Windows 10 IoT

Compatibility with Partner Solutions

COM-Imprivata (W10IoT)

The following IGEL devices officially support Imprivata OneSign Embedded:

IGEL Thin Clients

IGEL Device	IGEL Firmware	Imprivata Ready	Citrix Receiver Support	VMware Horizon Support
UD5 W10	any (1)	✓	✓	✓
UD6 W10	any (1)	✓	✓	✓

(1) Imprivata client needs to be installed by the customer

W10 IoT Manual

What is new in 4.02.100?

- During initial commissioning, the EULA must be accepted; see Quick Installation (see page 7).
- The RAM usage of the Unified Write Filter (UWF) is monitored periodically in order to avoid conflicts between the overlay buffer and the regular RAM usage; see Unified Write Filter (see page 152).
- Windows Defender can now be configured via IGEL Setup; see Windows Defender (see page 137).

Quick Installation

Perform the steps below to install the end device in your network environment in just a few minutes:

1. Connect the end device to a VGA, DVI or DisplayPort monitor, an AT-compatible keyboard with a PS/2 or USB connection, a USB mouse and the LAN using an RJ45 connector.
2. Connect the end device to the power supply.
3. Switch on the end device, and wait until the graphic desktop is launched.
4. Log in either as a
   - **User** with the preset password `user` or
   - **Admin** with the preset password `admin.`
5. If the EULA is displayed, read and accept it. This step is part of the initial startup since IGEL *Windows 10 IoT 4.20.100*.

   > The EULA is displayed when the device has not been started yet and has not been registered with the UMS.

6. Change the administrator password.

   > Find information such as the product version, IP address or MAC address in IGEL Device Information (see page 11).

Windows Activation

IGEL thin clients with Windows 10 IoT receive a Microsoft Digital License and are initially activated at the IGEL warehouse.

When a snapshot is created, the system image is generalized and the activation is canceled. On installing a snapshot, the system is activated by connecting to a Microsoft online service if Internet access is available. However, running the thin client in an environment without Internet access is also possible.

If the thin client is never connected to the Internet, it remains in the state "deferred activation", and the thin client can be operated without any restrictions. If activation fails, the thin client goes into the state "not activated"; in this case, a watermark may be displayed.

To determine the current state of the Windows activation:

▶ Right-click the Windows start menu and select **System**.

In the base information, under **Windows activation**, you find the currect state of the Windows activation.
The following states are possible:

- Windows is activated. Message: "Windows is activated."
- Deferred activation. Message: "Connect to the Internet to activate Windows."
- Not activated. Message: "Windows is not activated."

Boot Options

To select your desired boot options, proceed as follows:

1. Wait until the message `Booting, please wait` appears during the boot process.
2. Press the [Esc] key.
   A selection menu opens.
3. Select one of the three boot options:
   - **Windows Boot Manager:** The system boots normally.
   - **Start IGEL Rescue Shell:** In this case, you access the underlying *Linux* system, e.g. in order to restore the system or reset the *IGEL* setup data.
   - **Download Snapshot:** The firmware download menu is shown. In order to download a snapshot file from your server or a connected USB stick, you will need to provide the necessary connection details.

- Reset to Factory Defaults (see page 10)

Reset to Factory Defaults

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

First, you have to enable your Secure Shell, see Boot Options (see page 9).

Press the option **Reset to factory defaults**.

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

Do you know the password?

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

Do you not know the password?

1. Confirm the warning message.
2. When you are prompted to enter the password, press the Enter key three times.
3. Press [c].
   The Terminal Key will appear.
4. Contact us using license@igel.com[1].[2]
5. Enter the Terminal Key shown, the firmware version, and your contact details.
   IGEL will send you a so-called Reset to Factory Defaults Key specially for your device. To ensure that the process is as straightforward and yet as secure as possible, each key is valid for just one device.

You can also reset your device to factory defaults in the UMS Console under **Devices > Other commands > Reset to Factory Defaults**, see Devices.

1 mailto:license@igel.com
2 https://support.igel.com/overview.html

IGEL Device Information

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

Double-click the info icon in the Windows taskbar in order to bring up the device information.

The IGEL Device Information window opens. You can open the following sections with a single click:

- **About**: Product name, total uptime, last boot time
- **Network info**: Terminal name, IP address, MAC address, default gateway, DNS servers
- **Hardware**: CPU version and speed, RAM, disk capacity, chipset driver, IGEL device name
- **Licensed Features**: A list of features such as RDP, Citrix Program Neighborhood, VMware View or Adobe Reader
- **Updates**: Hotfixes and partial updates.

IGEL Setup

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

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

Using Microsoft system management

A separate set of documentation for *Windows* system management is available from Microsoft[3]. We do not recommend that you configure the thin client via *Windows* system management because the settings cannot be saved in a profile and will not be retained during an update with a snapshot.

With the local IGEL Setup

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

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

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

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

To end the setup, proceed as follows:

1. Click on **Apply** to save the changes you have made.
2. Click on **OK** to save your changes and close the application.
3. Click on **Cancel** to close the application without saving your changes.

- Setup Areas (see page 13)
- Searching Setup Pages (see page 14)

3 https://docs.microsoft.com/en-us/windows/client-management/administrative-tools-in-windows-10

Setup Areas

The setup application comprises the following main areas:

- Sessions (see page 15) - In this area, you can create and configure application sessions such as ICA, RDP, terminal emulation, browser and others.
- Accessories (see page 87) - The *IGEL S*etup application can be restricted for users (but not for 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 115) - In this area, you can configure all the network settings for LAN / WLAN interfaces. Network drives are also configured here.
- Devices (see page 126) - 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 131) - 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 with the *IGEL S*etup.
- System (see page 139) - A number of basic parameters such as time synchronization, firmware update information, write filter configuration (*Unified Write Filter, UWF*) 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

Menu path: **Setup > Sessions**

The session types which are available for configuration depend on the license for your *IGEL* thin client. An overview of the functions included with each license level can be found in the product list on the IGEL[4]website[5].

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

To add a new session, proceed as follows:

▶ Click on **Add**.

or

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

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

How to work with sessions:

▶

To create a session, click

1 Add

.

▶ To remove a session, click  .

▶ To change a session, click  .

▶ To copy a session, click  .

_____

4 http://www.igel.com
5 http://www.igel.com

Sessions Summary

Menu path: **Setup > Sessions > Sessions Summary**

This area gives you an overview of all available sessions.

- **Add**: Add a session from the selection of available session types.
- **Filter**: Filter sessions shown in the list according to the string of characters entered.

Citrix

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

- **Use IGEL Setup for configuring Citrix settings**
  - ☑ The IGEL Setup changes the Citrix settings.
  - ☐ The Citrix sessions are changes elsewhere.
- **Installation root path for Citrix client**: Enter the path to the directory in which the Citrix client is installed (default: `C:\Program Files (x86)\Citrix\ICA Client`).
- **Installation root path for Citrix Selfservice Plug-In**: Enter the path to the directory in which the Citrix Selfservice Plug-In is installed. (default: `C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin`).
- **Use IGEL Setup for configuring Citrix settings**
  - ☑ The IGEL Setup will change the Citrix settings.
  - ☐ The Citrix settings will be changed in another way.
- **Installaton 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`.
- **Installaton 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 18)
- ICA Sessions (see page 25)
- Self-Service Plugin (see page 34)

ICA Global

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

The global settings define default parameters that 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

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 call up a list of all *Citrix* servers and all published applications that are accessible over 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 in this case.

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: 640)
- **Default vertical resolution**: Specifies the window height in pixels. (default: 480)

Firewall

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

Here you can configure ICA connections that run through 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 19).
  ☐ The Citrix server has no alternate IP address.
  You will find more information on server configuration by searching 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 (default: 443)

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. (default: 1024)

> 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. (Default: 1024)
- **Persistent Cache Path**: Specify the directory where the files are to be stored locally. (default: `C:\Program Files (x86)\Citrix\ICA Client\Cache`)
- **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.
  - ☐ You cannot 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**.

To work with rules, proceed as follows:
▶

To create a rule, click

2 Add

.

▶ To remove a rule, click  .

▶ To change a rule, click  .

▶ To copy a rule, click  .

HDX

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

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

  Redirecting Flash content can improve playback.
- **File access**: Specify what access to local client files is allowed.
  - No access
  - Read-only access
  - Full access
  - Prompt user for access
- **Microphone and webcam access**: Specify what access to local microphones and webcams is allowed.
  - No access
  - Read-only access
  - Full access
  - Prompt user for access
- **PDA access**: Specify what access to personal digital assistants (PDAs) is allowed.
  - No access
  - Read-only access
  - Full access
  - Prompt user for access
- **USB and other devices access**: Specify what access to USB devices, scanners, digital cameras and the like is allowed.
  - No access
  - Read-only access
  - Full access
  - Prompt user for access

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.

How to work with sessions:

▶

To create a session, click

3 Add

.

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

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

_____

Server

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

- **Browser Protocol**: The protocol that is to be used when searching for servers and published applications.
  - Default
  - TCP/IP + HTTP
  - SSL + HTTPS
- **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 18). 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 through 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 by searching 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 P**roxy Server** and the **Proxy port**, unless you have selected **None**.
- **Secure Gateway (relay mode):** Enter the **SSL Proxy Server** and **SSL Proxy Port** (default: 443).

Reconnect

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 during 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 through 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 has first been enabled and configured on the *Citrix* server.

- **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**: Name of the session.

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

Session start options

- **Start menu**
  ☑ The session can be started with the start menu.
- **Desktop**
  ☑ The session can be started with a program starter on the desktop.
- **Autostart**
  ☑ The session will be launched automatically when the thin client boots.

Self-Service Plugin

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

The Self-Service Plugin lets the user find and launch published applications and desktops..

- **Login Session Name**: Enter the name to be displayed for the session..
- **Put shortcuts in Start menu**
  - ☑ Shortcuts are created on the Start menu.
  - ☐ No Shortcuts are created on the Start menu.
- **Put shortcuts on Desktop**
  - ☑ Shortcuts are created on the Desktop.
  - ☐ No Shortcuts are created on the Desktop.
- **Autostart**
  - ☑ The session is started automatically after logging in to the device..
  - ☐ The session is not started automatically.

_____

- Server (see page 35)
- Logon (see page 36)
- Appearance (see page 37)
- Desktop Integration (see page 38)

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 configure sessions for various Citrix XenApp/XenDesktop versions.

▶

To add a connection click

4 Add

.

▶ To remove a connection click  .

▶ To edit a connection click  .

▶ To copy a connection click  .

Citrix XenApp 6.x oder older

- **URL Prefix**:
  - http://
  - https://
- **Citrix Server**: DNS name or IP address of the server, plus TCP port (default: 80)
- **Path to config.xml file**: Relative path to configuration file (default: CitrixPNAgent/config.xml)
- **Store Name**: Name of the Citrix Store

Citrix XenApp/XenDesktop 7.x Store

- **URL Prefix for Citrix-Store**:
  - http://
  - https://
- **Citrix Store Address**: DNS name or IP address of the server, plus TCP port (default: 443)
- **Path toStore**: Path to the Citrix Store (default: Citrix/Store/discovery)
- **Store Name**: Name of the Citrix Store

Citrix XenApp/XenDesktop 7.x Legacy Mode

- **URL Prefix for Citrix-Store (legacy)**:
  - http://
  - https://
- **Citrix Store Address (legacy)**: DNS name or IP address of the server, plus TCP port (default: 443)
- **Path to Store**: Path to the Citrix Store (default: Citrix/Store/PNAgent/config.xml)
- **Store Name**: Name of the Citrix Store

Logon

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

- **Allow user to save password**:
  Possible values:
  - Do not allow the user to save a password
  - Allow the user to save a password for https stores only
  - Allow the user to save a password for http and https stores
- **Allow user to add stores**:
  Possible values:
  - Do not allow the user to add stores
  - Allow the user to add https stores only
  - Allow the 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 that contains the applications in the start menu.
- **Additional sub-menu on desktop**: Here you can specify a directory that 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 using the *Citrix Receiver* context menu in the system tray.
  ☐ The user cannot edit accounts using the Citrix Receiver context menu in the system tray.

Desktop Integration

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

- **Session name**: Name of the session.

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

Session start options

- **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.
- **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 be launched automatically when the thin client boots.
  - ☐ The session will not start automatically.

RDP

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

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

You can find detailed information regarding *Microsoft RDP* on the website `http://technet.microsoft.com`[6] .

- **Use IGEL Setup for configuring Microsoft RDP settings**
  - ☑ Configure RDP using the *IGEL* Setup.
  - ☐ Do not use setup.

_____

- RDP (Global Settings) (see page 40)
- RDP Sessions (see page 48)

6 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 41)
- Window (see page 42)
- Keyboard (see page 43)
- Mapping (see page 44)
- Performance (see page 45)
- Options (see page 46)
- USB Redirection (see page 47)

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.
  - ☐ The desktop will not be spanned. (default)
- **True multimonitor support**:
  - ☑ The user can connect to multimonitor configurations. (default)
  - ☐ No true multimonitor support.
- **Window size**: Choose the size of the window.
  - Full screen
  - 800x600
  - 640x480
  - 800x600
  - 1024x768
  - 1280x720
  - 1280x1024
  - 1600x900
  - 1600x1050
  - 1600x1200
  - 1920x1080
  - 1920x1200
- **Display the connection bar:**
  - ☑ A symbol bar for minimizing and closing the full-screen session will be shown. (default)
  - ☐ A connection bar will not be shown.

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. (default)
  - ☐ Clipboard mapping is not enabled.
- **Override local window manager keyboard shortcuts**
  - ☑ All keys are sent to the Windows server, including keys that might otherwise be intercepted by the local window manager. (default)
  - ☐ Keyboard shortcuts will not be overwritten.
- **Redirect Ctrl-Alt-Delete to sessions**
  - ☑ This key combination will be forwarded to the session.
  - ☐ This key combination will be processed by the local thin client. (default)

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. (default)
  - ☐ The local microphone will not be passed.
- **Override local window manager keyboard shortcuts:**
  - ☑ The session hotkeys will override equivalent local ones. (default)
  - ☐ Do not override hotkeys.
- **Enable Printer Mapping**
  - ☑ Make the local printer available in the RDP session. (default)
  - ☐ Printer mapping is disabled.
- **Enable COM Port Mapping**
  - ☑ Make local COM ports available in the session. (default)
  - ☐ COM port mapping is disabled.
- **Enable Smartcard Mapping**
  - ☑ Redirect smartcards.
  - ☐ Do not redirect smartcards. (default)
- **Enable Clipboard Mapping**
  - ☑ Content can be shared between the local system and the session via the clipboard. (default)
  - ☐ Clipboard mapping is disabled.
- **Enable Drive Mapping**
  - ☑ Make drives available in the session. (default)
  - ☐ Drive mapping is disabled.
- **Drives**
  - ☑ Make all selected drives available in the session. (default)
  - ☐ Do not map all drives.
- **Drives that I connect to later**
  - ☑ Automatically map newly connected drives
  - ☐ Do not map new drives. (default)

Performance

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

- **Detect connection quality automatically**
  ☑ 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. (default)
  ☐ Videos will be played back on the server.
- **Redirect DirectX commands**:
  ☑ Graphics functions will be executed locally. (default)
  ☐ Graphics functions will be executed on the server.
- **Disable Bitmap cache**:
  ☑ Images will not be cached locally. (default)
  ☐ Images will be cached locally.
- **Compression**:
  ☑ Compression is enabled. (default)
  ☐ Compression is disabled.

  > ⓘ 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 consume 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.

RD Gateway Options

- Automatically detect RD Gateway server settings
- Do not use an RD Gateway 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).
    - Smartcard
  - **Bypass RD Gateway server for local addresses**
    - ☑ No gateway will be used for connections in the local network. (default)
    - ☐ RD Gateway will be used also for connections in the local network.
  - **Use my RD Gateway credentials for the remote computer**
    - ☑ Pass on logon information on the RD Gateway to the remote computer. (default)
    - ☐ RD gateway credentials are not passed on.

USB Redirection

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

Use this area to enable or disable USB redirection and for defining rules for USB devices.

Enable RemoteFX USB Redirection

☑ Enable the RemoteFX USB Redirection for all devices that are not using other redirection mechanisms and do not already have drivers installed. If a driver is installed for that device, use a redirection policy.

☐ RemoteFX USB Redirection is disabled.

Device Rules
Define rules for individual devices by entering the Instance ID of the device.

> You can find the **Instance ID of the device** as follows:
> 1. Right-click the Windows start icon.
> 2. Click **Device Manager**.
> 3. Go to **Details**.
> 4. Choose **Deviceinstancepath** as **Property.**

How to work with device rules:

▶

To create a rule, click

5 Add

.

- ▶ To remove a rule, click  .
- ▶ To change a rule, click  .

RDP Sessions

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

Configure one or more RDP sessions.

- **Session name**: Name of the session.

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

Session start options

- **Start menu**
  ☑ The session can be started with the start menu.
- **Desktop**
  ☑ The session can be started with a program starter on the desktop.
- **Autostart**
  ☑ The session will be launched automatically when the thin client boots.

Server

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

Choose between the following modes:

- Server
- Enable RemoteApps mode

Server

- **Server**: Enter the server or the IP address.

RemoteApps Mode

- **RemoteApp Server Port**: Network port on which the application is offered. (default: 3389)
- **Program to execute**: Enter the program as follows: `||mspaint`.
- **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
  - 8 bit
  - 16 bit
  - 24 bit
  - 32 bit
- **Span desktop**
  - ☑ The session will use all available monitors as the desktop.
  - ☐ The session will use only one monitor as the desktop. (default)
- **True Multimonitor Support**
  - ☑ You can connect to multi-monitor configurations. (default)
  - ☐ No true multi-monitor support
- **Display the Connection Bar**
  - ☑ A symbol bar for minimizing and closing a full-screen session will be shown. (default)
  - ☐ 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**
  - ☑ Compression is enabled.
  - ☐ Compression is disabled.

  ⓘ 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 consume CPU power.

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. (default)
  - ☐ The local microphone will not be passed.
- **Override local window manager keyboard shortcuts:**
  - ☑ The session hotkeys will override equivalent local ones. (default)
  - ☐ Do not override hotkeys.
- **Enable Printer Mapping**
  - ☑ Make local printer available in the RDP session. (default)
  - ☐ Printer mapping is disabled.
- **Enable COM Port Mapping**
  - ☑ Make local COM ports available in the session. (default)
  - ☐ COM port mapping is disabled.
- **Enable Smartcard Mapping**
  - ☑ Redirect smartcards.
  - ☐ Do not redirect smartcards. (default)
- **Enable Clipboard Mapping**
  - ☑ Content can be shared between the local system and the session via the clipboard. (default)
  - ☐ Clipboard mapping is disabled.
- **Enable Drive Mapping**
  - ☑ Make drives available in the session. (default)
  - ☐ Drive mapping is disabled.
- **Drives**
  - ☑ Make all selected drives available in the session. (default)
  - ☐ Do not map all drives.
- **Drives that I connect to later**
  - ☑ Automatically map newly connected drives
  - ☐ Do not map new drives. (default)

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.

RD Gateway Options

- Automatically detect RD Gateway server settings
- Do not use an RD Gateway 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).
    - Smartcard
  - **Bypass RD Gateway server for local addresses**
    - ☑ No gateway will be used for connections in the local network. (default)
    - ☐ RD Gateway will be used also for connections in the local network.
  - **Use my RD Gateway credentials for the remote computer**
    - ☑ Pass on logon information on the RD Gateway to the remote computer. (default)
    - ☐ RD gateway credentials are not passed on.

Desktop Integration

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

- **Session name**: Name of the session.

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

Session start options

- **Start menu**
  ☑ The session can be started with the start menu.
- **Desktop**
  ☑ The session can be started with a program starter on the desktop.
- **Autostart**
  ☑ The session will be launched automatically when the thin client boots.

Horizon Client

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

Here you can configure *Horizon Client* sessions.

- **Use IGEL Setup for configuring Horizon settings**
  - ☑ The Horizon settings are defined in the IGEL Setup.
  - ☐ The Horizon settings are not defined in the IGEL Setup.
- **Path to "vmware-view.exe"**: File path to the *Horizon* executable, for instance `C:\Program Files\VMware\VMware Horizon View Client\vmware-view.exe`
  You will find a detailed description of the client parameters in the original documentation for *Horizon* at http://www.vmware.com/support/pubs/view_pubs.html.
  For information about using a printer in Horizon sessions, see Printer (see page 128).

_____

- Horizon Client Global (see page 57)
- Horizon Client Sessions (see page 60)

Horizon Client Global

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

USB Redirection

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

Here you can activate or deactivate the USB redirection and define rules for USB devices.

- **Enable USB redirection**
  - on: The local computer's USB devices can be used in Horizon sessions.

    To use the USB redirection, the option **Start VMWare Horizon View Client USB redirection service** must be activated under **Accessories > Windows Services**.

  - off: USB devices can not be used in Horizon sessions.
- **Default rule**: Choose between **Deny** and **Allow** to set a rule for all devices to which no more specific rule applies.
- **Class rules**: Define rules by selecting a **class ID** and **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

6 Add

.

▶ To remove a rule, click  .

▶ To change a rule, click  .

Keyboard

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

Here you can change the behavior of the keyboard in Horizon sessions.

- **Redirect Ctrl-Alt-Del 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 local thin client; it will not be forwarded to the session.

Horizon Client Sessions

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

You can configure one or more Horizon Client sessions.

The settings for launching the session are described below.

- **Session name**: Name of the session.

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

Session start options

- **Start menu**
  ☑ The session can be started with the start menu.
- **Desktop**
  ☑ The session can be started with a program starter on the desktop.
- **Autostart**
  ☑ The session will be launched automatically when the thin client boots.

_____

- Connection Settings (see page 61)
- Window (see page 62)
- Mapping (see page 63)
- Desktop Integration (see page 64)

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.
  - ☐ The connection will not use TLS/SSL encryption.
- **User name**: User name 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.
- **Desktop name**: Defines a name for the desktop. This option is available if **Session type** is set to "Desktop".
- **Application name**: Defines a name for the application. This option is available if **Session type** is set to "Application".
- **Hide client after session launch**:
  - On: The client window is miminized after session launch.
  - Off: The client window is displayed in the default size.
- **Protocol**
  - Server default
  - VMWare Blast
  - RDP
  - PCoverIP
- **Log in as current user**
  - ☑ The current user name will be used in the Horizon session.
  - ☐ The current user name will not be used .
- **Kiosk mode**
  - On: The session is executed in the kiosk mode. Here the user does not have to log on; the user has only limited operating options.
  - Off: The session is not executed in the kiosk mode.
- **Single autoconnect**
  - On: Connect only to a single desktop or a single application.
  - Off: No single autoconnect
- **No VMware add-ins**
  - 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 available in the session when they are inserted.
  - ☐ USB devices will not be available when they are inserted. (default)
- **Connect USB on startup**
  - ☑ USB devices that have already been inserted will be connected when the session starts.
  - ☐ USB devices that have already been inserted will not be connected automatically. (default)

Desktop Integration

Menu path: **Setup > Horizon Client > Horizon Client Sitzungen > [Session Name] > Desktop integration**

- **Session name**: Name of the session.

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

Session start options

- **Start menu**
  ☑ The session can be started with the start menu.
- **Desktop**
  ☑ The session can be started with a program starter on the desktop.
- **Autostart**
  ☑ The session will be launched automatically when the thin client boots.

Browser Sessions

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

In this area, you can define basic settings for the browser (Internet Explorer)

- **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 of 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 settings is only valid for the LAN, not for 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 66)
- Security (see page 67)
- Advanced (see page 76)
- Start (see page 77)
- Window (see page 78)
- Proxy (see page 79)
- Toolbar Items (see page 80)
- Toolbars (see page 81)

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 > Browser Sessions > Security**

- **Allow SSL 2.0**
  - ☑ Connections encrypted with SSL 2.0 are allowed.

    ⓘ SSL 2.0 encryption is considered insecure; it is recommended not to allow connections encrypted with SS 2.0.

  - ☐ SSL 2.0 connections are not allowed. (default)
- **Allow SSL 3.0**
  - ☑ Connections encrypted with SSL 3.0 are allowed. (default)
  - ☐ SSL 3.0 connections are not allowed.
- **Warn if changing between secure and not secure mode**
  - ☑ When the browser changes from one security zone to another, a warning is displayed.
  - ☐ No warning is displayed when the security zone changes. (default)

_____

.NET Framework

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

Here you can specify how the browser processes .Net components.

- **Loose XAML**
  Possible options:
  - Enable: XAML files will be loaded into the browser.
  - Prompt: XAML files will be loaded into the browser if the user confirms the dialog.
  - Disable: XAML files will not be loaded into the browser.
- **XAML browser applications**
  Possible options:
  - Enable: XAML browser applications will be loaded into the browser.
  - Prompt: XAML browser applications will be loaded into the browser if the user confirms the dialog.
  - Disable: XAML files will not be loaded into the browser.
- **XPS documents**
  Possible options:
  - Enable: The browser will open XPS documents.
  - Prompt: The browser will open XPS documents if the user confirms the dialog.
  - Disable: The browser will not open XPS documents.
- **Run components signed with Authenticode**
  Possible options:
  - Enable: The browser will execute components signed with Authenticode.
  - Prompt: The browser will execute components signed with Authenticode if the user confirms the dialog.
  - Disable: The browser will not execute components signed with Authenticode.
- **Run components signed with Authenticode**
  Possible options:
  - Enable: The browser will execute components that are not signed with Authenticode.
  - Prompt: The browser will execute components that are not signed with Authenticode if the user confirms the dialog.
  - Disable: The browser will not execute components that are not signed with Authenticode.

ActiveX Controls and Plug-ins

Menu path: **Setup > Sessions > Browser Sessions > Security > ActiveX Controls and Plug-ins**

Here you can specify how the browser processes ActiveX control components and plugins.

- **Script ActiveX controls marked safe for scripting**
  Possible options:
  - Enable: The browser will execute scriptlets.
  - Prompt: The browser will execute scriptlets if the user confirms the dialog.
  - Disable: The browser will not execute scriptlets.
- **Initialize and script ActiveX controls**
  Possible options:
  - Enable: The browser will initialize ActiveX control elements with parameters und execute them without considering their object security. The setting **Script ActiveX controls marked safe for scripting** is overriden.
  - Prompt: The browser will initialize ActiveX control elements with parameters und execute them without considering their object security if the user confirms the dialog.
  - Disable: The browser will not execute ActiveX control elements whose object security has not been determined.
- **Run ActiveX controls and plug-ins**
  Possible options:
  - Enable: The browser will execute ActiveX controls and plug-ins.
  - Prompt: The browser will execute ActiveX controls and plug-ins if the user confirms the dialog.
  - Disable: The browser will not execute ActiveX controls and plug-ins.
- **Download signed ActiveX controls**
  Possible options:
  - Enable: The browser will download ActiveX controls.
  - Prompt: The browser will download ActiveX controls if the user confirms the dialog.
  - Disable: The browser will not execute ActiveX controls and plug-ins.
- **Allow Scriptlets**
  Possible options:
  - Enable: The browser will execute scriptlets.
  - Prompt: The browser will execute scriptlets if the user confirms the dialog.
  - Disable: The browser will execute scriptlets.
- **Download unsigned ActiveX controls**
  Possible options:
  - Enable: The browser will download unsigned ActiveX controls.
  - Prompt: The browser will download unsigned ActiveX controls if the user confirms the dialog.
  - Disable: The browser will not download unsigned ActiveX controls.

Download

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

Here you can specify how the browser processes downloadable fonts from the internet.

- **Font download**
  Possible options:
  - Enable: The browser will download fonts automatically.
  - Prompt: The browser will download fonts if the user confirms the dialog.
  - Disable: The browser will not download fonts.

Scripting

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

Here you can specify how the browser will process JavaScript and Java applets. Additionally, you can control the browser's access to the clipbard.

- **Active scripting**
  Possible options:
  - Enable: The browser will execute JavaScript.
  - Prompt: The browser will exeute JavaScript if the user confirms the dialog.
  - Disable: The browser will not execute JavaScript.
- **Clipboard acess**: Web sites can access contents of the clipboard via the browser.
  Possible options:
  - Enable: The browser will have access to the clipboard.
  - Prompt: The browser will have access to the clipboard if the user confirms the dialog.
  - Disable: The browser will not have access to the clipboard.
- **Scripting of Java applets**
  Possible options:
  - Enable: The browser will execute Java applets.
  - Prompt: The browser will execute Java applets if the user confirms the dialog.
  - Disable: The browser will not execute Java applets.

Sites

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

internetzone

- **Enable protected mode**
  - ☑ The protected mode is activated for this zone. (default)
  - ☐ The protected mode is not activated for this zone.

localinternetzone

- **Require server verification (https:) for all sites in this zone**
  - ☑ For sites in this zone, the connection must be secured by HTTPS.
  - ☐ For sites in this zone, the connection does not have to be secured by HTTPS. (default)
- **Enable protected mode**
  - ☑ The protected mode is activated for this zone. (default)
  - ☐ The protected mode is not activated for this zone.

To add a website to the zone "local intranet":

1. Click
   
   7 Add
   .
2. Enter the URL for the website.
3. Click **Ok**.

trustedzone

- **Require server verification (https:) for all sites in this zone**
  - ☑ For sites in this zone, the connection must be secured by HTTPS.
  - ☐ For sites in this zone, the connection does not have to be secured by HTTPS. (default)
- **Enable protected mode**
  - ☑ The protected mode is activated for this zone. (default)
  - ☐ The protected mode is not activated for this zone.

To add a website to the zone "trusted zone":

1. Click
   
   8 Add
   .
2. Enter the URL for the website.
3. Click **Ok**.

restrictedzone

- **Enable protected mode**
  - ☑ The protected mode is activated for this zone. (default)
  - ☐ The protected mode is not activated for this zone.

To add a website to the zone "restricted zone":

1. Click
   
   9 Add
   .
2. Enter the URL for the website.
3. Click **Ok**.

Miscellaneous

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

Here you can edit miscellaneous security settings.

- **Launching programs and files in an iFRAME**
  Possible options:
  - Enable: Programs and files that are referenced via an IFRAME on a website will be executed or loaded automatically.
  - Prompt: Programs and files that are referenced via an IFRAME on a website will be executed or loaded automatically if the user confirms the dialog.
  - Disable: Programs and files that are referenced via an IFRAME on a website will not be executed or loaded.
- **Launching applications and unsafe files**
  Possible options:
  - Enable: The browser will open unverifiable applications and files without a warning.
  - Prompt: The browser will open unverifiable applications and files if the user confirms the dialog.
  - Disable: The browser will not open unverifiable applications and files.
- **Drag and drop or copy and paste files**
  Possible options:
  - Enable: The user can drag files from a web page to the desktop by "drag and drop".
  - Prompt: The user can drag files from a web page to the desktop by "drag and drop" if he confirms the dialog.
  - Disable: The user can not drag files from a web page to the desktop.
- **Desplay mixed content**: Specifies how the browser will process websites that offer content both via a secured connection (HTTPS) and over an unsecured connection (HTTP).
  Possible options:
  - Enable: The browser will display mixed content automatically.
  - Prompt: The browser will display mixed content if the user confirms the dialog.
  - Disable: The browser will not display mixed content.
- **Allow websites to use restricted protocols for active content**: Specifies whether the browser will be allowed to execute active contents like scripts, ActiveX, Java and binary behavior from a website that is hosted by a restricted protocol in the intranet zone.
  Possible options:
  - Enable: The browser will execute active contents automatically.
  - Prompt: The browser will execute active contents if the user confirms the dialog.
  - Disable: The browser will not execute active contents.
- **Access data sources across domains**: Specifies if the browser will be enabled to access data from other security zones by means of Microsoft XML Parser (MSXML) or ActiveX Data Objects (ADO).
  Possible options:
  - Enable: The browser will automatically access data sources across domains.
  - Prompt: The browser will access data sources across domains if the user confirms the dialog.
  - Disable: The browser will not access data sources across domains.

- **Navigate windows and frames across different domains**
  Possible options:
  - Enable: The browser will open subframes from other domains and access applications from other domains.
  - Prompt: The browser will open subframes from other domains and access applications from other domains if the user confirms the dialog.
  - Disable: The browser will not open subframes from other domains and access applications from other domains.
- **Submit non-encrypted form data**: Specifies whether files in HTML forms may be submitted to websites. Forms submitted with SSL encryption are always allowed. This setting affects only the submission of form data that is not encrypted by SSL.
  Possible options:
  - Enable: The browser will submit unencrypted form data.
  - Prompt: The browser will submit unencrypted form data if the user confirms the dialog.
  - Disable: The browser will not submit unencrypted form data.

Advanced

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

Here you can edit miscellaneous browser settings.

- **Show pictures**
  - ☑ Websites will be loaded fully including all images. (default)
  - ☐ Images in websites will not be loaded; placeholders will be shown instead of the images. As a result of this, websites can be loaded more quickly, but the layout is impaired.
- **Play sounds in webpages**
  - ☑ The browser will play background music on a webpage automatically. (default)
  - ☐ The browser will not play background music on a webpage.
- **Show friendly HTTP error messages**: Specifies whether, in the case of an error, a page with more detailed information is displayed instead of the server message (example: "404 Not Found").
  - ☑ The friendly error message is displayed. (default)
  - ☐ The server message is displayed.
- **Automatically activate newly installed addons**
  - ☑ A newly installed addon will be active immediately.
  - ☐ A newly installed addon will not be active immediately after installation; to activate an addon, the user must confirm a dialog. (default)

Start

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

Here you can specify the start options for the browser session.

- **Session name**: Name of the session.

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

Session start options

- **Start menu**
  ☑ The session can be started with the start menu.
- **Desktop**
  ☑ The session can be started with a program starter on the desktop.
- **Autostart**
  ☑ The session will be launched automatically when the thin client boots.

Window

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

- **Start in fullscreen mode**
  - ☑ The browser window will fill the entire screen.
  - ☐ The browser window will be displayed in the default size. (default)
- **Global home page**: Start page for the browser.
- **Search provider**: Default search engine for the browser.
  Possible options:
  - Google
  - Bing
  - Yahoo!
  - Lycos
  - ASK.com
  - Altavista
  - Wikipedia
  - Custom: The browser's default search engine can be defined with **Custom search provider**.
- **Custom search provider**: URL of the user-defined default search engine.

Custom search provider display name: Display name of the user-defined default search engine.

Proxy

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

- **Use a proxy server for your LAN**
  - ☑ The browser will use the proxy configured here for websites in the LAN.
  - ☐ The browser will not use a proxy for websites in the LAN.
- **HTTP Proxy**: URL of the proxy for HTTP
- **Port**: Port of the proxy for HTTP
- **FTP Proxy**: URL of the proxy for FTP
- **Port**: Port of the proxy for FTP
- **SOCKS-Host**: URL of the proxy for SOCKS
- **Port**: Port of the proxy for SOCKS
- **SSL-Proxy**: URL of the proxy forSSL
- **Port**: Port of the proxy for SSL
- **Do not use proxy server for addresses beginning with**: List uf URLs for which no proxy should be used
- **Automatic proxy configuration URL**: With this proxy configuration, the PAC file (Proxy Auto Config) available under URL will be used.

Toolbar Items

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

- **Hide menu bar**
  - ☑ The browser's menu bar will not be displayed. (default)
  - ☐ The browser's menu bar will be displayed.
- **Lock the toolbars**
  - ☑ The menu bars can not be changed by "drag and drop". (default)
  - ☐ The menu bars can be changed by "drag and drop".

Toolbars

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

Here you can edit settings for the browser's toolbars.

- **Hide status bar**
  - ☑ The status bar will not be displayed. (default)
  - ☐ The status bar will be displayed.
- **Hide command bar**
  - ☑ The command bar will not be displayed. (default)
  - ☐ The command bar will be displayed.
- **Disable dev tools**
  - ☑ The developer tools will be deactivated.
  - ☐ The developer tools will be activated. (default)
- **Warn when closing multiple tabs**
  - ☑ A confirmation dialog is displayed when the user wants to close multiple tabs. (default)
  - ☐ No confirmation tab is displayed when closing multiple tabs.
- **Always switch to new tabs when they are created**
  - ☑ When opening a new tab by clicking on a link, the focus switches to the new tab.
  - ☐ When opening a new tab by clicking on a link, the focus will not change. (default)
- **Enable tab groups**
  - ☑ Tabs can be organized in groups. (default)
  - ☐ Tab groups are not available.
- **When a new tab is opened, open**
  - a blank page
  - your first home page
  - the new tab page (default)
- **Open links from other programs in**
  - a new window
  - a new tab in the current window
  - the current tab or window

Windows Media Player

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

Here you can edit the options for configuring and starting the Windows Media Player.

- **Use IGEL Setup for configuring Microsoft Media Player settings**
  - ☑ *The Windows Media Player settings can be edited using the IGEL Setup.*
  - ☐ *The Windows Media Player settings can be edited using the IGEL Setup. (default)*
- **Session name**: Name of the session.

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

Session start options

- **Start menu**
  - ☑ The session can be started with the start menu.
- **Desktop**
  - ☑ The session can be started with a program starter on the desktop.
- **Autostart**
  - ☑ The session will be launched automatically when the thin client boots.

- Player Control (see page 83)
- Security (see page 84)
- Performance (see page 85)
- Desktop Integration (see page 86)

Player Control

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

Here you can edit basic settings for the Windows Media Player.

- **Video size**: Initial zoom factor for the Windows Media Player.
  Possible options:
  - 50
  - 100
  - 200
- **Volume**: The sound volume when starting the Windows Media Player can be changed using the slider or by entering a value.
  Possible values: 0 - 100
- **Add media files to library**
  - ☑ Media files are added to the media library.
  - ☐ Media files are not added to the media library. (default)
- **Enable screensaver**
  - ☑ The screen saver can start during media playback and in doing so interrupt the media playback.
  - ☐ The screen saver can-not start during media playback. (default)
- **Start maximized**
  - ☑ The Windows Media Player will start in a fullscreen window.
  - ☐ The Windows Media Player will start in a default size window. (default)
- **Repeat**
  - ☑ When the media file is completed, playback will start again.
  - ☐ The media file will be played once. (default)
- **Shuffle**
  - ☑ The items on the playlist will be played in random order.
  - ☐ The items on the playlist will be played in list order. (default)
- **Mute**
  - ☑ The media will be played without sound.
  - ☐ The media will be played with sound. (default)

Security

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

Here you can edit the security settings of the Windows Media Player.

- **Disable automatic updates**
  - ☑ The Windows Media Player will not be updated automatically.
  - ☐ The Windows Media Player will be updated automatically. (default)
- **Save history in the player**
  - ☑ The names of the media files that have been played will be stored. (default)
  - ☐ The names of the media files will not be stored.
- **Retrieve media info from the internet**
  - ☑ Information about the media files will be updated automatically.
  - ☐ Information about the media files will not be updated. (default)
- **Send unique ID**
  - ☑ The ID of this Windows Media Player will be sent to content providers.
  - ☐ The ID of this Windows Media Player will not be sent. (default)
- **Download usage rights automatically**
  - ☑ The media usage rights will be updated automatically.
  - ☐ The media usage rights will not be updated. (default)
- **Set clock on devices automatically**
  - ☑ The Windows Media Player will sync the device clock automatically to ensure that the media usage rights are correct.
  - ☐ The Windows Media Player will not sync the device clock. (default)
- **Customer experience improvement**
  - ☑ The Windows Media Player will send usage data to Microsoft to support customer experience improvement.
  - ☐ The Windows Media Player will not send usage data to Microsoft

Performance

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

Here you can edit performance settings for the Windows Media Player.

- **No video smoothing**
  - ☑ The Windows Media Player will not use video smoothing.
  - ☐ The Windows Media Player will use video smoothing. (default)
- **Enable DirectX video acceleration**
  - ☑ The Windows Media Player will use DirectX video acceleration. (Standard)
  - ☐ The Windows Media Player will not use DirectX video acceleration.
- **Keep AV in sync**
  - ☑ Single images can be discarded to keep sound and images in sync.
  - ☐ Single images will not be discarded.
- **Display fullscreen controls**
  - ☑ The Windows Media Player controls will be displayed in fullscreen mode. (default)
  - ☐ The Windows Media Player controls will not be displayed in fullscreen mode.

Desktop Integration

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

Here you can edit the start options for the Windows Media Player.

- **Session name**: Name of the session.

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

Session start options

- **Start menu**
  ☑ The session can be started with the start menu.
- **Desktop**
  ☑ The session can be started with a program starter on the desktop.
- **Autostart**
  ☑ The session will be launched automatically when the thin client boots.

Accessories

Menu path: **Setup > Accessories**

Here you can edit settings for the IGEL Setup, sound settings, and settings for Windows services.

_____

Setup Session

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

You can configure your thin client with the IGEL Setup. To find out how to allow the user to access specific setup areas, see User Page Permissions (see page 89). To find out how to edit the setup options, see Options (see page 90).

The start options are described below.

- **Session name**: Name of the session.

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

Session start options

- **Start menu**
  ☑ The session can be started with the start menu.
- **Desktop**
  ☑ The session can be started with a program starter on the desktop.
- **Autostart**
  ☑ The session will be launched automatically when the thin client boots.

- Setup User Permissions (see page 89)
- Options (see page 90)

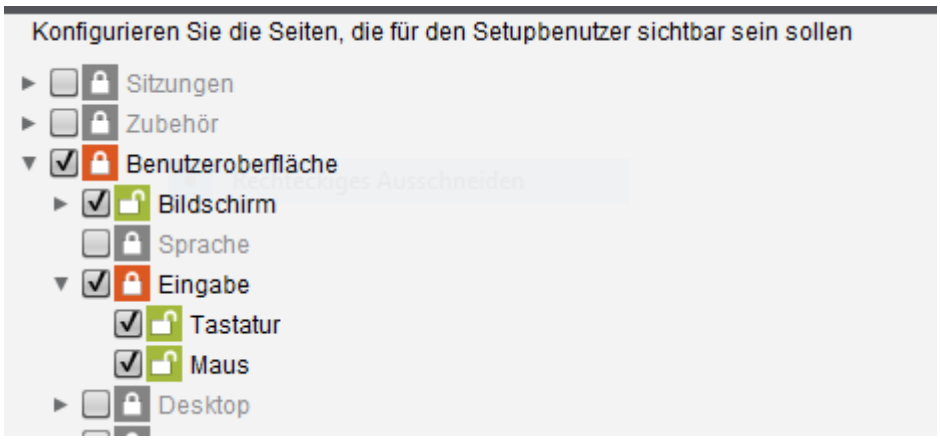
Setup User Permissions

Menu path: **Setup > Accessories > Setup Session > User Page Permissions**

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 132)). However, individual areas of the setup can be enabled for the user, e.g. to allow them to change the system language or configure a left-handed mouse.

To enable setup areas for the user:

1. Under **Security > Password**, enable the password for the **administrator** and the **setup user**.
2. Under **Accessories > Setup Session > Page Permissions**, enable the areas to which the user is to have access.
    - A check in the checkbox indicates that the node is visible in the setup.
    - A red symbol  indicates that the parameter is password-protected by the administrator.
    - A green symbol  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

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

You can configure the display of tooltips in the setup.

- **Enable tooltips**
  ☑ When the mouse pointer is hovering over a parameter, the appropriate tooltip is displayed after the configured **Tooltip delay**. (default)
  ☐ No tooltip is displayed.
- **Tooltip delay**: Time interval in tenths of a second within which the mouse pointer must hover over a parameter in order to trigger the tooltip.

Sound Mixer

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

- Options (see page 92)

Options

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

- **Use IGEL Setup for configuring system audio settings**
  - ☑ *The system-wide audio settings can be configured using the IGEL Setup.*
  - ☐ *The system-wide audio settings can not be configured using the IGEL Setup. (default)*
- **Mute**
  - ☑ The audio output is not activated
  - ☐ The audio output is activated. Default)
- **Master volume**: The sound volume when starting the Windows Media Player can be changed using the slider or by entering a value.
  Possible values: 0 - 100
- **Enable DisplayPort audio device**
  - ☑ Audio data is played through the DisplayPort.
  - ☐ No audio data is played through the DisplayPort. (default)

Windows Services

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

Here you can edit the settings for specific Windows services.

- **Use IGEL Setup for configuring Windows Services settings**
  - ☑ *The settings for Windows services can be edited using the IGEL Setup.*
  - ☐ *The settings for Windows services can not be edited using the IGEL Setup. (default)*
- **Start .NET runtime optimization service**
  - ☑ The service ".NET Runtime Optimization" will be started on system start.
  - ☐ The service ".NET Runtime Optimization" will not be started on system start. (default)
- **Start discovery of UPnP devices service**
  - ☑ The service "discovery of UPnP devices" will be started on system start.
  - ☐ The service "discovery of UPnP devices" will not be started on system start. (default)
- **Start remote desktop support service**
  - ☑ The service "Remote desktop support" will be started on system start. (default)
  - ☐ The service "Remote desktop support" will not be started on system start.
    - **Deny TS connections**
      - ☑ Terminal Services connections (Remote Desktop Services) will be denied.
      - ☐ Terminal Services connections (Remote Desktop Services) will be accepted. (default)
- **Start IEEE 802.1X authentication service for wired Ethernet interfaces**
  - ☑ The IEEE 802.1X authentication service will be started on system start.
  - ☐ The IEEE 802.1X authentication service will not be started on system start. (default)
- **Starte SCCM-Voraussetzungen**
  - ☑ The Windows update service is available after the system has started.
  - ☐ The Windows update service is not available on system start. (default)
- **Start BITS service**
  - ☑ The BITS service (Background Intelligent Transfer Service) will be started on system start.
  - ☐ The BITS service will not be started on system start. (default)
- **Start UNIX printing services**
  - ☑ The UNIX printing services will be started on system start.
  - ☐ The UNIX printing services will not be started on system start. (default)
- **Start Microsoft Keyboard Filter**
  - ☑ The keyboard filter will be started on system start.
  - ☐ The keyboard filter will be started on system start. (default)

USB Redirection Services

- **Start VMware Horizon View Client USB Redirection Service**
  - ☑ The USB redirection for the VMware Horizon client will be started on system start. (default)
  - ☐ The USB redirection for the VMware Horizon client will not be started on system start.

User Interface

Menu path: **Setup > User Interface**

The user interface can be customized according to your needs and requirements.

_____

Display

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

Here you can configure the settings for the screens used.

- **Use IGEL Setup for configuring display settings**
  ☑ The display settings are configured using this setup page.
  ☐ The display settings are not configured using the IGEL setup. The deactivation will be effective after a reboot.
- **Number of screens**: Number of screens used.
-  Arranges a number of screens in a single row.
-  Arranges a number of screens in two rows.
-  Rotates the selected screen counter clockwise.
-  Rotates the selected screen clockwise.
-  or **Selected screen**: Selects the screen whose settings are to be changed.
- **Screen resolution**: Specifies the resolution for the selected screen. From Version *3.12.100*, the setting is configured using a slider. If the slider is at the far left, the screen resolution will be detected automatically.

> In order for automatic detection to work, the monitor must supply the correct data.

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

> For the rotation (pivot), at least 128 MB as video memory must be configured in the thin client's BIOS.

Advanced

- **Refresh rate**: Specifies the refresh rate for the selected screen.

- Options (see page 97)

Options

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

Here you can set the color depth of the screen and the screen saver.

- **Color Depth**
  Possible values:
  - True Color: Up to 16.8 million colors are displayed.
  - 65535 Colors: Up to 65535 colors are displayed.
- **Use blanking screensaver**

  > You can also set up a screen saver in the Energy options.

  ☑ If no user interaction takes place within the period defined under **Inactivity timeout for the blanking of screensaver**, the screen saver will start.

  ☐ The screen saver will never be started.
- **On resume, password protect**

  ☑ The user must enter their password in order to end the screen saver and gain access to the screen, keyboard and mouse again.

  ☐ Access to the screen, keyboard and mouse is possible without entering a password.
- **Inactivity timeout for the blanking of screensaver**: If no user interaction takes place within the number of minutes specified here, the screen saver will start.
  Possible values: **1** to **300** (default: 10)

Language

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

You don't need to install any language packs for Windows 10 IoT. All languages are already integrated!

- **Use IGEL Setup for configuring region and language options**
  ☑ The region and language options are configured using this setup page.
- **Setup language**: Language of the setup GUI
  Possible values:
  - Chinese (simplified)
  - Chinese (traditional)
  - Dutch
  - English
  - French
  - German
  - Italian
  - Spanish
  - Japanese
- **Keyboard layout** - Selection of country specific keyboards (default: English (USA))
- **Standards und formats** - Selection of country specific standards und formats (default: English (USA))
- **Locations** - Selections of locations (default: United States)

Input

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

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

> These settings override the *Windows* system settings.

_____

Keyboard

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

- **Use IGEL Setup for configuring keyboard settings**
  - ☑ The keyboard settings are configured using this setup page.
- **Keyboard layout** - Selection of country specific settings.

Character Repeat

- **Repeat delay** – Sets the delay (time in ms) between pressing a key and auto repeat mode. (default: 500ms)
- **Repeat rate** - Numbers of characters per second (default: 30 characters)
- **Enable NumLock key**
  - ☑ NumLock key enabled (default)
  - ☐ NumLock disabled
- **Start onscreen keyboard at logon**
  - ☑ Start onscreen keyboard at Windows logon.
  - ☐ No automatic start

Mouse

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

- **Use IGEL Setup for configuring mouse settings**
  ☑ The mouse settings are configured using this setup page.
- **Left-handed mode**
  ☑ Left-handed mouse enabled
- **Pointer Speed** - Value of the mouse speed in percentage between 1 (slow) and 100 (fast).
- **Double Click Interval** - Maximum interval in milliseconds between two mouse clicks to still be recognized as a double-click.
- **Double Click Distance** - Maximum distance in pixles between two mouse clicks to still be recognized as a double-click.

Desktop

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

In this area, you can make settings regarding the desktop.

- **Use IGEL Setup for desktop settings**
  - ☑ The desktop settings are configured using this setup page. (Default)
  - ☐ Desktop settings will not be configured using the IGEL Setup.
- **Show recycle bin on the desktop**: The recycle bin is hidden by default.
  - ☑ The recycle bin is shown.
  - ☐ The recycle bin is not shown. (Default)
- **Enable Aero Glass**: Enables *Aero Glass* effects (transparent windows, thumbnails).
  - ☑ Aero Glass effects are applied.
  - ☐ Aero Glass effects are not applied. (Default)
- **Use IGEL for configuring Windows desktop background picture**: Enable to define a background image in IGEL Setup.
  - ☑ The background image is used.
  - ☐ The background image is not used. (Default)
- **Filename Desktop background picture**: The absolute path to the background image file.

_____

- Users (see page 103)
- Administrators (see page 105)

Users

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

In Windows 10 you have different possibilities to change layout and function according to your needs:

- Configure settings also for domain users.
- Show Checkboxes in Windows Explorer
- Disable Preview Desktop
- Show File and Folder Names Using the Correct Case
- Show Filter in Active Directory
- Show info Tooltip of folder
- Show Hidden Files and Folders
- Hide known extensions of files
- Hide all Icons on Desktop
- Show only Icons on Desktop
- Transparent selection rectangle
- Transparent Icon Background
- Show network connect buttons in Explorer
- Expand to Current Folder in Explorer
- Show All Folders in Navigation Pane
- Launch Folder Windows in a Separate Process
- Show Adminstrator Tools in Start Menu
- Other color for compressed files and folders
- Quickinfo (Tooltip) for Icons in Explorer
- Show hidden system files in Explorer
- Show icon of assigned application
- Show hidden files in Explorer
- Activate Taskbar animations
- Taskbar buttons: only combine when taskbar is full
- Set Taskbar changeable
- Show small Icons in Taskbar
- Show Preview and filter in Windows folder
- Enable Autorun for Unknown Drive Types
- Enable Autorun for Swappable Drive Types
- Enable Autorun for Harddisk Drive Types
- Enable Autorun for Network Drive Types
- Enable Autorun for CD-ROM Drive Types
- Enable Autorun for RAM Drive Types
- Disable Windows Update mechanism
- Disable customizing of toolbar from explorer
- Enable the possibility to modify the toolbar from Explorer
- Enable the Classic Start Menu
- Show control panel in classic view
- Show small icons in control panel
- Disable customizing browser toolbars
- Prevent users being able to modify the Start Menu

- Disable the Shutdown command
- Disable the display of Common Groups
- Hide Control Panel
- Hide all icons on the desktop
- Disable Autorun of the drives
- Hide drive A: in My Computer
- Hide drive B: in My Computer
- Hide drive C: in My Computer
- Hide drive E: in My Computer
- Hide drive Z: in My Computer
- Hide Favorites checkbox in Start Menu
- Hide Filemenu from Explorer
- Remove Search Entry in Start Menu
- Disable Folderoptions
- Hide the Log Off button in the Ctrl+Alt+Del Menu
- Remove the Connect/Disconnect Entry in Context menu from Explorer
- Hide the Run command on Start Menu
- Disable save settings (icons on desktop etc.) on log off or reboot
- Hide Control Panel, Printer and Network Settings
- Remove Taskbar and Start Menu settings from Control Panel
- Disable the All Programs button in Start Menu
- Disable view Custom sub folders on Start Menu
- Disable the context menu of the taskbar
- Disable the context menu on the desktop
- Disable Window Hotkey combinations
- Hide Entire Network button
- Disable the change password button
- Disable Task Manager in Window after Ctr+Alt+Del
- Disable Registry Editing Tools
- Hides Display icon in Control Panel
- Disable Lock Workstation

Administrators

Menu path: **Setup > User Interface > Desktop > Administrators**

In Windows 10 you have different possibilities to change layout and function according to your needs:

- Configure settings also for domain users.
- Show Checkboxes in Windows Explorer
- Disable Preview Desktop
- Show File and Folder Names Using the Correct Case
- Show Filter in Active Directory
- Show info Tooltip of folder
- Show Hidden Files and Folders
- Hide known extensions of files
- Hide all Icons on Desktop
- Show only Icons on Desktop
- Transparent selection rectangle
- Transparent Icon Background
- Show network connect buttons in Explorer
- Expand to Current Folder in Explorer
- Show All Folders in Navigation Pane
- Launch Folder Windows in a Separate Process
- Show Adminstrator Tools in Start Menu
- Other color for compressed files and folders
- Quickinfo (Tooltip) for Icons in Explorer
- Show hidden system files in Explorer
- Show icon of assigned application
- Show hidden files in Explorer
- Activate Taskbar animations
- Taskbar buttons: only combine when taskbar is full
- Set Taskbar changeable
- Show small Icons in Taskbar
- Show Preview and filter in Windows folder
- Enable Autorun for Unknown Drive Types
- Enable Autorun for Swappable Drive Types
- Enable Autorun for Harddisk Drive Types
- Enable Autorun for Network Drive Types
- Enable Autorun for CD-ROM Drive Types
- Enable Autorun for RAM Drive Types
- Disable Windows Update mechanism
- Disable customizing of toolbar from explorer
- Enable the possibility to modify the toolbar from Explorer
- Enable the Classic Start Menu
- Show control panel in classic view
- Show small icons in control panel
- Disable customizing browser toolbars
- Prevent users being able to modify the Start Menu

- Disable the Shutdown command
- Disable the display of Common Groups
- Hide Control Panel
- Hide all icons on the desktop
- Disable Autorun of the drives
- Hide drive A: in My Computer
- Hide drive B: in My Computer
- Hide drive C: in My Computer
- Hide drive E: in My Computer
- Hide drive Z: in My Computer
- Hide Favorites checkbox in Start Menu
- Hide Filemenu from Explorer
- Remove Search Entry in Start Menu
- Disable Folder options
- Hide the Log Off button in the Ctrl+Alt+Del Menu
- Remove the Connect/Disconnect Entry in Context menu from Explorer
- Hide the Run command on Start Menu
- Disable save settings (icons on desktop etc.) on log off or reboot
- Hide Control Panel, Printer and Network Settings
- Remove Taskbar and Start Menu settings from Control Panel
- Disable the All Programs button in Start Menu
- Disable view Custom sub folders on Start Menu
- Disable the context menu of the taskbar
- Disable the context menu on the desktop
- Disable Window Hotkey combinations
- Hide Entire Network button
- Disable the change password button
- Disable Task Manager in Window after Ctr+Alt+Del
- Disable Registry Editing Tools
- Hides Display icon in Control Panel
- Disable Lock Workstation

Start Menu

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

- **Use IGEL Setup for configuring start menu settings**
  - ☑ The start menu settings are configured using this setup page. (default)
  - ☐ Start menu settings will not be configured using the IGEL Setup.

_____

- Users (see page 108)
- Administrators (see page 110)

Users

Menu path: **Setup > User Interface > Start Menu > Users**

- Configure settings also for domain users.
- Display "Administrative Tools" in the "Start" menu under "All Programs".
- Extend "All Programs" menu if mouse points to it.
- Enable "drag and drop" in the "Start" menu.
- Show large icons from most frequently used programs in the "Start" menu.
- Highlight new entries in the "Start" menu.
- Default "Start" menu power button action:
    - Log Off
    - Lock
    - Restart
    - Sleep
    - Shutdown
- Use file index in file search from the "Start" menu.
- Search programs and control panel.
- Show control panel in "Start" menu:
    - Don't display
    - Display as link
    - Display as a menu
- Show the downloads folder in the "Start" menu:
    - Don't display
    - Display as link
    - Display as a menu
- Show the "Help" button in the "Start" menu.
- Show the home group network in the "Start" menu.
- Show "My Computer" in "Start" menu:
    - Don't display
    - Display as link
    - Display as a menu
- Show the "My Docs" folder in "Start" menu:
    - Don't display
    - Display as link
    - Display as a menu
- Show the "My Music" folder in "Start" menu:
    - Don't display
    - Display as link
    - Display as a menu
- Show the "My Pictures" folder in "Start" menu:
    - Don't display
    - Display as link
    - Display as a menu
- Show the "Recorded TV" folder in "Start" menu:
    - Don't display

        - Display as link
        - Display as a menu
- Show the "Videos" folder in "Start" menu:
    - Don't display
    - Display as link
    - Display as a menu
- Show network connections in "Start" menu.
- Show network places in "Start" menu.
- Shows Printers Item in "Start" menu.
- Show list of recent docs in "Start" menu.
    - Don't display
    - Display as link
    - Display as a menu
- Show 'Run' in the "Start" menu.
- Show program access and defaults.
- Show the personal folder of the user:
    - Don't display
    - Display as link
    - Display as a menu
- Sort "Start" menu items alphabetically.
- Show recently opened items in jump lists in the "Start" menu or on the taskbar.
- Show most used apps.
- Show 'Favorites' in the "Start" menu.

Administrators

Menu path: **Setup > User Interface > Start Menu > Administrators**

- Configure settings also for domain users
- Display "Administrative Tools" in Start Menu and All Programs Menu
- Extend All Programs Menu, if Mouse Points on it
- Enable drag and drop in Start Menu
- Show large icons from most frequently used programs in Start menu
- Highlight new entries in the Start Menu
- Default Start Menu Power Button Action
    - Log Off
    - Lock
    - Restart
    - Sleep
    - Shutdown
- Use Fileindex in filesearch from startmenu
- Search Programs and Control Panel
- Show Control Panel in start menu
    - Don't display
    - Display as link
    - Display as a menu
- Show downloads folder in start menu
    - Don't display
    - Display as link
    - Display as a menu
- Show 'help' button in start menu
- Show Homegroup network in start menu
- Show 'My Computer' in start menu
    - Don't display
    - Display as link
    - Display as a menu
- Show 'My Docs' folder in start menu
    - Don't display
    - Display as link
    - Display as a menu
- Show 'My Music' folder in start menu
    - Don't display
    - Display as link
    - Display as a menu
- Show 'My Pictures' folder in start menu
    - Don't display
    - Display as link
    - Display as a menu
- Show 'Recorded TV' folder in start menu
    - Don't display

        - Display as link
        - Display as a menu
- Show 'Videos' folder in start menu
    - Don't display
    - Display as link
    - Display as a menu
- Show Network Connections on start menu
- Show Network Places on start menu
- Shows Printers Item in start menu
- Show list of recent docs in start menu
    - Don't display
    - Display as link
    - Display as a menu
- Show 'run' on start menu
- Show Programaccess and defaults
- Show personal folder from user
    - Don't display
    - Display as link
    - Display as a menu
- Sort Start Menu Items Alphabetically
- Show recently opened items in Jump Lists on Start or the taskbar
- Show most used apps
- Show Favorites in start menu

Shell

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

- **Use IGEL Setup for configuring shell settings**
  - ☑ The start menu settings are configured using this setup page. (default)
  - ☐ Start menu settings will not be configured using the IGEL Setup.

_____

- Users (see page 113)
- Administrators (see page 114)

Users

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

- Configure settings also for domain users

Enable components to be shown in the control panel:

- Accessibility Options control panel
- Administrative Tools
- Add/Remove Programs
- Display Properties
- Firewall
- Fonts Folder
- Hardware Manager
- Home Group
- Internet Properties
- Regional Settings
- Mouse Properties
- Keyboard Properties
- Multimedia Properties
- Modem Properties
- Network Properties
- User Management
- Power Management
- Devices and Printers
- System
- Date/Time Properties
- Taskbar and Start Menu Settings
- Windows Update

Administrators

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

- Configure settings also for domain users
- Shows Accessibility Options control panel

Enable components, which shall be shown in the control control:

- Administrative Tools
- Add/Remove Programs
- Display Properties
- Firewall
- Fonts Folder
- Hardware Manager
- Home Group
- Internet Properties
- Regional Settings
- Mouse Properties
- Keyboard Properties
- Multimedia Properties
- Modem Properties
- Network Properties
- User Management
- Power Management
- Devices and Printers
- System
- Date/Time Properties
- Taskbar and Start Menu Settings
- Windows Update

Network

Menu path: **Setup > Network**

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

_____

LAN Interface

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

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

The internal **LAN** interface is pre-configured for DHCP by default.

In the **Wireless** area, you will find all parameters for the wireless network including the options for encrypting the connection. Configure hidden networks by entering the Wi-fi network 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 Wireless in the setup.

_____

- Interface [number] (see page 117)
- Wireless (see page 118)

Interface [number]

Menu path: **Setup > Network > LAN Interface > Interface [number]**

- **Use IGEL Setup for configuring the LAN interface**
  - ☑ The LAN interface is configured using the IGEL Setup.
  - ☐ The LAN interface is configured in another manner.
- Get the IP from the DHCP server.
  - ☑ The IP address is configured automatically via DHCP.
- Specify an IP address
  - ☑ The IP address is configured manually below
    - **IP Address**: IP address, e.g 192.168.100.123
    - **Network Mask**: Network mask, e.g. 255.255.255.0
- **Gateway**
  - **enable**
    - ☑ The interface will use the specified gateway.
  - (Gateway address): IP address of the gateway, e.g. 192.168.100.1
  - **Terminal Name**: Network name of the thin client
- **Enable DNS Caching**
  - ☑ The system uses a cache for DNS information.
- **Enable DNS**
  - ☑ DNS is activated manually.

    When using DHCP or BOOTP, manual DNS configuration is not necessary.

    - **Default Domain**: Usually the name of the local network
    - **Name server**: IP address of the nameserver to use.

Wireless

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

Here you will find the configuration parameters for the wireless interface.

- **Use IGEL Setup for configuring the wireless network interface**.
  - ☑ The wireless interface is configured using the IGEL Setup.
  - ☐ The wireless interface is configured in another manner.
- **Activate Wireless interface**
  - ☑ The interface will be brought up.
- **Get IP from DHCP server**.
  - ☑ The IP address is configured automatically via DHCP.
- **Specify an IP address**
  - ☑ The IP address is configured manually below.
    - **IP Address**: IP address, e.g. 192.168.100.123.
    - **Network Mask**: Network mask, e.g. 255.255.255.0.

- Wi-Fi Network (see page 119)
- Wireless Regulatory Domain (see page 120)

Wi-Fi Network

Menu path: **Setup > Network > LAN Interfaces > Wireless > Default Wi-Fi Network**

Here you can configure wireless network connections.

- **Disable encryption**: No encryption will be used. (default)
- **Enable WEP encryption**: WEP encryption will be used.
- **Enable WPA encryption**: WPA encryption will be used.

  ⓘ You will need to give further information depending on the encryption method chosen.

- **Wireless network name (SSID)**: Name of the wireless network (SSID)

For WEP encryption

- **Transmit key ID**: Choose from a maximum of four configurable keys (default 1).
- **Key format**:
  - ASCII
  - Hexadecimal
- **Key** [1 - 4]: Enter the key here.

  ⓘ Characters to be entered for WEP keys:
  - For 64 bit encryption, 5 characters (ASCII) or 10 hex digits (hexadecimal)
  - For 128 bit encryption, 13 characters (ASCII) or 26 hex digits (hexadecimal)

For WPA encryption

- **Network authentication**:
  - WPA Personal: Wi-fi Protected Access pre-shared key (WPA / IEEE 802.11i/D3.0)
  - WPA Enterprise: Wi-fi Protected Access with 802.1X authentication (WPA / IEEE 802.11i/D3.0)
  - WPA2 Personal: Wi-fi Protected Access pre-shared key (WPA2 / IEEE 802.11i/RSN)
  - WPA2 Enterprise: Wi-fi Protected Access with 802.1X authentication (WPA2/IEEE 802.11i/RSN)
- **Network key**: WPA network key/passphrase as set at the dial-in point. This is either an ASCII character string with a length of 8...63 or exactly 64 hexadecimal digits.
- **Show**

  ☑ The network key is shown.

  ☐ The network key is hidden. (default)
- **Data encryption**:
  - Default: The default value depends on which network authentication method is selected - TKIP for WPA, AES (CCMP) for WPA2.
  - TKIP: Temporal Key Integrity Protocol (IEEE 802.11i/D7.0)
  - AES (CCMP): AES in counter mode with CBC-MAC (RFC 3610, IEEE 802.11i/D7.0)
  - AES (CCMP) + TKIP: One of two encryption methods is selected by the access point.
  - Automatic: The access point can choose the encryption method freely – nothing is stipulated.

Wireless Regulatory Domain

Menu path: **Setup > Network > LAN Interfaces > Wireless > Wireless Regulatory Domain**

This page allows you to set the wireless device in accordance with local regulations.

- **Wireless regulatory domains**: Select the area in which the device is located.
  - Not configured
  - Africa
  - Arctic
  - Asia
  - Europe
  - North America
  - South America
  - World
- **Location**: Select the country in which the device is located.
  - Not configured
  - Albania
  - Armenia
    [...]
  - Cyprus
  - Austria

The list below sets out the technical requirements for the selected location for your information.

VPN

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

Here you can configure a virtual private network (VPN).

_____

- NCP VPN Client (see page 122)

NCP VPN Client

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

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

Further information regarding configuration and use is available from NCP: https://www.ncp-e.com/en/service-resources/library/

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

Routing

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

- **Use IGEL Setup for configuring network routing settings**
  - ☑ Routing settings are configured in the IGEL Setup.
  - ☐ Routing settings are configured in another manner.
- **Enable**
  - ☑ Apply these routing settings.
- **Gateway**: The gateway routing packets to the target network.
- **Interface**: The network interface to use. If no device is specified, the route affects all network devices.

Network Drives

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

Here you can mount Windows shares as network drives.

_____

- Windows Drive (see page 125)

Windows Drive

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

Here you specify both the drives that are to be connected during booting and the associated logon data.

Working with the Windows Network Drives List:

▶

To add an entry, click

⊞

10 Add

.

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

Adding a Windows Drive

- **Enabled**:
  ☑ The drive will be automatically connected on boot.
- **Local Drive Letter**: 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 letter allocated is already reserved, only the drive connected first will be shown. An error entry for the second drive will appear in the event log.
- **Server**: IP Address or DNS name of the server exporting the share
- **Share name**: Name of the Windows share
- **User name**: User name for the server

  ⓘ To supply a domain alongside the user name, use the following pattern. `DOMAIN\Username` .
- **Password**: User password for the server

Devices

Menu path: **Setup > Devices**

In this area, you configure printers and other connected devices.

_____

Printer

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

Printer

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

In this area, you can set up your local printers. You can configure the printer using the IGEL Setup or a configuration file.

Please note our FAQs regarding Thin Print.

To add a printer and configure it in the IGEL Setup:

1. Click
   
   11 Add
   .
2. Enter an appropriate **Printer name**.
3. Enable **Configure the printer with the IGEL Setup**.
4. Modify the settings according to your needs:
   - **Papersize**
   - **Orientation**
   - **Print quality**
   - **Media type**
   - **Color mode**
   - **Duplex mode**
5. Click **Ok**.

To add a printer and configure it using a configuration file:

1. Click
   
   12 Add
   .
2. Enter an appropriate **Printer name**.
3. Enable **use a printer settings file at the defined location**.
4. Enter the **Path to the printer settings file**.

   > The file should reside on a local drive, as network drives may not be available at logon time.

   Example: `C:\Temp\config_file`
5. Click **Ok**.

Attached Devices

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

- USB Storage Hotplug (see page 130)

USB Storage Hotplug

Menu path: **Setup > Devices > Attached Devices > USB Storage Hotplug**

- **Disable USB storage devices**
  - ☑ Access to USB storage devices is denied.
  - ☐ Access to USB storage devices is allowed. (default)
- **Enable write protection fur USB devices**
  - ☑ Write access to USB storage devices is denied.
  - ☐ Write access to USB storage devices is allowed. (default)
- **Disable WLAN Devices**
  - ☑ Access to WLAN devices is denied.
  - ☐ Access to WLAN devices is allowed. (default)
- **Disable Bluetooth devices**
  - ☑ Access to Bluetooth devices is denied.
  - ☐ Access to Bluetooth devices is allowed. (default)

Security

Menu path: **Setup > Security**

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

> Use an additional user password, which gives you different options to give the user restricted configuration rights.

_____

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 administrators 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.
  ☐ The settings are not specified in the setup. (default)

Local 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.

IGEL 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,** enable those areas to which the user is to have access.

Local User

- **Use password**
  ☑ You specify a password for the user.

Rescue Shell User

- **Use password**
  ☑ You specify a password for the rescue shell.
- **Auto Logon** - Specify a user to be automatically logged on when the system starts. (default: `user`)
  - **Username** - Name of the user
  - **Password** - Password of the user
  - **Domain** - Only needed for an Active Directory user

☑ When the system boots (and the shift key is not pressed), the user will automatically be logged on.

Active Directory

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

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

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

- **Use IGEL Setup for configuring Active Directory settings**
  - ☑ The settings for active directory are specified in the setup.
  - ☐ The settings are not specified in the setup. (default)
- **Disable local caching**
  - ☑ Local caching will be carried out. (default)
  - ☐ Local caching will not be carried out.
- **Thin client is member in a domain**
  - ☑ The thin client will be in a domain.
  - ☐ The thin client will not be in a domain.
- **Domain name**
- **Domain user**
- **Password**
- **Organisational unit** - OU under which to create the thin client account. This must be a fully qualified RFC 1779 for the OU, e.g. ou=mytest,dc=mysubdomain,dc=mydomain,dc=de. If not specified, the account will be created under the default organization unit for machine objects for that domain.
- **Timeout** - Timeout for contacting the domain server.
  - 30 seconds
  - 45 seconds
  - 60 seconds
  - 75 seconds
  - 90 seconds

Network

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

Deactivate administrative shares here or hide the device by activating **Do not show Thin Client in network**. In addition you can manage the rules for the Windows firewall. This local firewall is enabled by default and has preconfigured rules allowing the use of remote desktop clients and management of the thin client through 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 network security settings**
  - ☑ The setup manages the network security settings. (default)
  - ☐ The setup does not manage the network security settings.
- **Deactivate administrative shares**
  - ☑ Administrative shares are deactivated.
- **Do not show thin client in network**
  - ☑ The thin client will not be displayed in the network.
- **Deactivate windows firewall**
  - ☑ The firewall is disabled.

    > It is recommended to always keep the firewall active.

- **Allow ICMP-Ping requests**
  - ☑ Allow ping requests to be sent to the thin client.
- **Do not allow exceptions**
  - ☑ No exceptions for blocked programs can be added.

List of Program Rules

These rules allow local programs to establish network connections.

How to work with device rules:

▶

To create a rule, click

⊞

13 Add

.

▶ To remove a rule, click 🗑.

▶ To change a rule, click  .

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

Windows Defender

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

In this area, you can configure Windows Defender's download behavior for antimalware definition updates.

- **Use IGEL Setup for configuring Microsoft Windows Defender**: Defines whether the the thin client's local configuration of Windows Defender will be overwritten by the settings made here.
  - ☑ The thin client's local settings will be overwritten. (Default)
  - ☐ The thin client's local settings will not be overwritten.
- **Enable Windows Defender**: Enable or disable Windows Defender.
  - ☑ Windows Defender is enabled. (Default)
- **Source for downloading definition updates**: The source from which to download definition updates.
  Possible values:
  - Microsoft Update Server: Definition updates will be downloaded from the Microsoft Update Server.
  - Windows Server Update Services (WSUS): Definition updates will be downloaded from the Windows Server Update Services.
  - File share: Definition updates will be downloaded from the file share/s specified under **File share for downloading definition updates**.
- **File shares for downloading definition updates**: The file share/s for downloading definition updates.

> You can provide one or several file shares. The file shares must be seperated by a pipe smybol **|**. File shares are used in the order their of appearance in the list. Example: `\\server1\share1|\\server1\share2`.

- **Windows Defender updates timeout**: The timeout for downloading updates for Windows Defender.
  This option applies only if **Microsoft Defender update definition download** is set to **Schedule**.
  Possible values:
  - 10 minutes
  - 20 minutes
  - 30 minutes
- Windows Defender update definition download: Defines if update definitions are to be downloaded, and according to which configuration.
  - Enabled: Windows Defender will download definition updates according to its local configuration on the thin client.

> **Important:** If **Windows Defender update definition download** is **Enabled** with activated write filter, the overlay usage will grow significantly. Excess memory consumption will degrade system performance.

- Disabled: Windows Defender will be prevented from downloading any definition updates.

- Schedule: Windows Defender will download definition updates according to the schedule specified under **Start** and **Recur every days**.

When **Schedule** is selected, the write filter will be deactivated during definition updates to keep RAM usage low.

Important: When a scheduled update is executed, the thin client will be automatically force-rebooted several times. Due to this, it is strongly recommended to configure the schedule so that updates are only executed during times nobody is using the thin client.

- **Start**: The date and time when definition updates are to be downloaded for the first time.

The date and time specified under **Start** is the date time relative to the thin client's local timezone.

- **Choose time**: Click this button to choose a starting time.
- **Recur every days**: The interval in days at which signatures are downloaded, beginning on **Start**. Possible values: [1-999] (Default: 1)

System

Menu path: **Setup > System**

Here you can configure a number of basic system settings:

Date and Time

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

Here you configure time and date settings for the device.

- **Use IGEL Setup for configuring Time settings**
  - ☑ Time settings are made using theIGEL Setup.
  - ☐ Time settings are made in another manner.
- **Poll interval**: Choose the interval for polling network time.
  - One day
  - Two days
  - Three days
  - Four days
  - Five days
  - Six days
  - Seven days
- **Timezone**: Choose a timezone for the device, e.g. (GMT-08:00) Pacific Time (US and Canada)
- **Activate Timesync:**
  - ☑ System time is synchronized with a time server.
  - ☐ System time is not synchronized with a time server.
- **Timeserver**: Specify a timeserver (default: time.windows.com)

Update

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

Two procedures for updating the system are available:

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

_____

- Snapshots (see page 142)
- Partial Update (see page 147)

Snapshots

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

A snapshot is an image of the first partition (drive C:) which contains the *Windows 10 IoT* operating system. You can use this image either for system restoration or for distribution to other *IGEL devices with Windows 10 IoT* that are equipped with the same hardware. Firmware updates from *IGEL* too are made available as a snapshot file (`.snp`).

The *web server* of the *IGEL Universal Management Suite* can be used to create and install snapshots. Further information can be found in the UMS Manual under Universal Firmware Update.

_____

- Upload (see page 143)
- Download (see page 145)

Upload

Menu path: **System > Update > Snapshots > Upload**

Here you can create a snapshot of the current system.

- **Name of firmware for new snapshot**: This name will appear in in its own field in UMS.
- **Leave domain before snapshot**: Enable this option if the snapshot file is to be ported to another thin client.
  - ☑ The thin client will be taken from the domain before the snapshot is created.
  - ☐ The thin client will remain in the domain.
- **Protocol**: Protocol with which the snapshot file is uploaded to a server or saved in a local directory.
  Possible values:
  - File: The snapshot file will be saved locally, e.g. on a USB storage device.

  A local storage device must be NTFS-formatted. It needs to have 32 GB of free space. USB hard drvies, which Windows does not recognize as 'removable media', cannot be used for this purpose.
  - SMB: The snapshot file will be saved to a Windows network drive.
  - HTTP: The snapshot file will be saved to a WebDAV server (e.g. UMS).
  - HTTPS: The snapshot file will be saved to a WebDAV server (e.g. UMS) with transport encryption.

Fields for the File Protocol

- **File name**: File name of the snapshot file on the local storage device.

Fields for the SMB Protocol

- **File name**: File name of the snapshot file.
- **Server**: Host name or IP address of the server to which the snapshot file will be uploaded.
- **Share name**: Name of the Windows share.
  If you want to specify a path on the share, append it to **Share name**.
- **Username**: User name for the server to which the snapshot file will be uploaded.
  To supply a domain alongside the user name, use the following pattern. `DOMAIN\Username`.
- **Password**: Password for the server to which the snapshot file will be uploaded.

Fields for the HTTP and HTTPS Protocols

- **File name**: File name of the snapshot file.
- **Server**: Host name or IP address of the server to which the snapshot file will be uploaded.
- **Path**: Directory path for the snapshot file on the server. (Default: ums_filetransfer)
- **Port**: Port of the server to which the snapshot file will be uploaded. (Default: 9080 for HTTP, 8443 for HTTPS)
- **Proxy**: Host name or IP address of the proxy.
- **Port**: Port of the proxy. (Default: 1080)
- **Username**: User name for the server to which the snapshot file will be uploaded.

- **Password**: Password for the server to which the snapshot file will be uploaded.
- **New Snapshot**: Reboots the device, creates the snapshot file and saves it to the specified location.

Download

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

Here you can download and install a snapshot.

- **Reset Terminal Settings**
  ☑ After the reboot, the following data are reset or deleted:
  - The configuration parameters are reset to their defaults.
  - The *UMS* registration and the associated client-side certificate are deleted.
  - The user's data on drive F are deleted.
  The firmware licenses are retained.
  ☐ All data are retained.
- **Protocol**: Protocol with which the snapshot file is downloaded from a server or obtained from a local directory.
  Possible values:
  - File: The snapshot file will be obtained from a local storage device, e.g. from a USB storage device.
  - SMB: The snapshot file will be downloaded from a Windows network drive.
  - HTTP:The snapshot file will be downloaded from a WebDAV server (e.g. UMS).
  - HTTPS:The snapshot file will be downloaded from a WebDAV server (e.g. UMS) with transport encryption.

Fields for the File protocol

- **File name**: File name of the snapshot file on the local storage device

Fields for the SMB protocol

- **File name**: File name of the snapshot file
- **Server**: Host name or IP address of the server from which the snapshot file will be downloaded
- **Share name**: Name of the Windows share.
  If you want to specify a path on the share, append it to **Share name**.
- **Username**: User name for the server from which the snapshot file will be downloaded
  To supply a domain alongside the user name, use the following pattern. `DOMAIN\Username`.
- **Password**: Password for the server from which the snapshot file will be downloaded

Fields for the HTTP and HTTPS protocols

- **File name**: File name of the snapshot file
- **Server**: Host name or IP address of the server from which the snapshot file will be downloaded
- **Pfad**: Directory path for the snapshot file on the server. (default: ums_filetransfer)
- **Port**: Port of the server from which the snapshot file will be downloaded(default: 9080 for HTTP, 8443 for HTTPS)
- **Proxy**: Host name or IP address of the proxy
- **Port**: Port of the proxy (default: 1080)
- **Username**: User name for the server from which the snapshot file will be downloaded

- **Password**: Password for the server from which the snapshot file will be downloaded
- **Download Snapshot**: Loads the snapshot onto the thin client and begins a reboot.

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 10 IoT* without transferring the complete system via snapshot.

- **Use IGEL Setup for configuring partial update settings**
  - ☑ Partial update settings are configured in the IGEL Setup.
  - ☐ Partial update settings are configured in another manner.
- **Enable auto-update on boot**
  - ☑ The partial update will be installed automatically the next time that the thin client reboots.
  - ☐ Partial updates are not installed on reboot.

  > Auto-update on boot should only be enabled when required.

- **Protocol**: Protocol with which the partial update is downloaded from a server or obtained from a local directory
  Possible values:
  - HTTP: The partial update will be downloaded from a WebDAV server (e.g. UMS).

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

  - HTTPS: The partial update will be downloaded from a WebDAV server (e.g. UMS) with transport encryption.

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

  - File: The partial update will be obtained from a local storage device, e.g. from a USB storage device.
  - FTP: The partial update will be downloaded from an FTP server .
- **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..

  > The thin client notifies the *UMS* about installed partial updates, which will be listed in System Information.

For further information see Partial Update for IGEL Thin Clients with Windows Embedded Standard

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**:
  ☑ The thin client can be managed by UMS.
  ☐ Remote management is not allowed.
- **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 successfully contact a UMS.

  To add a further UMS instance , click
  ⊞
  14 Add
  :
  - **UMS Server**: Name or IP of the UMS server
  - **Port Number**: Port number of the UMS server. (default: 30001)
- **Enable User information:**
  ☑ A message window will inform the user that the client is receiving new settings from the UMS or is being shut down.
  ☐ The user will not be informed when 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.

Remote Access

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

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

_____

- Shadowing (see page 150)

Shadowing

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

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

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

- **Use IGEL Setup for configuring VNC server settings**
  - ☑ Shadowing is configured usingIGEL Setup.
  - ☐ Shadowing is configured in another manner.
- **Allow Remote Shadowing**:
  - ☑ Makes desktop contents viewable from remote computers via VNC
  - ☐ The desktop cannot be viewed remotely.
- **Enable IGEL secure VNC mode**:
  - ☑ Communication will be secured through SSL/TLS and shadowing will only be possible for *UMS* administrators.
  - ☐ VNC will not be encrypted and will be available to any VNC client.

  Further information regarding secure shadowing can be found in the Secure Shadowing (VNC with SSL/TLS) How-To.
- **Use password:**
  - ☑ Remote users must enter a password before they can begin shadowing.
  - ☐ No password is required.
    - **Password**: The password needed for shadowing.
- **Prompt user to allow remote session:**
  - ☑ The user is asked for permission before shadowing.
  - ☐ The user is not asked for permission.

  > 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**:
  - ☑ Remote users may make keyboard and mouse entries as if they were the local user.
  - ☐ No input from remote is allowed.
- **Maintenance screen: Show Image to hide Desktop** (Windows):
  - ☑ An image hides what is happening on the desktop during the VNC session.
  - ☐ No image is laid over the desktop.
    - **Path to image file:** Local file path, for example `F:\directory\image.png`

  You can transfer the required image file to the thin client using the UMS: UMS Manual > Files.

- **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

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

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[7].

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

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

requirements of the data to be written. The remaining physical RAM space is available to the system as regular RAM.

> 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

15 Add

.

▶ To remove an entry, click  .

▶ To edit an entry, click  .

▶ To copy an entry, click  .

- **List of registry excludes**: Insert registry keys that you want to exclude from the write filter here, 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.

Power Management

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

The usual energy saving options found in *Windows* are included in the *IGEL S*etup .

You can configure the following parameters:

- **Use IGEL Setup for configuring Power Management settings**
  - ☑ Power Management settings are configured using the IGEL Setup.
  - ☐ Power Managemenr is configured in another manner.
- **Turn off monitor:** Choose after which timespan of inactivity the monitor is turned off
  - After 10 minutes
    [...]
  - After 5 hours
  - Never
- **System Standby**:Choose after which timespan of inactivity the system is put into standby .
  - After 1 minutes
    [...]
  - Never
- **Prompt for password when computer resumes from standby**
  - ☑ The user must enter a password after standby.
  - ☐ The user does not need to enter a password.
- **Power Button Action**: Configure what happens when the power button is pressed
  - Shutdown
  - Standby
  - Do nothing

Firmware Customization

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

Here you can add custom applications to the system or activate and deactivate features.

_____

Custom Application

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

Here you can add custom applications to the system.

- List **Custom Applications**:

▶

To create an entry, click

16 Add

.

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

Adding an application

Desktop integration:

- **Session name**: Name of the session.

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

Session start options

- **Start menu**
  ☑ The session can be started with the start menu.
- **Desktop**
  ☑ The session can be started with a program starter on the desktop.
- **Autostart**
  ☑ The session will be launched automatically when the thin client boots.
- **Settings**
  - **Icon name**: Name of icon file for Desktop and Start menu
  - **Application**: Complete path to the executable, beginning with the drive letter, e.g. `C:\Program Files\Internet Explorer\iexplore.exe`
  - **Parameter**: Parameters for the application

Corporate Design

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

Here you can alter the look and feel of the system according to your corporate design.

_____

- Custom Bootpslash (see page 158)

Custom Bootpslash

Menu path: **Setup > System > Firmware Customization > Corporate Design > Custom Bootsplash**

In this area, you can define a custom bootsplash.

- **Use IGEL Setup for configuring a bootsplash ima´ge**
  ☑ The bootsplash defined in IGEL Setup is used.
  ☐ The bootsplash defined in IGEL Setup is not used. (Default)
- **Filename**: The absolute path to the bootsplash file.
  The bootsplash file can be in any of the following graphic formats:
  - PNG (Portable Network Graphics)
  - JPEG (Joint Photographic Experts Group)
  - GIF (Graphics Interchange Format)
  - SVG (Scalable Vector Graphics)

Features

Menu path: **Setup > System > Firmware Configuration > Features**

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

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

Features:

- Adobe PDF Reader
- Citrix ICA Client
- Fabulatech USB Redirection
- Microsoft Internet Explorer
- Microsoft RDP
- NCP Enterprise VPN Client
- VMware Horizon Client
- ThinPrint

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

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.

> Changes to the thin client configuration made in 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 using a snapshot.

- Click on **Parameter Search...** in order to search for specific parameters in the IGEL Registry.
- Search for the parameter name `wpa` if you require WPA encryption settings to secure your Wi-fi.

The parameter found in the structure is highlighted.

W10 IoT How-To

Updating the Firmware Without Using IGEL Setup or UMS (W10)

Symptom

The thin client's Windows system does not start up properly and you may want to re-install the firmware snapshot.

Problem

If the thin client's local setup cannot be used, and the thin client can not be contacted via IGEL Universal Management Suite either, the firmware snapshot cannot be installed in the usual way.

Solution

> These are the instructions for IGEL Windows 10 IoT. For IGEL Windows Embedded Standard 7 (WES7), please refer to the FAQ Updating the Firmware Without Using IGEL Setup or UMS (WES7).

Booting Into the Firmware Download Menu

1. Wait until the message `Booting, please wait` appears during the boot process.
2. Press the [Esc] key.
   A selection menu opens
3. Using the arrow keys, select **Download snapshot** and press [Return]
   The thin client boots IGEL Rescue Linux and opens the Firmware Download window. Here you can choose between different protocols for the firmware download.

Updating via the File Protocol

1. Save the unpacked snapshot file (`*.snp`) to a NTFS formatted USB stick.
2. Attach the USB stick to the thin client.
3. Optional: Enable **Reset Settings** if you want to reset the thin client settings
4. Optional: Enable **Reset User partition** if you want to erase all data on the `E:` drive
5. Select **File** as the **Protocol**.
6. Enter the Snapshot **Filename** or use the disk symbol to browse the USB stick.
7. Click **OK** to start the snapshot download, **Reset** to reset the input fields or **Discard and Reboot** to cancel the snapshot download and reboot the device.

Updating via the SMB Protocol

1. Put the unpacked snapshot file (`*.snp`) on a windows network share that is accessible to the thin client.
2. Optional: Enable **Reset Settings** if you want to reset the thin client settings
3. Optional: Enable **Reset User partition** if you want to erase all data on the `E:` drive
4. Select **SMB** as the **Protocol**

5. Enter the DNS name or IP address of the server into **Server.**
6. Enter the name of the Windows share into **Share.**

   > If you want to specify a path on the share, append it to **Share**.

7. Enter the **Username** for the server.

   > To supply a domain alongside the user name, use the following pattern. `DOMAIN\Username`.

8. Enter the **Password** for the server (tick the checkbox to make it readable)
9. Enter the name of the snapshot file into **Filename**.
10. Click **OK** to start the snapshot download, **Reset** to reset the input fields or **Discard and Reboot** to cancel the snapshot download and reboot the device.

Updating via the HTTP and HTTPS Protocols

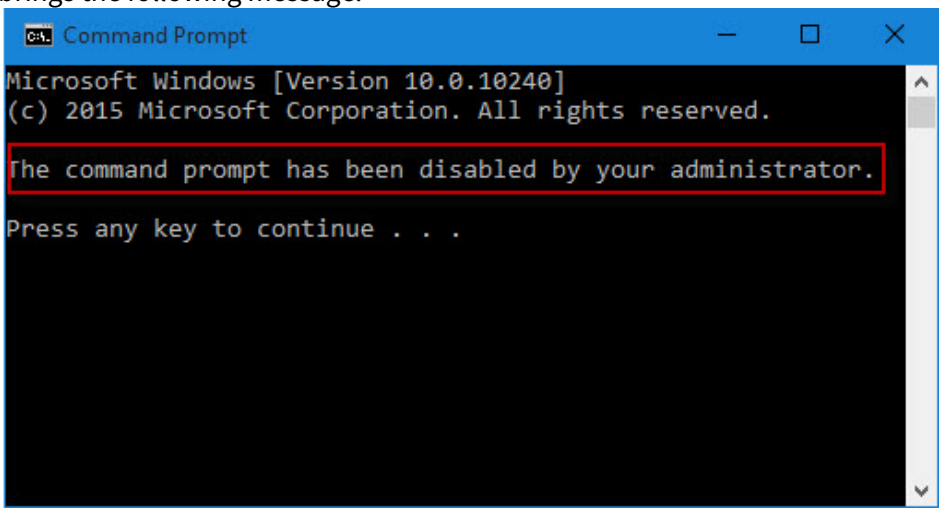
1. Put the snapshot file (`*.snp`) on an HTTP or HTTPS server. You can also use UMS to host Universal Firmware Update files.
2. Optional: Enable **Reset Settings** if you want to reset the thin client settings
3. Optional: Enable **Reset User partition** if you want to erase all data on the `E:` drive
4. Select **HTTP** or **HTTPS** as the **Protocol**.
5. Enter the DNS name or IP address of the server into **Server.**
6. Enter the TCP the server is listening on into **Port**. 9080 for HTTP, 8443 for HTTPS)
7. Enter the directory path on the server into **Path** (defaul(Defaultt: ums_filetransfer)
8. Optional: Enter the **Username** for the server
9. Optional: Enter the **Password** for the server (tick the checkbox to make it readable).
10. Optional: Enter the DNS name or IP address for a **Proxy**.
11. Optional. Enter a Proxyport : 1080)
12. Optional: Enter the **Proxyport** for the proxy.
13. Enter the Snapshot **Filename.**(default
14. Click **OK** to start the snapshot download, **Reset** to reset the input fields or **Discard and Reboot** to cancel the snapshot download and reboot the device.

Enabling CMD/CommandPrompt for Windows Users

Issue

The IGEL Windows firmware has the following standard configuration for the two user types:

- **Administrator**: CMD can be fully called and executed. Also displayed in the Windows Start menu.
- **User**: CMD is not displayed in the start menu. By typing in "CMD" manually, it can be called and brings the following message:

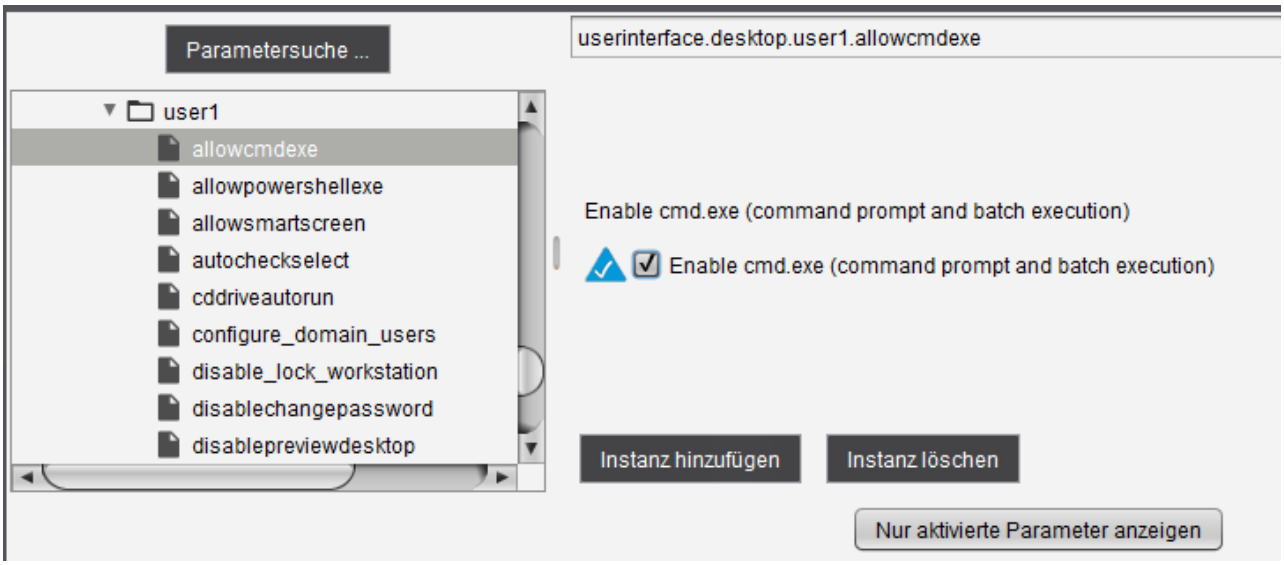


Even changes in the settings of the following parameters do not lead to the desired result:

- **User Interface > Desktop > Users > Hide the run command on start menu**
- **User Interface > Start menu > Users > Show run on start menu**

Solution

If you want to allow/prevent execution of the command prompt (cmd.exe), use the egistry key `userinterface.desktop.user1.allowcmdexe` :



USER1 = **User**
USER0 = **Administrator**

W10 IoT Tips & Tricks

Removing Thin Clients from a Domain

Issue

The WES7 thin client is joined to a domain and has to be removed from the domain.

Problem

Simply resetting the thin client's configuration will result in orphaned entries on the domain controller.

Solution

A thin client has to leave the domain it is joined to before resetting the client's configuration. A thin client can also leave the domain without resetting the configuration.

Removing the thin client from a domain without resetting its configuration:

1. In the IGEL Setup (or the UMS) navigate to **Security > Active Directory**.
2. Disable **Thin Client is member of a domain**.
3. Do not remove the domain logon data now.
4. Save the changes with **Apply** or **OK**.
   The thin client will leave the domain. You may now remove the domain logon data.

Removing the thin client from a domain when resetting its configuration (implies installing a snapshot):

1. In the IGEL Setup (or the UMS) navigate to **System > Update > Snapshots**.
2. Enable **Reset Terminal Settings**.
3. Enable **Leave domain before snapshot**.
4. Configure all necessary snapshot data depending on your snapshot source.
5. Do not remove the domain logon data (**Security > Active Directory**).
6. Save the changes with **Apply** or **OK**.
7. Launch the update process via **Download Snapshot** in local setup or UMS.
   The thin client will leave the domain, install the snapshot and reset all configuration parameters to the factory default settings.

Updating the Firmware Using a USB Storage Device

Issue

You want to update the thin client's firmware locally (without *IGEL Universal Management Suite* or HTTP/FTP server).

Solution

You can use a USB storage device to update the firmware locally. This method is particularly suitable if only one device or only a few thin clients are to be updated and it would not be worth installing an FTP or HTTP server purely for the update.

Procedure for Windows 10 IoT

1. Download the update file (.zip) for your device from the IGEL download server[8].
2. Unpack the update file.
   A snapshot file (.snp) is created.
3. Save the snapshot file (.snp) on an NTFS-formatted USB storage device.
4. Configure the firmware update in the local setup under **System > Update > Snapshots > Download**:
   a. Select **File** the **Protocol** selection box.
   b. Enter the **File name** of the snapshot file (.snp) you want to download and install.
   c. [optional] Enable **Reset IGEL configuration settings** in order to reset all configuration parameters to the factory default settings.
   d. [optional] Enable **Reset User partition** in order to delete all files on the user partition `E:`
   e. **Apply** the changes so that they are effective for the thin client.
5. Connect the USB storage device to the thin client and wait until the device has been detected.
6. Launch the update process via **Download Snapshot**.
   Download and installation of the update will begin.

   > Do not interrupt the update process when it is in progress. This can result in system inconsistencies. Do not remove the USB device until the update has finished.

8 https://www.igel.com/software-downloads/

Updating the Firmware via Customized Snapshot

This is relevant for IGEL WES 7 and IGEL W10.

You can update the thin client's firmware globally (without USB storage device).

With a master client you can create a customized snapshot of the firmware and use HTTPS via the UMS to roll it out globally. This method is particularly suitable if many thin clients are to be updated.

Take the following steps:

▶ Make one Windows device your master client and load it with all the required certificates, settings and installations.

▶ Create a profile in the UMS.

▶ Assign the profile to the master client and to the recipient clients.

Creating a New "Customized Snapshot" Profile in the UMS

1. In the thin client configuration go to **System > Update > Snapshots > Upload**.
2. Select `HTTPS` as **Protocol**.
3. Enter the name of your UMS **Server**.
4. Enter `ums-filetransfer` as **Path**.
5. Enter the **File Name** of your new snapshot, e. g. `snapshot_file.snp`
6. Enter the **Name of Firmware for new Snapshot**, e. g. `UniversalDesktopWES-3.13.100.snp`
7. Enter **User Name** and **Password**.
8. In the thin client configuration go to **System > Update > Snapshots > Download**.
9. Enter the same **File Name** as in the upload entry, here: `snapshot_file.snp`
10. Click **Save** to finish the creation of the profile.

Assigning the Profile to the Master Client and to the Recipient Clients

1. In the UMS navigation tree, right-click the master client.
2. Select **Update & snapshot commands > Create Firmware Snapshot**.
   The snapshot is stored in the ums-filetransfer.
3. Right-click the recipient clients.
4. Select **Update & snapshot commands > Download Firmware Snapshot**.
   The snapshot is downloaded and installed.

   > Do not interrupt the update process. This can result in system inconsistencies. Do not remove the USB device until the update has finished.

   See also: Updating the Firmware Using a USB Storage Device (see page 168).

Exporting and Importing Printer Settings

Issue
How can I configure a printer in my W10 device using the local *IGEL Setup* or *IGEL Universal Management Suite*?

Solution
Prerequisite:

A printer has already been installed to the system via **Settings > Devices > Printers & Scanners**.

Printer configuration in *IGEL Setup* or *UMS*:

1. Go to **Devices > Printer > Printer >**
   
   17 Add
   .
2. Specify the exact **Printer name** and
   - either configure your printer settings
   - or specify path to a printer settings file.

Export the current printer configuration:

1. Open a local shell (command prompt) on the device.
2. Execute command
   `rundll32 printui.dll,PrintUIEntry /Ss /n "PRINTERNAME" /a "SETTINGSFILE"`

Example: `rundll32 printui.dll,PrintUIEntry /Ss /n "hp deskjet 940c series" /a hp_settings.dat`

Legal Note

IGEL's Terms & Conditions[9] apply.

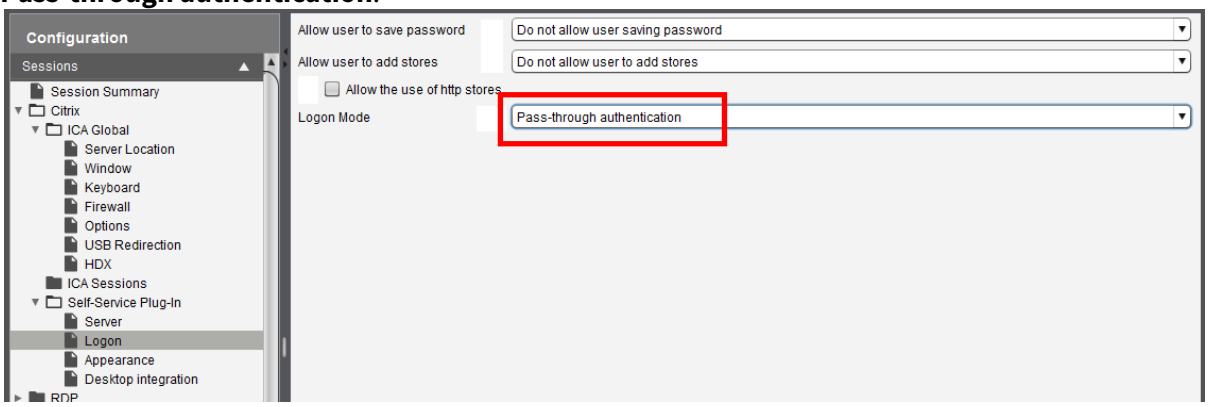
9 https://www.igel.com/terms-conditions/

Single Sign-On with AD Login and Citrix Self-Service Plugin

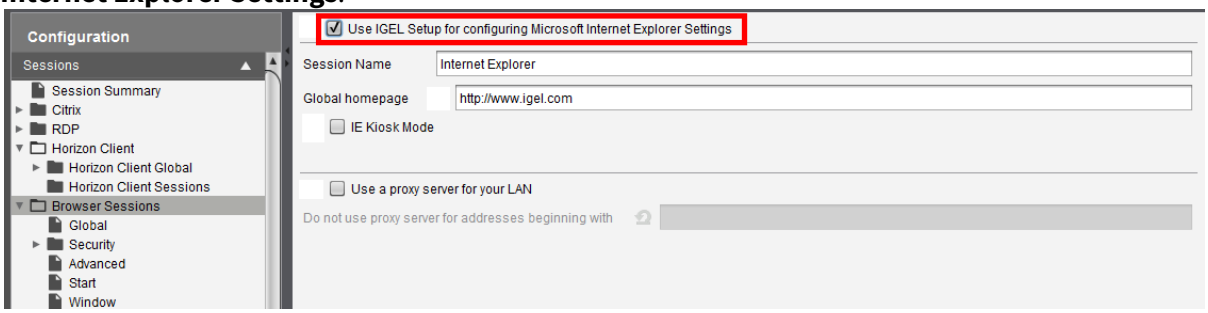
You can configure Single-Sign On for Citrix sessions for users who have an Active Directory (AD) account.

To configure single sign-on:

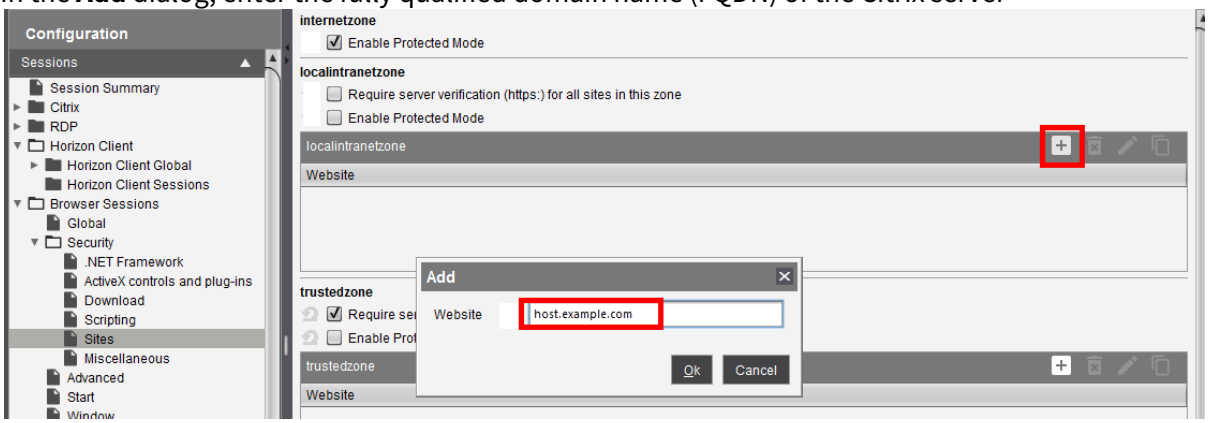
1. Open the Setup, go to **Sessions > Citrix > Self-Service Plug-In > Logon** and set Logon mode to **Pass-through authentication**.



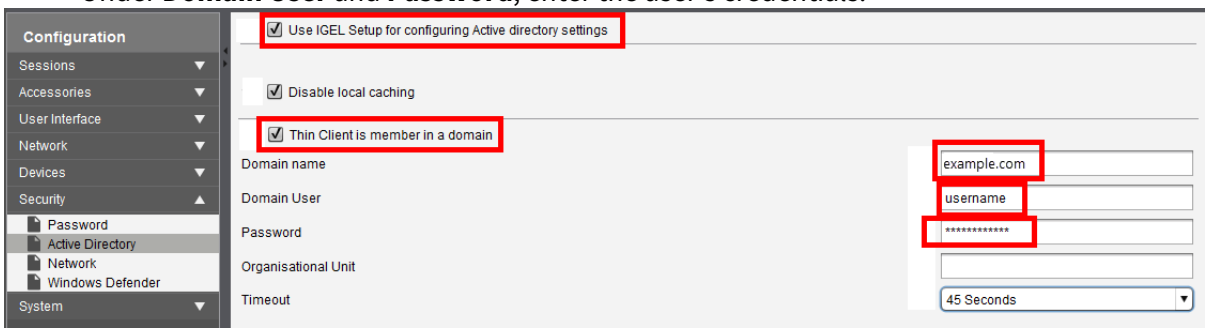
2. Go to **Sessions > Browser Sessions** and activate **Use IGEL Setup for configuring Microsoft Internet Explorer Settings**.



3. Go to **Sessions > Browser Sessions > Security > Sites** and click
   ⊞
   18 Add
   in the area **localintranetzone**.
4. In the **Add** dialog, enter the fully qualified domain name (FQDN) of the Citrix server



5. Go to **Securiy > Active Directory** and make the following settings:
   - Activate **Use IGEL Setup for configuring Active directory settings**.
   - Activate **Thin Client is member in a domain**.
   - Enter the **Domain name** of the user's AD domain.
   - Under **Domain User** and **Password**, enter the user's credentials.



6. Reboot the device.
   After reboot, the device will join the domain you have specified. The user can login to the device using his AD credentials. When the user starts a Citrix session, his AD credentials will be reused; no further data entry is required.

W10 IoT Troubleshooting

Using Thin Print with VMware Horizon

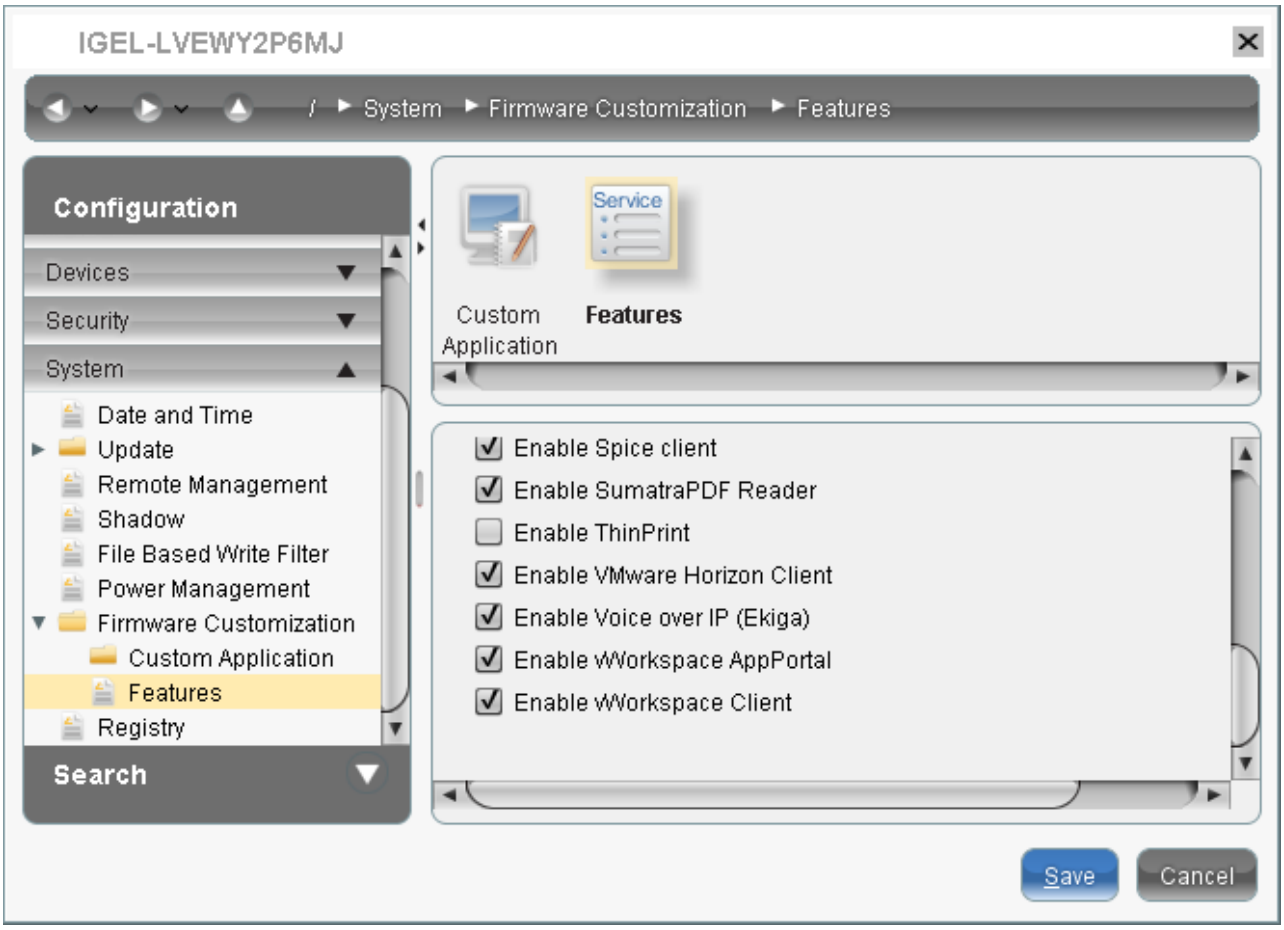
Environment
Valid for WES 2009, WES7 and Windows 10 IoT

Symptom
You cannot use *Thin Print* with *VMware Horizon*.

Problem
IGEL Universal Desktop Windows Embedded contains two different *Thin Print* implementations:

- a stand-alone client with plugins for ICA and RDP sessions (active by default)
- another implementation that is embedded in the *VMware Horizon* client with plugins for RDP and PCoIP

Solution
In oder to use *Thin Print* with *VMware Horizon*, deactivate the stand-alone client by unchecking **Enable Thin Print** under **System > Firmware Customization > Features** in *IGEL* setup.



10 https://www.igel.com/terms-conditions/

Adding a Printer on a Windows 10 IoT / Windows Embedded Thin Client

Symptom

A local printer configured on a thin client with Windows 10 IoT / *Windows Embedded Standard* disappears after a reboot.

Problem

How can you add a printer permanently?

Solution

1. For *Windows 10 IoT*: Disable the Unified Write Filter (UWF) under **System > Unified Write Filter** in IGEL Setup. For *Windows Embedded Standard 7*: Disable the *File Based Write Filter* (FBWF) under **System > File Based Write Filter** in *IGEL* Setup.
2. Reboot the thin client.
3. Add the printer via **Settings > Devices > Printers & Scanners** (*Windows 10 IoT*) resp. Windows **Control Panel > Devices and Printers** (*Windows Embedded Standard*).
4. Enable the Unified Write Filter (*Windows 10 IoT*) resp. the *File Based Write Filter* (*Windows Embedded Standard 7*).
5. Reboot the thin client.

Do not forget to enable the UWF resp. FBWF again after adding the printer. Running a thin client with permanently disabled write filter is not supported.

Various Issues When Thin Clients Wakes After Longer Period in Sleep Mode

Environment: *IGEL Windows 10 IoT 4.02.100*

Issue

When the thin client wakes after a longer period of time in sleep mode, e. g. over the weekend, various anomalies are experienced.

Examples include:

- The logon screen is missing.
- After logon, the start menu is missing.
- When you sign out, the "Signing out" screen appears, but never finishes.
- ...

Cause

The problem is caused by the combined use of the Unified Write Filter (UWF) and Windows Defender. As of *Windows 10 IoT 4.02.100*, Windows Defender antimalware definition updates are enabled by default. At the same time, it is normal behavior of the UWF that the overlay will grow no matter a path is excluded from the UWF. When Windows Defender definition updates are executed, the overlay usage grows to about a few hundred megabytes. This causes excess memory consumption, which results in the described anomalies.

You can learn more in the chapter Unified Write Filter (UWF).

Solution

The recommended solution is to configure Windows Defender for scheduled definition updates with IGEL Setup, see Windows Defender. In schedule mode, the UWF is automatically deactivated during definition updates.

11 https://www.igel.com/terms-conditions/

No Activation after Snapshot Has Been Installed

Problem

You have downloaded and installed a new Windows IoT 10 Snapshot, but the activation could not be restored. As a result, your Windows desktop shows a watermark and a message that Windows is not activated.

Lösung

1. Right-click in the Windows taskbar  and select **Enable Windows**.
   If the write filter is activated, a corresponding message appears.
2. If the write filter is enabled, open the setup, go to **System > Unified Write Filter** and deactivate **Enable UWF**.
3. Restart the thin client.
4. Select **Enable Windows**.
5. Restart the thin client.
6. Select **Enable Windows again**.
   The activation should be successful. If not, you can try restarting the thin client and reactivating Windows.

Snapshot Download Stops Before Finished

Issue

In the UMS, snapshot downloads via HTTP do not finish, but stop after a few seconds.

Solution

Use a download method other than HTTP, e.g. HTTPS.

W10 IoT Release Notes

Notes for Release 4.04.100

IGEL Universal Desktop W10

Software:	Version	4.04.100
Release Date:	2019-05-31	
Release Notes:	Version	RN-404100-1
Last update:	2019-05-31	

Supported Devices

Supported Devices

UD3-W10 50, UD3-W10 51

UD5-W10 50

UD6-W10 51

UD7-W10 10

UD9-W10 40, UD9-W10 Touch 41

Versions

- **Drivers**

Product	Version
Intel(R) HD Graphics	10.18.10.4425 (04/04/2016)
Intel(R) Audio	6.16.00.3154 (09/09/2014)
Intel(R) Trusted Execution Engine Interface	1.1.0.1064 (12/01/2014)
Realtek High Definition Audio	6.0.1.7541 (06/18/2015)
Realtek PCIe GBE Family Controller	10.014.0123.2017 (01/23/2017)
AMD Radeon(TM) R3E Graphics	16.300.2501.0000 (07/26/2016)
AMD IOIC device	1.2.0.0034 (11/08/2015)
AMD Security Accelerator	2.22.0.0005 (06/27/2016)
AMD GPIO v2 Controller	2.2.0.57 (04/01/2017)
AMD SMBus device	5.12.0.0031 (04/01/2017)
AMD Embedded Radeon E9173	23.20.808.1280 (02/14/2018)

- **Applications**

Citrix Workspace App	1903
Citrix HDX RealTime Media Engine	2.7
Microsoft Internet Explorer	11
Microsoft RDP Client	10.2
NCP Enterprise Client	10.11
Azul Zulu JAVA RE	1.8.0.212
ThinPrint	11.0.120
Tight VNC Server	2.8.11
VMware Horizon Client	5.0.0
Microsoft Windows Media Player	12
Microsoft .NET Framework	4.6
Adobe PDF Reader DC	15.23
FabulaTech USB for Remote Desktop	5.2.3

IGEL WinLinux	11.01.110.13828

- **Language Packs**

Microsoft-Windows-Client-Language-Pack_x64_de-de.cab
Microsoft-Windows-Client-Language-Pack_x64_es-es.cab
Microsoft-Windows-Client-Language-Pack_x64_fr-fr.cab
Microsoft-Windows-Client-Language-Pack_x64_it-it.cab
Microsoft-Windows-Client-Language-Pack_x64_ja-jp.cab
Microsoft-Windows-Client-Language-Pack_x64_nl-nl.cab

- **Microsoft Updates**

KB4493473
KB4493478
KB4346087
KB4485447
KB4465659
KB4132216
KB4093137

Known Issues

System

- **Start onscreen keyboard at logon** does not work.
  The Setup setting **User Interface > Input > Keyboard > Start onscreen keyboard at logon** sets the onscreen keyboard for a logged-in user only.
  Furthermore, the **Ease of Access** menu on welcome screen appears delayed and an error message is shown: *Could not start On-Screen keyboard <OK>.*
- **VNC Maintenance** screen does not work.
- **Snapshot upload/download** via **Proxy** does not work.
- **Snapshot download** with **HTTP** protocol and **UMS version 5.08.100** does not work on **UD7**.

VMware

- When session is started via **Horizon Client**, a folder named **GPUcache** appears on the user desktop.

New Features

System

- Added **OpenJDK Zulu** from **Azul 1.8.0.212**.
- Added a list of **installed (third party) software** in **IGEL Device Information**.

Citrix

- Added **Citrix Workspace App** version **1903**.
- Added **Citrix HDX Realtime Media Engine** version **2.7**.

VMware

- Added **VMware Horizon Client** version **5.0.0**.

Resolved Issues

System

- Fixed: **IGEL Device Information** tool does not update **network information**. **IP address of the device** will now be **updated every ten seconds**.
- Fixed: **Session shortcuts** are not deleted after removing a **UMS profile** or disabling **Use IGEL Setup for configuring...**
- Fixed: **Windows Defender definitions** can not be updated after deactivating the **Unified Write Filter**.
- Fixed: **File share for downloading definition updates** always disabled.
- Fixed: **reboot loops** while configuring the **Unified Write Filter**.
  Reboot loops were caused by:
  - Multiple entries with **different notations** like **c:\temp** and **C:\Temp**.
  - **Incorrect notations** like relative paths, e.g. **/temp** or **temp**.
- Fixed: **Snapshot** is only possible without any **whitespaces in path/filename** entry.
- Fixed: **File snapshot** does not work with **enabled Unified Write Filter** feature and **plugged-in USB** sticks. **USB** sticks **have** now **to be removed** after snapshot upload/download and before returning to Windows.

Notes for Release 4.03.100

IGEL Universal Desktop W10

Software:	Version	4.03.100
Release Date:	2018-11-26	
Release Notes:	Version	RN-403100-1
Last update:	2018-11-26	

Supported Devices

Supported Devices

UD3-W10 50, UD3-W10 51

UD5-W10 50

UD6-W10 51

UD7-W10 10

UD9-W10 40, UD9-W10 Touch 41

Versions

- **Drivers**

Product	Version
Intel(R) HD Graphics	10.18.10.4425 (04/04/2016)
Intel(R) Audio	6.16.00.3154 (09/09/2014)
Intel(R) Trusted Execution Engine Interface	1.1.0.1064 (12/01/2014)
Realtek High Definition Audio	6.0.1.7541 (06/18/2015)
Realtek PCIe GBE Family Controller	10.014.0123.2017 (01/23/2017)
AMD Radeon(TM) R3E Graphics	16.300.2501.0000 (07/26/2016)
AMD IOIC device	1.2.0.0034 (11/08/2015)
AMD Security Accelerator	2.22.0.0005 (06/27/2016)
AMD GPIO v2 Controller	2.2.0.57 (04/01/2017)
AMD SMBus device	5.12.0.0031 (04/01/2017)
AMD Embedded Radeon E9173	23.20.808.1280 (02/14/2018)

- **Applications**

Citrix Workspace App	1808
Citrix HDX RealTime Media Engine	2.6
Microsoft Internet Explorer	11
Microsoft RDP Client	10.2
NCP Enterprise Client	10.11
Sun JAVA RE	1.8 Update 40
ThinPrint	11.0.120
Tight VNC Server	2.8.11
VMware Horizon Client	4.9.0
Microsoft Windows Media Player	12
Microsoft .NET Framework	4.6
Adobe PDF Reader DC	15.23
FabulaTech USB for Remote Desktop	5.2.3

IGEL WinLinux	10.06.100.10195

- **Language Packs**

Microsoft-Windows-Client-Language-Pack_x64_de-de.cab
Microsoft-Windows-Client-Language-Pack_x64_es-es.cab
Microsoft-Windows-Client-Language-Pack_x64_fr-fr.cab
Microsoft-Windows-Client-Language-Pack_x64_it-it.cab
Microsoft-Windows-Client-Language-Pack_x64_ja-jp.cab
Microsoft-Windows-Client-Language-Pack_x64_nl-nl.cab

- **Microsoft Updates**

KB4462928
KB4091644
KB4132216
KB4093137

Known Issues

System

- Start **onscreen keyboard** at logon does not work. The TC-Setup setting **Userinterface > Input > Keyboard > Start onscreen keyboard at logon** sets the onscreen keyboard for a logged in user only.
  Furthermore the **Ease of Access** menu on welcome screen appears delayed and an error message is shown: *Could not start On-Screen keyboard <OK>*
- **VNC Maintenance** screen does not work.
- **Snapshot upload/download** via **File** protocol does not work if the USB device is plugged into a USB 3.0 port.
- **Snapshot upload/download** via **Proxy** does not work.

VMware

- When session is started via **Horizon client**, a folder named **GPUcache** appears on the user desktop.

New Features

System

- Added support for **UEFI Secure Boot**.
  IMPORTANT: With enabled UEFI Secure Boot, it is not possible to downgrade to a W10 firmware version lower than 4.03.100!
  https://kb.igel.com/securitysafety/uefi-secure-boot-enabling-guides-2271735.html
- Added information about **current boot mode** into **IGEL Device Information** tool (Hardware tab).
- Added information about **current Microsoft Windows activation state** into **IGEL Device Information** tool (Windows Activation tab).
- Added command to **activate Windows** into **IGEL Device Information** tool.
- Added command to **save support information** into **IGEL Device Information** tool.
- Added configuration of **ForceAutoLogon**. **IMPORTANT**: After setting "resetforceautologon" to "false" the login process can not be interrupted!
  More...

Parameter	Reset Force-Auto Logon
Registry	`system.auto_logon.resetforceautologon`
Value	enabled / disabled

- Added **network speed information** of Windows Client to display and use in UMS.
- Added **FTP snapshot protocol**.
  More...

  System > Update > Snapshots > Upload

  System > Update > Snapshots > Download

Parameter	Server
Registry	`firmware_snapshot.ftp.server`
Parameter	Path
Registry	`firmware_snapshot.ftp.path`
Parameter	Filename
Registry	`firmware_snapshot.ftp.upload_filename` `firmware_snapshot.ftp.download_filename`
Parameter	Username
Registry	`firmware_snapshot.ftp.username`

Parameter	Password
Registry	`firmware_snapshot.ftp.crypt_password`

Parameter	Port
Registry	`firmware_snapshot.ftp.port`
Value	21

Parameter	Proxy
Registry	`firmware_snapshot.ftp.proxy`

Parameter	Port
Registry	`firmware_snapshot.ftp.proxy_port`
Value	2121

Citrix

- Added **Citrix Workspace App version 1808**
- Added **Citrix HDX Realtime Media Engine version 2.6**

VMware

- Added **VMware Horizon client version 4.8.1**

VNC

- Added **TightVNC Server version 2.8.11**

Resolved Issues

System

- Fixed configured **IP address** is not used in IGEL Rescue Shell.
- Fixed configured **UWF exclusions results** in a bootloop.
- Fixed issues with **multi-monitor configuration** on UD7.
- Fixed **UMS shutdown/reboot command** does not work after disable "Prompt user on UMS actions".
- Fixed strange characters are shown when using **Swedish(Sweden)** at "Standards and Formats".
- Fixed **device drivers are updated automatically** when UWF is disabled on UD3.

VMware

- Fixed issues with **USB redirection**.

Notes for Release 4.02.100

IGEL Universal Desktop W10

Software:	Version	4.02.100
Release Date:	2018-05-11	
Release Notes:	Version	RN-402100-1
Last update:	2018-05-11	

Following formatting is used in this document:

format type	example	use
bold and underlined	enable/disable	the default setting of a value
bold and arrow	**menu → path**	menu path in the IGEL setup
bold	**GUI** [keyboard]	elements of the graphical user interface or commands that are entered using the keyboard
within brackets	**[session name]**	variable values

Windows 10 IoT

Supported Devices

UD3-W10 50, UD3-W10 51

UD5-W10 50

UD6-W10 51

UD7-W10 10

UD9-W10 40, UD9-W10 Touch 41

W10 IoT Versions

- **Drivers**

Product	Version
Intel(R) HD Graphics	10.18.10.4425 (04/04/2016)
Intel(R) Audio	6.16.00.3154 (09/09/2014)
Intel(R) Trusted Execution Engine Interface	1.1.0.1064 (12/01/2014)
Realtek High Definition Audio	6.0.1.7541 (06/18/2015)
Realtek PCIe GBE Family Controller	10.014.0123.2017 (01/23/2017)
AMD Radeon(TM) R3E Graphics	16.300.2501.0000 (07/26/2016)
AMD IOIC device	1.2.0.0034 (11/08/2015)
AMD Security Accelerator	2.22.0.0005 (06/27/2016)
AMD GPIO v2 Controller	2.2.0.57 (04/01/2017)
AMD SMBus device	5.12.0.0031 (04/01/2017)
AMD Embedded Radeon E9173	23.20.808.1280 (02/14/2018)

- **Applications**

Citrix Receiver	4.11
Citrix HDX RealTime Media Engine	2.3
Microsoft Internet Explorer	11
Microsoft RDP Client	10.2
NCP Enterprise Client	10.11
Sun JAVA RE	1.8 Update 40
ThinPrint	11.0.120
Tight VNC Server	2.7.10
VMware Horizon Client	4.7.0
Microsoft Windows Media Player	12
Microsoft .NET Framework	4.6
Adobe PDF Reader DC	15.23
FabulaTech USB for Remote Desktop	5.2.3

- **Language Packs**

Microsoft-Windows-Client-Language-Pack_x64_de-de.cab
Microsoft-Windows-Client-Language-Pack_x64_es-es.cab
Microsoft-Windows-Client-Language-Pack_x64_fr-fr.cab
Microsoft-Windows-Client-Language-Pack_x64_it-it.cab
Microsoft-Windows-Client-Language-Pack_x64_ja-jp.cab
Microsoft-Windows-Client-Language-Pack_x64_nl-nl.cab

- **Microsoft Updates**

KB4093137
KB4093120

Known Issues

System

- **Start onscreen keyboard at logon** does not work.
  The TC-Setup-Setting Userinterface/Input/Keyboard **Start onscreen keyboard at logon** sets the onscreen keyboard for a logged in user only.
  Furthermore the **Ease of Access** menu on welcome screen appears delayed and an error message is shown: "Could not start On-Screen keyboard "
- **VNC Maintenance screen** does not work.
- Snapshot **upload/download via "File" protocol** does not work on UD3/UD7 if the USB device is plugged into a USB 3.0 port.
- **Configuration of more than two screens** sometimes results in a wrong display order on UD7.

VMware

- When session is started via **Horizon client**, a folder named **GPUcache** appears on the user desktop.

New Features

System

- Added hardware support for **UD7-W10 10**.
- Added hardware support for **UD9-W10 40 and UD9-W10 Touch 41**.
- Added configuration of **Windows activation** while snapshoting.
  More

Registry	firmware_snapshot.activate_windows
Value	enabled / disabled

- Added **file transfer of certificate files** from UMS.
- Added configuration of **custom desktop background picture**.
  More

IGEL Setup	**User Interface > Desktop**
Registry	userinterface.customization.use_custom_wallpaper
Value	enabled / disabled

IGEL Setup	**User Interface > Desktop**
Registry	userinterface.customization.custom_wallpaper_filename
Value	

- Added configuration of **custom boot splash picture**.
  More

IGEL Setup	**System > Firmware Customization > Corporate Design > Custom Bootsplash**
Registry	userinterface.customization.use_custom_bootsplash
Value	enabled / disabled

IGEL Setup	**System > Firmware Customization > Corporate Design > Custom Bootsplash**
Registry	userinterface.customization.custom_bootsplash_filename
Value	

- Added configuration of **Microsoft Windows Defender**.
  More

IGEL Setup	**Security > Windows Defender**
Registry	system.windows_defender.use_igel_setup
Value	enabled / disabled

IGEL Setup	**Security > Windows Defender**
Registry	system.windows_defender.enable
Value	enabled / disabled

IGEL Setup	**Security > Windows Defender**
Registry	system.windows_defender.definition_download
Value	enabled / disabled

IGEL Setup	**Security > Windows Defender**
Registry	system.windows_defender.definition_download_scheduled_timestamp
Value	

IGEL Setup	**Security > Windows Defender**
Registry	system.windows_defender.definition_download_scheduled_recur_every_days
Value	1

IGEL Setup	**Security > Windows Defender**
Registry	system.windows_defender.definition_download_source
Value	MicrosoftUpdateServer

IGEL Setup	**Security > Windows Defender**
Registry	system.windows_defender.definition_download_source_file_shares
Value	

IGEL Setup	**Security > Windows Defender**
Registry	system.windows_defender.update_timeout
Value	600000

- Added **Unified Write Filter** low overlay watcher.
  More

Registry	system.uwf.ramcheck_showwarning
Value	enabled / disabled

Registry	system.uwf.ramcheck_threshold
Value	250

Registry	system.uwf.ramcheck_interval_seconds
Value	60

Registry	system.uwf.ramcheck_observation_seconds
Value	30

Citrix

- Added **Citrix Receiver version 4.11**
- Added **Citrix HDX RealTime Media Engine version 2.3**

VMware

- Added **VMware Horizon client version 4.7.0**

FabulaTech

- Added **FabulaTech USB for Remote Desktop version 5.2.3**

Resolved Issues

System

- Fixed **IGEL Secure Shadowing** does not work.
- Fixed unclear **unjoin domain behaviour**. Client is added to Workgroup "WORKGROUP" after leaving the domain now.
- Fixed **UMS file transfer** without setting a target path does not work (Default target path: C:\Program Files (x86)\IGEL\igel_temp).
- Fixed **after creating a snapshot** with a device registered in UMS and applying it to another device, **same MAC address** is shown in UMS.
- Fixed **after a snapshot download old partial update informations will remain in the UMS**.
- Fixed **reset to factory defaults** does not work if auto logon is configured.
- Fixed **error in dual screen configuration** when only one monitor is connected.
- Fixed **disable USB storage devices** does not work.
- Fixed **VNC shadowing** does not work after changing the admin password.
- Fixed watching **videos with Microsoft Internet Explorer fills up the Unified Write Filter RAM overlay**.

RDP

- Fixed **configuration of credential saving on connect** has no effect.
  More

Registry	rdp.winconnect.allowcredentialsaving
Value	enabled / disabled

Citrix

- Fixed **deletion of ICA session** does not delete **session icons** from desktop.
- Fixed **lockdown conflict** "LegacyLocalUserNameAndPassword" after configuring domain passthrough authentication.

VMware

- Fixed **VMware session autostart** does not work.

Notes for Release 4.01.100

IGEL Universal Desktop W10

Software:	Version	4.01.100
Release Date:	2017-05-15	
Release Notes:	Version	RN-301100-1
Last update:	2017-05-15	

Following formatting is used in this document:

format type	example	use
bold and underlined	enable/disable	the default setting of a value
bold and arrow	**menu → path**	menu path in the IGEL setup
bold	**GUI** [keyboard]	elements of the graphical user interface or commands that are entered using the keyboard
within brackets	**[session name]**	variable values

Windows 10 IoT

Supported Devices

UD5-W10

UD6-W10

W10 IoT Versions

- **Clients**

Product	Version
Intel(R) HD Graphics	10.18.10.4425 (04/04/2016)
Intel(R) Audio	6.16.00.3154 (09/09/2014)
Intel(R) Trusted Execution Engine Interface	1.1.0.1064 (12/01/2014)
Realtek High Definition Audio	6.0.1.7541 (06/18/2015)
Realtek PCIe GBE Family Controller	10.014.0123.2017 (01/23/2017)

- **Applications**

Citrix Receiver	4.7
Citrix HDX RealTime Media Engine	2.2.100
Microsoft Internet Explorer	11
Microsoft RDP Client	10.2
NCP Enterprise Client	10.11
Sun JAVA RE	1.8 Update 40
ThinPrint	11.0.120
Tight VNC Server	2.7.10
VMware Horizon Client	4.4.2
Microsoft Windows Media Player	12
Microsoft .NET Framework	4.6
Adobe PDF Reader DC	15.23

- **Language Packs**

Microsoft-Windows-Client-Language-Pack_x64_de-de.cab
Microsoft-Windows-Client-Language-Pack_x64_es-es.cab
Microsoft-Windows-Client-Language-Pack_x64_fr-fr.cab
Microsoft-Windows-Client-Language-Pack_x64_it-it.cab
Microsoft-Windows-Client-Language-Pack_x64_ja-jp.cab
Microsoft-Windows-Client-Language-Pack_x64_nl-nl.cab

- **Microsoft Updates**

KB3150513
KB4013418
KB4015217
KB4018483

Known Issues

System

- **Start onscreen keyboard at logon** does not work.
  The TC-Setup-Setting Userinterface/Input/Keyboard "Start onscreen keyboard at logon" sets the onscreen keyboard for a logged in user only. Furthermore the "Ease of Access" menu on welcome screen shows up delayed and an error message appears: "Could not start On-Screen keyboard "
- **VNC Maintenance screen** does not work.