
- [Logon](#) (see page 49)
 - [Window](#) (see page 50)
 - [Keyboard](#) (see page 51)
 - [Mapping](#) (see page 52)
 - [Performance](#) (see page 53)
 - [Options](#) (see page 54)
 - [USB Redirection](#) (see page 55)

Logon

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

- **Server:** Address of the server
- **User name:** Allows you to specify the user name
- **Domain:** Allows you to specify the domain
- **Reconnect:**
 - The client will automatically reconnect if the connection was terminated.
 - The client will not automatically reestablish the connection.


Window

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

- **Number of colors:** Allows you to specify the default color depth
 - **8 bit**
 - **16 bit**
 - **24 bit**
 - **32 bit**
- **Span desktop:**
 - The RDP session will use all available monitors as the desktop.
 - No, do not span desktop
- **True Multimonitor support:**
 - The user can connect to multimonitor configurations.
 - No true multimonitor support
- **Window size:** Choose between **full screen** and a range of fixed sizes.
- **Display the Connection bar:**
 - A symbol bar for minimizing and closing the full-screen session will be shown.
 - No, do not show Connection Bar.

Keyboard

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

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

- **Enable Clipboard Mapping:**

- Content can be shared between the local system and the session via the Clipboard.
- No, do not enable Clipboard Mapping

- **Override local window manager keyboard shortcuts:**

- The session hotkeys will override equivalent local ones.
- No, do not override hotkeys.

- **Redirect Ctrl-Alt-Delete to sessions:**

- This key combination will not be processed by the local thin client. It will be forwarded to the session instead.
- No, do not redirect.

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**
 - The local microphone will be passed on to the RDP session.
 - Do not redirect.
- **Override local window manager keyboard shortcuts:**
 - The session hotkeys will override equivalent local ones.
 - Do not override hotkeys.
- **Enable Printer Mapping**
 - Make local printer available in the RDP session.
 - Do not enable.
- **Enable COM Port Mapping:**
 - Make local COM ports available in the session.
 - No mapping of COM ports.
- **Enable Smartcard Mapping:**
 - Redirect smartcards
 - No, do not enable.
- **Enable Clipboard Mapping:**
 - Content can be shared between the local system and the session via the clipboard.
 - Do not enable.
- **Enable Drive Mapping**
 - Make drives available in the session
 - No, do not map drives.
- **Drives**
 - Make all drives available in the session
 - No, do not map all drives.
- Specific drives (select)
- **Drives that I connect to later**
 - Automatically map newly connected drives
 - Do not map new drives


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 content of window while dragging**
- **Disable Menu and Window animation**
- **Disable Themes**
- **Disable Cursor Settings**
- **Disable Font smoothing**
- **Disable Desktop composition**
- **Video Redirection**
 - Videos will be played back locally.
 - Videos will be played back on the server.
- **Redirect DirectX commands:**
 - Graphics functions will be executed locally.
 - Graphics functions will be executed on the server.
- **Disable Bitmap cache:**
 - Images will not be cached locally.
 - Images will be cached locally.
- **Compression:**
 - **Default**
 - **On**
 - **Off**

 In low-bandwidth environments, you should use **Compression** in order to reduce network traffic. Please note that the use of compression reduces the burden on the network but does use CPU power.

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 an 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 **Smartcard**.
 - **Bypass RD Gateway server for local addresses:**
 - No gateway will be used for connections in the local network.
 - No, do not bypass.
 - **Use my RD Gateway credentials for the remote computer**
 - Pass on logon information on the RD Gateway to the remote computer
 - Do not use

USB Redirection

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

- **Enable RemoteFX USB Redirection:** If this option is enabled, you can allow or prohibit redirection.
- **Device Rules:** Define rules for individual devices by entering the **Instance ID of the device**.

How to work with device rules:

- ▶ To create a rule, click  in the **Device Rules** area.
 - Choose between **Deny** and **Allow**.
 - Specify the **Instance ID of the device**.
- ▶ To remove a rule, click  .
- ▶ To change a rule, click  .


RDP Sessions

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

Many of the session parameters can be pre-populated through the global settings. However, a number of them can only be set in the session configuration, for example logon data or desktop integration.

You can edit sessions using the following icons:

 add

 remove

 edit

 copy

-
- [Server](#) (see page 57)
 - [Logon](#) (see page 58)
 - [Window](#) (see page 59)
 - [Performance](#) (see page 60)
 - [Mapping](#) (see page 61)
 - [Options](#) (see page 62)
 - [Desktop Integration](#) (see page 63)

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 on 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
- **Enable reconnect:**
 - The client will automatically reconnect if the connection was terminated.
 - The client will not automatically reestablish the connection.

Window

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

- **Window size:** Choose between **full screen** and a range of fixed sizes.
- **Number of colors:** Allows you to specify the default color depth
- **Span desktop**
 - The session will use all available monitors as the desktop.
 - The session will use only one monitor as the desktop.
- **True Multimonitor Support**
 - You can connect to multi-monitor configurations.
 - No true multi-monitor support
- **Display the Connection Bar**
 - A symbol bar for minimizing and closing a full-screen session will be shown.
 - No symbol bar 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 which reduce visual effects in order to conserve resources:

- **Disable Wallpaper**
- **Do not show content of window while dragging**
- **Disable Menu and Window animation**
- **Disable Themes**
- **Disable Cursor Settings**
- **Disable Font smoothing**
- **Disable Desktop Composition**

- **Video Redirection**

- Videos will be played back locally.
- Videos will be played back on the server.

- **Redirect DirectX Commands**


- Graphics functions will be executed locally.
- Graphics functions will be executed on the server.

- **Disable Bitmap cache**

- Images will not be cached locally.
- Images will be cached locally.

- **Compression:**

- **default**
- **on**
- **off**

 In low-bandwidth environments, you should use **compression** in order to reduce network traffic. Please note that the use of compression reduces the burden on the network but does use CPU power.

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**
 - The local microphone will be passed on to the RDP session.
 - Do not redirect.
- **Override local window manager keyboard shortcuts:**
 - The session hotkeys will override equivalent local ones.
 - Do not override hotkeys.
- **Enable Printer Mapping**
 - Make local printer available in the RDP session.
 - Do not enable.
- **Enable COM Port Mapping:**
 - Make local COM ports available in the session.
 - No, no mapping of COM ports.
- **Enable smartcard mapping:**
 - Redirect smartcards
 - No, do not enable.
- **Enable Clipboard mapping:**
 - Content can be shared between the local system and the session via the clipboard.
 - Do not enable.
- **Map all drives**
 - Make all drives available in the session
 - No, do not map all drives.
- Specific drives (select)
- **Drives that I connect to later**
 - Automatically map newly connected drives
 - Do not map new drives

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 an 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 **Smartcard**.
 - **Bypass RD Gateway server for local addresses:**
 - No gateway will be used for connections in the local network.
 - No, do not bypass.
 - **Use my RD Gateway credentials for the remote computer**
 - Pass on logon information on the RD Gateway to remote computers
 - Do not use

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:**
 - Create an entry in the start menu.
 - Do not create an entry.
 - **Desktop:**
 - Create an entry on the desktop.
 - Do not create an entry.
 - **Autostart:**
 - The session will start automatically after you log on to the device.
 - No autostart

VMware Horizon Client

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

Here, you can configure *Horizon* client sessions

- **Use IGEL Setup for configuring Horizon settings**
 - The IGEL Setup will change the *Horizon* settings.
 - The *Horizon* settings will be changed in another way.
- **Path to "vmware-view.exe"**: File path to the Horizon executable, for example `C:\Program Files\VMware\VMware Horizon View Client\vmware-view.exe`

You will find a detailed description of the client configuration in the original documentation for *Horizon* at http://www.vmware.com/support/pubs/view_pubs.html.

-
- [Horizon Client Global](#) (see page 65)
 - [Horizon Client Sessions](#) (see page 66)




Horizon Client Global

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

USB redirection

- **Enable USB redirection**
 - You can use the local computer's USB devices in sessions.
 - No, do not enable
- **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 **sub-class 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 change a rule, click .

Keyboard (cannot be overridden in the sessions):




- **Redirect Ctrl-Alt-Delete to sessions:**
 - The key combination will not be processed by the local thin client. It will be forwarded to the session instead.
 - No, do not redirect.

Horizon Client Sessions

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

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

How to work with sessions:

- ▶ To create a session, click  .
- ▶ To remove a session, click  .
- ▶ To change a session, click  .

-
- [Connection Settings](#) (see page 67)
 - [Window](#) (see page 68)
 - [Mapping](#) (see page 69)
 - [Desktop Integration](#) (see page 70)

Connection Settings

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

- **Server URL:** The address of the Horizon server
- **Use SSL encryption:**
 - The connection will use TLS/SSL encryption.
 - No, do not use this.
- **Username:** Username for the Horizon server.
- **User password:** Password for the Horizon server
- **Domain:** The domain for logging on
- **Session type:**
 - **Desktop:** Show the entire desktop of the remote system.
 - **Application:** Show only one application window.
- **Name of the desktop:**
- For the Application session type: **Application name:**
- **Hide client after launch session:**
 - **On:** Yes, hide it.
 - **Off:** No, do not hide it.
- **Protocol:**
 - **Server default**
 - **RDP**
 - **PCoIP**
- **Log on as current user:**
 - Use the current user name.
 - Do not use the current user name.
- **Kiosk mode**
 - **On:** Use the kiosk mode, where the user does not need to log on and has only limited operating options.
 - **Off:** Do not enable kiosk mode.
- **Single autoconnect**
 - **On:** Connect only to a single desktop or a single application.
 - **Off:** No single autoconnect
- **No VMware addins**
 - **On:** Do not use VMware addins.
 - **Off:** Use VMware addins.

Window

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

Here, you can specify how the Horizon session is displayed.

- **Display:**
 - **Full Screen:** The session will fill a monitor.
 - **Multimonitor:** The session will fill several monitors.
 - **Window - Large:** The session will be shown in a large window.
 - **Window - Small:** The session will be shown in a small window.

Mapping

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

Here, you can select whether and when USB devices are made available in the session.

- **Connect USB on insert:**

- USB devices will be connected when they are inserted.
- Do not connect upon insert.

- **Connect USB on startup:**

- USB devices will be connected when the session starts.
- Do not connect

Desktop Integration

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

- **Session name:** Give the name of the session which is to be shown.
- **Starting methods for session:**
 - **Start menu:**
 - Create an entry in the start menu.
 - Do not create an entry.
 - **Desktop:**
 - Create an entry on the desktop.
 - Do not create an entry.
 - **Autostart:**
 - The session will start automatically after you log on to the device.
 - No autostart

Browser Sessions

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

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

- **Use IGEL Setup for configuring Microsoft Internet Explorer Settings**
 - The *IGEL* setup will change the settings for the browser.
 - The settings for the browser will be defined in the browser's **Internet options**.
- **Session name:** Name for the browser session
- **Global home page:** Specifies the URL of the startup page.
- **IE kiosk mode**
 - The browser will run in kiosk mode. In the kiosk mode, the browser will appear in full-screen mode; control bars, tool bars and bookmarks will not be shown.
- **Use a proxy server for your LAN:** This setting applies to the LAN only, it does not apply to VPN or dial-up connections.
 - The browser will use the proxy configured under **Setup > Sessions > Browser Sessions > Proxy** for websites in the LAN.
 - The browser will use a direct connection for websites in the LAN.
- **Do not use proxy server for addresses beginning with:** List of URLs for which no proxy is to be used

-
- [Global](#) (see page 72)
 - [Security](#) (see page 73)
 - [Advanced](#) (see page 82)
 - [Start](#) (see page 83)
 - [Window](#) (see page 84)
 - [Proxy](#) (see page 85)
 - [Toolbar Items](#) (see page 86)
 - [Toolbars](#) (see page 87)

Global

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

You can define how the URL is displayed.

- **Show full URL**

The address bar shows the full URL, including the protocol prefix, e.g. `http://www.igel.com`.

The address bar does not show the protocol, e.g. `www.igel.com`.

Security

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

In this section you can configure the allowed SSL versions and to the browser's behavior when changing between security modes.

- **Allow SSL 2.0**
 - SSL 2.0 connections are allowed.
 - SSL 2.0 connections are not allowed.
- **Allow SSL 3.0**
 - SSL 3.0 connections are allowed.
 - SSL 3.0 connections are not allowed.
- **Warn if changing between secure and not secure mode**
 - When changing from HTTPS to HTTP a warning will be shown.

-
- [.NET Framework](#) (see page 74)
 - [ActiveX controls and plug-ins](#) (see page 75)
 - [Download](#) (see page 76)
 - [Scripting](#) (see page 77)
 - [Sites](#) (see page 78)
 - [Miscellaneous](#) (see page 80)

.NET Framework

Menu path: **Setup > Sessions > Browser Sessions > Security > .NET Framework**

Configure how the browser handles .NET applications.


- **Loose XAML**
 - **Enable:** Run Loose XAML browser applications.
 - **Prompt:** Run Loose XAML browser applications after confirmation from the user.
 - **Disable:** Do not run Loose XAML browser applications.
- **XAML browser applications**
 - **Enable:** Run XAML browser applications.
 - **Prompt:** Run XAML browser applications after confirmation from the user.
 - **Disable:** Do not run XAML browser applications.
- **XPS documents**
 - **Enable:** Display XPS documents.
 - **Prompt:** Display XPS documents after confirmation from the the user.
 - **Disable:** Do not display XPS documents.
- **Run components signed with Authenticode:**
 - **Enable:** Run components signed with Authenticode.
 - **Prompt:** Run components signed with Authenticode after confirmation from the user.
 - **Disable:** Do not run components signed with Authenticode.
- **Run components not signed with Authenticode:**
 - **Enable:** Run components not signed with Authenticode.
 - **Prompt:** Run components not signed with Authenticode after confirmation from the user.
 - **Disable:** Do not run components not signed with Authenticode.

ActiveX controls and plug-ins

Menu path: **Setup > Sessions > Browser Sessions > Security > ActiveX controls and plug-ins**

Configure how the browser handles ActiveX controls and plug-ins.

- **Script ActiveX controls marked safe for scripting.**

 The classification as "safe for scripting" is made by the publisher of a control. It does not guarantee any degree of security.

- **Enable:** Script ActiveX controls marked safe for scripting.
- **Prompt:** Script ActiveX controls marked safe for scripting after confirmation from the user.
- **Disable:** Do not script ActiveX controls marked safe for scripting.
- **Initialize and script ActiveX controls**
 - **Enable:** Initialize and script ActiveX controls.
 - **Prompt:** Initialize and script ActiveX controls after confirmation from the user.
 - **Disable:** Do not initialize and script ActiveX controls.
- **Run ActiveX controls and plug-ins**
 - **Enable:** Run ActiveX controls and plug-ins.
 - **Prompt:** Run ActiveX controls and plug-ins after confirmation from the user.
 - **Disable:** Do not run ActiveX controls and plug-ins.
- **Download signed ActiveX controls**
 - **Enable:** Download signed ActiveX controls.
 - **Prompt:** Download signed ActiveX controls after confirmation from the user.
 - **Disable:** Do not download signed ActiveX controls.
- **Allow Scriptlets**
 - **Enable:** Run Scriptlets.
 - **Prompt:** Run Scriptlets after confirmation from the user.
 - **Disable:** Do not run Scriptlets.
- **Download unsigned ActiveX controls**
 - **Enable:** Download unsigned ActiveX controls.
 - **Prompt:** Download unsigned ActiveX controls after confirmation from the user.
 - **Disable:** Do not download unsigned ActiveX controls.

Download

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

Configure how the browser handles downloadable fonts.

- **Font download**

- **Enable:** Download fonts.
- **Prompt:** Download fonts after confirmation from the user.
- **Disable:** Do not download fonts.

Scripting

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

Configure how the browser handles scripts embedded in websites.

- **Active Scripting**
 - **Enable:** Allow Active Scripting.
 - **Prompt:** Allow Active Scripting after confirmation from the user.
 - **Disable:** Do not allow Active Scripting.
- **Clipboard access**
 - **Enable:** Allow scripts to access the clipboard.
 - **Prompt:** Allow scripts to access the clipboard after confirmation from the user.
 - **Disable:** Do not allow scripts to access the clipboard.
- **Scripting of Java applets**
 - **Enable:** Allow scripts to access Java applets.
 - **Prompt:** Allow scripts to access Java applets after confirmation from the user.
 - **Disable:** Do not allow scripts to access Java applets.

Sites

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

Assign websites to one of the security zones.

internetzone

- **Enable Protected Mode**

- Protected Mode is enabled for sites in the Internet zone.

localintranetzone


- **Require server verification (https:) for all sites in this zone.**

- The browser only accepts secured web sites and forces HTTPS connections.
- The browser also accepts non-secured web sites and plain HTTP connections.

- **Enable Protected Mode**

- Protected Mode is enabled for sites in the Local Intranet zone.

In order to add a site to the Local Intranet zone, do the following:

1. In the **localintranetzone** section, click .
2. Enter the site to add into the **Website** input field.
3. Click **Ok**.

trustedzone


- **Require server verification (https:) for all sites in this zone.** The browser only accepts secured web sites and forces HTTPS connections.

- The browser also accepts non-secured web sites and plain HTTP connections.

- **Enable Protected Mode**

- Protected Mode is enabled for sites in the Trusted sites zone.

In order to add a site to the Trusted Sites zone, do the following:


1. In the **trustedzone** section, click .
2. Enter the site to add into the **Website** input field.
3. Click **Ok**.

restrictedzone

- **Enable Protected Mode**

- Protected Mode is enabled for sites in the Restricted sites zone.

In order to add a site to the Restricted sites zone, do the following:

1. In the **restrictedzone** section, click .
2. Enter the site to add into the **Website** input field.



3. Click **Ok**.

Miscellaneous

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

Configure various security settings.

- **Launching programs and files in an IFRAME**
 - **Enable:** The browser launches programs or opens files contained in an inline frame (HTML element `<iframe>`).
 - **Prompt:** The browser launches programs or opens files contained in an inline frame (HTML element `<iframe>` after confirmation from the user.
 - **Disable:** The browser does not launch programs or open files contained in an inline frame (HTML element `<iframe>`).
- **Launching applications and unsafe files:** Configure how the browser handles applications and files considered unsafe for the current security zone.
 - **Enable:** Launch applications and unsafe files.
 - **Launch** applications and unsafe files after confirmation from the user.
 - **Disable:** Do not launch applications and unsafe files.
- **Drag and drop or copy and paste files**
 - **Enable:** Allow dropping as well as copying and pasting files.
 - **Prompt:** Allow dropping as well as copying and pasting files after confirmation from the user.
 - **Disable:** Do not Allow dropping or as copying and pasting files.
- **Display mixed content:** Configure how the browser handles web pages containing insecure as well as secure contents.
 - **Enable:** Display mixed contents.
 - **Prompt:** Display mixed contents after confirmation from the user.
 - **Disable:** Do not display mixed content.
- **Allow websites to use restricted protocols for active content:** Configure how the browser handles active contents delivered via protocols disabled by the current security settings: `res:`, `shell:`
 - **Enable:** Display pages containing active contents delivered via restricted protocols.
 - **Prompt:** Display pages containing active contents delivered via restricted protocols after confirmation from the user.
 - **Disable:** Do not display pages containing active contents delivered via restricted protocols.
- **Access data sources across domains**
 - **Enable:** The browser may access data sources from other security zones via Microsoft XML Parser (MSXML) or ActiveX Data Objects (ADO).
 - **Prompt:** The browser may access data sources from other security zones via Microsoft XML Parser (MSXML) or ActiveX Data Objects (ADO) after confirmation from the user.
 - **Disable:** The browser must not access data sources from other security zones via Microsoft XML Parser (MSXML) or ActiveX Data Objects (ADO).
- **Navigate windows and frames across different domains**
 - **Enable:** The browser may open subframes from other domains and access applications on other domains.

- **Prompt:** The browser may open subframes from other domains and access applications on other domains after confirmation from the user.
- **Disable:** The browser must not open subframes from other domains and access applications on other domains.
- **Submit non-encrypted form data:** Configure, whether form data may be submitted via plain HTTP in this security zone. SSL-secured submission is always allowed.
 - **Enable:** Form data may be submitted over plain HTTP in this zone.
 - **Prompt:** Form data may be submitted over plain HTTP in this zone after confirmation from the user.
 - **Disable:** Form data must not be submitted over plain HTTP in this zone.

Advanced

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

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

- **Show pictures**
 - Images in websites will be shown.
 - Images in websites will not be shown.
- **Play sounds in webpages**
 - The background sound of websites will be played. Playback will begin as soon as the page is opened.
 - The background sound of websites will not be played.
- **Show friendly HTTP error messages**
 - A user friendly error message without details will be shown in the event of a problem with HTTP communication.
 - A detailed error message which may make troubleshooting easier will be shown in the event of a problem with HTTP communication.
- **Automatically activate newly installed add-ons**
 - Newly installed add-ons will be activated automatically.
 - A user prompt asking whether the add-on is to be activated will appear the first time the browser starts following installation.

Start

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

Configure the start options for the browser.

- **Enable entry in Autostart.**
 - Der Launch the browser with the system start,
- **Enable entry in Start Menu**
 - The browser can be launched from the Start Menu.
- **Enable entry on Desktop**
 - The browser can be launched from a Desktop icon.

Window

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

Configure basis browser settings.

- **Start in fullscreen mode**

- The browser starts in fullscreen mode. It fills the entire display, showing the browser contents only.

- The browser is display in a standard window.

- **Global home page:** Set the start page URL.

- **Search provider:** Sets the search engine, used in the browser's Search field.

Possible values:

- **Google**

- **Bing**

- **Yahoo!**

- **Lycos**

- **ASK.com**

- **AOL Search**

- **Altavista**

- **Wikipedia**

- **Custom**

- **Custom search provider:** Configure a custom search provider URL, if **Search provider** is set to **Custom**.

- **Custom search provider display name:** Name to be displayed for the custom search provider.

Proxy

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

Configure proxy servers.

- **Use a proxy server for your LAN.**
 - The browser uses a proxy server to connect to sites within the LAN.
 - The browser makes direct connections to sites within the LAN.
- **HTTP Proxy:** HTTP proxy URL
- **Port:** HTTP proxy port
- **FTP Proxy:** FTP proxy URL
- **Port:** FTP proxy port
- **SOCKS Host:** SOCKS proxy URL
- **Port:** SOCKS proxy port
- **SSL Proxy:** SSL proxy URL
- **Port:** SSL proxy port
- **Do not use proxy server for addresses beginning with:** List of URLs for which no proxy will be used.
- **Auto Config URL:** Automatic configuration file URL

Toolbar Items

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

Configure browser toolbars.

- **Hide Menu bar**
 - The browser Menu bar will not be displayed.
 - The browser Menu bar will be displayed.
- **Lock the toolbars**
 - The display of the toolbars can not be modified.
 - The display of the toolbars can be modified.

Toolbars

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

Configure toolbar display and tab behavior.

- **Hide the Status bar**
 - The browser Status bar will not be displayed.
 - The browser Status bar will be displayed.
- **Hide Command bar**
 - The browser Command bar will not be displayed.
 - The browser Command bar will be displayed.
- **Disable Dev Tools**
 - Developer Tools will not be available.
 - Developer Tools will be available.
- **Warn when closing multiple tabs.**
 - A warning will be displayed when the user tries to close multiple tabs.
- **Always switch to new tabs when they are created.**
 - When opening a link in a new tab, move focus to the new tab.
 - Do not move focus when opening a link in a new tab.
- **Enable Tab Groups**
 - Mark related tabs with the same color. Tabs are related, when one tab has been opened from a link in the other.
- **When a new tab is opened, open:**
 - **A blank page:** The new tab will show a blank page.
 - **Your first home page:** The new tab will show the home page configured for the browser.
 - **The new tab page:** The new tab will show a default browser page with a search field and a list of the most frequently visited pages.
- **Open links from other programs in:**
 - **A new window:** Links from another program are opened in a new browser window.
 - **A new tab in the current window:** Links from another program are opened in a new tab in the current browser window.
 - **The current tab or window:** Links from another program are opened in the current tab or window.

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](#)⁸.

⁸ <https://support.microsoft.com/en-us/products/windows?os=windows-7>

Accessories

Menu path: **Setup > Accessories**

Information on other accessories provided by the *IGEL Universal Desktop* can be found here:

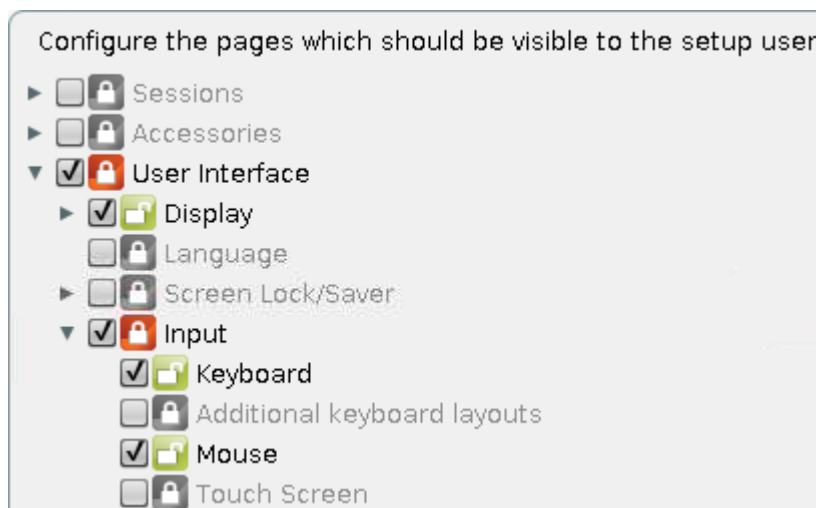
- [Setup Session](#) (see page 90)
- [Sound Mixer](#) (see page 92)
- [Windows services](#) (see page 93)


Setup Session

Menu path: **Setup > Accessories > 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](#) (see page 106)). However, individual areas of the setup can be enabled for the user, e.g. to allow them to change the system language or configure a left-handed mouse.

1. Under **Security > Password**, enable the password for the **administrator** and the **setup user**.
2. Under **Accessories > Setup Session > 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).

- [Options](#) (see page 91)

Options

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

- **Enable tool tips**
 - Tool tips will be displayed.
 - Tool tips will be displayed.
- **Tool tip delay:** Time in seconds after which the tool tip is displayed

Sound Mixer

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

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

- **Use IGEL Setup for configuring system audio settings:**
 - Use IGEL Setup
 - Do not use IGEL Setup
- **Mute sound:**
 - Mute
 - Do not mute
- **Master volume:** Adjust the master volume by moving the volume control or entering a number between 0 and 100.
- **Enable display port audio device:**
 - Switch on
 - Do not switch on

Windows services

Here, you can launch or disable Windows services.

- **Use IGEL Setup for configuring Windows service settings:**

- Use IGEL Setup
- Do not use IGEL Setup

- **Start remote desktop support service:**

- Start
- Do not start

If the service is started: **Deny TS connections:**

- Deny
- Do not deny

- **Start VMware Horizon client USB redirection service:**

- Start
- Do not start

User Interface

Menu path: **Setup > User Interface**

- [Display](#) (see page 95)
- [Language](#) (see page 96)
- [Input](#) (see page 97)
- [Desktop and Start Menu](#) (see page 98)

Display

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

In this area, you can change the display settings.

- **Use IGEL Setup for configuring display settings**
 - The *IGEL* setup will change the screen settings.
 - The *Windows* control panel or software from a third-party provider will change the screen settings.
- **Color Depth**
 - **65535 Colors**
 - **True Color:** 16.7 million colors
- **Number of screens:** You can use up to two screens.
- **Selected screen:** Specifies which screen serves as the main screen.
- **Resolution:** Specifies the screen resolution.
 - **Autodetect:** The screen resolution will be detected automatically.
 - **800x600** etc.: The screen resolution is specified manually.
- **Frequency:** Specifies the refresh rate.
- **Screen rotation:** Specifies whether and how the second screen is to be rotated.
 - **Rotate right:** The screen will rotate 90° to the right.
 - **Rotate left:** The screen will rotate 90° to the left.
 - **None:** The screen will not rotate.
- **Use blanking screensaver**
 - The screen saver will start after the time specified under **Inactivity timeout for the screen saver**.
 - The screen saver will not be used.
- **On resume, password protect**
 - When the screen saver is running, the user must enter their password in order to close the screen saver and make the desktop visible again.
 - The user can close the screen saver without entering a password.
- **Inactivity timeout for the blanking of screen saver:** If, during the time period in minutes specified here, no user action is performed, the screen saver will start and the computer will be put on standby.



Language

Select **Setup Language** and **Keyboard Layout** and configure **Standards** and formats as well as **Location**.

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.

 The settings in the IGEL Setup override the Windows system settings.

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].
- **Enable Aero Glass:** Enables *Aero Glass* effects (transparent windows, thumbnails)
- **Sort Start Menu Item Alphabetically:** This allows you to arrange all entries in the start menu in alphabetical order.

Network

Menu path: **Setup > Network**

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

-
- [LAN and Wireless](#) (see page 100)
 - [Routing](#) (see page 101)
 - [Network Drives](#) (see page 102)


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.

 If you want to change the computer name of a thin client which is a member of an AD (Active Directory) domain, refer to the article [Renaming the Thin Client Results in a Reboot Loop](#).

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.

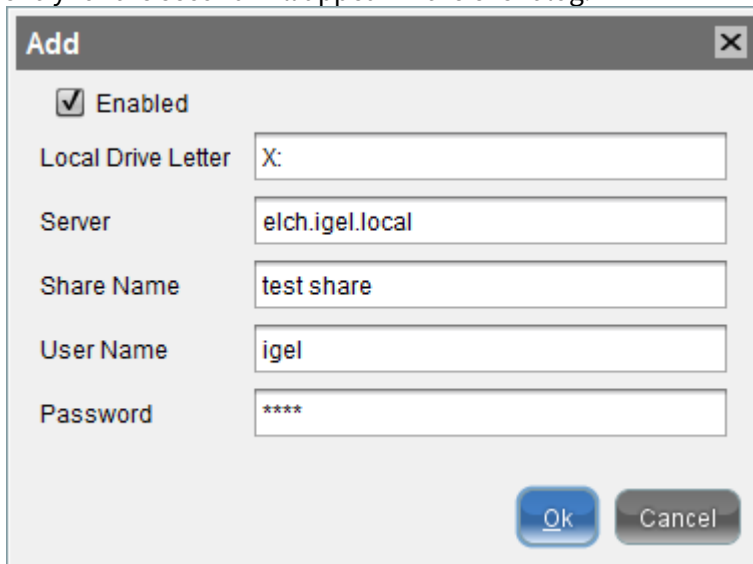
Network Drives

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.



Add [X]

Enabled

Local Drive Letter: X:

Server: elch.igel.local

Share Name: test share

User Name: igel

Password: ****

[Ok] [Cancel]

Devices

Menu path: **Setup > Devices**

Configure printer or other connected devices.

-
- [Printer](#) (see page 104)



Printer

Configure local printers here.

Security

Menu path: **Setup > Security**


After the initial configuration define an administrator password to avoid unauthorized access to the thin client setup.


-
- [Password](#) (see page 106)
 - [Active Directory](#) (see page 107)
 - [Network](#) (see page 108)
 - [Windows Firewall](#) (see page 109)

Password

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

Here, you can restrict access to various areas of the thin client with a password.

 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.

 Changes to passwords are only saved if you click on the **OK** or **Apply** button.

- **Use IGEL Setup for auto-logon settings:**
 - The settings for automatic logon are specified in the setup (default).
- **Administrator: Use password:**
 - Logging on as an administrator is only possible with a password.

To set or change a password, click on **Change password** and enter the desired password twice.

- **Setup user: Enable user access:**
 - With this password, the user is given access to selected areas of the setup.
Under [Accessories > Setup Session > Page Authorizations](#) (see page 90), enable those areas to which the user is to have access.
- **User name: Use password**
 - You specify a password for the user.
- **Rescue shell user: Use password**
 - You specify a password for the rescue shell.
 - The rescue shell can be launched with the administrator password.
- **Auto Logon:** Specify a user who is automatically logged on when the system starts. Auto Logon of the user `user` is preset by default.
 - **Username:** Name of the user
 - **Password:** Password of the user
 - **Domain:** Only needed for an Active Directory user
 - **Enable auto logon:**
 - When the system boots (and the Shift key is not pressed), the user will automatically be logged on.
 - **Forces auto logon:**
 - When the user logs off (and the Shift key is not pressed), they will automatically be logged on again.



Active Directory

Configure access to your Active Directory domain here. Enter the domain and user information required for access.



Network


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

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

Windows Firewall

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

Here, you can manage the rules for the Windows Firewall. This local firewall is enabled by default and has preconfigured rules which allow the use of remote desktop clients and the management of the thin client via the UMS.

 Do not remove any of the preconfigured rules! Otherwise, certain network services such as logging on to Active Directory, VNC and management of the thin client via UMS will not work.

- **Use IGEL setup for configuring Windows firewall settings:**

- The setup manages the firewall settings (default).

- **Deactivate Windows Firewall:**

- The firewall is switched off.

 It is recommended that you leave the firewall switched on at all times!

- **Allow ICMP ping requests:**

- Allow ping requests to be sent to the thin client.


- **Do not allow firewall exceptions:**

- No exceptions for blocked programs can be added.

List of Program Rules:

These rules allow local programs to establish network connections.

You can edit the list of rules using the following icons:

 hinzufügen

 entfernen

 ändern

 kopieren

In the editing window for a **program rule**:

- **Enable firewall rule:**

- The rule will be used.

- **Rule name:** A descriptive, recognizable name

- **Path to executable:** The complete path to the executable file beginning with the drive letter and including the file name and extension. `%windir%` can be used as a placeholder for the Windows directory.

- **Scope:**

- **Any:** The rule applies to any connections.

- **Local:** The rule applies to connections within the local subnet.
- **Custom.** Define the area in **Custom Scope**.
- **Custom scope:** Enter IP addresses or subnets, e.g.:
 - 192.168.0.12
 - 192.168.1.0/24
 - 2002:9d3b:1a31:4:208:74ff.fe39:6c43
 - 2002:9d3b:1a31:4:208:74ff.fe39:0/112

List of Port Rules:

These rules allow network communication via the ports entered.

In the editing window for a **port rule**:

- **Enable firewall rule:**
 - The rule will be used.
- **Rule name:** A descriptive, recognizable name
- **Port:** The number of the local network port used
- **Protocol:** TCP or UDP
- **Scope:**
 - **Any:** The rule applies to any connections.
 - **Local:** The rule applies to connections within the local subnet.
 - **Custom.** Define the area in **Custom Scope**.
- **Custom scope:** Enter IP addresses or subnets, e.g.:
 - 192.168.0.12
 - 192.168.1.0/24
 - 2002:9d3b:1a31:4:208:74ff.fe39:6c43
 - 2002:9d3b:1a31:4:208:74ff.fe39:0/112

System

Menu path: **Setup > System**

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

- [Date and Time](#) (see page 112)
- [Update](#) (see page 113)
- [Remote Management](#) (see page 118)
- [Shadowing](#) (see page 119)
- [Energy Options](#) (see page 121)
- [Write Filter](#) (see page 122)
- [Firmware Customization](#) (see page 126)
- [Registry](#) (see page 127)

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.

Update

Add new features or language packs to the Windows system by using Partial Updates.

-
- [Partial Update](#) (see page 114)
 - [Available Options](#) (see page 117)

Partial Update

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

- **Enable partial update**

- The service `upd-service` is launched. Partial updates can be carried out.
- The service `upd-service` is stopped. Partial updates cannot be carried out.

- **Enable auto-update on boot**


- The partial update will be installed automatically the next time that the thin client reboots.

 The automatic update when booting function should only be enabled if it is needed.


- **Protocol:** Protocol with which the partial update is downloaded from a server or obtained from a local directory

Possible values:

- **HTTP**

 In order to provide the partial update, the server must be configured so that it accepts requests regardless of the MIME type.

- **HTTPS**

 In order to provide the partial update, the server must be configured so that it accepts requests regardless of the MIME type.

- **FTP**

- **FILE:** The partial update will be obtained from a local storage device, e.g. from a USB storage device.


- **Host:** Host name or IP address of the server from which the partial update will be downloaded
- **Port:** Port of the server from which the partial update will be downloaded
- **Path:** Directory path on the server from which the partial update will be downloaded
- **Username:** User name for the server from which the partial update will be downloaded
- **Password:** Password for the server from which the partial update will be downloaded
- **Check for updates:** The thin client searches in the selected source for available updates.
- **Show installed packages:** The partial updates already installed are shown.

To install a partial update, proceed as follows:

1. Enable the option **Enable partial update**.
2. Select the **protocol**.
3. Under **Host** and **Path**, specify the source for the partial update.

4. Click on **Apply** to save the settings.
5. Click on **Check for updates** to search the source for updates.

When the download is complete, the system will reboot. The partial update will be available after the reboot.

 From Version 3.12.100, the thin client notifies the *UMS* about installed partial updates; this information is supported from *UMS* Version 5.3.100.

-
- [Installing Partial Updates \(see page 116\)](#)

Installing Partial Updates

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

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.

Available Options

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

- **Enable auto-update on boot:** 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.

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 How-To.

Shadowing

Menu path: **Setup > System > Shadowing**

For helpdesk purposes, you can observe the client through shadowing. This is possible via the *IGEL UMS* or another VNC client (e.g. *TightVNC*).

 The user can terminate the VNC connection at any time by clicking on the **End shadowing** button.

- **Allow Remote Shadowing:**

- Makes desktop contents viewable from remote computers via VNC

You can change the following settings:

- **Enable IGEL secure VNC mode:**

- Communication will be secured via SSL/TLS and shadowing will only be possible for *UMS* administrators.


Further information regarding secure shadowing can be found in the Secure Shadowing (VNC with TLS/SSL) How-To.

- **Use password:**

- The remote user must enter a password before they can begin shadowing.

- **Prompt user to allow remote session:**

- The user is asked for permission before shadowing.

 In a number of countries, unannounced shadowing is prohibited by law. Do not disable this option if you are in one of these countries!

- **Allow input from remote:**

- The remote user may make keyboard and mouse entries as if they were the local user.

- **Maintenance screen: Show Image to hide Desktop (Windows):**

- An image hides what is happening on the desktop during the VNC session


- **Path to image file:** Local file path, for example `F:\verzeichnis\bild.png`

You can transfer the required image file to a thin client using the UMS

- **Drawing mode for the overlay image:** Determines how the image is adapted to the screen size:
 - original
 - ignore aspect ratio
 - keep aspect ratio
 - keep aspect ratio by expanding

- **Scale image window (Linux):**

- The screen content of the shadowed client is reduced or enlarged by a factor before being transferred.

 Further parameters for the VNC server on the client are accessible in the *IGEL* registry (**Setup > System > Registry > network.vncserver**).

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.

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

- **Turn off monitor:** Specify how long the system must be inactive until the monitor is shut down.
- **System Standby:** Specify how long the system must be inactive until it switches to standby mode.
- **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.

Write Filter

You can activate or deactivate the write filter. Depending on the Windows version in use, one of the following write filters can be used:

- Windows 7: [File-based write filter \(FBWF\)](#) (see page 123)
- Windows 10: [Unified write filter \(UWF\)](#) (see page 124)

File Based Write Filter (Windows Embedded Standard 7)



Menu path: **Setup > System > 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, for example 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.


FBWF status display in the taskbar

-  Red symbol: FBWF disabled
-  Green symbol: FBWF enabled (default setting)

Settings in the IGEL setup

- **Toggle FBWF**
 - The write filter is enabled and protects the system against changes.
 - The write filter is disabled.
- **Enable the compression of the overlay**
 - The write filter's cache will be compressed in order to save storage space.
 - The write filter's cache will not be compressed.
- **Threshold for FBWF:** Figure in MB, max. 1024 MB, the default setting is 64 MB
- **Excluded directory:** The directories in this list are writable, even if the write filter is enabled. This is suitable for configuration files or the signatures of a virus scanner for example.

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

 The FBWF must be enabled during regular system operation! Disable the write filter only temporarily, for example 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.

Unified Write Filter (UWF)

Menu path: **Setup > System > Unified Write Filter**

The Unified Write Filter (UWF) is the write filter in Windows 10 IoT. The UWF intercepts all I/O write attempts and forwards them to the overlay buffer. The overlay buffer is an area in the RAM. Thus, the programs running on the device do not access the flash memory of the device. In this way, the operating system is protected from changes. All changes are discarded when the system is rebooted.

The behavior of the UWF with regard to the overlay buffer can be configured in IGEL Setup.

You can find further information on the Unified Write Filter on [this page at the Microsoft Developer Network](#)⁹.

UWF status display in the taskbar

- UWF enabled: Locked padlock symbol.




- UWF disabled: Unlocked padlock symbol.




Settings in IGEL Setup

- **Use IGEL Setup for UWF settings**
 - UWF settings are configured in IGEL Setup. (Default)
 - UWF settings are configured in another manner.
- **Enable UWF**
 - The write filter is enabled. (Default)
 - The write filter is disabled.


 The Unified Write Filter must be enabled during regular system operation. IGEL does not provide support services if the write filter is disabled.





- **Warning threshold for UWF:** A warning is issued when the buffer exceeds this size (in MB). The user is prompted to save his data, close all programs, and restart the device. (Default: 512)
- **Critical threshold for UWF:** Normal operation is no longer possible when the buffer exceeds this size (in MB). A dialog is displayed; the user is prompted to save his data immediately. When the dialog is closed, the device is restarted. (Default: 900)
- **Maximum Overlay size for UWF:** Maximum size for the temporary buffer for saving writes. (Default: 1024)
The actual size of the overlay buffer changes during runtime according to the memory requirements of the data to be written. The remaining physical RAM space is available to the system as regular RAM.

⁹ <https://msdn.microsoft.com/en-us/windows/hardware/commercialize/customize/enterprise/unified-write-filter>


 Avoid very high values for the maximum size of the overlay buffer. With increasing maximum size, the probability of a conflict between overlay buffer and regular RAM demand rises. The behavior in case of conflict depends on the firmware version in use. IGEL WES 4.01.100 or older: There is no guarantee that the maximum overlay size is available at any time. Thus, it can happen that regular RAM usage and overlay buffer together require more physical RAM than is available. In this case, system failure will occur. IGEL WES 4.02.100 or newer: The RAM usage is monitored periodically. As soon as the margin between the currently required regular RAM space and the maximum overlay size has decreased to a threshold (default: 250 MB), a message is issued. The user is prompted to restart the device as soon as possible.


- **List of directory excludes:** Insert directories that you want to exclude from the Write Filter here, in order to allow writing to these. Use the complete path, including the drive letter.

 Please note that also write accesses to memory locations increase the Write Filter's RAM demand. This is a property of the Windows Write Filter and therefore systemic.

- ▶ To create an entry, click .
- ▶ To remove an entry, click .
- ▶ To edit an entry, click .
- ▶ To copy an entry, click .

- **List of registry excludes:** Insert here registry keys that you want to exclude from the write filter, in order to allow writing to these. Use the full key path.

 Please note that also write accesses to memory locations increase the Write Filter's RAM demand. This is a property of the Windows Write Filter and therefore systemic.

 Directory and registry excludes defined by IGEL and needed for system operation are not shown and cannot be edited.

Firmware Customization

The list of **Features** allows you to activate or deactivate features such as session types.

After deactivating a feature the corresponding session type will no longer be available after a reboot. Existing sessions of this type will no longer be displayed, but are not deleted.

Possible features:

- Enable Citrix ICA Client
- Enable Citrix Online plug-in
- Enable Microsoft Internet Explorer
- Enable Microsoft Media Player
- Enable Microsoft RDP
- Enable rotation support
- Enable VMWare Horizon Client

You can also register a **Custom Application** here by specifying the path of the executable and its parameters.

Registry

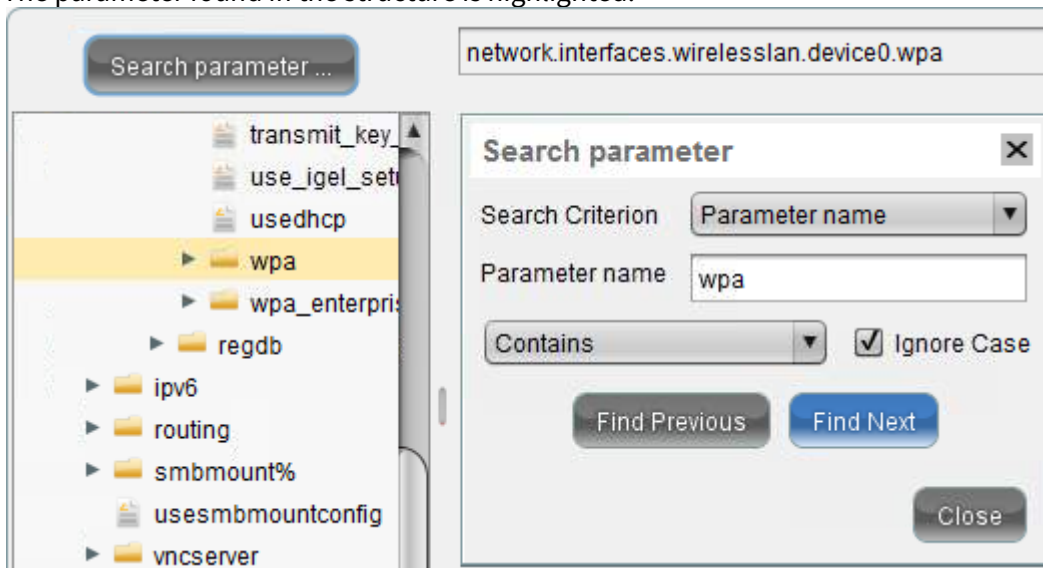
Menu path: **Setup > System > Registry**

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`, for instance, if you require WPA encryption settings for securing your WLAN.
3. Click **Find next**.

The parameter found in the structure is highlighted:





UMA How-Tos

- [Deploying UMA with Group Policies \(see page 129\)](#)

Deploying UMA with Group Policies

This document describes how to install IGEL Unified Management Agent (UMA) on a group of computers automatically via Group Policies.

Prerequisites

- Windows Server 2008 or 2012R2
- IGEL Unified Management Agent (UMA) *.msi package (can be downloaded from the [IGEL Download Server](#)¹⁰)

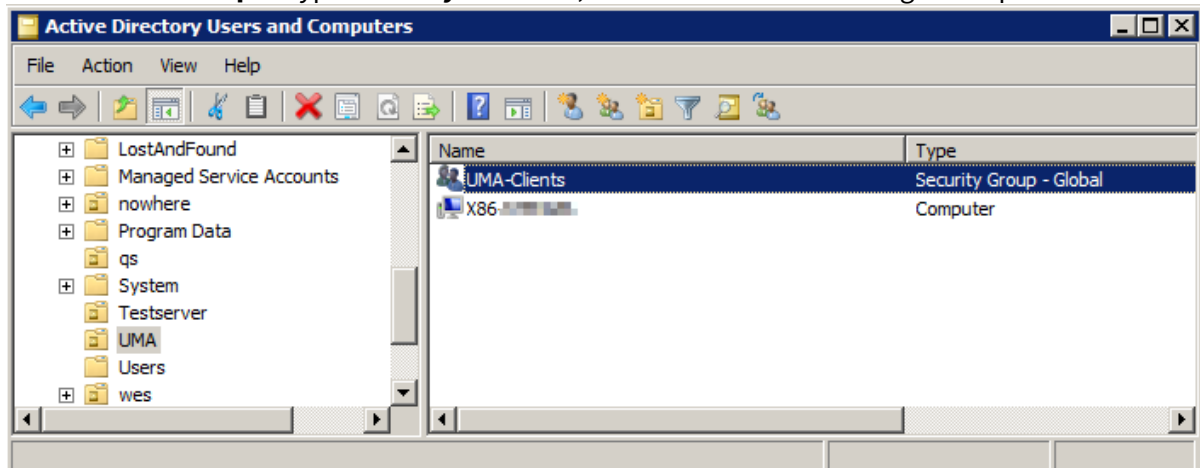
-
- [Creating a Security Group](#) (see page 130)
 - [Creating a Group Policy](#) (see page 132)

¹⁰ <https://www.igel.com/software-downloads/enterprise-management-pack/>

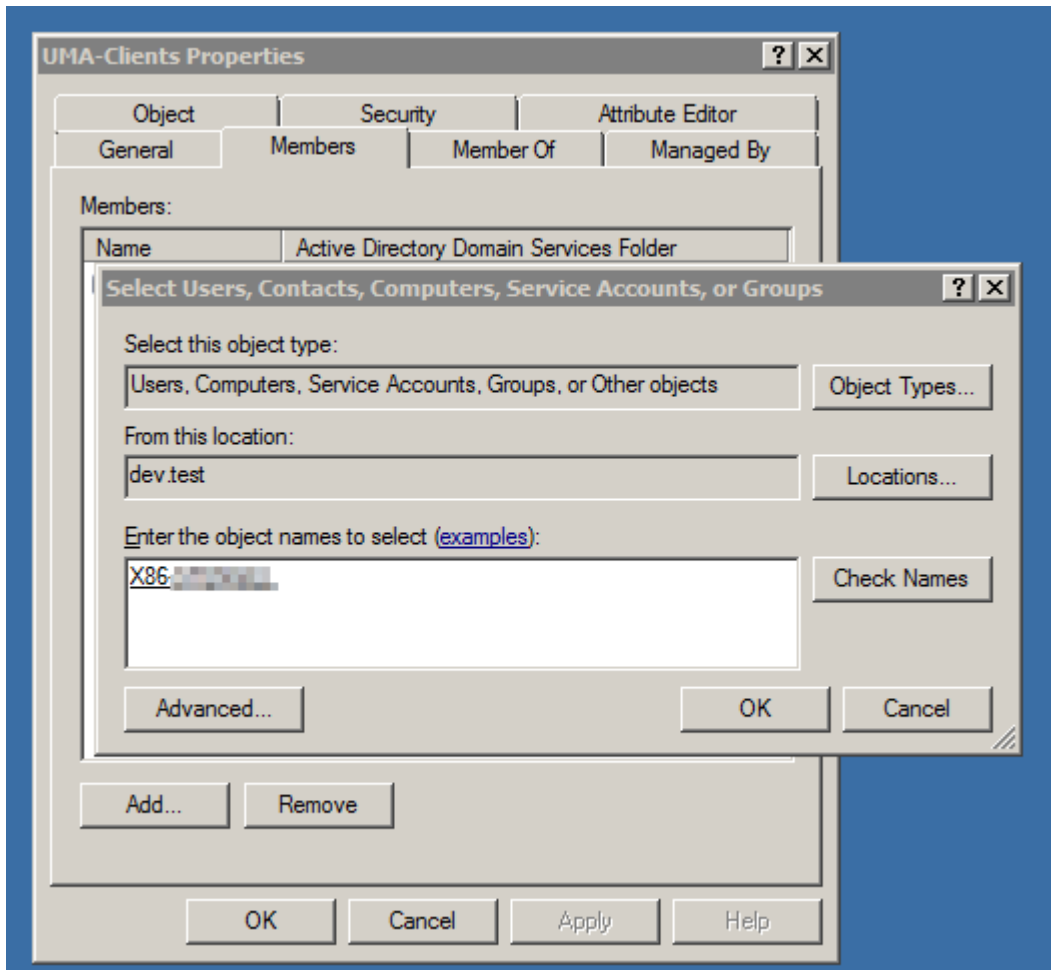
Creating a Security Group

On *Windows Server*:

1. Open **Start Menu > Administrative Tools > Active Directory Users and Computers**.
2. Create a **New Organizational Unit (OU)** in your domain.
3. Create a **New Group** of type **Security** in the OU, which will contain the target computers.



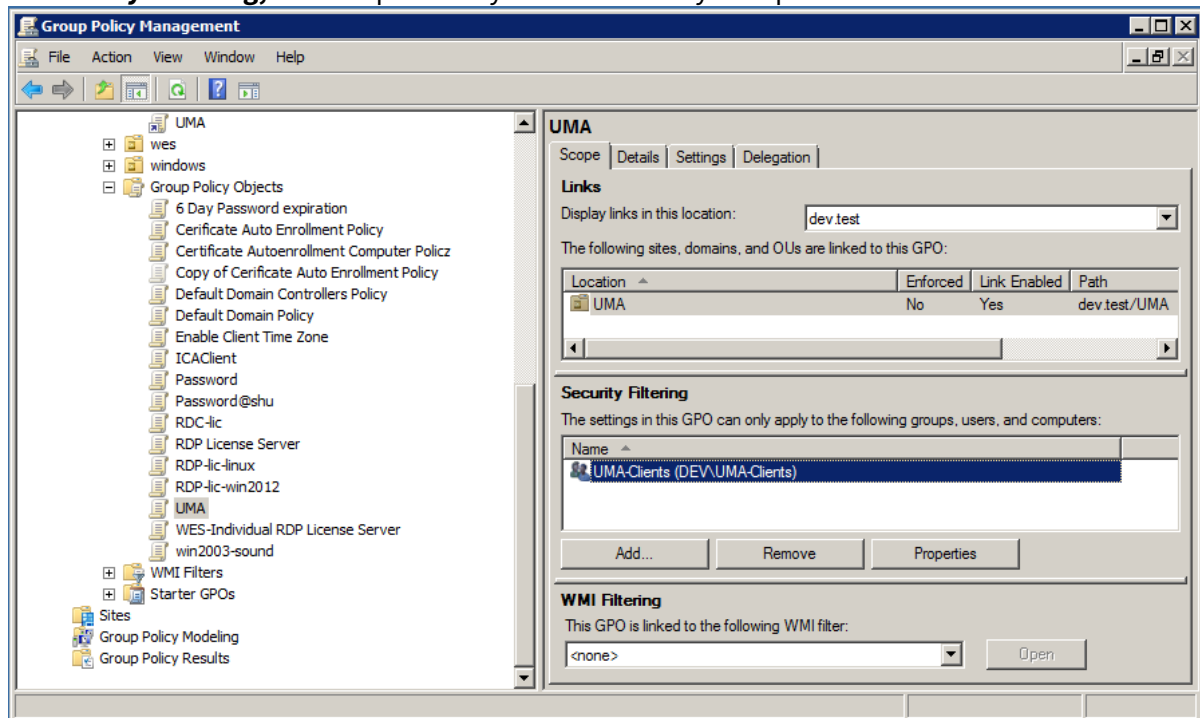
4. Right-click the newly created group and select **Properties**.
5. In the **Members** tab, add the target computers to the group.



Creating a Group Policy

On *Windows Server*:

1. Open **Start Menu > Administrative Tools > Group Policy Management**.
2. In **Group Policy Objects**, create a **New Group Policy Object (GPO)**.
3. Select the newly created GPO.
4. In **Security Filtering**, **Add** the previously created Security Group to the GPO.



5. Create a **New Organizational Unit (OU)** in your domain.
6. Right-click on the newly created OU and select **Link an Existing GPO...**
7. Select the GPO from the list.
8. Right-click on the newly created GPO link and select **Edit...**
9. Go to **Computer configuration > Policies > Software Settings > Software Installation**
10. Create a **New Package** and select the `*.msi` installer package for *UMA*.

i These changes will be applied (and the installation started) when the new policies have arrived on the clients and these have been rebooted. In order to trigger the update manually, run `gpupdate /force` at the clients' *Windows* command prompt.



UMA Troubleshooting

- [UMA Is Unable to Download License from UMS \(see page 134\)](#)
- [Configuring UMA DNS Autoregistration Queries \(see page 135\)](#)

UMA Is Unable to Download License from UMS

Symptom

Unified Management Agent (UMA) is unable to download subscription license from Universal Management Suite (UMS).

Problem

UMA tries to contact UMS via its network name, not IP address.

Solution

The UMS host needs to have an entry in the DNS server used by UMA.

Configuring UMA DNS Autoregistration Queries

Symptom

Booting device with the IGEL Universal Management Agent (UMA) takes too long.

Problem

The device queries DNS for the name `igelrserver`. The default is 15 queries, with a timeout of 1 second each. This can add 15 seconds to boot time if the name cannot be resolved.

Solution

1. In Setup, go to **System > Registry**.
2. Go to `system.remotemanager.dnsqueries`.
3. Set **Number of DNS queries** for `igelrserver` to a lower integer value.