Endpoint Management (UMS)

Installation and Configuration

UMS Installation and Update (see page 202), Database (see page 202), Requirements (see page 203), Connecting to the UMS (see page 228), User Management (see page 510), UMS Administration (see page 422), Getting Started (see page 5)

Licenses

Automatic License Deployment, UMS Licenses (see page 433), Devices' Licenses (see page 434)

Endpoint Devices Deployment

Registering Devices (see page 229), Mobile Devices (see page 439), Configuring (see page 366) and Managing Devices (see page 356)

User Assistance

Support Information (see page 263), VNC (see page 385), Shadowing (see page 383), Terminal (see page 379), Messages (see page 269), Logging (see page 503)

Endpoint Configuration

Using Profiles (see page 281), Master Profiles (see page 319), Template Profiles (see page 321), Effectiveness of Settings (see page 280)

Firmware Management

Firmware Update (see page 415), Export Firmwares (see page 370), Import Firmwares (see page 371), Check for new Universal Firmware Updates (see page 416)

Custom Design

Themes (see page 256), Background Images (see page 348), Firmware Customizations (see page 339)

Views and Searches

Quick Search (see page 273), Views (see page 390), Search with regular expressions (see page 188)

UMS Articles

Getting Started: Setting Up the UMS

Problem

You want to set up the UMS for the first time and you are not sure how to proceed.

Goal

The aim is not only to install the UMS, but also to achieve a solid setup of the most important features.

Solution

We will show you an easy method for best practice setup with the following steps:

> You can also use the **IGEL Software Suite: Step-by-Step Getting Started Guide** provided by the IGEL Community[1]. Its goal is to provide you with the tools, knowledge, and understanding of how to download the IGEL software and perform basic installation and configuration without being forced to read many manuals and numerous web support articles.
> This document will walk you, step-by-step, through what is required for you to get up and running in a proof-of-concept or lab scenario. When finished, you will have a fully working IGEL endpoint management platform consisting of the IGEL Universal Management Suite (UMS), IGEL Cloud Gateway (ICG), and IGEL OS devices installed, connected and centrally managed.
> You can download the guide here: http://files.igelcommunity.com/IGEL-Getting-Started-Guide.zip.

1 https://www.igelcommunity.com/igel-getting-started-guide

Installation on Windows

Standard Installation

To install the IGEL Universal Management Suite under Windows, proceed as follows:

1. Download the current version of the IGEL Universal Management Suite from the IGEL Download Server[2].
2. Launch the installer.

   > You will need administrator rights in order to install the UMS.

3. Read and confirm the **License Agreement**.
4. Read the **Information** regarding the installation process and click **Next**.
5. Select the folder for the installation under **Select Destination Location**. (Default: `C:\Program Files\IGEL\RemoteManager`)
6. If you already have a UMS installation, select the file name for the **backup** of your embedded database. If you do not choose a file name and click on **Next**, no backup will be created. See also Updating under Windows (see page 219).
7. Choose the components to be installed under **Select Components.**
   - **Standard UMS**
     - **with UMS Console**
     - **with Embedded Database**
   - **Only UMS Console**
   - **UMS High Availability Network**
     - **UMS Server**
     - **UMS Load Balancer**

     > The embedded database is suitable for most purposes. If not disabled, the embedded database will automatically be installed if you select **Standard UMS**.
     > The use of an external database system is recommended in the following cases:
     > - You manage a large network of devices.
     > - A dedicated database system is already in use in your company.
     > - You integrate the High Availability solution.

8. Select the **UMS data directory**. (Default: `\RemoteManager`)
9. Under **User Credentials for DB-connect**, enter a user name and password for the database connection.
10. Choose a folder name under **Select Start Menu Folder**.
11. Read the summary and start the installation process.
    The installer will install the UMS, create entries in the Windows software directory and in the start menu and will place a shortcut for the UMS Console on the desktop.

2 https://www.igel.com/software-downloads/workspace-edition/

12. Close the program after completing the installation by clicking on **Finish**.
    If you have chosen the standard installation, the UMS Server will run with the embedded database.
13. Start the UMS Console.
14. Connect the UMS Console to the UMS Server using the access data for the database that you entered during the installation.
    You will find information regarding the use of the UMS with external databases under Connecting External Database Systems (see page 220).

Silent Installation of the UMS Console

You can carry out the installation silently by first creating an `.inf` file and then launching the installation using a command line.

> Silent installation is only possible for the UMS Console. It is not possible for the UMS Administrator and the UMS Server.

For further information, see Unattended/Silent Installation of UMS Console (see page 214).

Installation on Linux

For the supported operating systems, see the "Supported Environment" section of the release notes (see page 649).

The procedure for installing the IGEL Universal Management Suite under Linux is as follows:

1. Download the current version of the IGEL Universal Management Suite from the IGEL Download Server[3].
2. Open a terminal emulator such as xterm and switch to the directory in which the installation file `setup-igel-ums-linux-[Version].bin` is located.
3. Check whether the file is executable. If not, it can be made executable using the following command:
   `chmod u+x setup*.bin`

   You will need `root/sudo` rights to carry out the installation.
4. Execute the installation file as `root` or with `sudo`:
   `sudo ./setup-igel-ums-linux-[Version].bin`
   This unzips the files into the `/tmp` directory, starts the Java Virtual Machine contained and removes the temporary files after the installation procedure.
5. Start the installation procedure by pressing **Enter**.

   You can cancel the installation at any time by pressing the [Esc] key twice.
6. Read and confirm the license agreement.
7. Decide whether the installer will automatically install the required dependencies:
   - **Now**: Installs the necessary dependencies automatically.
   - **Manual**: Skips the installation. You will have to install the required dependencies manually if this has not already been done.
   - **Cancel installer**: Aborts the installation procedure.
8. Under **Destination directory**, select the directory in which the UMS is to be installed. (Default: `/opt/IGEL/RemoteManager`)
9. If you update an existing UMS installation: Under **Database backup**, select a file for the backup of the embedded database as well as licenses and certificates. If you have already created a backup, you can also select **No (continue)** in order to skip this step. See also Updating under Linux (see page 217).
10. Under **Installation type**, select the scope of installation:
    - Complete: UMS Server and UMS Console
    - Client only: UMS Console only
    - HA net: High Availability configuration

3 https://www.igel.com/software-downloads/workspace-edition/

> Freely selectable directories for file transfers are no longer supported. After completing the installation, move the existing files to the `ums_filetransfer/` directory and use the **Files** and **Firmware Update** points in the UMS Console to make them available online again. You may also need to amend download addresses in the device configurations and profiles.

11. Under **Data directory**, select the directory in which Universal Firmware Updates and files are to be saved. (Default: `/opt/IGEL/RemoteManager`)
12. Select the **run levels** in which the UMS Server is to run.
13. Under **Database**, select the desired database system.
    - Internal: The internal database (embedded database)
    - Other: An external database server

    > The embedded database is suitable for most purposes. It is included in the standard installation. If you have to manage a large network of devices and a dedicated database system is already in use in your company, it is advisable to use this system. The same applies if the High Availability solution is used.
14. Enter a **user name** and **password** for database access.
15. Specify whether you would like to create **shortcuts** for the UMS Console and UMS Administrator in the menu.
16. Check the summary of the installation settings and start the procedure by selecting **Start installation**.
    If you have selected the standard installation, the UMS Server along with the internal database will be installed and started.
17. Once the installation procedure is complete, open the UMS Console via the menu or with the command `/opt/IGEL/RemoteManager/RemoteManager.sh`
18. Connect the UMS Console to the UMS Server by entering the login data for the database that you specified during installation.

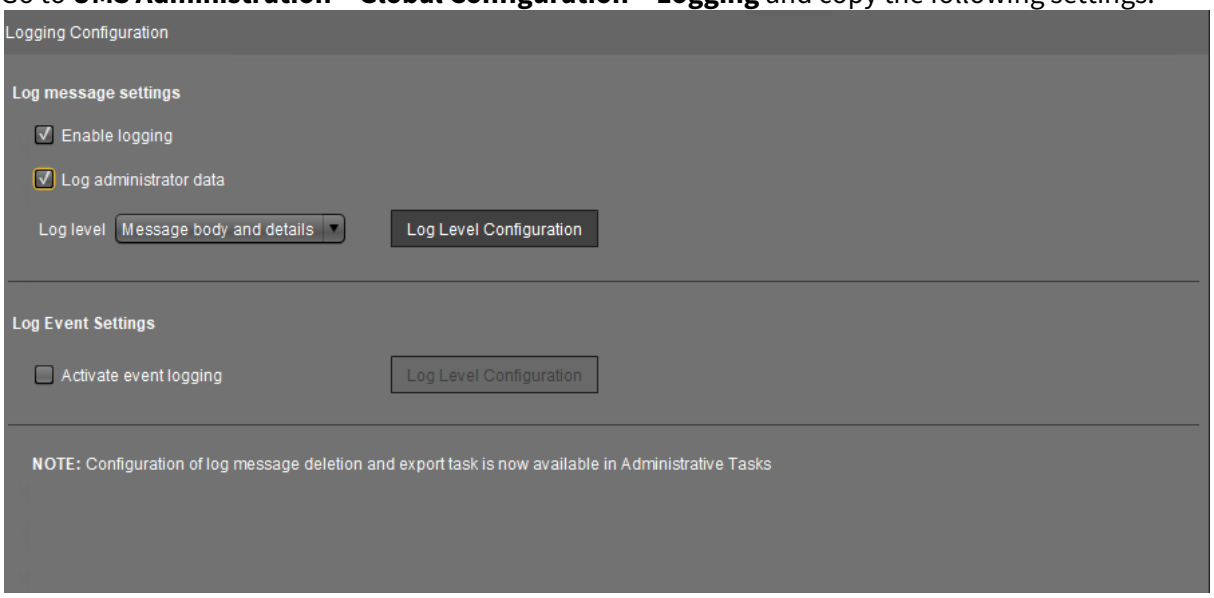
- Installing UMS on Red Hat Enterprise Linux (RHEL) 7.3 (see page 208)
- Installing UMS on Oracle Linux Server (see page 210)

System Configuration

This document describes various recommended settings for UMS.

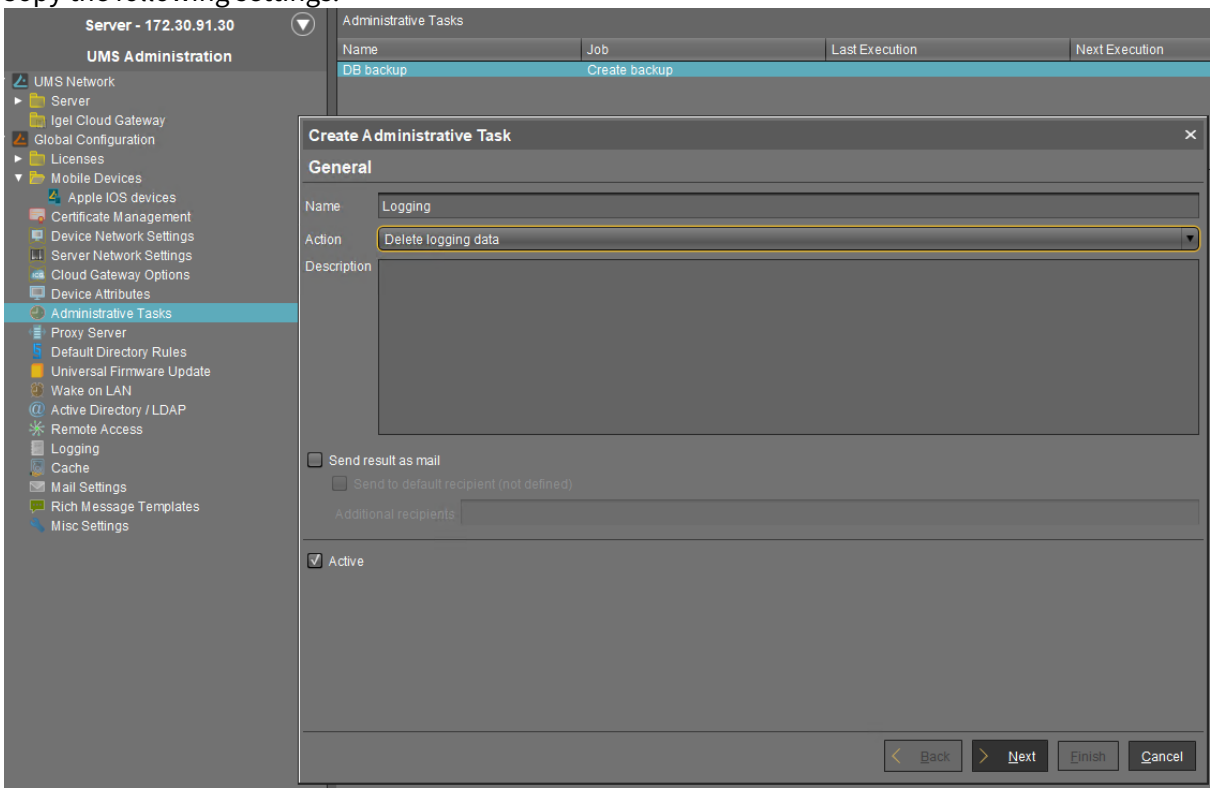
To define the settings, proceed as follows:

1. Start the **UMS Console**.
2. Go to **UMS Administration > Global Configuration > Logging** and copy the following settings:

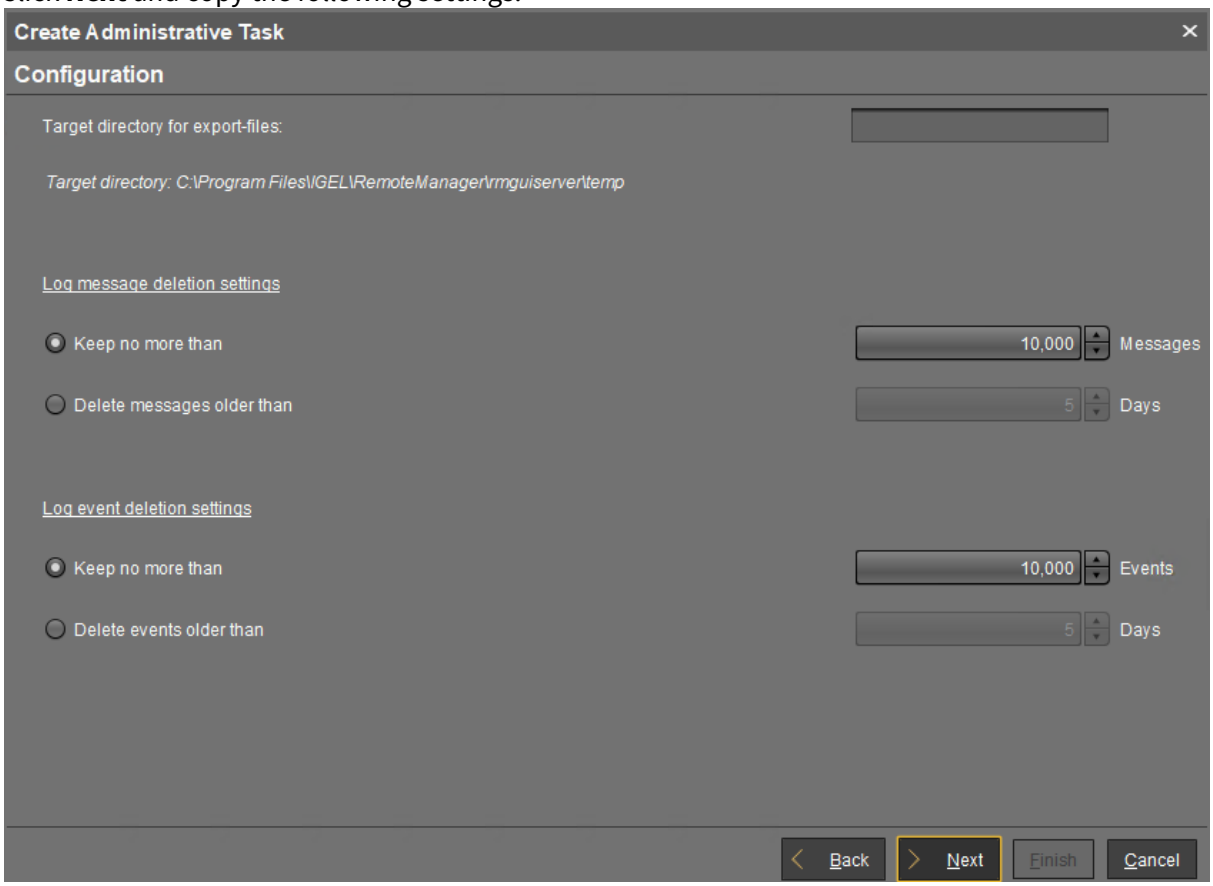


3. Confirm the setting with **Yes**.
4. Go to **Administrative Tasks**.
5. Click **add (+)** to create a new administrative task.
   The **Create Administrative Task** dialog opens.

6. Copy the following settings:



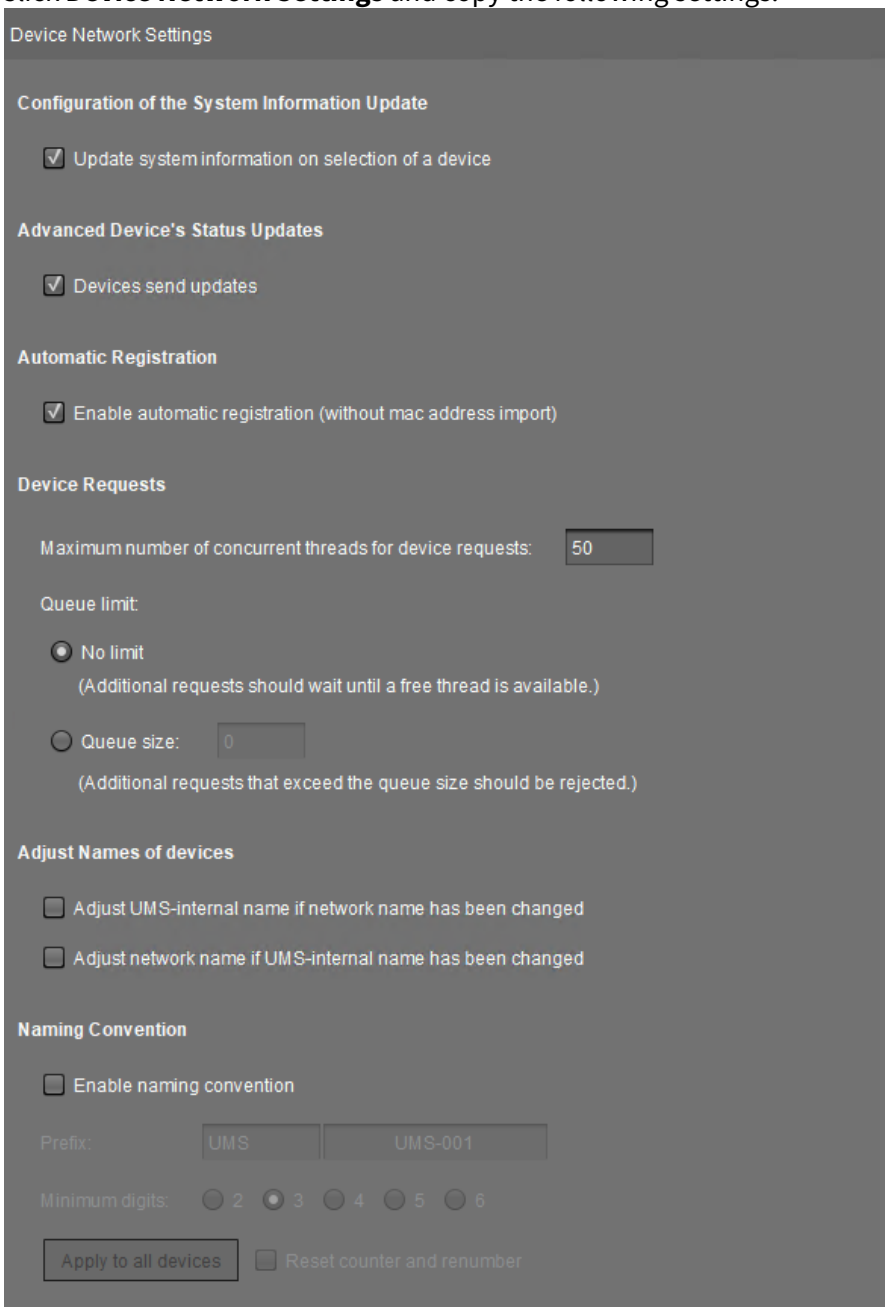
7. Click **Next** and copy the following settings:



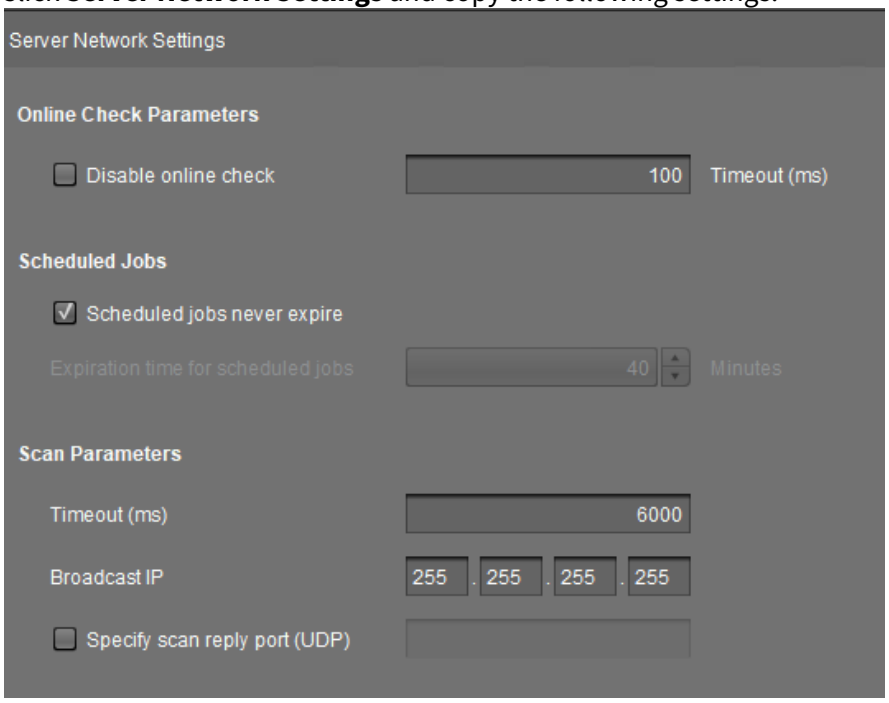
8. Click **Next** and **Finish.**

> ⓘ Having logging activated is important for reproducing errors. In this way, you are able to trace the log and event messages in the UMS under **System > Logging**.

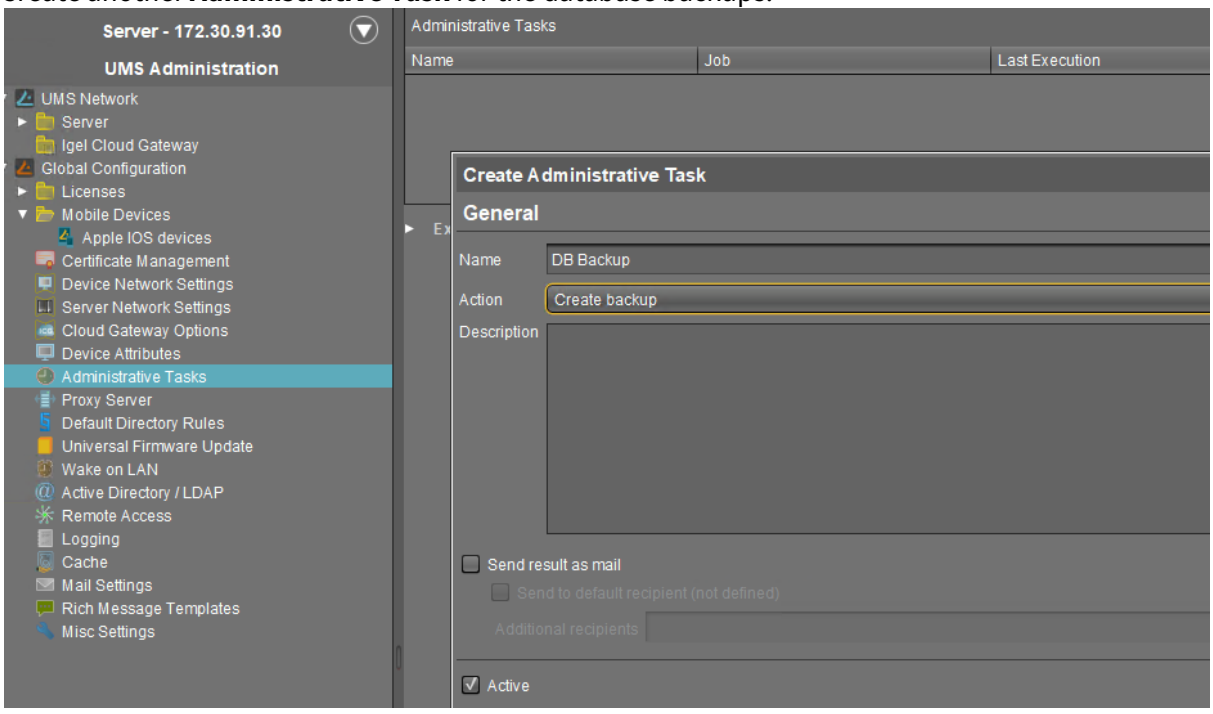
9. Click **Device Network Settings** and copy the following settings:



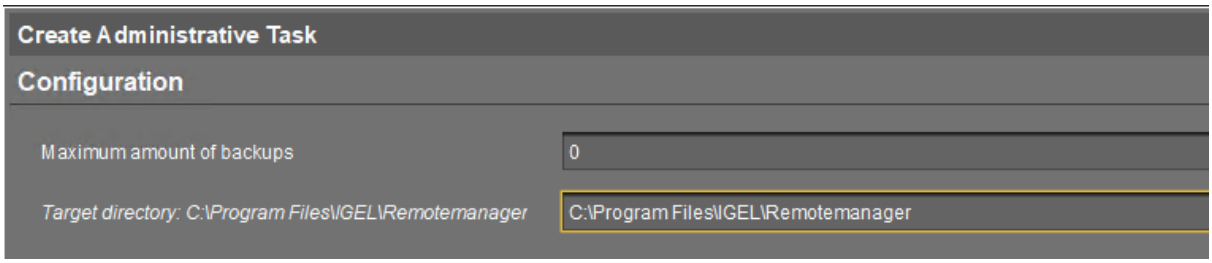
10. Click **Server Network Settings** and copy the following settings:



11. Go back to **Administrative Tasks** in the **UMS Administration** tree.
12. Create another **Administrative Task** for the database backups:

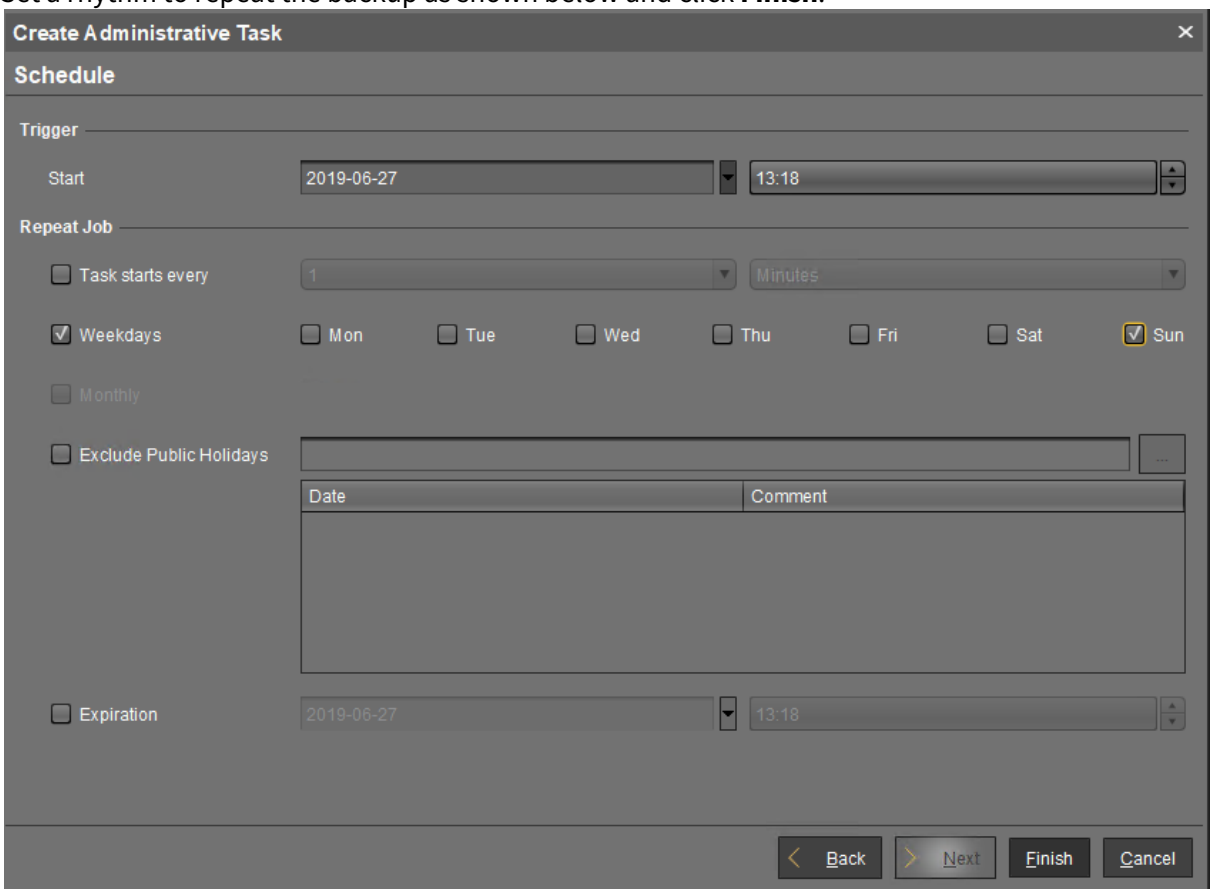


13. Click **Next.**
14. Enter the required **target directory**:

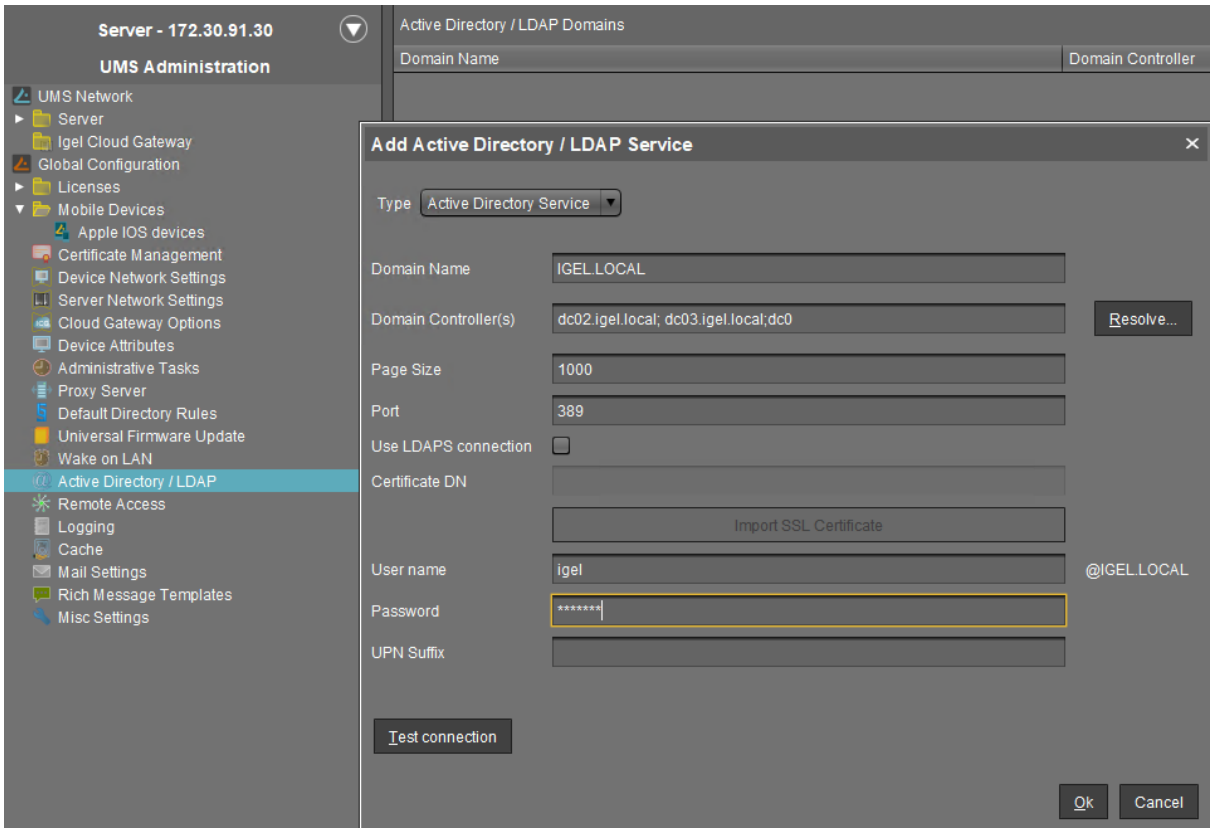


> We recommend that you create a database backup in order to be able to recover the original UMS data in the event of data loss.

15. Click **Next**.
16. Set a rhythm to repeat the backup as shown below and click **Finish**:



17. Go to **Active Directory / LDAP** and add a new Active Directory/LDAP service with the following values:



18. Click the **Test connection** button to check if your configuration is working.

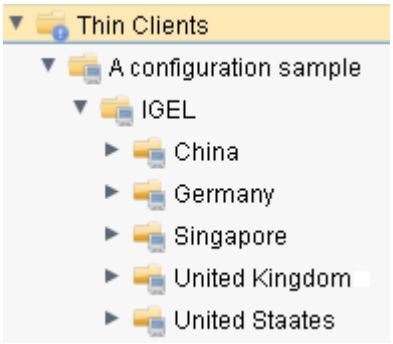
Creating Device Structures

You may freely organize your device structure in the IGEL UMS tree.

Take advantage of this freedom and build well thought out, intelligent directory structures. How deeply you want to structure your tree is up to you. The system allows you to nest directories as deeply as you want.

It would be advisable to arrange the directories referring to your company's structure.

You could classify the devices according to branch offices, departments or tasks, for example:



Keep in mind that you also need a smart structure for automatic registration with indirect profiles. Devices will inherit the profiles assigned to the root directory they are subordinated to.

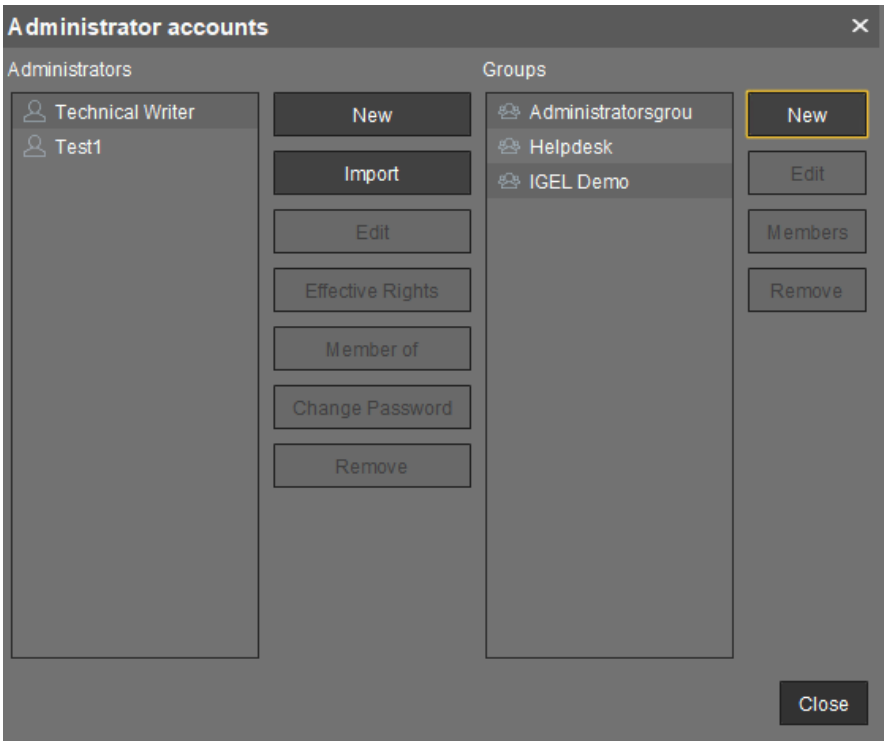
Administrator Accounts

Import administrative accounts from the Active Directory, groups as well as users.

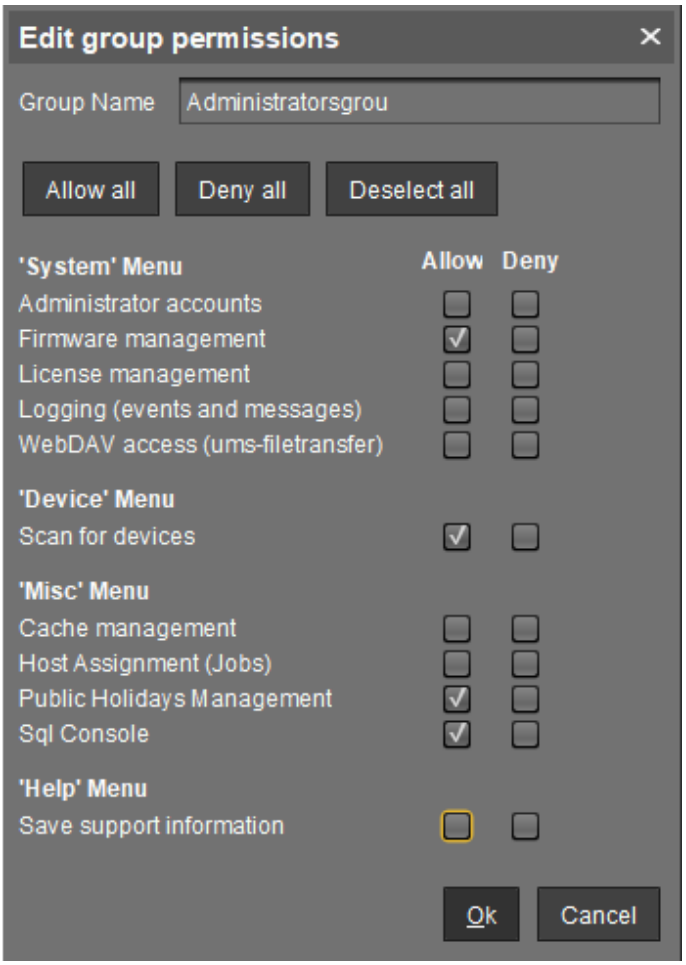
▶ Click **System > Administrator Accounts** to set up groups of administrators in order to manage their permissions more conveniently.

Where required, add local administrators. Permission settings are performed in the same way for both groups and individual administrators.

> If you do not wish to completely adopt the Active Directory structure, you may create new local administrators or groups.

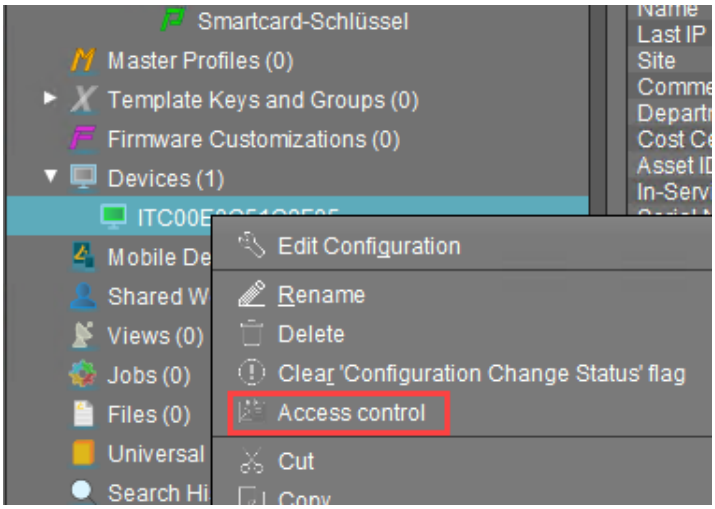


▶ Click **Edit** in the **Administrator Accounts** mask to set permissions for specific menu items:

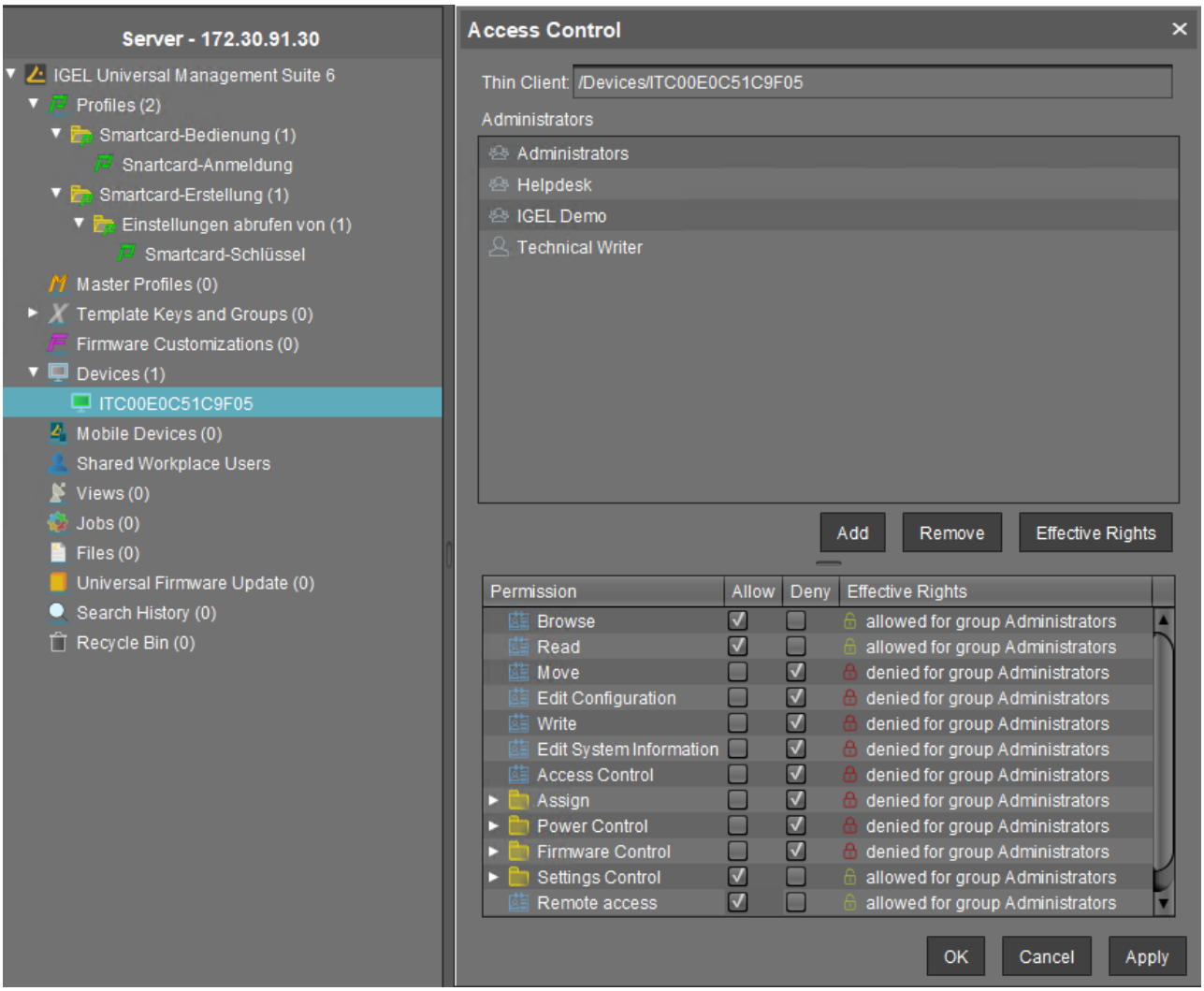


Note for all other value sets: Each administrator can be granted specific permissions with regard to objects in the navigation tree.

▶ Right-click an object in the structure tree.



▶ Click **Access Control** in the context menu to set object permissions.



For more information on UMS administrator accounts and their access rights, refer to Create Administrator Accounts (see page 514).

Registering Devices

During the preparation and System Configuration (see page 10), we put in place the basis for automatic device registration; see also Registering Devices Automatically on the IGEL UMS (see page 242). For more information on the registration of devices, refer to Registering IGEL OS Devices on the UMS Server (see page 229).

- All you need to do is to start the devices or, if they are already in operation, to restart them.

If automatic registration fails, e.g. in WAN with NAT, register the missing devices manually.

After the registration, refresh the console editor view (F5) to show the new devices. Check the device structure and, if necessary, move the devices into the desired directories.

A device can only be registered to one UMS Server. If it is registered once, no other UMS can capture it.

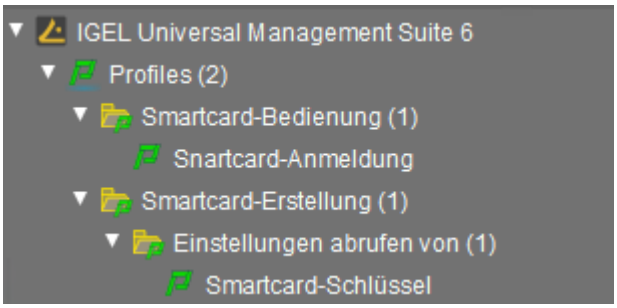
> We highly recommend disabling automatic registration after the roll-out to avoid all types of devices automatically being registered without your control.

Now you have a well-configured IGEL UMS which will allow you to work with the system professionally.

Creating Profiles

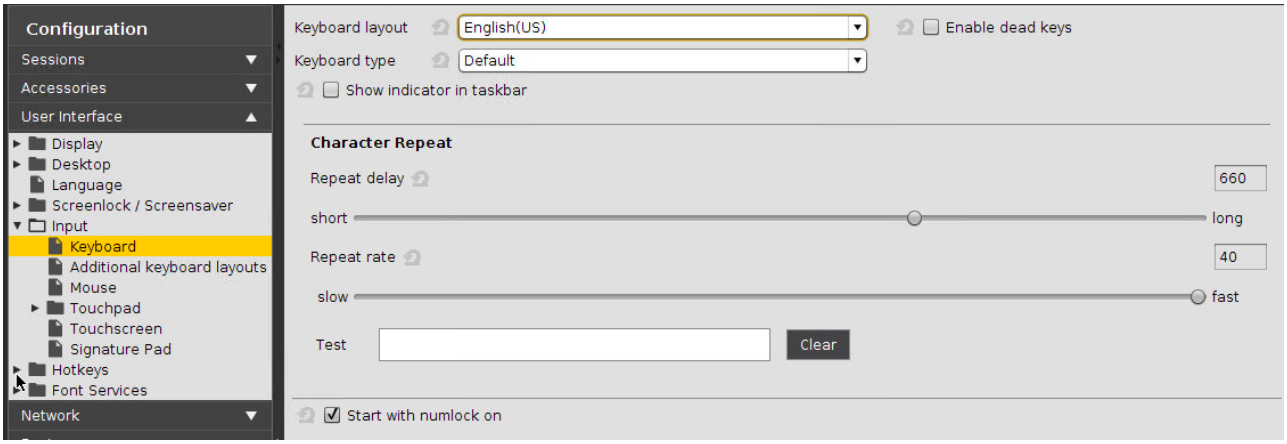
Create **Profiles** according to the different task areas such as

- Network configuration
- Sessions
- Printer
- Monitor configuration



The best practice is to define one profile for each task and not to mix them up. Otherwise, you will have problems maintaining your configuration settings later on.

In this case, we created a profile exclusively for the English keyboard layout:



After creating a profile and adjusting its settings, you can assign it to some Devices. You can assign an arbitrary number of profiles to each device.

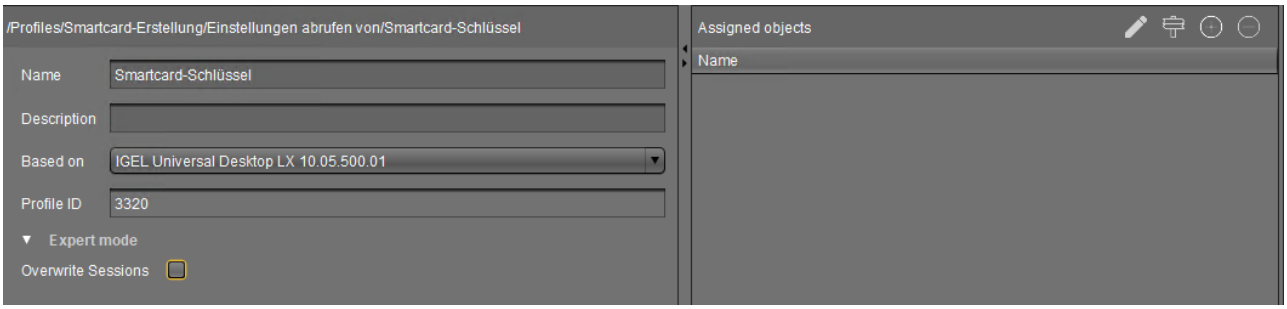
Basically, there are two modes of assignment: **direct** or **indirect**.

Indirect means that you assign the profile to a device directory rather than to a single device. All devices within the directory then inherit the settings of this profile.

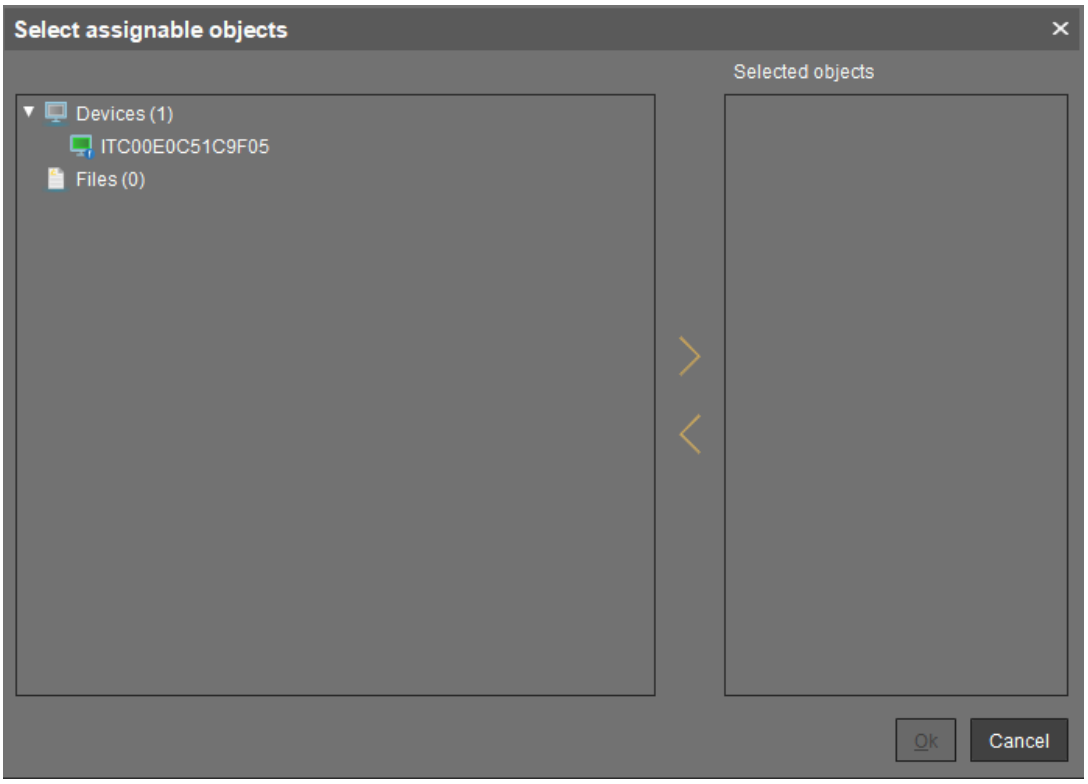
▶ Select a **Profile** in the UMS tree and drag and drop the selection onto a device or device directory.

or

▶ Select a device directory in the UMS tree and click the **Add (+)** button above the **Assigned Objects** panel.



▶ In the **Profile Selection** dialog that appears, select the profile to assign and press **Ok**:



ⓘ You can also do it the other way round: Select a profile in the UMS tree and assign a device directory to it.

For more information on profiles and their assignment to devices, refer to Profiles (see page 276).

Devices Supported by IGEL Universal Management Suite (UMS)

Question

Which devices are supported by IGEL Universal Management Suite (UMS)?

Answer

⚠ To ensure that you can use all new features of IGEL OS:

- ▶ Update your UMS to the current version.
- ▶ For all relevant profiles, set **Based on** to the appropriate firmware version.

The latest UMS version supports

- all IGEL devices that have not yet reached their end of maintenance;
- devices converted with IGEL OS Creator (OSC);
- devices converted with IGEL Universal Desktop Converter 3 (UDC3);
- devices converted with IGEL Universal Desktop Converter 2 (UDC2);
- Windows 7 devices with IGEL Unified Management Agent (UMA) installed.

Older UMS releases support

- IGEL devices that were released before the UMS release
- and that had not reached their end of maintenance at the time of the UMS release.

UMS Communication Ports

Which ports are used by the components of IGEL UMS and the other components of a UMS infrastructure?

The following table shows the ports used by the components that play a role in a UMS infrastructure.

Port (Protocol)	Who is Listening? Applications/ Service Binding to Port	Who is Talking? Applications/ Services Initiating Communications	Description	Required by UMS Feature
9 (UDP)	Device	UMS Server	The UMS Server sends magic packets to the devices.	Core (Wake on LAN)
80 (TCP)	IGEL download server (HTTP server at fwu.igel.com)	UMS Server	The UMS Server requests the connection details required for connecting to the IGEL license server (at susi.igel.com). See UMS Contacting the Licensing Server (see page 52).	Automatic License Deployment (ALD)
80 (TCP)	IGEL download server (HTTP server at fwu.igel.com)	UMS Server	See UMS Contacting the Download Server to Check for New Updates (see page 47).	Core (Universal Firmware Update)
88 (TCP/ UDP)	MS Active Directory Service	UMS Server	The UMS Server sends a Kerberos request to MS Active Directory.	Core (if Active Directory is used), Shared Workplace
389 (TCP)	MS Active Directory Service	UMS Server	The UMS Server sends an LDAP request to MS Active Directory.	Core (if Active Directory is used), Shared Workplace
443 (TCP)	IGEL licensing server (at susi.igel.com)	UMS Server	The UMS Server requests licenses; see UMS Contacting the Licensing Server (see page 52).	Automatic License Deployment (ALD)

Port (Protocol)	Who is Listening? Applications/ Service Binding to Port	Who is Talking? Applications/ Services Initiating Communications	Description	Required by UMS Feature
636 (TCP)	LDAPS server (other than MS Active Directory)	UMS Server	The UMS Server sends an LDAP request over SSL.	Core (if LDAPS server is used)
1433 (TCP)	Microsoft SQL Server database	UMS Server	See UMS with External Database (see page 34).	Core (if MS SQL Server is used)
1521 (TCP)	Oracle database	UMS Server	See UMS with External Database (see page 34).	Core (if Oracle is used)
1527 (TCP)	Apache Derby database (Derby Network Server)	UMS Server	See UMS with External Database (see page 34).	Core (if Apache Derby is used)
5432 (TCP)	PostgreSQL database	UMS Server	See UMS with External Database (see page 34).	Core (if PostgreSQL is used)
5900 (TCP)	Device (UMS agent)	UMS Console	The UMS Console initiates a VNC session for shadowing; see UMS and Devices: Shadowing (see page 41).	Core (shadowing)
6155 (UDP)	HA Load Balancer UMS Server	HA Load Balancer UMS Server	Both HA Load Balancer and UMS Server listen on port 6155 and use it for communication.	High Availability (HA)
8443 (TCP)	UMS Server (Windows: service IGELRM GUIServer; Linux: daemon igelRM Server)	UMS Console	See UMS with Internal Database (see page 33) or UMS with External Database (see page 34).	Core

Port (Protocol)	Who is Listening? Applications/ Service Binding to Port	Who is Talking? Applications/ Services Initiating Communications	Description	Required by UMS Feature
8443 (TCP)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	Device	The device requests a file from the UMS; see UMS and Devices: File Transfer (see page 45).	Core (file transfer)
8443 (TCP)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	Device	In the course of a Universal Firmware Update, the device requests a file from the UMS; see UMS and Devices: File Transfer (see page 45).	Core (Universal Firmware Update)
8443 (TCP)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	Device	The UMS provides files for customizing the look and feel of the device's GUI; see UMS and Devices: File Transfer (see page 45).	Core (firmware customization)
8443 (TCP)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	Device	The UMS provides license files for the devices; see UMS and Devices: File Transfer (see page 45).	Core (licenses)

Port (Protocol)	Who is Listening? Applications/ Service Binding to Port	Who is Talking? Applications/ Services Initiating Communications	Description	Required by UMS Feature
8443 (TCP)	UMS Server (Windows: service IGELRM GUIServer; Linux: daemon igelRM Server)	3rd party component using IMI (IGEL Management Interface)	See IGEL Management Interface (IMI) (see page 35).	IMI
8443 (TCP)	ICG (IGEL Cloud Gateway)	UMS Server	See Devices and UMS Server Contacting Each Other via ICG (see page 37).	Core (with ICG)
8443 (TCP)	ICG (IGEL Cloud Gateway)	Device	See Devices and UMS Server Contacting Each Other via ICG (see page 37).	Core (with ICG)
8443 (TCP)	UMS Server (Windows: service IGELRM GUIServer; Linux: daemon igelRM Server)	UMS Server (Windows: service IGELRM GUIServer; Linux: daemon igelRM Server)	File synchronization between UMS Servers	High Availability (HA)
9080 (TCP)	UMS Server (Windows: service IGELRM GUIServer; Linux: daemon igelRM Server)	Device	The device requests a file from the UMS (regular file transfer or Universal Firmware Update). This port is only used if **Allow SSL Connections only** is deactivated in the UMS Administrator. If **Allow SSL Connections only** is activated, port 8443 is used for firmware updates and file transfer.	Core (unencrypted, no SSL)

Port (Protocol)	Who is Listening? Applications/ Service Binding to Port	Who is Talking? Applications/ Services Initiating Communications	Description	Required by UMS Feature
Auto ("high port")	UMS Server (Windows: service IGELRM GUIServer; Linux: daemon igelRM Server)	UMS Console	The GUI is started via Java Webstart console. This port is only used if **Allow SSL Connections only** is deactivated in the UMS Administrator. If **Allow SSL Connections only** is activated, port 8443 is used for firmware updates and file transfer.	Core (unencrypted, no SSL)
30001 (TCP)	UMS Server (Windows: service IGELRM GUIServer; Linux: daemon igelRM Server)	Device	See Devices Contacting UMS (see page 39).	Core (direct device communication, not used with communication via ICG)
30002 (TCP)	UMS Server (Windows: service IGELRM GUIServer; Linux: daemon igelRM Server)	HA Load Balancer	If the UMS Server and the HA Load Balancer are running on the same host, the UMS Server will use port 30002 instead of 30001, and the HA Load Balancer will use port 30001.	Core (directly, without ICG)
30005 (TCP/ UDP)	Device (UMS agent)	UMS Server	To scan for devices, the UMS Server sends a broadcast. The UDP packets of this broadcast contain the port to which the device should send the response. The UMS sends new settings to the device. The UMS periodically checks if the device is online.	Core (scanning for devices, sending new settings, checking if the device is online etc.)

Port (Protocol)	Who is Listening? Applications/ Service Binding to Port	Who is Talking? Applications/ Services Initiating Communications	Description	Required by UMS Feature
30022 (TCP)	Device (UMS agent)	UMS Server	See UMS and Devices: Secure Terminal (see page 44)	Core (secure terminal)
61616 (TCP/ UDP)	HA Load Balancer UMS Server	HA Load Balancer UMS Server	Both HA Load Balancer and UMS Server listen on port 61616 and use it for communication.	High Availability (HA)
Auto ("high port")	UMS Server (Windows: service IGELRM GUIServer; Linux: daemon igelRM Server)	Device	The device responds to a broadcast sent by the UMS during a scan. The port number to be used is contained in the UDP packet sent by the UMS.	Core (scanning for devices)

- Internal Communication (see page 32)
- IGEL Management Interface (IMI) (see page 35)
- UMS and Devices: Settings and Control (see page 36)
- UMS and Devices: Shadowing (see page 41)
- UMS and Devices: Secure Shadowing (see page 42)
- UMS and Devices: Secure Terminal (see page 44)
- UMS and Devices: File Transfer (see page 45)
- Universal Firmware Update (see page 46)
- Automatic License Deployment (ALD) (see page 51)

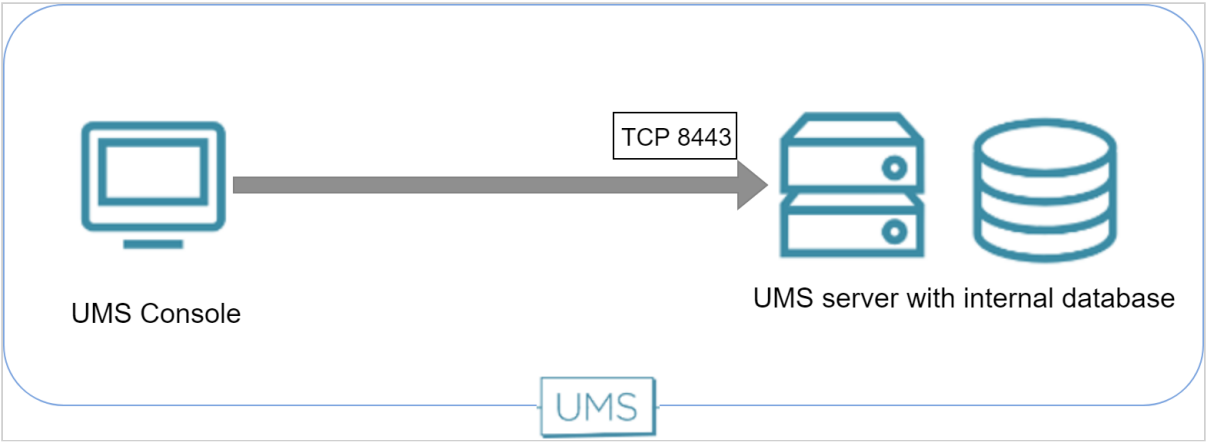
Internal Communication

UMS with Internal Database

Communication between the UMS Console and the UMS server happens via HTTPS. By default, the UMS server listens for requests on TCP port 8443. The port can be changed in the UMS Administrator under **Settings > GUI server port**.

The port used by the UMS for internal TCP requests to the embedded database can be changed in the UMS Administrator under **Settings > Database Port (Embedded DB)**. The default port is 1528.

The following figure illustrates the communication between the UMS components:



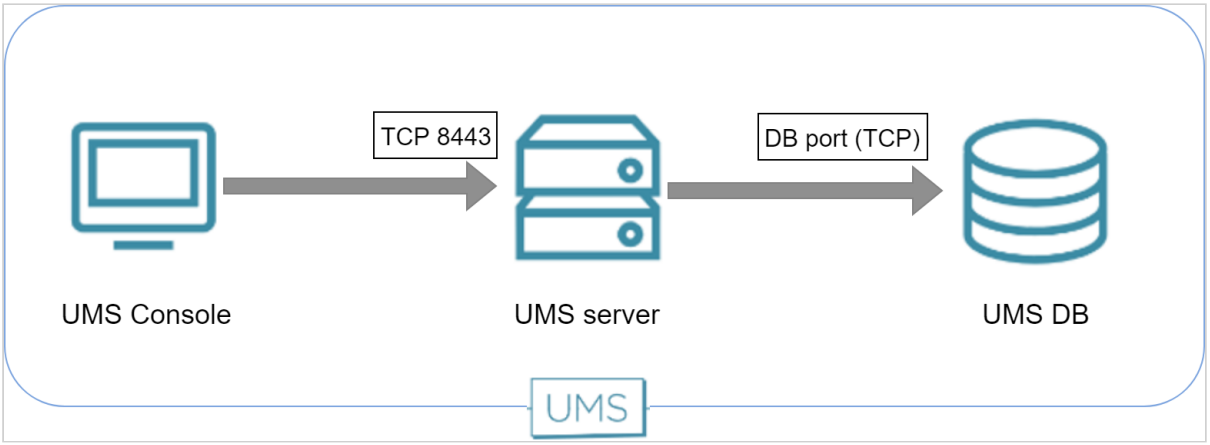
UMS with External Database

Communication between the UMS Console and the UMS server happens via HTTPS. By default, the UMS server listens to TCP requests on port 8443. The port can be changed in the UMS Administrator under **Settings > GUI server port**.

The ports used by the UMS for TCP requests to the database are defined as follows:

Database Type	Database Port (default)	Configuration
Apache Derby (Derby Network Server)	1527	(UMS Administrator) **Datasource > Add... >** [as DB-Type, select **Derby**] **> Port**
MS SQL Server	1433	(UMS Administrator) **Datasource > Add... >** [as DB-Type, select **SQL Server**] **> Port**
Oracle	1521	(UMS Administrator) **Datasource > Add... >** [as DB-Type, select **Oracle**] **> Port**
PostgreSQL	5432	(UMS Administrator) **Datasource > Add... >** [as DB-Type, select **PostgreSQL**] **> Port**

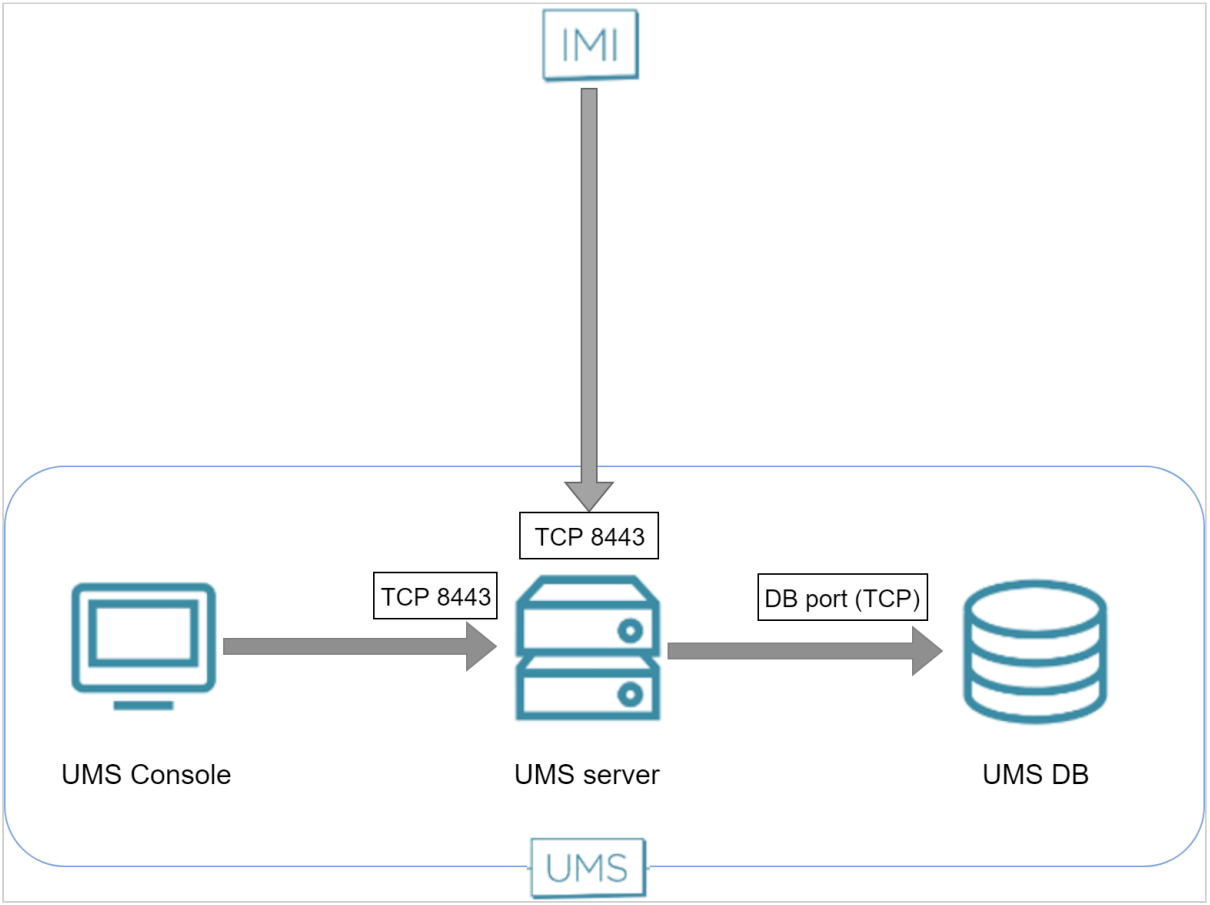
The following figure illustrates the communication between the UMS components:



IGEL Management Interface (IMI)

The REST API provided by the IGEL Management Interface is served via HTTP on port 8443 (TCP).

The following figure illustrates the communication with the UMS server via IMI:



UMS and Devices: Settings and Control

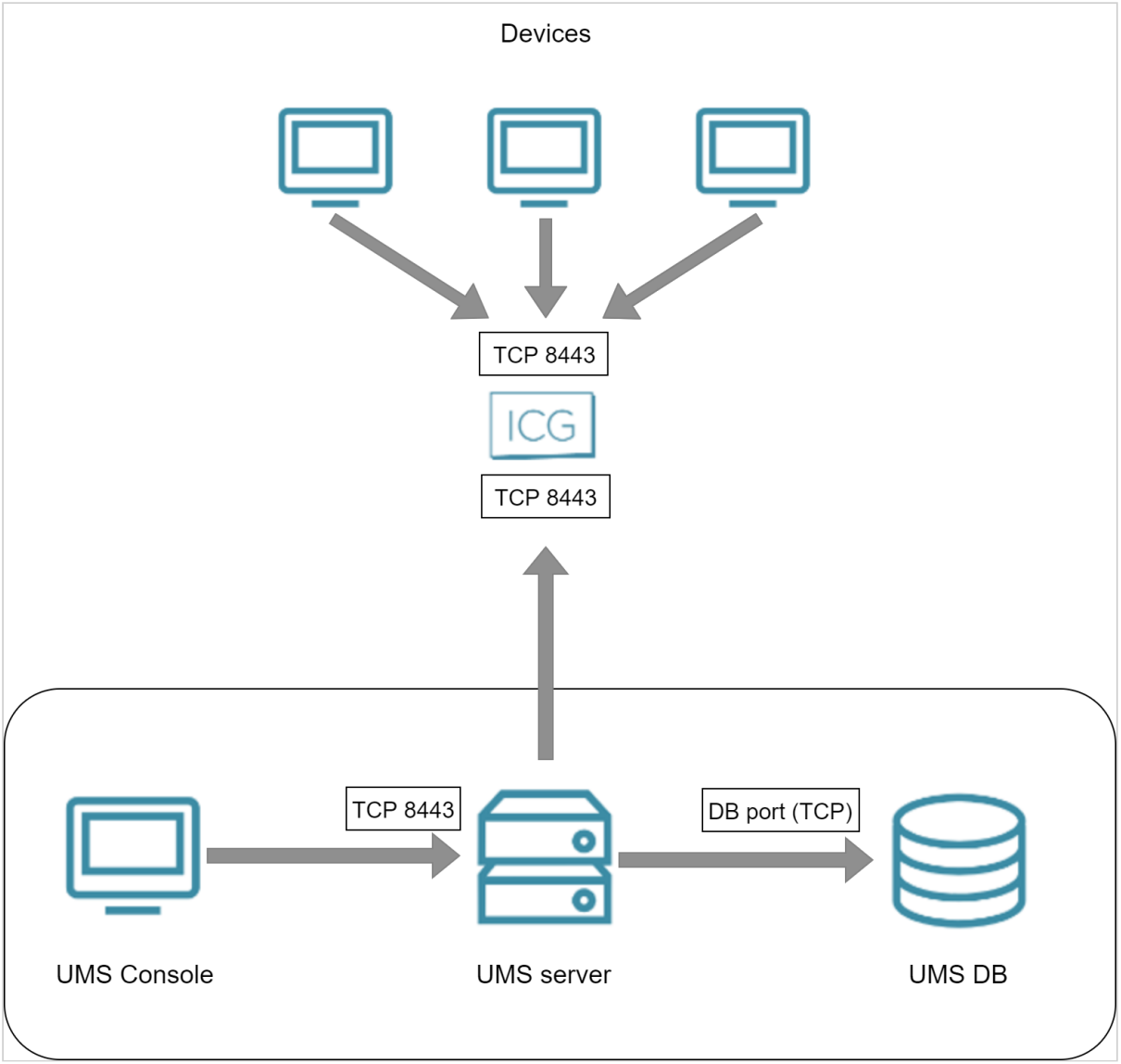
Devices and UMS Server Contacting Each Other via ICG

To communicate with the UMS, the devices initiate a TCP connection to the ICG. The default port on which the ICG is listening is port 8443.

To communicate with the devices, the UMS initiates a TCP connection to the ICG. The default port on which the ICG is listening is port 8443. It can be changed during the installation of the ICG. When the installation is completed, the port is fixed.

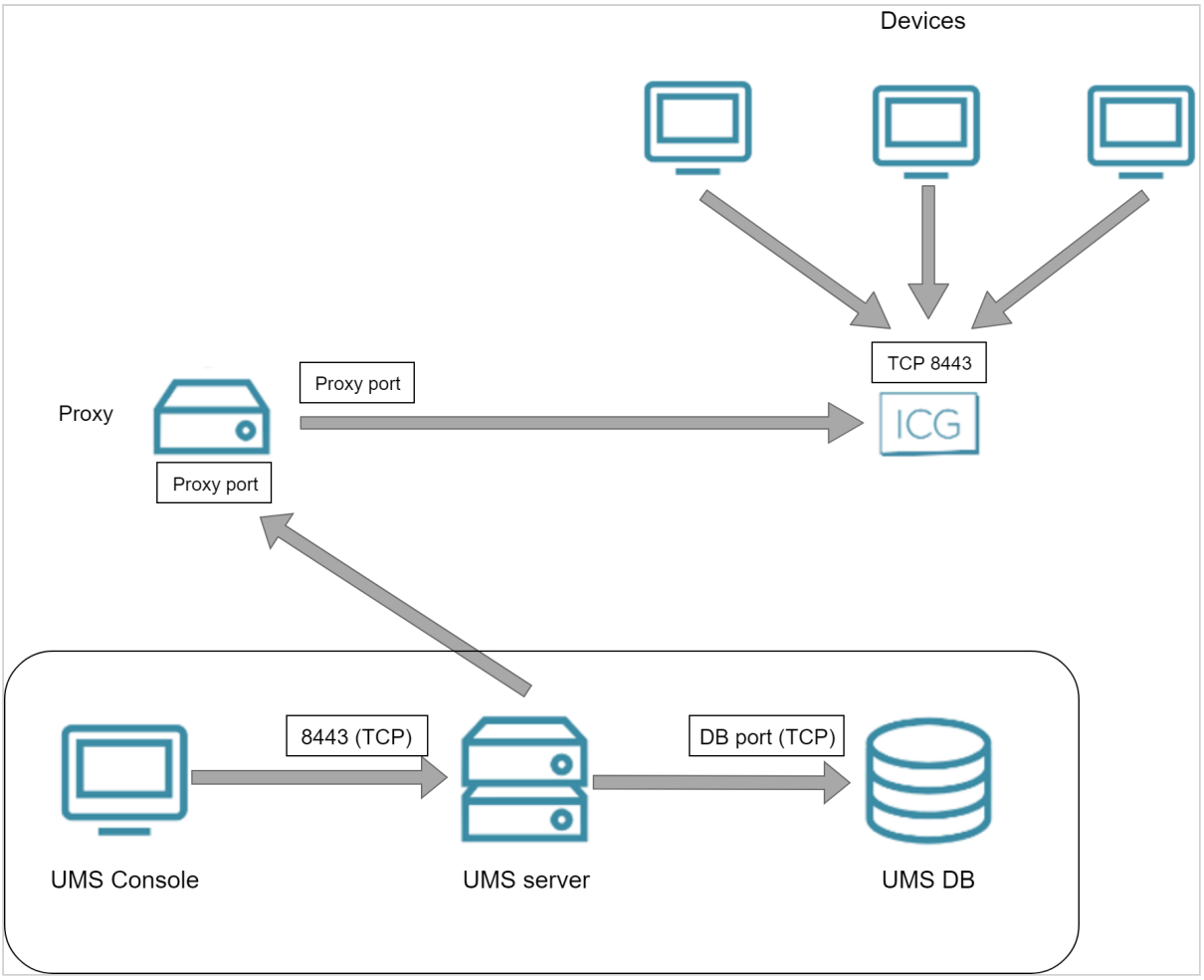
Direct Connection

The following figure illustrates the communication between the devices (thin clients) and the UMS via ICG:



Via Proxy

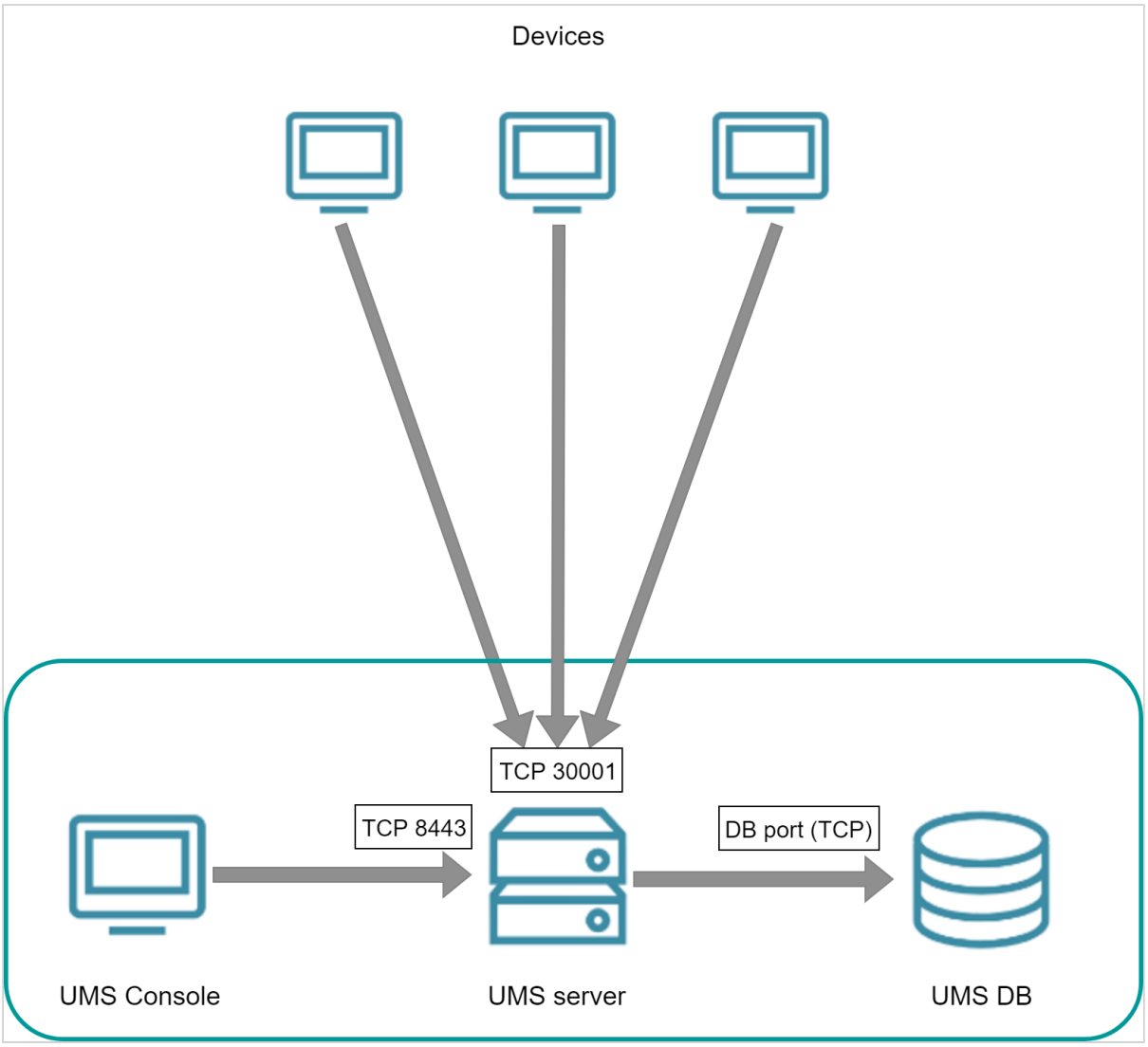
The following figure illustrates the communication between the devices (thin clients) and the UMS via ICG and a proxy:



Devices Contacting UMS

To communicate with the UMS, the devices initiate a TCP connection to the UMS server using port 30001.

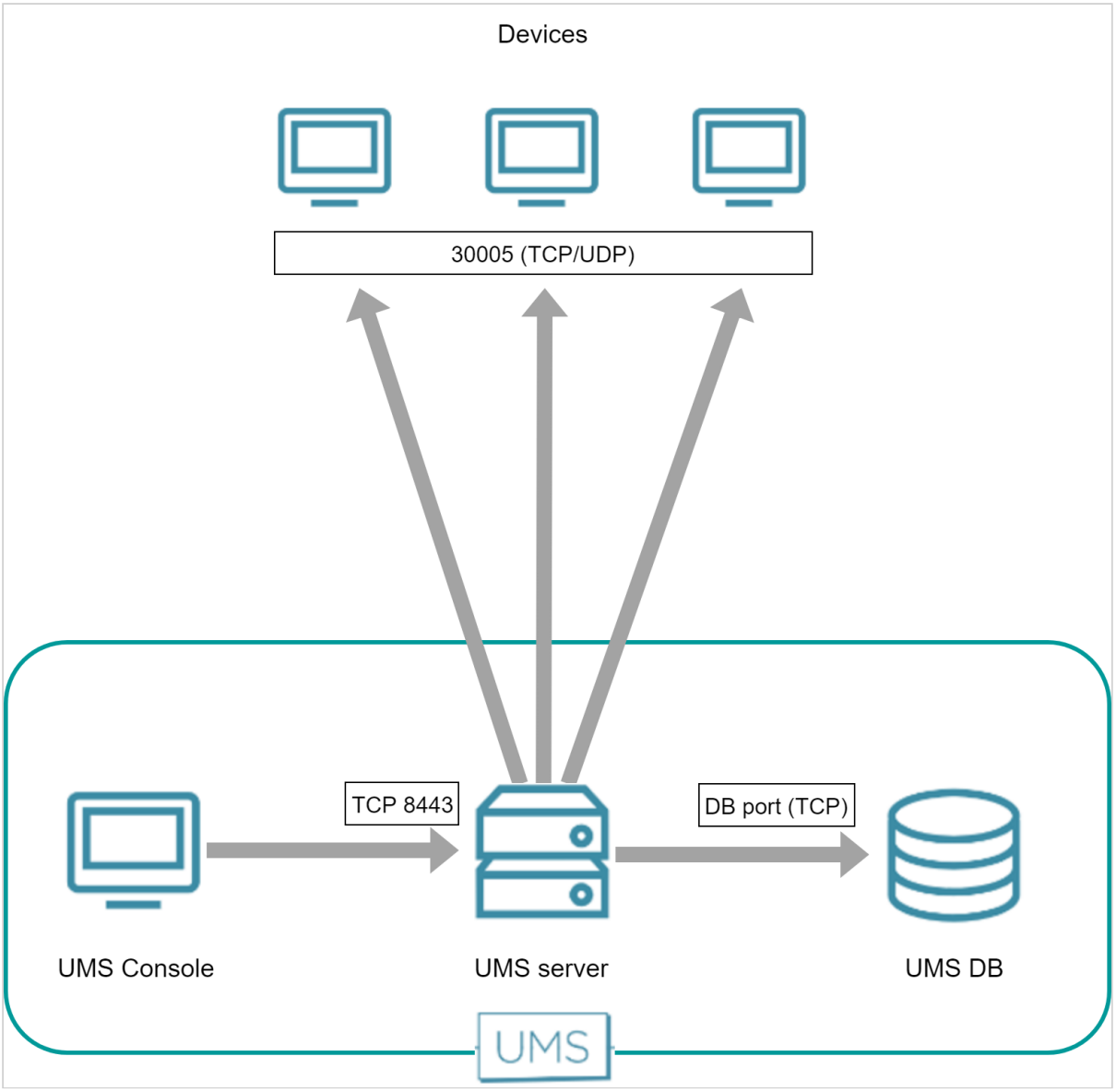
The following figure illustrates the communication between the devices (thin clients) and the UMS:



UMS Contacting Devices

To communicate with devices, the UMS initiates a TCP connection to the device's UMS agent using port 30005.

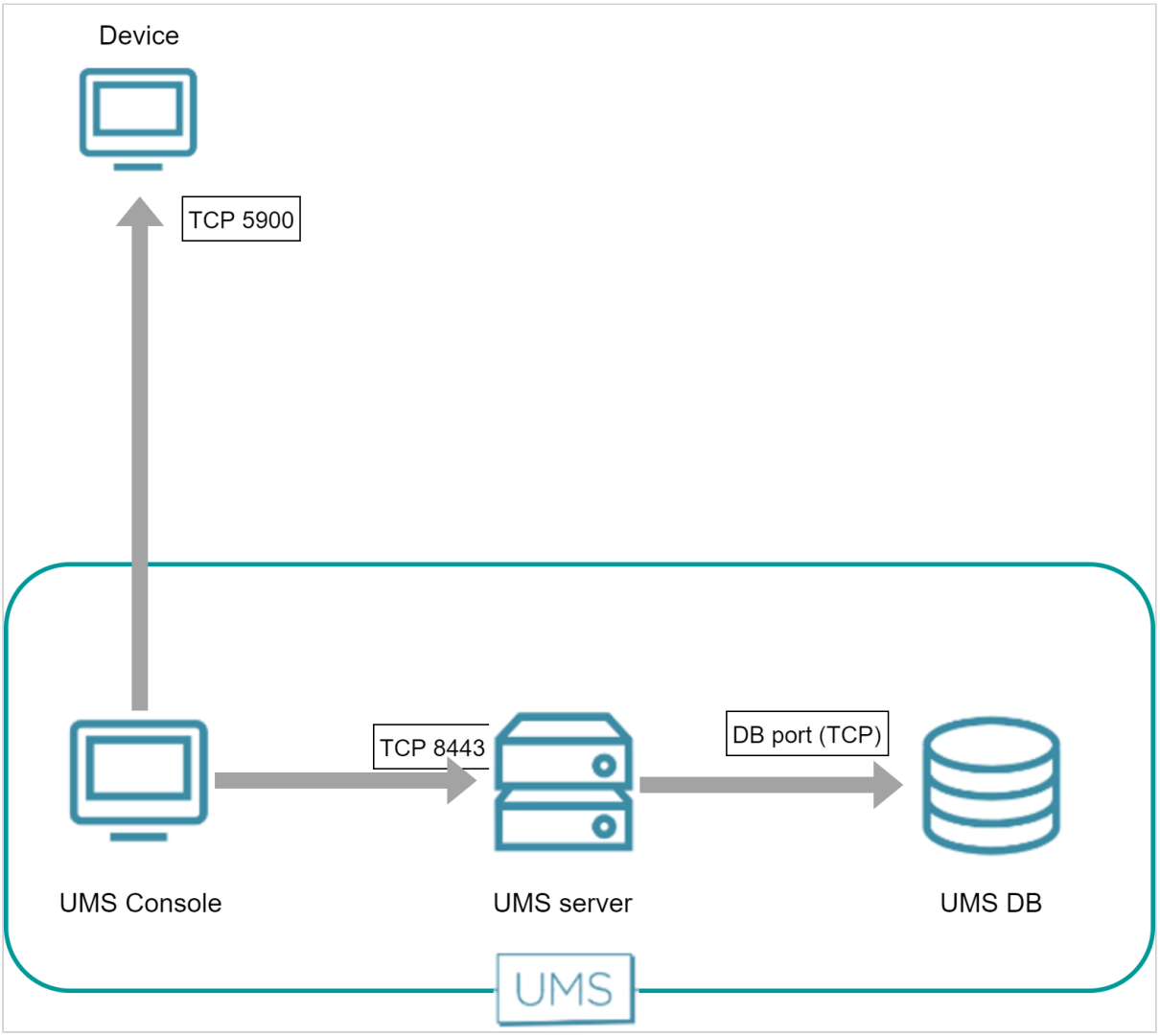
The following figure illustrates the communication between the UMS and the devices:



UMS and Devices: Shadowing

The UMS Console initiates a VNC session with the device. The standard port is 5900 (TCP); the port can be changed per session.

The following figure illustrates the communication between the UMS Console and a device:

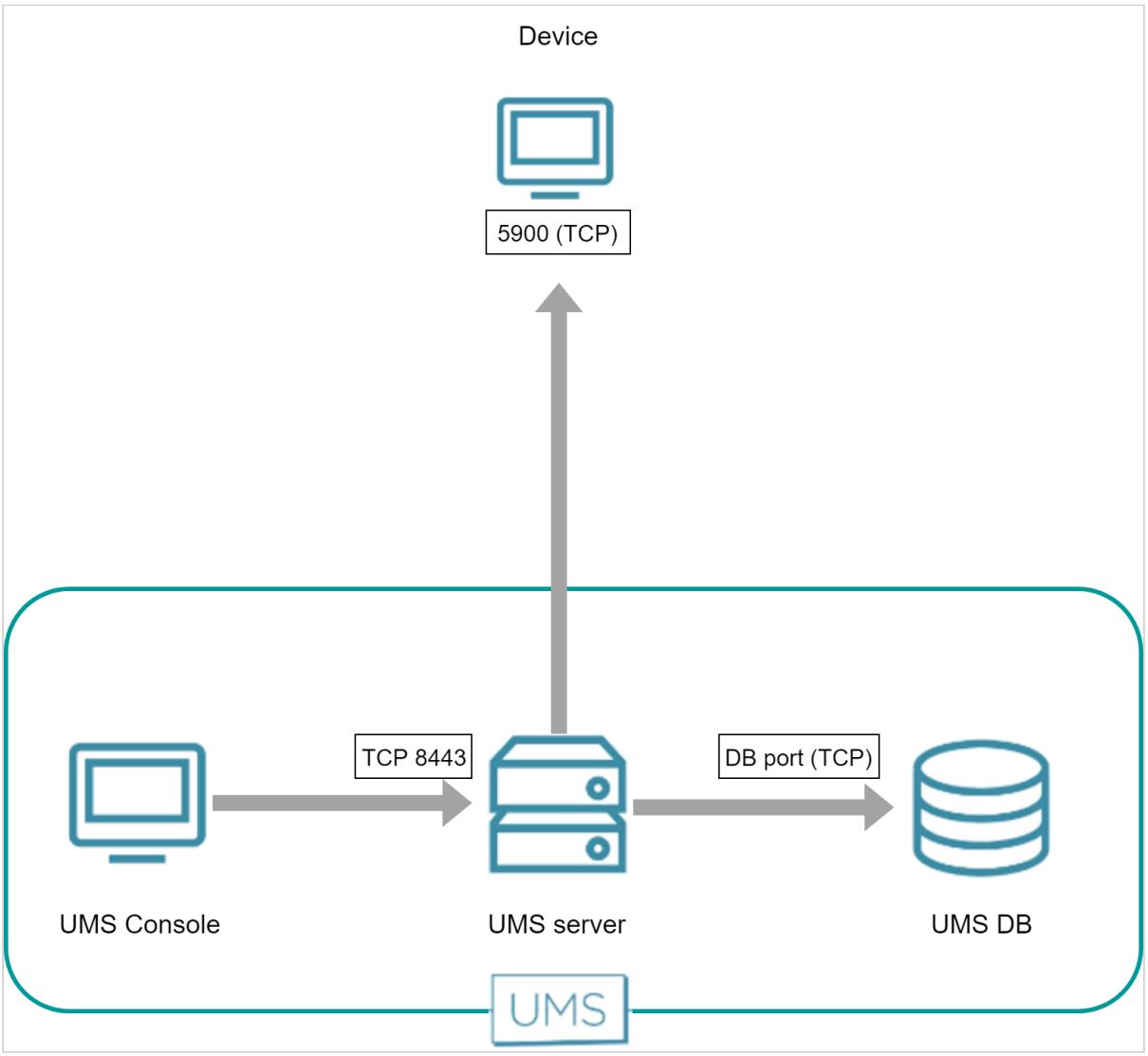


UMS and Devices: Secure Shadowing

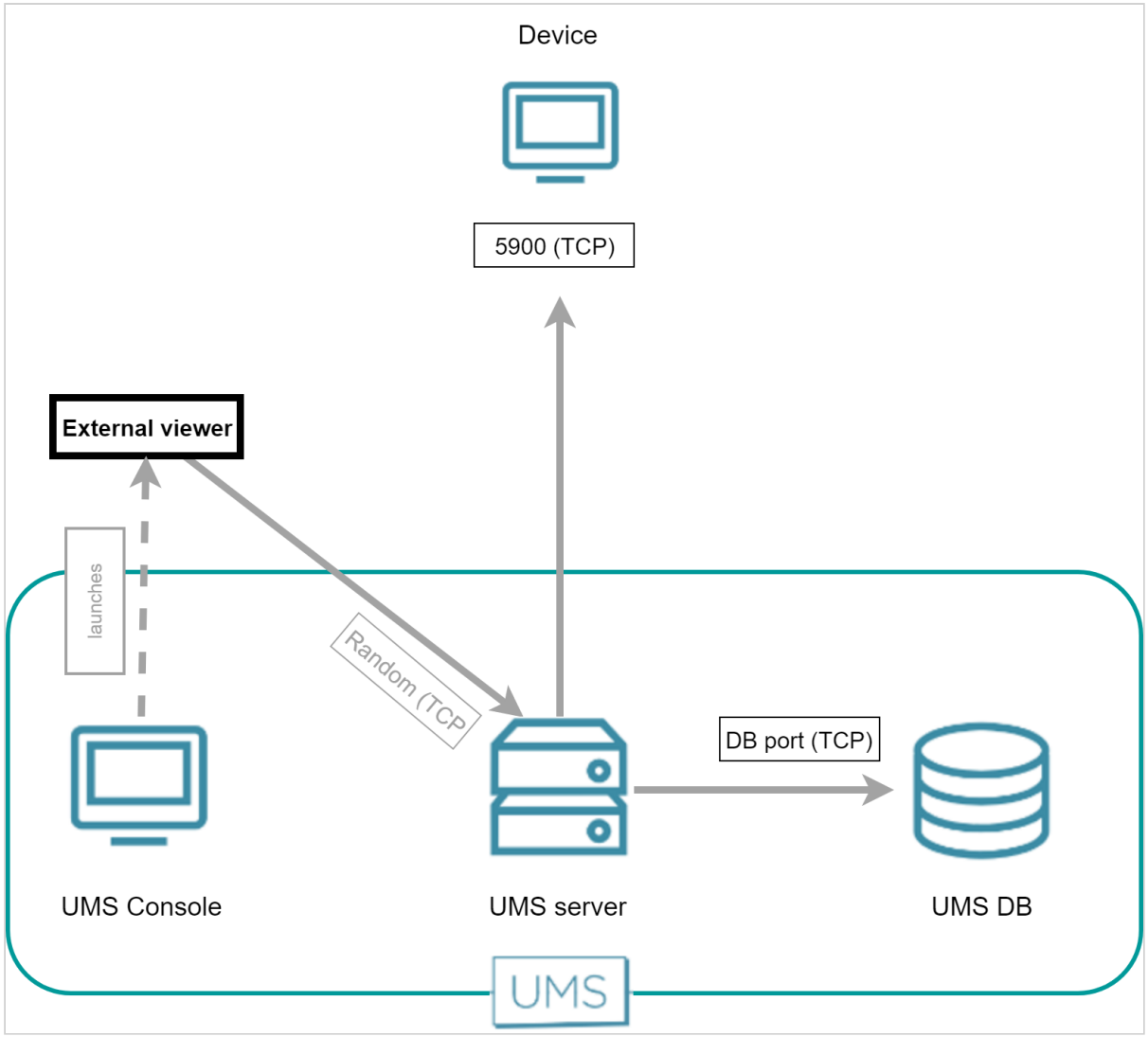
The UMS Console, or alternatively, an external VNC viewer, establishes a connection to the UMS server. The UMS server then establishes a TLS tunnel to the device.

The following figures illustrate the communication between the UMS Console, the VNC viewer, the UMS server, and a device:

Internal VNC Viewer



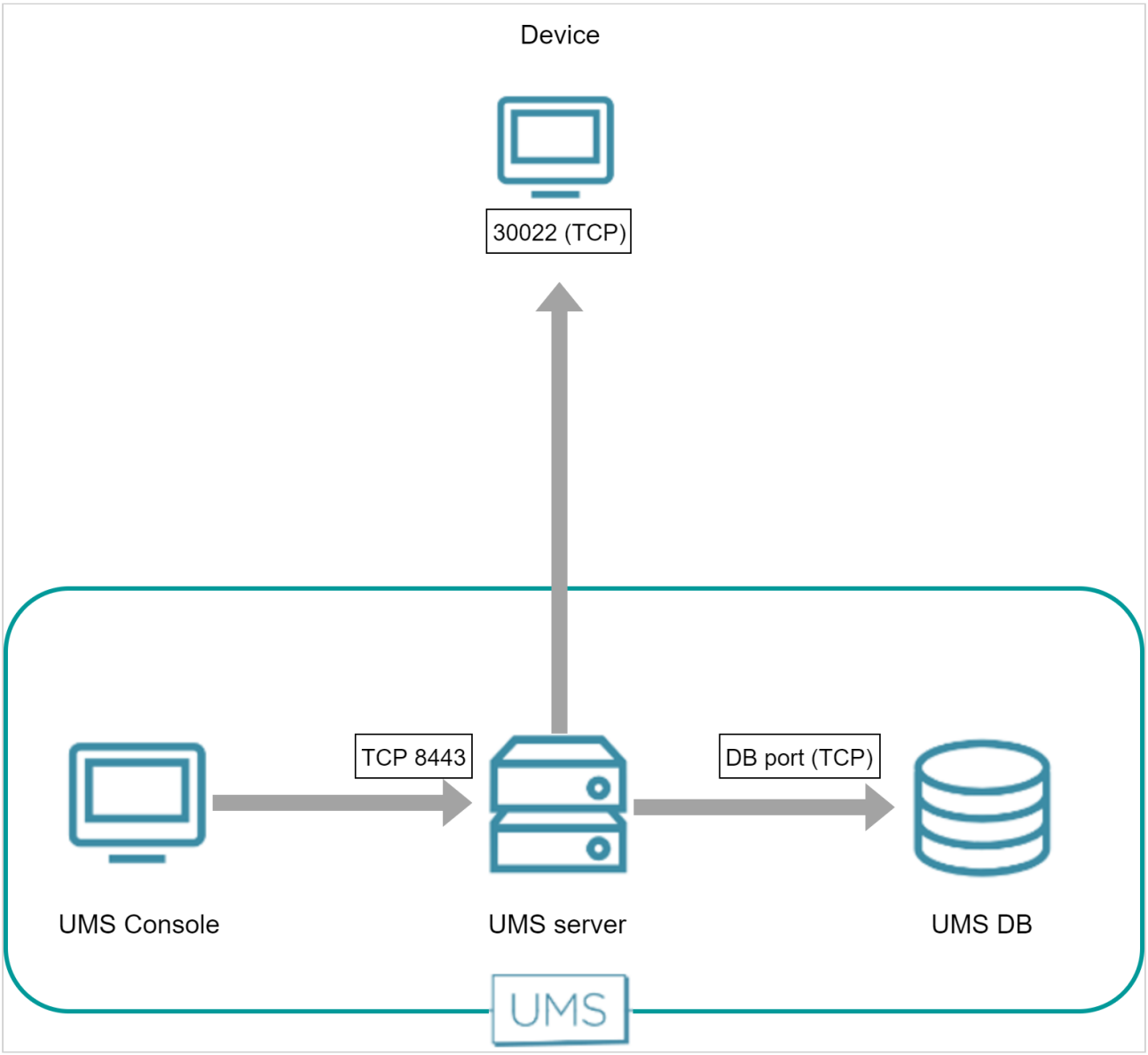
External VNC Viewer


Device
5900 (TCP)
External viewer
launches
Random (TCP
DB port (TCP)
UMS Console
UMS server
UMS DB
UMS

UMS and Devices: Secure Terminal

The UMS Console establishes a connection to the UMS server. The UMS server then establishes a TLS tunnel to the device.

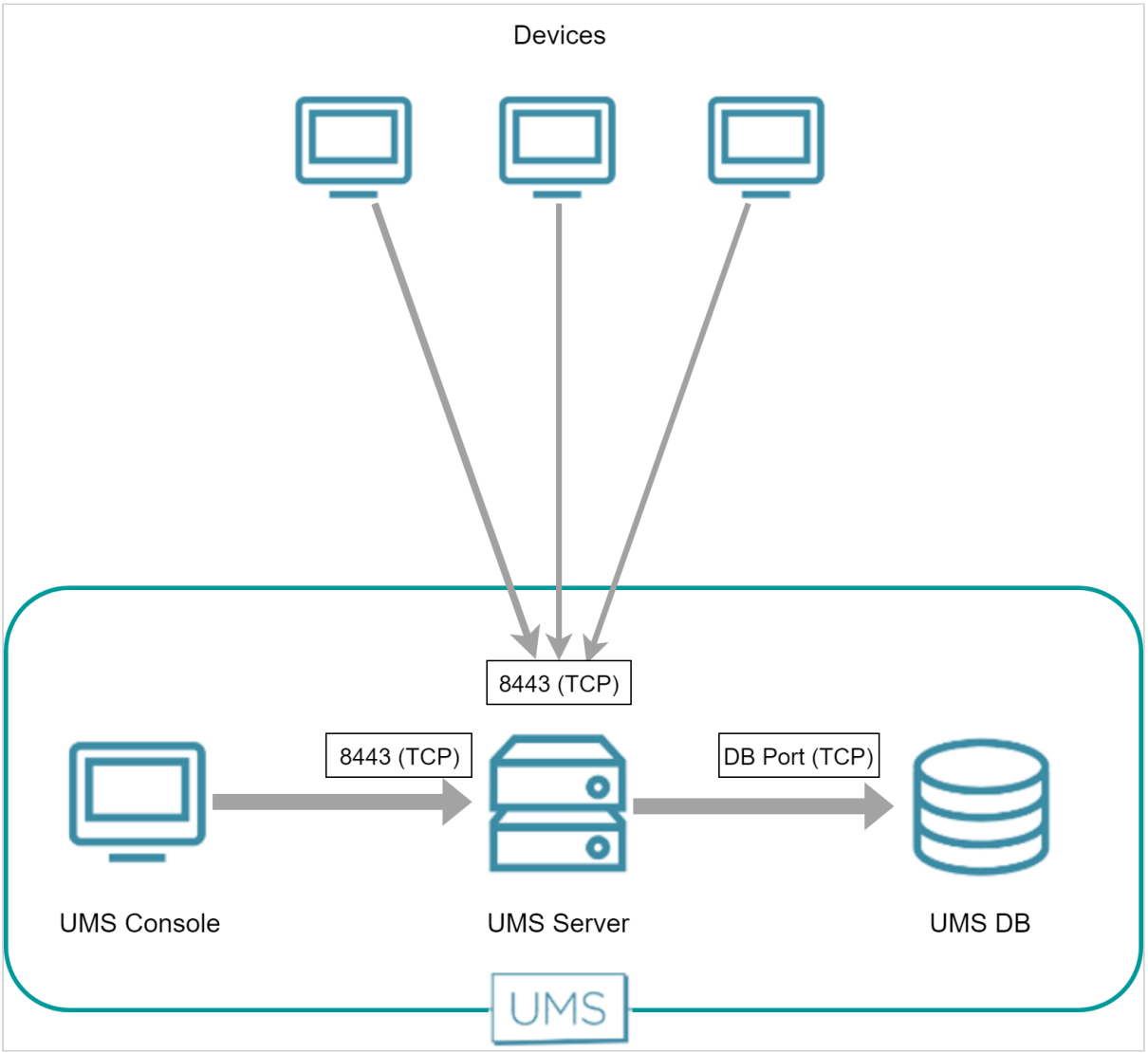
The following figure illustrates the communication between the UMS Console, the UMS server and a device:



UMS and Devices: File Transfer

To fetch files from the UMS, e.g. a background image or log files, the devices send an HTTPS request to the UMS server. The UMS server is listening on port 8443.

The following figure illustrates the communication between the devices and the UMS:



Universal Firmware Update

The Universal Firmware Update feature enables the UMS to check for new firmware updates and download the desired firmware to a WebDAV directory or FTP server. The connection to the IGEL download server can be direct or through a proxy.

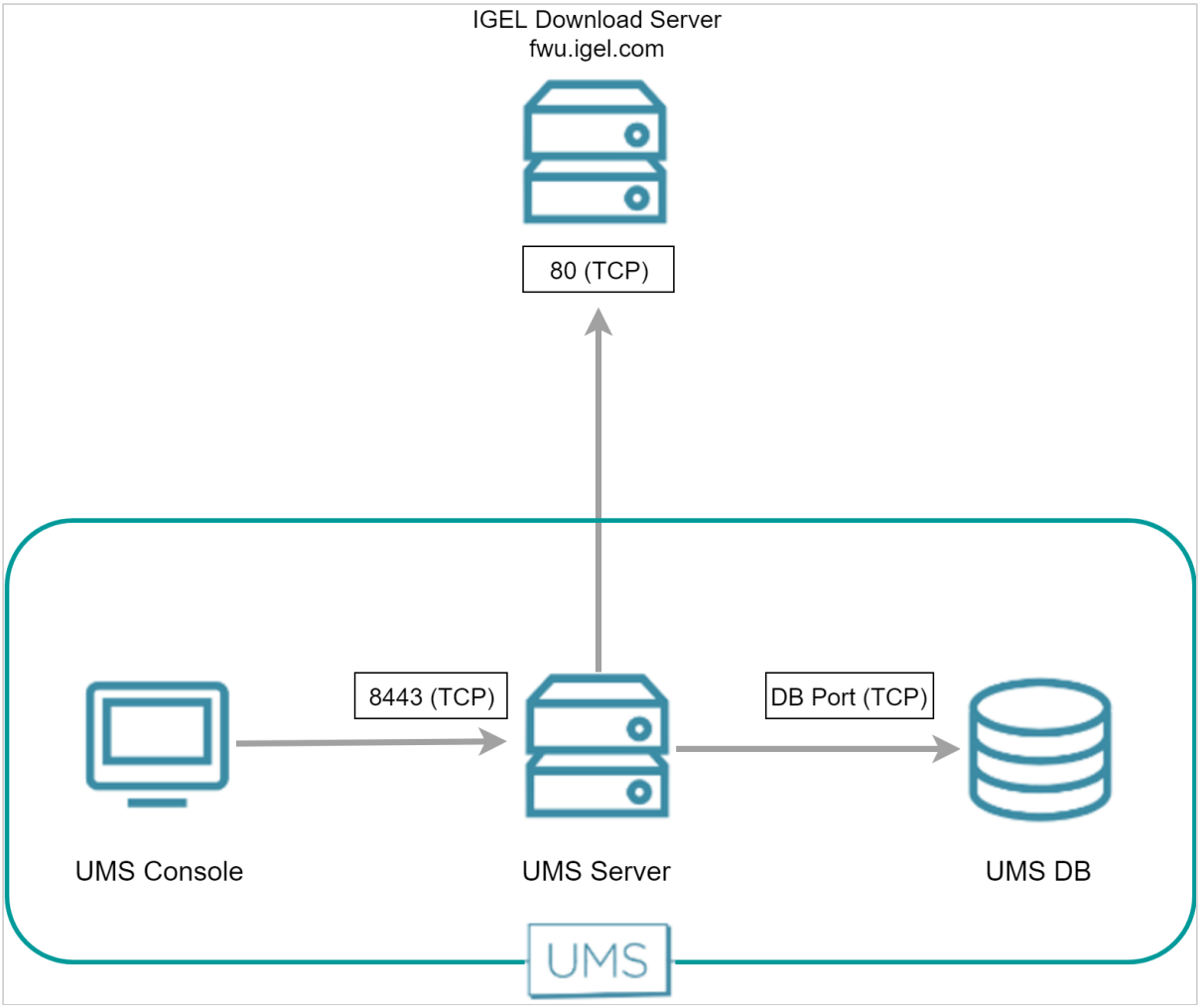
For more information about this feature, see Universal Firmware Update (see page 495) in the UMS manual.

UMS Contacting the Download Server to Check for New Updates

The UMS initiates a TCP connection to port 80 at fwu.igel.com. The IGEL download servers will send an answer containing a list of download links that enable the UMS to download the desired firmware.

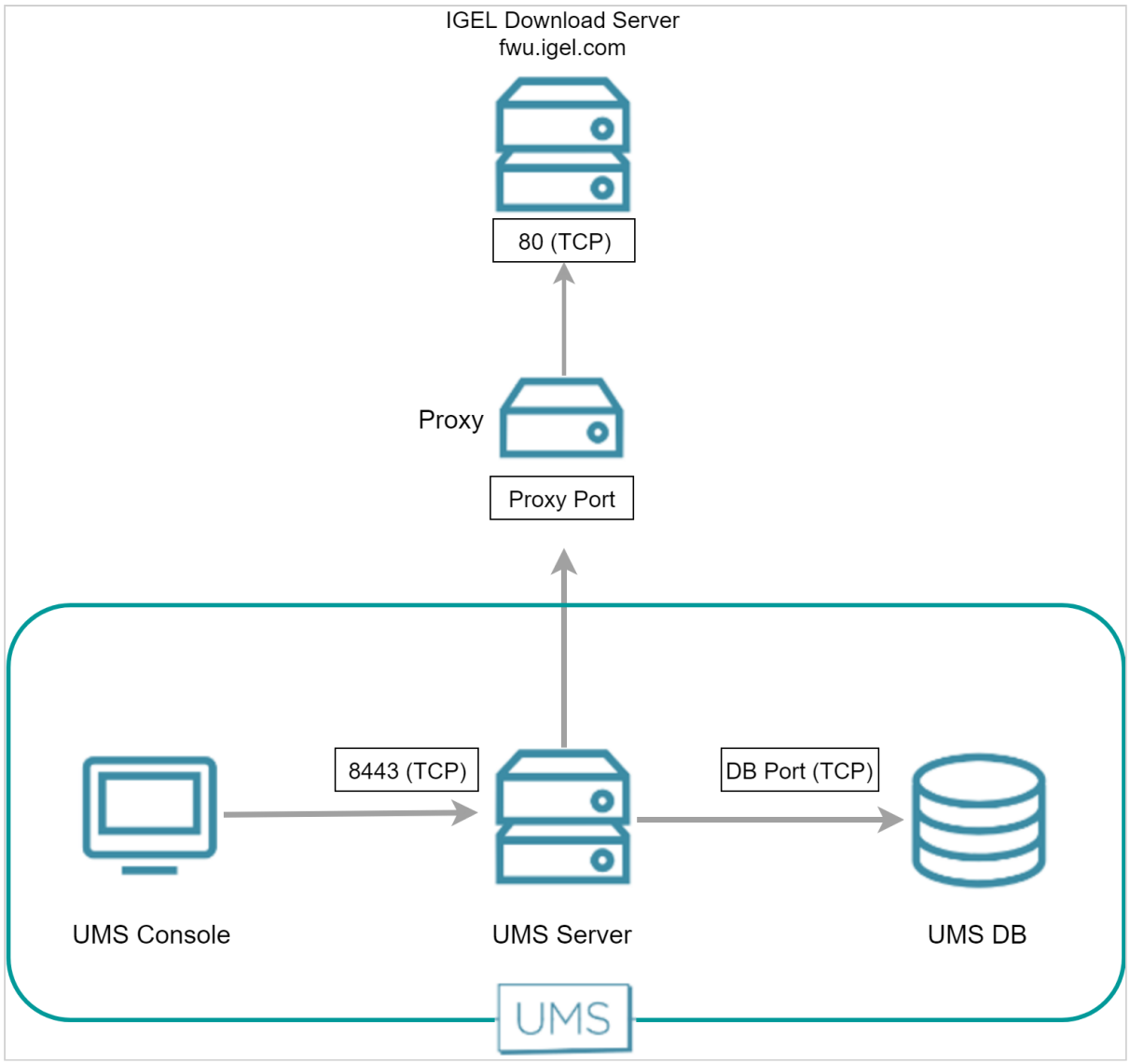
Direct Connection

The following figure illustrates the communication between the UMS server and the IGEL download servers:



Via Proxy

When a proxy is positioned between the UMS and the IGEL download servers, the port on which the proxy is listening must be specified under **UMS Administration > Global Configuration > Proxy Server**.

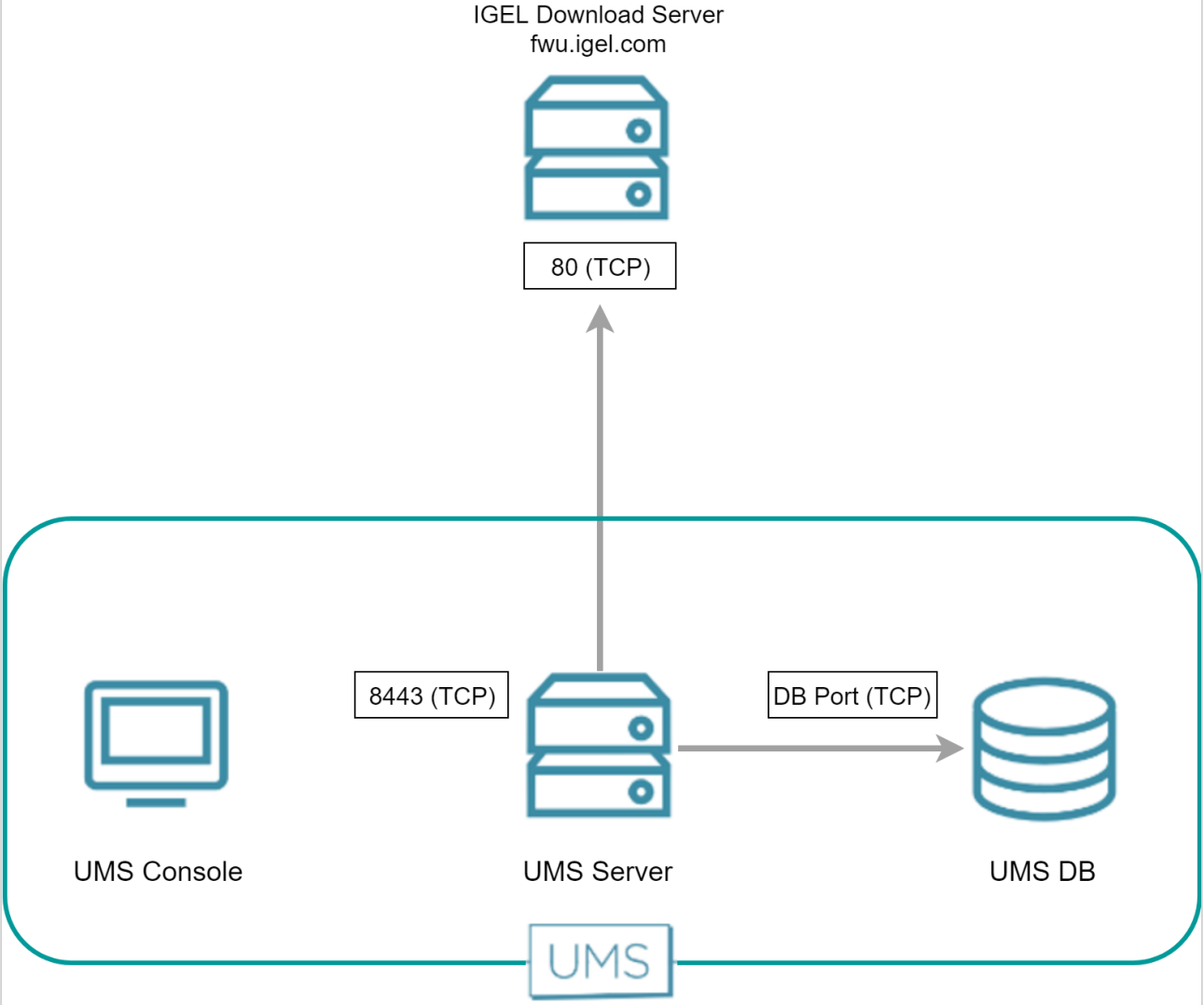

IGEL Download Server
fwu.igel.com
80 (TCP)
Proxy
Proxy Port
8443 (TCP)
DB Port (TCP)
UMS Console
UMS Server
UMS DB
UMS

UMS Downloading the Firmware

The UMS downloads the desired firmware using the URLs it received from the download server. The UMS uses port 80 for fwu.igel.com.

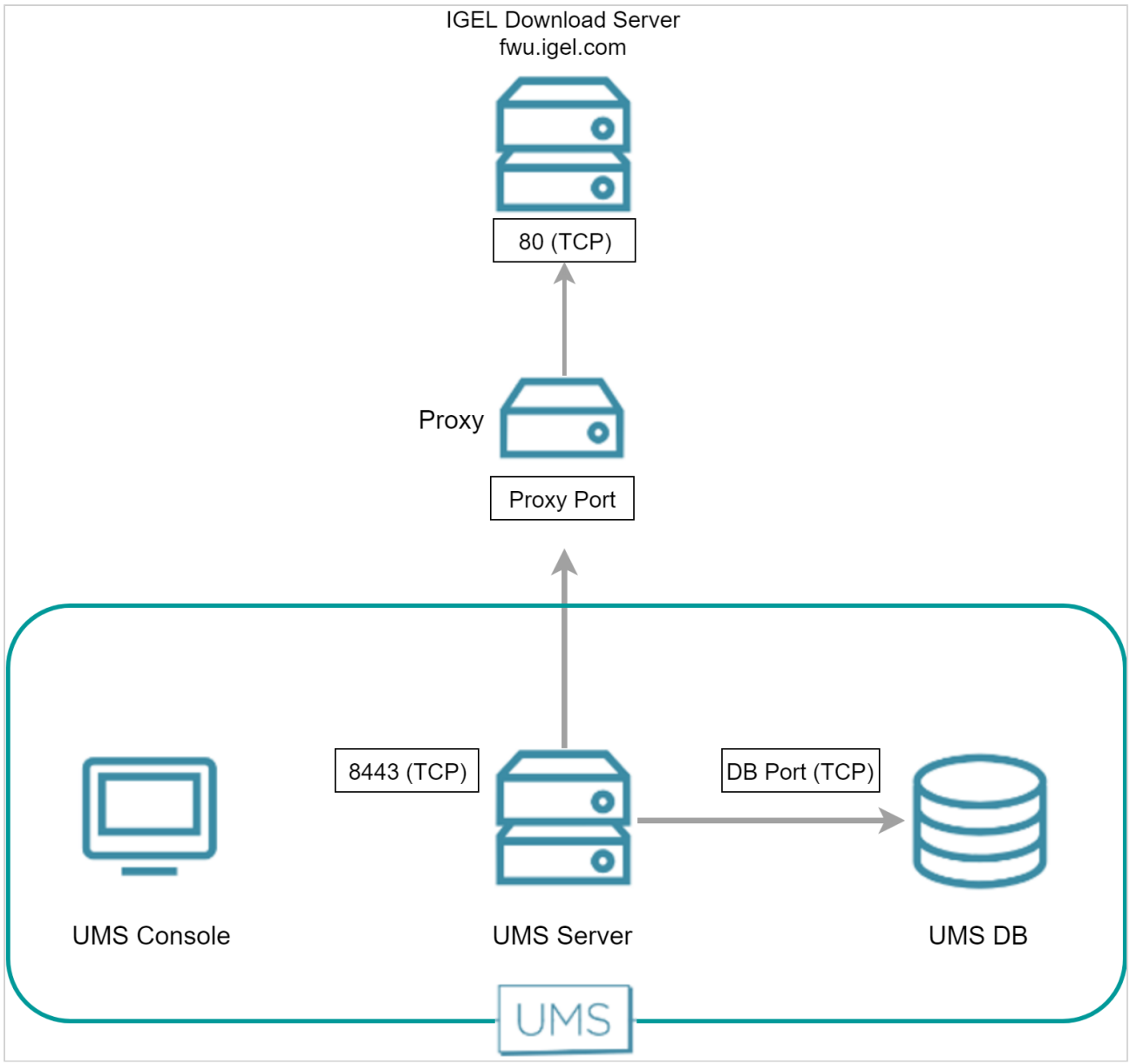
Direct Connection

The following figure illustrates the communication between the UMS server and the IGEL download servers:



Via Proxy

When a proxy server is placed between the UMS and the IGEL download server, the port for the proxy server must be specified under **UMS Administration > Global Configuration > Proxy Server**.


IGEL Download Server
fwu.igel.com
80 (TCP)
Proxy
Proxy Port
8443 (TCP)
DB Port (TCP)
UMS Console
UMS Server
UMS DB
UMS

Automatic License Deployment (ALD)

The Automatic License Deployment (ALD) feature is a method to deploy licenses to devices.

For more information about this feature, see Setting up Automatic License Deployment (ALD).

Automatic License deployment can be carried out via a direct connection or via a proxy.

The steps of the procedure are described in the following sections:

- UMS Contacting the Licensing Server (see page 52)
- UMS Sending New Settings to the Devices (see page 55)
- Devices Contacting the UMS to Download License Files (see page 56)

UMS Contacting the Licensing Server

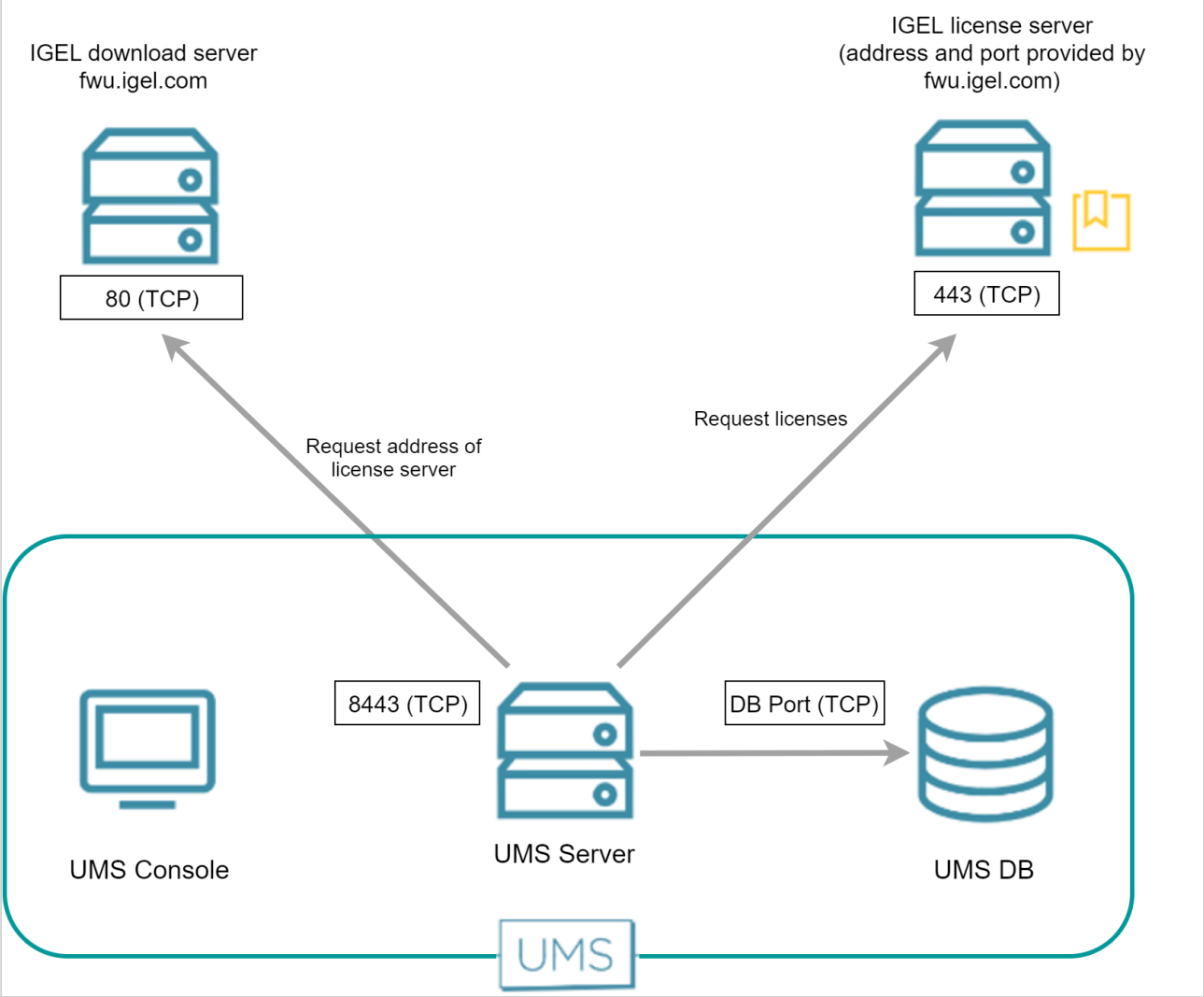
The UMS requests the connection details (URL and port) from IGEL download server fwu.igel.com and then contacts the IGEL licensing server. Currently, the connection details are as follows:

- URL: susi.igel.com
- Port: 443

> The connection details may be changed in the future.

Direct Connection

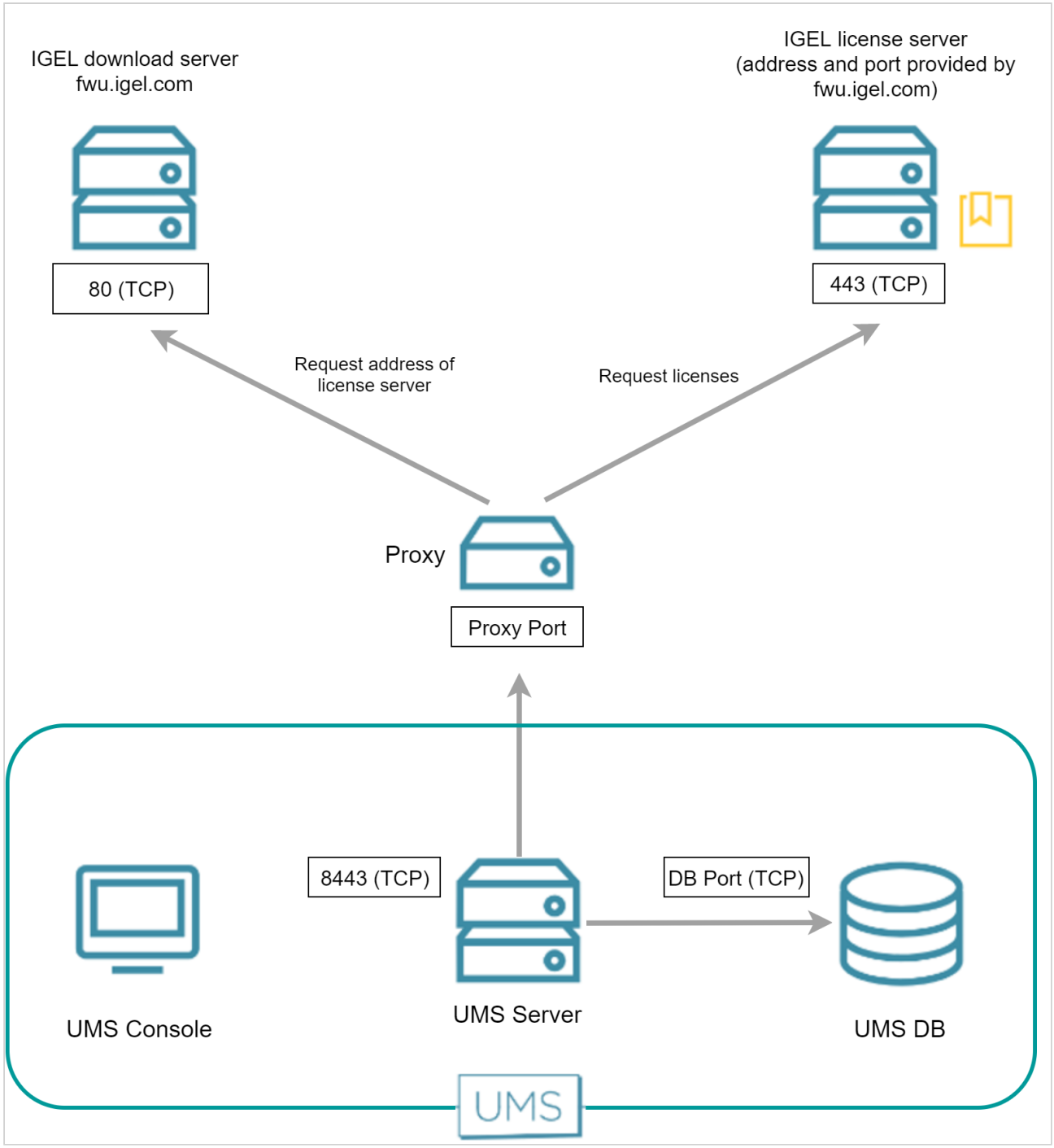
The following figure illustrates the communication between the UMS Server and the IGEL licensing server:



Via Proxy Server

When a proxy server is placed between the UMS and the IGEL licensing server, the port for the proxy server must be specified under **UMS Administration > Global Configuration > Proxy Server**.

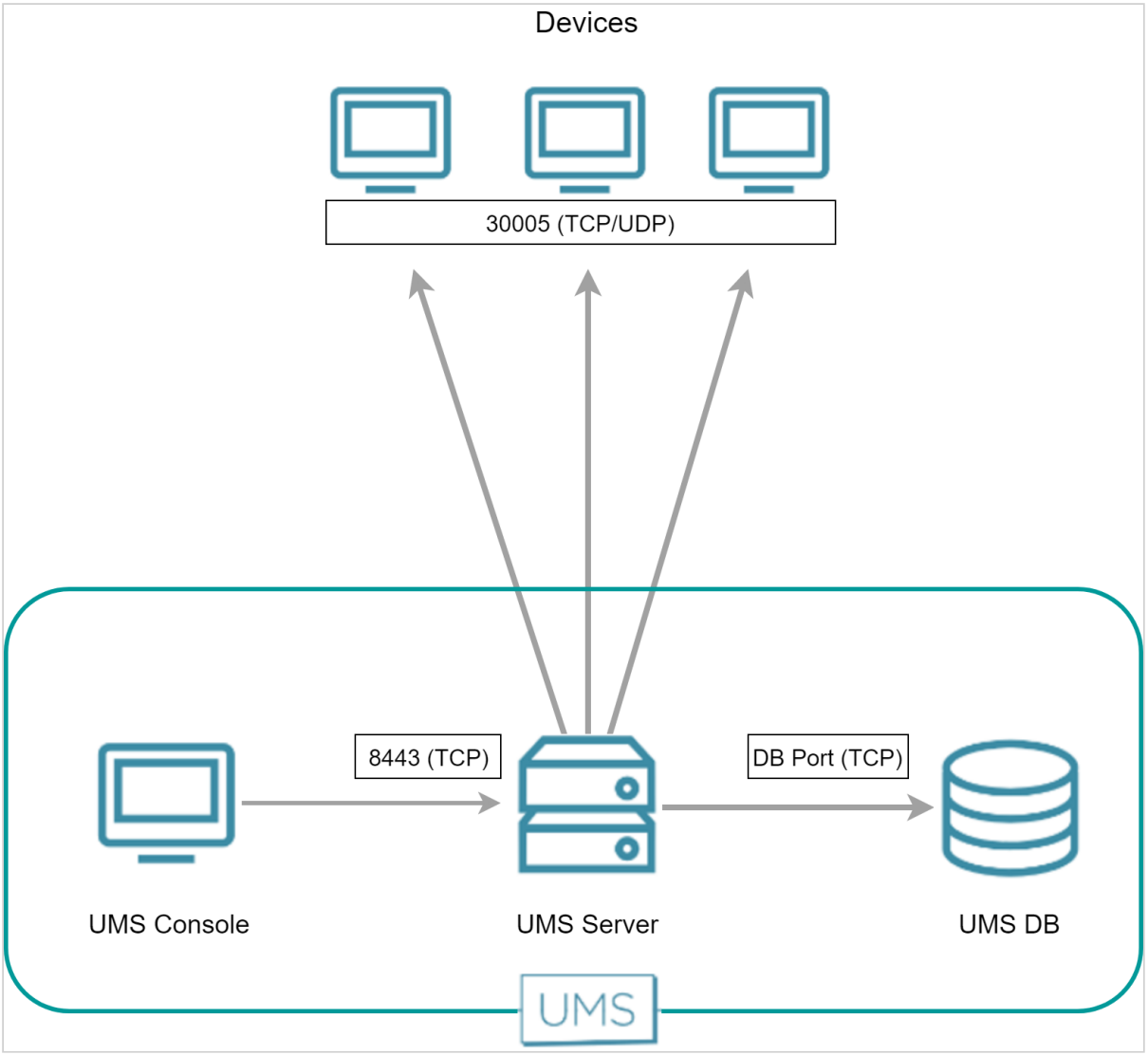
⚠ If multiple proxies are configured, ensure to select the one that is defined for license deployment.


IGEL download server
fwu.igel.com
IGEL license server
(address and port provided by
fwu.igel.com)
80 (TCP)
443 (TCP)
Request address of
license server
Request licenses
Proxy
Proxy Port
8443 (TCP)
DB Port (TCP)
UMS Console
UMS Server
UMS DB
UMS

UMS Sending New Settings to the Devices

After obtaining the licenses from the license server, the UMS sends new settings to each device in question, including a download link for the license files. The device is listening on port 30005.

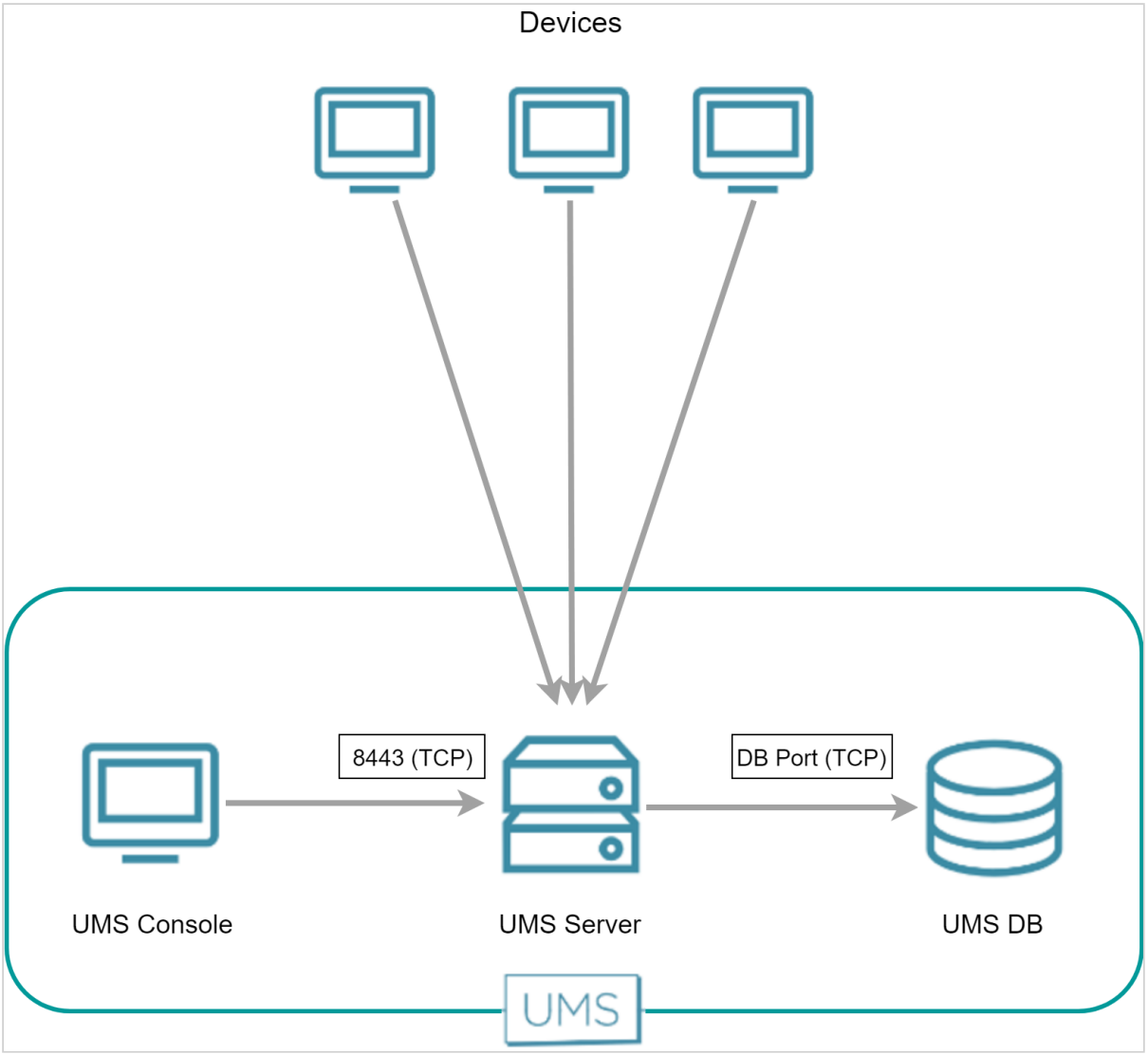
The following figure illustrates the communication between the UMS and the devices:



Devices Contacting the UMS to Download License Files

The devices have been informed by the UMS that license files are ready for download. Now, to fetch the license files from the UMS, the devices send an HTTPS request to the UMS server. The UMS server ist listening on port 8443.

The following figure illustrates the communication between the devices and the UMS:



UMS Installation

UMS Installation on 64-Bit Systems

Since version 5.09.100, IGEL UMS is 64-bit based. This article serves now for information purposes only.

Question

What are the prerequisites for the installation of IGEL Universal Management Suite on 64-bit operating systems?

Answer

Since UMS 5.09

From UMS Version 5.09, the installation of 32-bit libraries is no longer required. The necessary dependencies are automatically installed if the corresponding option has been chosen during the UMS installation procedure. For information on UMS installation, see Installing a UMS Server (see page 205).

Since UMS 5.07.100

From UMS Version 5.07.100, the required 32-bit libraries can automatically be installed by the UMS installer if the corresponding option is chosen during the UMS installation procedure.

Before UMS 5.07.100

- Windows: Use the 32-bit compatibility mode (which is activated by default) before installing IGEL UMS (e.g. on Windows Server 2008 R2).
  See also MSDN: "Running 32-bit Applications"[4]

- Linux (amd64/x86_64): Install the 32-bit compatibility packages before installing IGEL UMS. Examples with Ubuntu follow below, apart from that see:
  - Installing UMS on Red Hat Enterprise Linux (RHEL) 7.3 (see page 208)
  - Installing UMS on Oracle Linux Server (see page 210)

Example with Ubuntu 14.04 LTS 64-bit:

```
# add i386 support
sudo dpkg --add-architecture i386
sudo apt-get update
# install libraries
sudo apt-get install lib32z1 \ lib32ncurses5 \ lib32bz2-1.0 \ libxtst6:i386 \
libxinerama1:i386 \ libxi6:i386 \ libxext6:i386 \ libxrender1:i386
```

Example with Ubuntu 16.04 LTS 64-bit:

4 https://msdn.microsoft.com/en-us/library/aa384249%28VS.85%29.aspx

```
# add i386 support
sudo dpkg --add-architecture i386
sudo apt-get update
# install libraries
sudo apt-get install lib32z1 \ lib32ncurses5 \ libbz2-1.0:i386 \ libxtst6:i386 \ libxinerama1:i386 \ libxi6:i386 \ libxext6:i386 \ libxrender1:i386
```

Customization

User Authorization Rules

Problem

In the IGEL UMS, you want to assign permissions or roles to administrators according to various responsibilities.

Reason

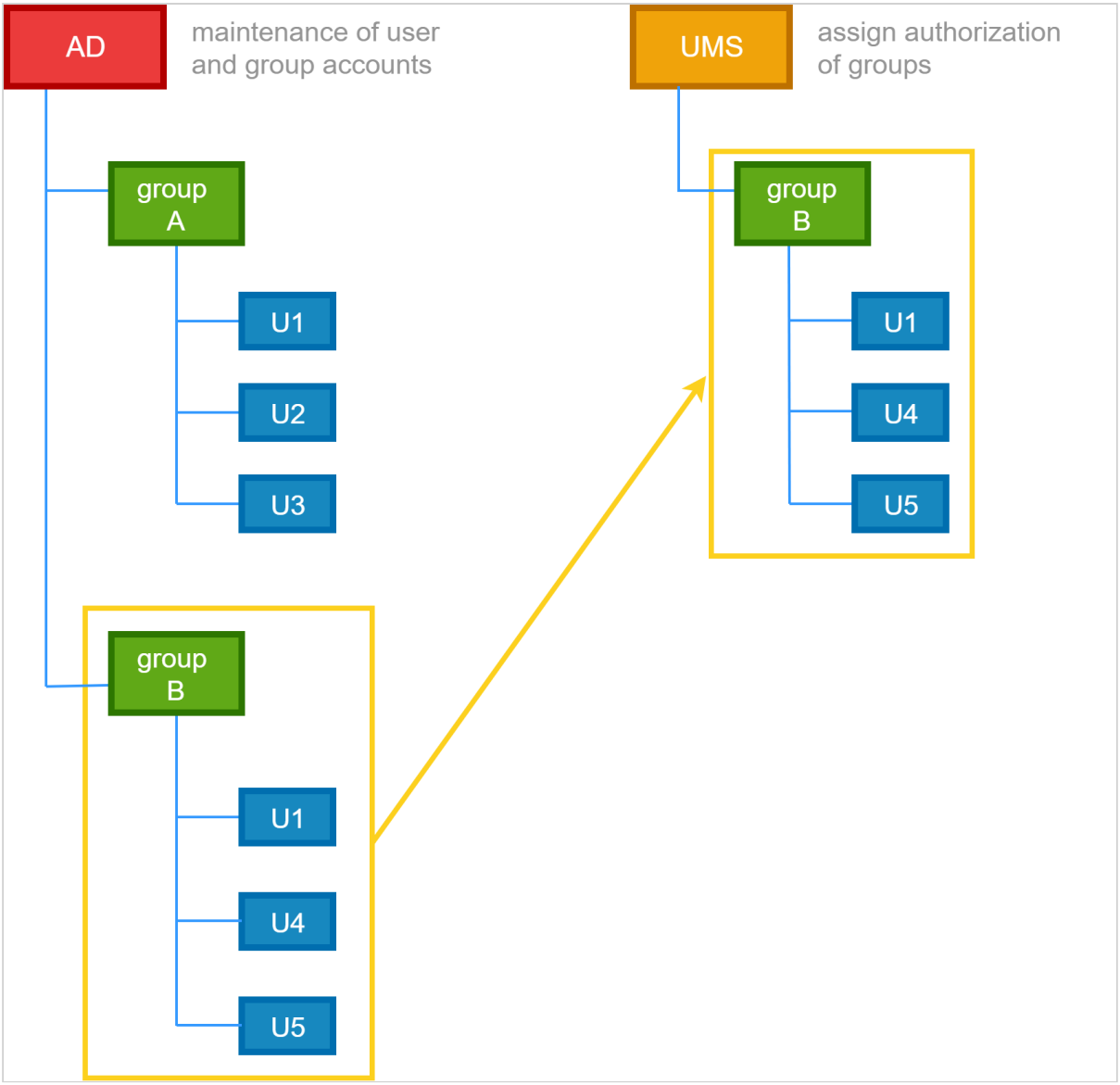
In the IGEL UMS, you can create user or administrator accounts, and you can assign rules to them, but it is not possible to assign roles.

You would like to group administrators according to their tasks in order to achieve a clearly structured management of user rights.

Within your company you already maintain employee accounts using an Active Directory or LDAP.

Solution

As best practice, we suggest connecting the UMS with the user accounts of the Active Directory. You maintain the user and group accounts in the Active Directory only. In the UMS, you assign rights to the imported groups.



Transferring Active Directory groups to the UMS and assigning permissions and roles to them:

▶ Click **UMS Administration > Global Configuration > Active Directory / LDAP** to integrate your Active Directory.

You may import Administrative Users / UMS administrators from an Active Directory as well as from an LDAP.

▶ In the UMS console click **System > Administrator accounts > Import**, to import groups from the tree of your Active Directory.

> The successful import of a group cannot be undone. You have to manually delete the wrongly created UMS group in the "Administrator account" management. The name of the imported Active Directory group is taken from the account.

▶ Assigning roles to groups in the IGEL UMS on the basis of authorization rules:

- Click **System > Administrator accounts > Groups > Edit** to directly assign general group rights.
- Assign object-related access rights via object permissions, choosing **Access Control** in the context menu of any object.

This way, you can assign certain roles to administrators of the UMS according to their group memberships.

Please note:

- Permissions are inherited from a parent directory to a child directory or to a subordinated object.
- It is possible to change indirect rights, i.e. rights which are given by group assignment. However, directly assigned rights take precedence over indirectly assigned rights.
- An administrator can be a member of different groups and receives the corresponding rights. If they are contradictory, the deprivation of a right takes precedence over the permission. If a prohibition for an action or an object of a group is issued, it will override any number of rights from other groups.
- Click **Effective Rights** to get more details about the rules collection, for example if a permission was given directly or if it was assigned by a group or by an inheritance within a tree structure.

Managing User Permissions via UMS

Purpose

It is necessary to globally manage the permissions of the thin client users, e.g. for editing system information.

Solution

Use the **Access Control** function in the UMS.

Additional Information

There are different places where to open the **Access Control** dialog:

- In the main menu under **Edit > Access Control**
- In the symbol bar under 
- In the context menu of a thin client or a thin client folder under **Access Control**

Defining end user permissions:

1. Click **Access Control** in the context menu of a thin client (folder).
   The **Access Control** dialog opens.
2. Click **Add** to select a new user/group.
3. The corresponding **Effective Rights** will be listed in the lower part of the mask.
4. **Allow** or **Deny** the permissions of the selected group or user for the selected thin clients.
5. Confirm the settings with **OK**.
6. Click the **Refresh** button of the console to apply the changes in the UMS.

   If you have changed the rights of registered users they only take effect after a refresh.

   For further details about authorization rules see our How-To IGEL UMS: User Authorization Rules (see page 61).

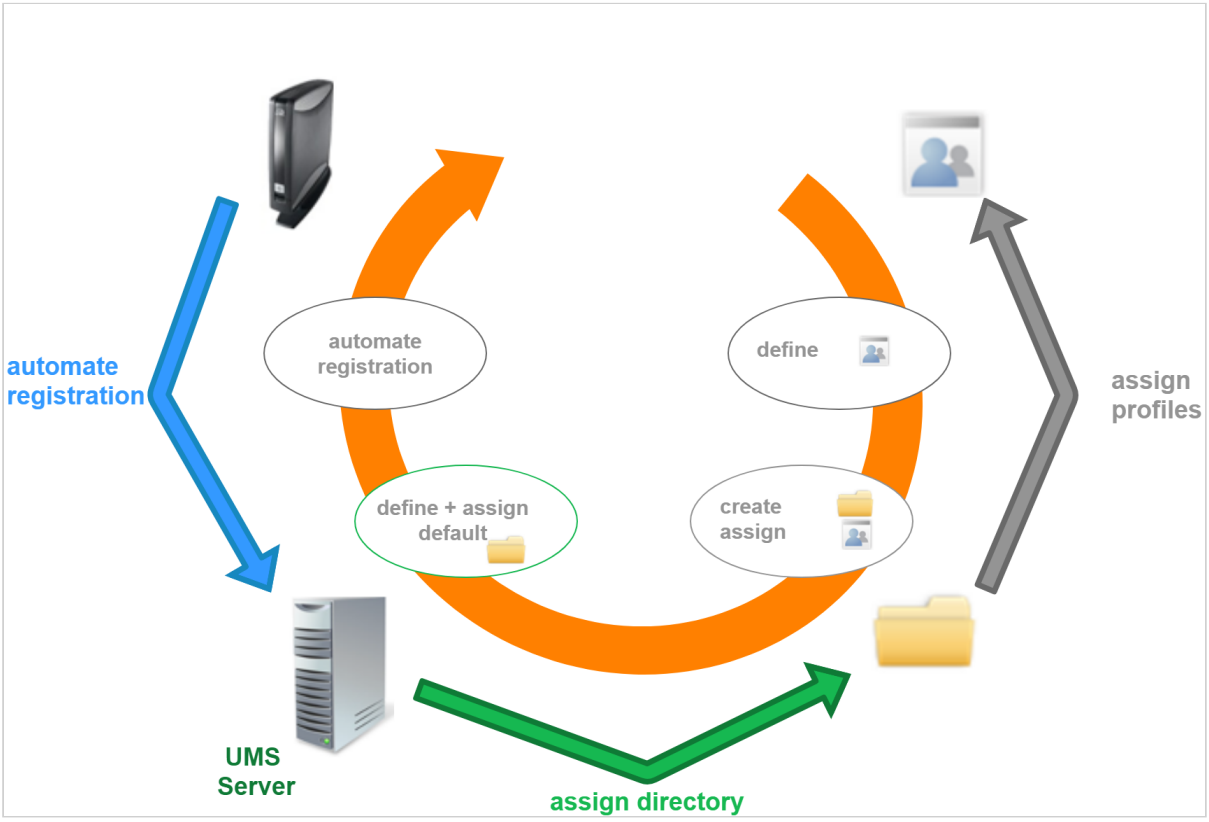
Access rights to objects or actions within the *IGEL* UMS are attached to the administrator accounts and groups. The rights of the database user account cannot be restricted. They are created during installation or when setting up the data source. The account always has full access rights in the UMS.

Automating the Rollout Process in the IGEL UMS

You want to set up the IGEL Universal Management Suite (UMS) in such a way that new devices will be stored directly in the correct directory and the right configurations will automatically be assigned to them. With Zero Touch Deployment in the rollout, devices will be configured automatically according to the profiles, with almost zero management outlay.

The idea of Zero Touch Deployment means automatic device registration with automatic assignment of profiles by default directory rules.

In the end, the device will automatically be registered in the UMS, assigned to the right directory, and related to the valid profiles. To prepare this automated process, you have to go the other way around. First, define the profiles, then assign them to the directories, then create default directory rules and automate the registration.



Preparing Automatic Rollout

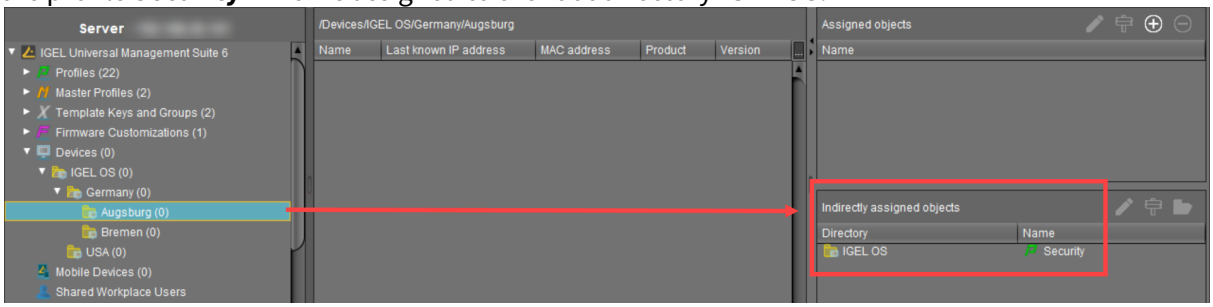
Configure your device globally, indirectly assigning profiles by a parent directory:

1. Create a new root directory, e.g. **IGEL OS**.
   For how to create a device directory, see Creating a Directory in the IGEL UMS (see page 357).

2. Assign certain profiles to this root directory, e.g. **Security**.
   For how to assign profiles, see How to Allocate IGEL UMS Profiles (see page 288). See also Prioritization of Profiles (see page 304).
   For detailed information on profiles, see Profiles (see page 276).

3. Move your devices or your directories containing devices to this root directory.
   These devices will inherit the profiles assigned to the root directory.

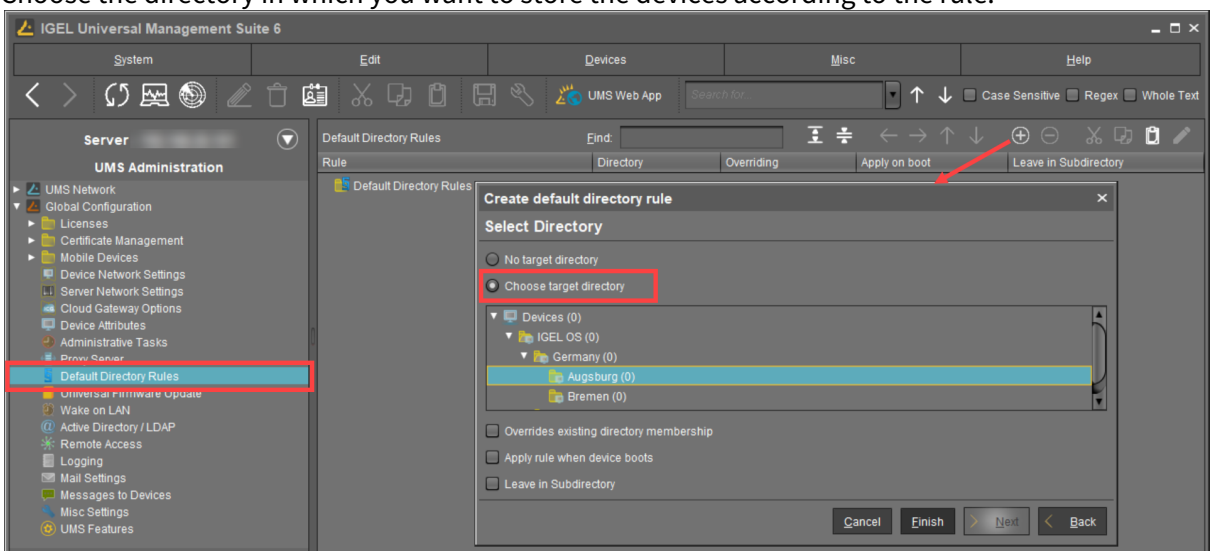
   Example: Devices that will be placed to the directory **Augsburg** during the registration will inherit the profile **Security** which is assigned to the root directory **IGEL OS**:

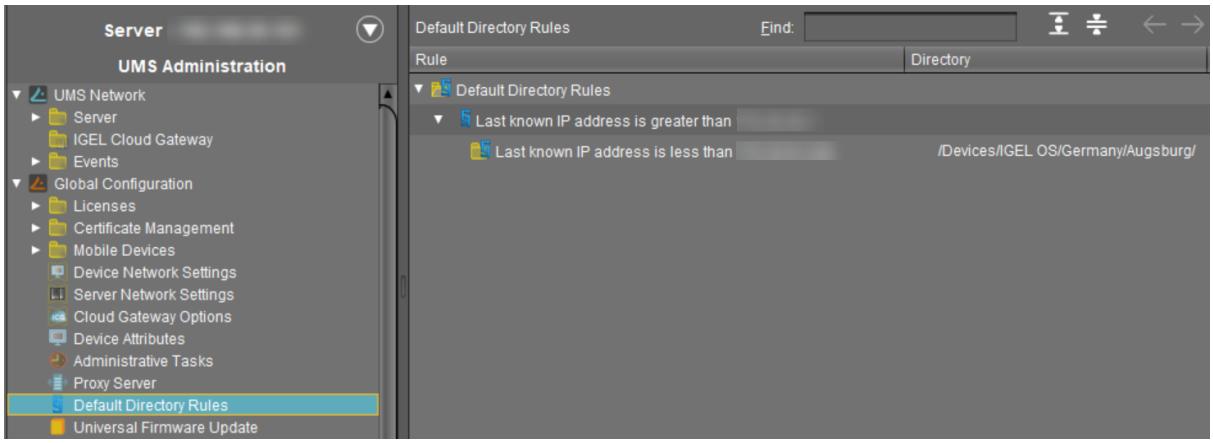


Automating the Rollout

1. Click **UMS Administration > Global Configuration > Default directory rules** to create a new default directory rule.
   For detailed information on default directory rules, see Default Directory Rules (see page 484).

2. Choose the directory in which you want to store the devices according to the rule.



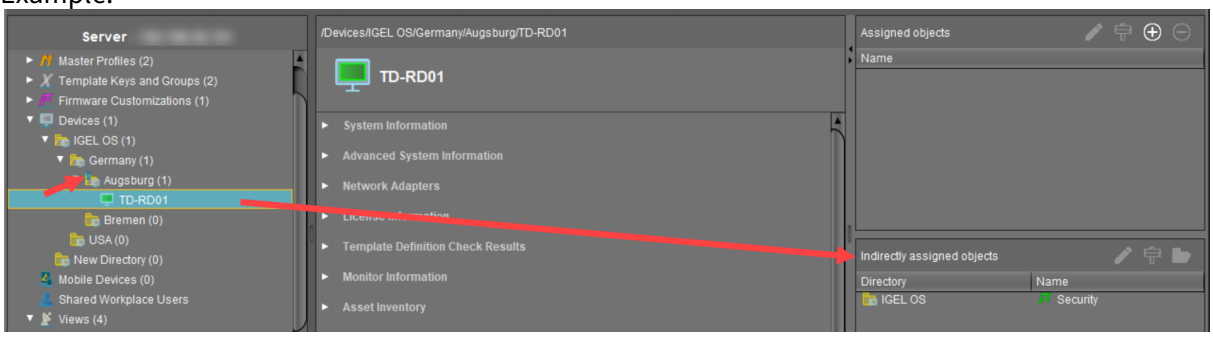


3. Configure your DNS or DHCP server and activate the automatic registration of devices as described under Registering Devices Automatically on the IGEL UMS (see page 242).

   > We recommend disabling automatic registration after the rollout, so that no unknown devices will be registered without your control and could obtain sensitive settings.

4. Start your devices. They will be automatically registered on the UMS Server.
   Thanks to the default directory rule, these devices will be stored in the right directory and will automatically receive the correct profiles.

   Example:



Related Topics

If you want to use structure tags for automating the rollout: Using Structure Tags (see page 68)

If you have problems with the device registration: Registration of a Device in the IGEL UMS Fails (see page 135)

Using Structure Tags

Problem

When rolling out devices automatically it can be difficult to assign each to the desired folder in the Universal Management Suite (UMS).

Goal

Newly registered thin clients will automatically have the information where they are to be placed in the structure tree of the UMS.

The UMS will have flexible rules to place a newly registered device into a folder of the structure tree.

Solution

One solution is using a structure tag, a text string bound to the device, that is transmitted to UMS. It can be assigned to devices either via a DHCP option or in their local setup.

> This works with UMS *Version 4.08.100* or newer, and IGEL Linux Version 5.05.100 or newer, IGEL WES 7 Version 3.11.100 or newer, and IGEL Unified Management Agent Version 1.02.100 (for Windows 7) / Version 2.01.100 (for Windows 10) or newer.

- Defining a Structure Tag in UMS (see page 69)
- Assigning a Structure Tag to the Client (see page 72)

Defining a Structure Tag in UMS

The information in this document depends on the UMS version you use. You can find out your version by looking at **Help > Info** in the UMS main menu.

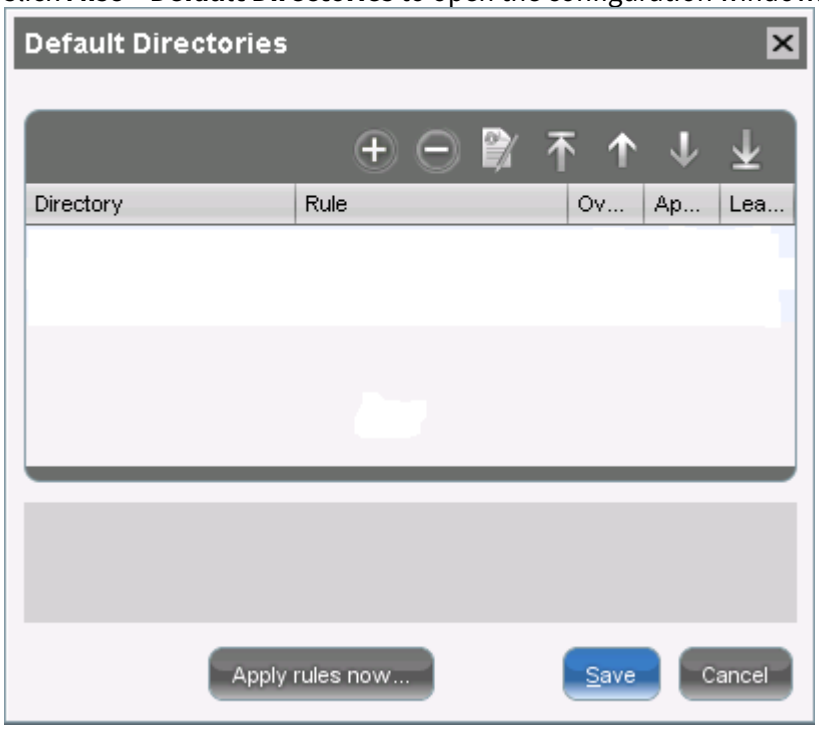
From UMS Version 5.03.100:

In UMS Version 5.03.100 the handling of the Structure Tag has been simplified. You can now use it like any other criterion in your Default Directory Rules under **UMS Administration > Global Configuration > Default Directory Rules**.

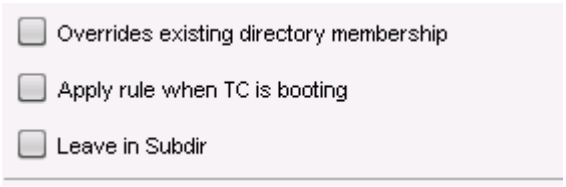
Learn more in the UMS manual: Default Directory Rules (see page 484).

Prior to UMS Version 5.03.100:

1. Open the UMS console.
2. Click **Misc > Default Directories** to open the configuration window.

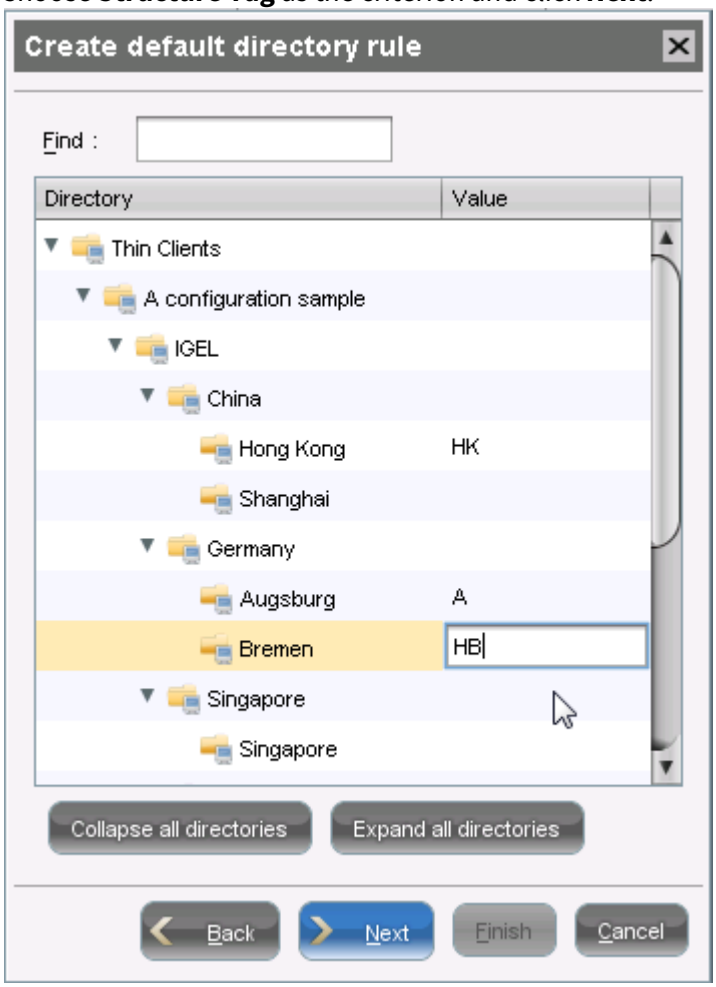


3. Click the **(+)** symbol.
4. Select a default directory for any devices which do not provide a tag.
5. Define if this rule is to override the existing directory membership and whether it is to be executed once (on first registration) or on every boot of the client.



> All devices with a structure tag that is not assigned to another directory will be sorted into this default directory.

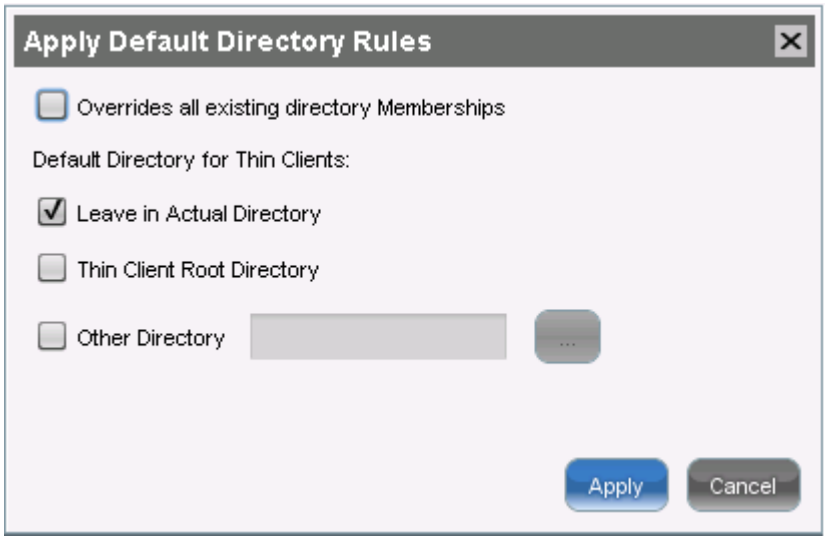
6. Click **Next**.
7. Choose **Structure Tag** as the criterion and click **Next**.



8. Define a **Value** (tag) for the relevant folders.
9. Click **Next** and **Finish**.
10. Sort the default directory rules by marking a rule and clicking the up and down arrows.

> The order of the structure tag rules is important, because they will be executed in a hierarchical way, just like all the other rules. It may be useful to move a structure tag rule to the bottom of the list so that it will be executed only if no other rule takes effect

11. Decide whether you want to **Apply rules now ...** or to **Save** the default directory rules.
If you want to apply the rules, you have to specify the default directory for devices not matching a rule:



General Note on Directory Rules

UMS executes the rules in the predefined order. As soon as one rule is fulfilled, no other rule will be executed. The option **Leave in Actual Directory** means that the UMS thinks a rule is fulfilled if a device is situated in the target directory or in its subdirectory. No other rule will then be executed, and the device will remain in the current directory.

If you enable **Overrides all existing directory Memberships** you can control if the directory holds only devices that are not members of a certain directory or if it houses all devices. Both options make sense only if you have enabled **Apply rule when TC is booting** or if you apply the rules manually.

Assigning a Structure Tag to the Client

There are two ways of assigning a structure tag to a device:

- Manual assignment on the client (IGEL Linux Version 5.05.100 or newer, IGEL WES7 Version 3.11.100 or newer , IGEL Unified Management Agent Version 1.02.100 (for Windows 7) or Version 2.01.100 (for Windows 10) or newer
- Assignment via DHCP server

Assigning a Structure Tag Manually on the Device

1. In **Setup**, go to **System > Remote Management**.
2. Enter the structure tag value in **Universal Management Suite Structure Tag**
3. Click **OK**

Assigning via DHCP Server

Use DHCP option 226 to distribute the tag value to the device.

Deploying an IGEL made Custom Partition via UMS

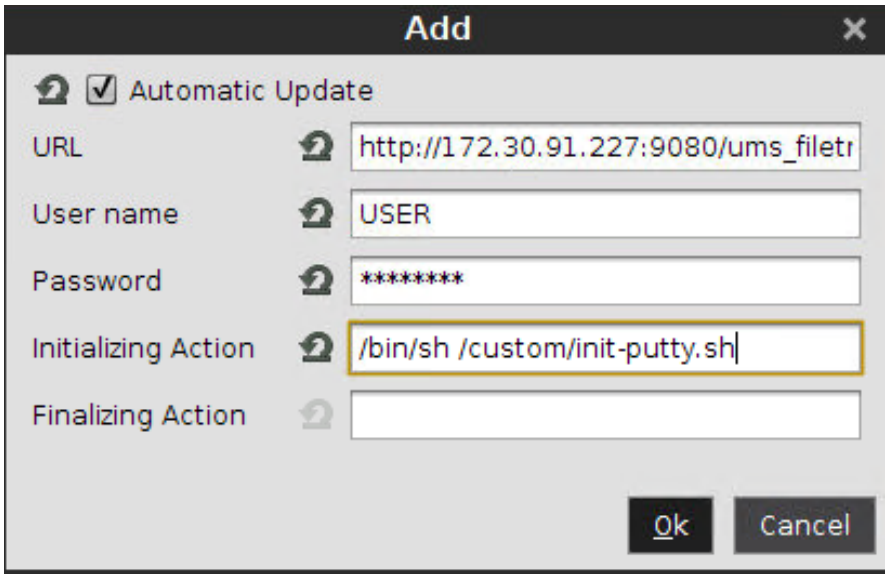
Goal

You want to deploy a custom partition that you received from IGEL to a number of thin clients via the Universal Management Suite (UMS).

Solution

> The procedure described here is only intended for installing custom partition packages that have been built by IGEL.

1. Save the `*.zip` archive you received locally and extract it.
2. Copy the contents of the directory `target` into the `ums_filetransfer` directory on the UMS Server, e.g. `C:\Program Files (x86)\IGEL\RemoteManager\rmguiserver\webapps\ums_filetransfer`
3. Check the accessibility of the data by opening its address in a web browser, e.g. `http://[ums_server]:9080/ums_filetransfer/[name]/[name].inf`
   This access is password-protected, and you need to enter your UMS credentials.
4. Import the file `profiles.zip` (located in the `igel\profiles` directory of the package) into the UMS via **System > Import > Import Profiles**.
   The imported profile should now appear in the UMS Console under **Profiles**.
5. Edit the profile and adapt the settings in **System > Firmware Customization > Custom Partition > Download** to match the **URL**, **Username** and **Password** for your UMS.



6. Assign the profile to one or more devices.
7. Reboot these devices.

UMS Environment

Migrating a UMS Server

Purpose

You want to migrate your IGEL Universal Management Suite to a new server.

Scenarios

The following scenarios can occur when migrating the UMS to a new server:

- Migrating the UMS with the embedded data source: With the Same Embedded Database (see page 77).
- Migrating the UMS with the external data source: With the Same External Database (see page 81).
- Migrating the UMS and changing the data source: With a Different Database (see page 85).

The switch from a standard UMS installation to a High Availability (see page 560) installation, which involves the migration of the existing UMS Server to a new host and, if the embedded database is in use, the move to the external database, is described separately under Switching from a Standard UMS Installation to an HA Installation (see page 581).

Recommendation: The Same Software and Database State

It is NOT recommended to combine the migration and update procedures, e.g. to move from UMS 6.01 to 6.08. It is advised to update the UMS Server and migrate it afterward, or vice versa.

During the migration, there will be no negative impact on your endpoint devices – they will continue to work autonomously. Exception: login via Shared Workplace (SWP) (see page 594). For details, see Which Features of IGEL OS Will Be Affected If the UMS Is Down?.

Tip

The move provides an opportunity to remove any UMS database data which are no longer used. For example, you can

- delete endpoint devices that no longer exist
- delete profiles that are no longer used
- remove files and firmware updates that are no longer needed

It is highly recommended to create a backup before carrying out the cleanup (as a backup of the system running) and another one after the cleanup.

With the Same Embedded Database

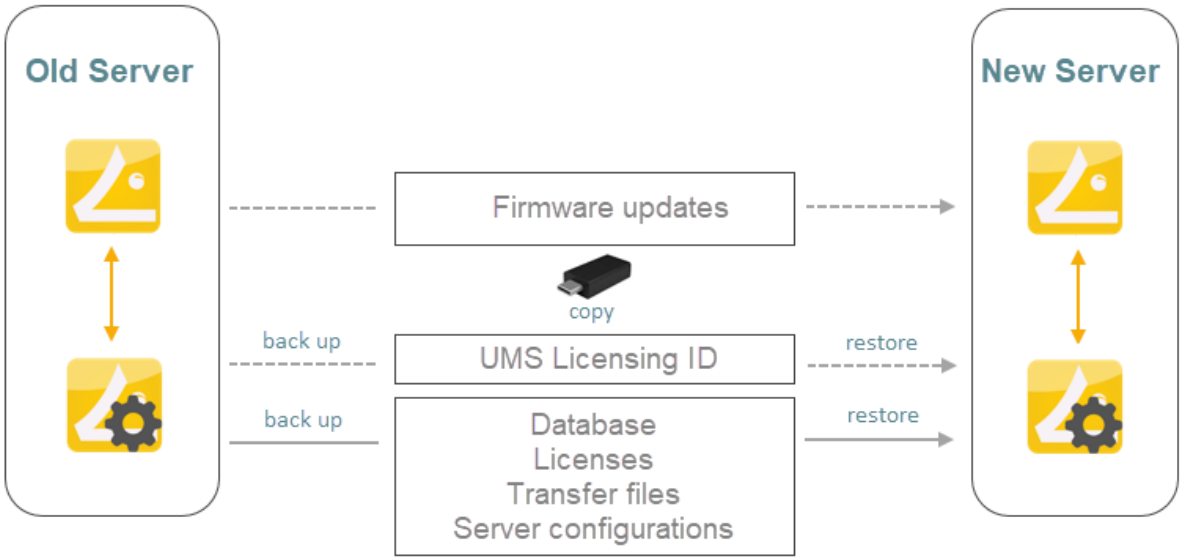
Use Case

You have a UMS installation with an embedded database and want to migrate to a new UMS Server with the same embedded database.

General Overview

The migration procedure generally involves the following steps:

1. Backing up the old server. Checklist for the backups:
   - ✅ **Database**
   - ✅ **Licenses**
   - ✅ **Transfer files**
   - ✅ **Server configurations** (host-specific server configurations that differ from the defaults are noted down separately)
   - ✅ **Firmware updates**
   - ✅ **UMS Licensing ID**
2. Stopping the `IGEL RMGUIServer` service on the old server
3. Transferring the created backups to the new server
4. Adjusting DHCP tag and DNS alias on the new server OR creating a profile with the IP of the new server for remote administration



Instructions

On the Old Server

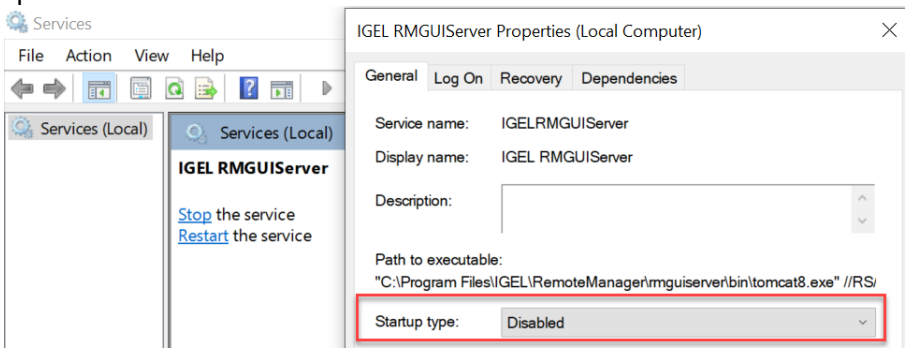
1. On the old server, create a backup under **UMS Administrator > Backups** and copy it to a storage medium. Include all options in the backup. For detailed instructions, see the "Embedded Database" section under Creating a Backup (see page 546).

   > The backup of **Server configurations** includes most configurations of the Settings (see page 540) area in the UMS Administrator application. Exceptions: **GUI server port**, **JWS server port**, and **ciphers** – they are host-specific, i.e. stored separately on each server and cannot be part of any backup. Therefore, you should note the values of these settings if they differ from the defaults and, in the case of recovery/migration procedure, they must be changed on each server manually.

2. Create a backup of the UMS Licensing ID in the **UMS Administrator > UMS Licensing ID Backup**. For detailed instructions, see Transferring or Registering the UMS Licensing ID (see page 86).
3. Copy all files from the following folders.

Device licenses	• `[IGEL installation directory]/rmguiserver/webapps/e08ce61-d6df-4d2b-b44a-14c1ec722c44`
Files and firmware updates	• `[IGEL installation directory]/rmguiserver/webapps/ums_filetransfer`

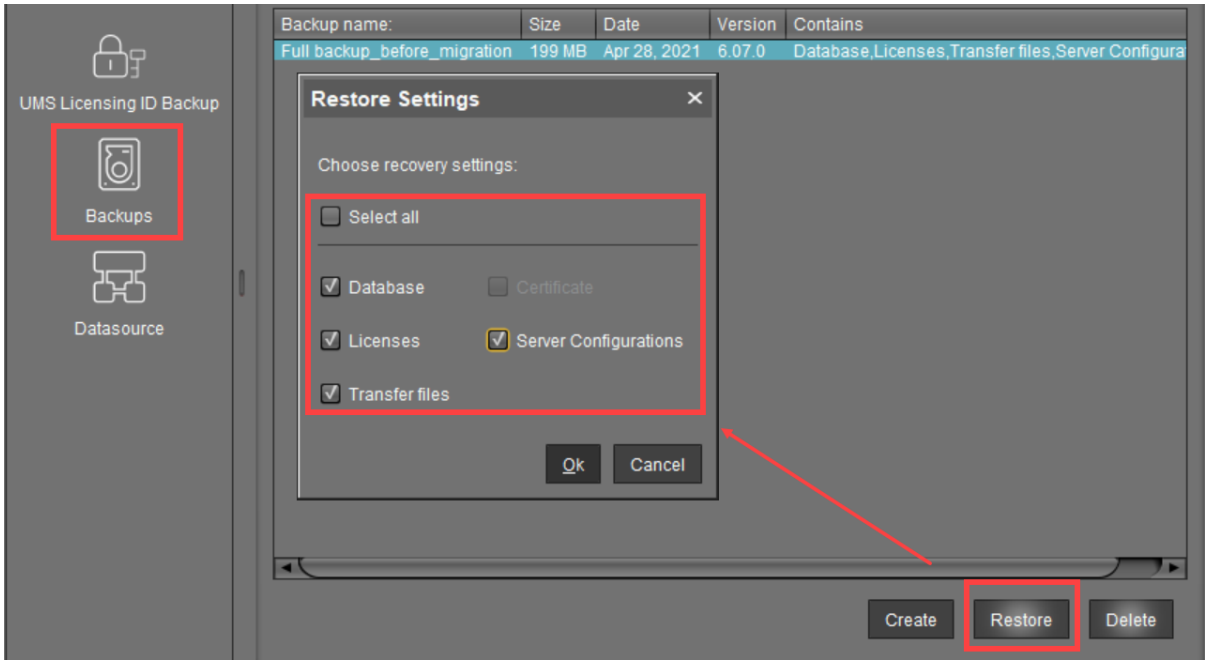
4. Stop the service `IGEL RMGUIServer` (for instructions, see HA Services and Processes (see page 592)) and set the startup type for it to "Disabled" in order to prevent accidental parallel operation with the new UMS Server.



On the New Server

1. Install the UMS on the new server. If possible, use the same database user and password. For the installation instructions, see Installing a UMS Server (see page 205).
2. Under **UMS Administrator** > **Backups**, select the folder with your backup and restore the respective backup file with all options. Wait until the UMS Server fully starts, i.e. the UMS Console

can connect with it.



3. If necessary, transfer host-specific server configurations to the new server.
4. Transfer the UMS Licensing ID of the previous UMS installation to the new server: **UMS Administrator > UMS Licensing ID Backup > Restore**. Alternatively, you can register the new UMS Licensing ID, which was created during the installation of the new server. For detailed instructions, see Transferring or Registering the UMS Licensing ID (see page 86).
5. Copy files from the following folders to the new server – without the `WEB-INF` folder:
   - `[IGEL installation directory]/rmguiserver/webapps/ums_filetransfer`
   - `[IGEL installation directory]/rmguiserver/webapps/e08ce61-d6df-4d2b-b44a-14c1ec722c44`
6. Restart the service `IGEL RMGUIServer`.
7. If ICG is used: All ICGs have to be reinstalled, see ICG Reinstallation after the Migration of the UMS Server (see page 103).
8. Adapt, if necessary, the DHCP tag and the DNS alias `igelrmserver` with the IP or FQDN of the new UMS Server. See Registering Devices Automatically on the IGEL UMS (see page 242).

> ⓘ The configuration of the DHCP tag and the DNS alias is not a setting that can be made within the IGEL software. You must configure these within your individual network environment on the corresponding DHCP and DNS servers.

If you have used and adjusted the DNS alias and the DHCP option, the following step is NOT required since the device can resolve the name `igelrmserver` correctly.

In the local configuration, the device always remembers the IP of the UMS Server of its first registration. It is thus possible that the old IP address is displayed under **System > Remote Management**. Therefore, it makes sense to manually set an entry for remote administration after the migration:

a. Create a profile in the UMS:
   - Go to **System > Remote Management** and click **Add**.
   - Under **UMS Server**, enter the IP of the new UMS Server.

b. Apply this profile globally, to the entire structure.

After the procedure is complete, open the UMS Console and go to **UMS Administration > UMS Network > Server** to check if there is an entry for the previous UMS Server among the listed components. If so, select the entry and click **Delete** in the context menu.

With the Same External Database

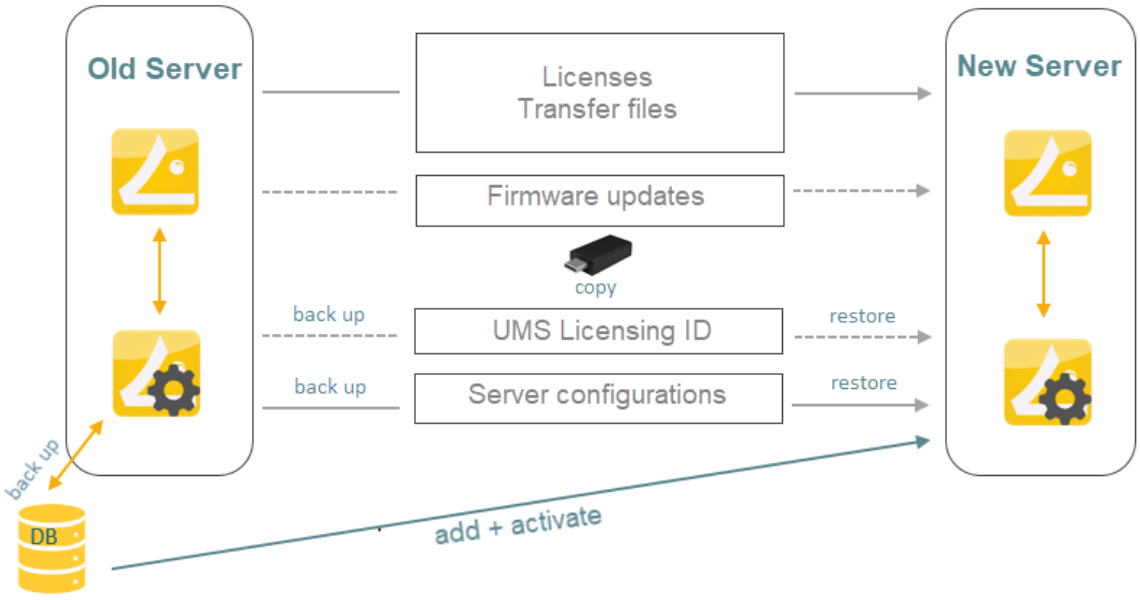
Use Case

You have a UMS installation with the external database and want to migrate to a new UMS Server with the same external database.

General Overview

The migration procedure generally involves the following steps:

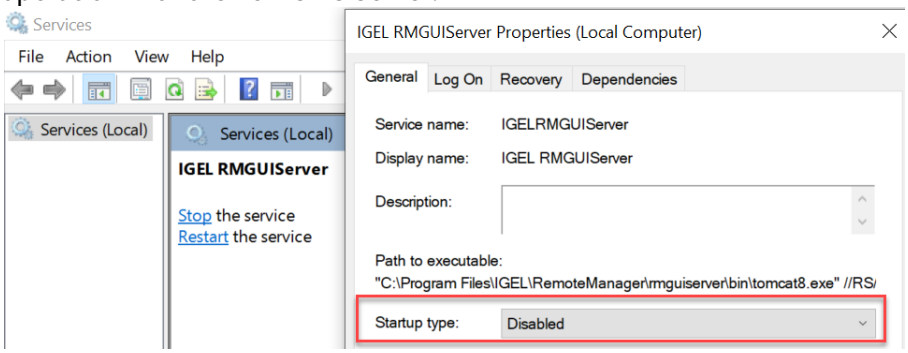
1. Backing up the old server. Checklist for the backups:
   - ✅ **Database**
   - ✅ **Licenses**
   - ✅ **Transfer files**
   - ✅ **Firmware updates**
   - ✅ **Server configurations** (host-specific server configurations (see page 547) that differ from the defaults are noted down separately)
   - ✅ **UMS Licensing ID** (see Transferring or Registering the UMS Licensing ID (see page 86))
2. Stopping the `IGEL RMGUIServer` service on the old server
3. Adding the existing external database as the data source for the new server
4. Activating the data source
5. Transferring the backed-up data to the new server
6. Adjusting DHCP tag and DNS alias on the new server OR creating a profile with the IP of the new server for remote administration



Detailed Instructions

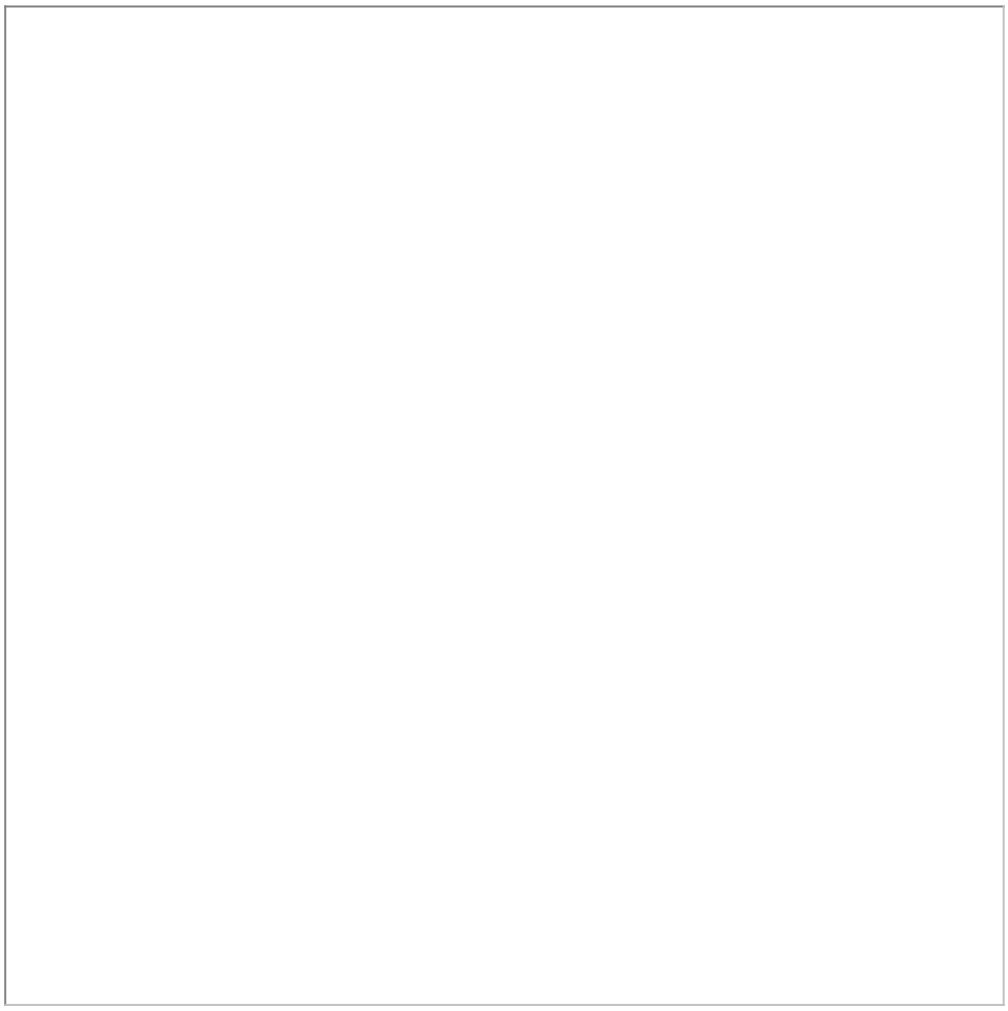
On the Old Server

1. Before the migration, make the backups as described in the "External Database" section under Creating a Backup (see page 546).
2. Stop the service `IGEL RMGUIServer` (for instructions, see HA Services and Processes (see page 592)) and set the startup type for it to "Disabled" in order to prevent accidental parallel operation with the new UMS Server.



On the New Server

1. Install the UMS on the new server. For the installation instructions, see Installing a UMS Server (see page 205).

2. Go to **UMS Administrator > Datasource > Add** and enter the connection properties of the existing database.

3. **Activate** the data source. Wait until the UMS Server fully starts, i.e. the UMS Console can connect with it.
4. In the **UMS Administrator > Backups**, restore the backup of server configurations. If necessary, transfer host-specific server configurations (see page 547) to the new server.
5. Transfer the UMS Licensing ID of the previous UMS installation to the new server: **UMS Administrator > UMS Licensing ID Backup > Restore**. Alternatively, you can register the new UMS Licensing ID, which was created during the installation of the new server. For detailed instructions, see Transferring or Registering the UMS Licensing ID (see page 86).
6. Copy all files from the following folders to the new server – without the `WEB-INF` folder:
   - `[IGEL installation directory]/rmguiserver/webapps/ums_filetransfer`
   - `[IGEL installation directory]/rmguiserver/webapps/e08ce61-d6df-4d2b-b44a-14c1ec722c44`

7. Restart the service `IGEL RMGUIServer`.
8. If ICG is used: All ICGs have to be reinstalled, see ICG Reinstallation after the Migration of the UMS Server (see page 103).
9. Adapt, if necessary, the DHCP tag and the DNS alias `igelrmserver` with the IP or FQDN of the new UMS Server. See Registering Devices Automatically on the IGEL UMS (see page 242).

   > The configuration of the DHCP tag and the DNS alias is not a setting that can be made within the IGEL software. You must configure these within your individual network environment on the corresponding DHCP and DNS servers.

   > If you have used and adjusted the DNS alias and the DHCP option, the following step is NOT required since the device can resolve the name `igelrmserver` correctly.
   >
   > In the local configuration, the device always remembers the IP of the UMS Server of its first registration. It is thus possible that the old IP address is displayed under **System > Remote Management**. Therefore, it makes sense to manually set an entry for remote administration after the migration:
   >
   > a. Create a profile in the UMS:
   > - Go to **System > Remote Management** and click **Add**.
   > - Under **UMS Server**, enter the IP of the new UMS Server.
   >
   > b. Apply this profile globally, to the entire structure.

10. For HA installations only: Update the host assignment for job execution. For the instructions, see Updating Host Assignment for Job Execution (see page 92).

> After the procedure is complete, open the UMS Console and go to **UMS Administration > UMS Network > Server** to check if there is an entry for the previous UMS Server among the listed components. If so, select the entry and click **Delete** in the context menu.

With a Different Database

Transfer the UMS data to the new database before the migration process, see also Data Source (see page 554):

1. Click **Data Source > Add...** in the UMS Administrator of the current server to set up a data source for the new database you wish to use.
2. Click **Copy** to copy the old data source to the new one.
3. Activate the new data source.
4. Wait until the UMS Server fully starts, i.e. the UMS Console can connect with it.
5. Now you can begin the migration procedure like described before:

If the new data source is	
• an embedded database:	UMS with embedded database (see page 77)
• an external database:	UMS with external database (see page 81)

Transferring or Registering the UMS Licensing ID

There are two different ways to handle the UMS Licensing ID (see page 431) if you migrate the UMS Server:

- Transferring the UMS Licensing ID (see page 86): With this method, you make a backup of the old UMS Licensing ID and take it with you. The UMS Licensing ID, which is automatically created during the installation of the new UMS Server, is overwritten. Advantage: You do not have to reassign the license packages in the ILP.
- Registering the New UMS Licensing ID in the ILP (see page 90): With this method, you register the UMS Licensing ID of the new server in the IGEL License Portal. Advantage: You do not need to know the UMS Licensing ID of the old server.

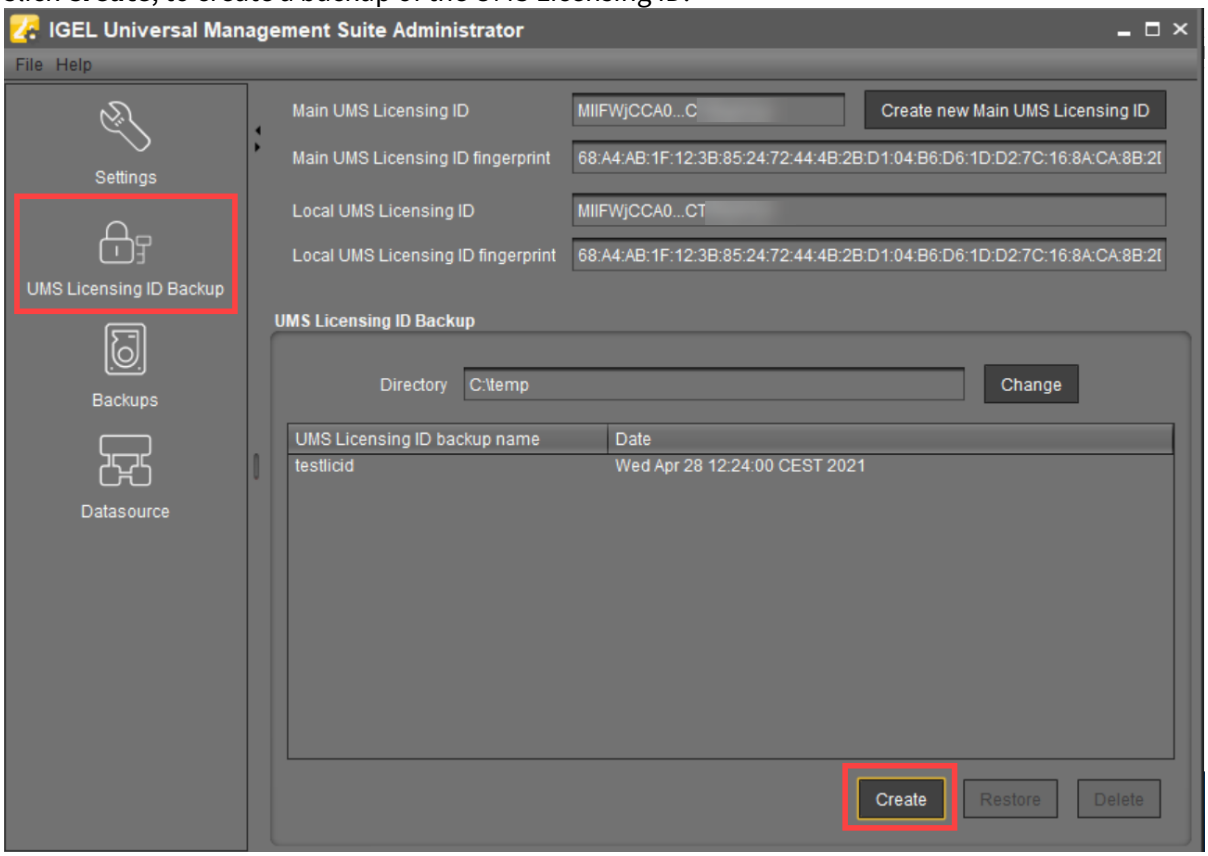
Transferring the UMS Licensing ID

Old Server: Create a Backup of the UMS Licensing ID

1. Open the UMS Administrator of your old server and go to **UMS Licensing ID Backup**.

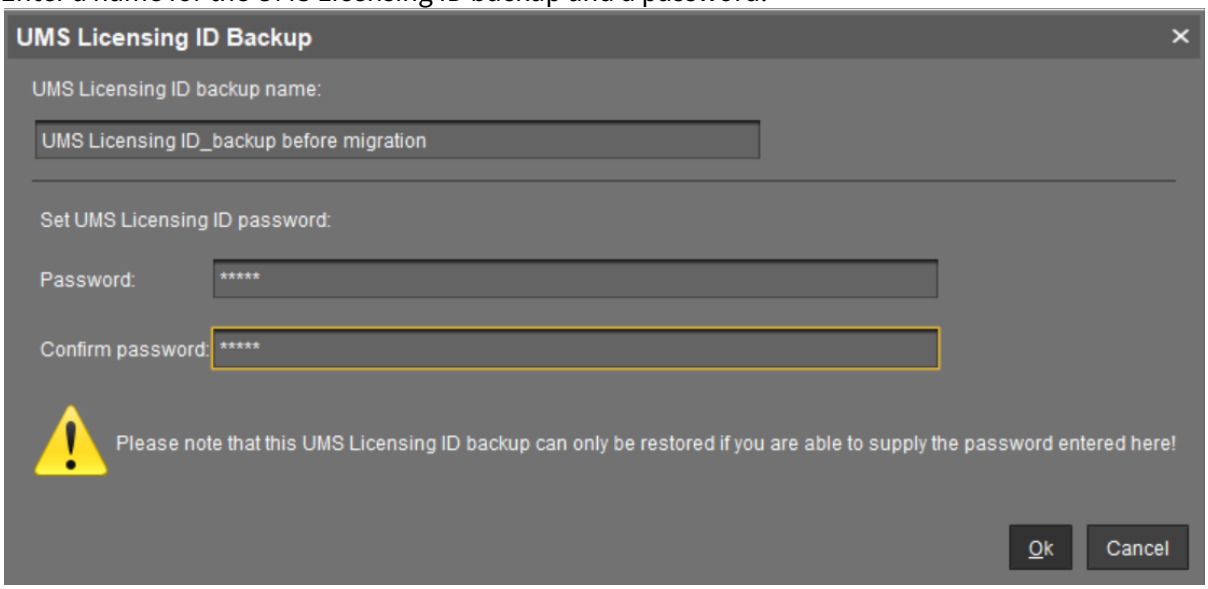
   Default path to the UMS Administrator:
   Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
   Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
   The IGEL UMS Administrator application can only be started on the UMS Server.

2. Click **Create**, to create a backup of the UMS Licensing ID.

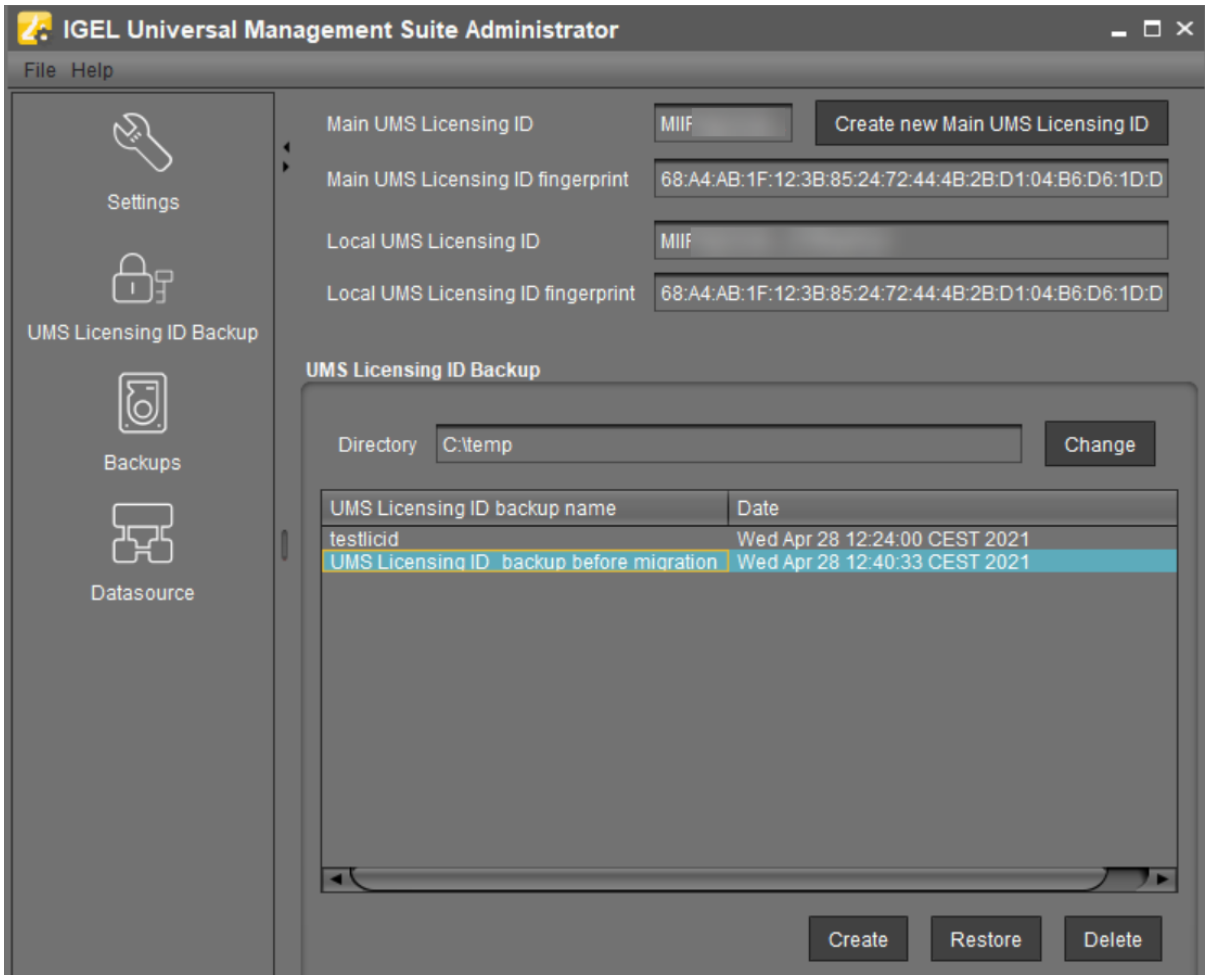


If you are using an HA environment, note the following:
It is always the UMS Licensing ID of the local server that is backed up. Therefore, make sure at first that the **local UMS Licensing ID** is the same as the **main UMS Licensing ID**. If not, restart the UMS Server to synchronize the local UMS Licensing ID with the main UMS Licensing ID and then proceed with creating the backup. See also Manual Synchronization of the UMS Licensing ID (see page 127).

3. Enter a name for the UMS Licensing ID backup and a password.



4. Click **OK**.
   The new backup file is listed under **UMS Licensing ID Backup**.

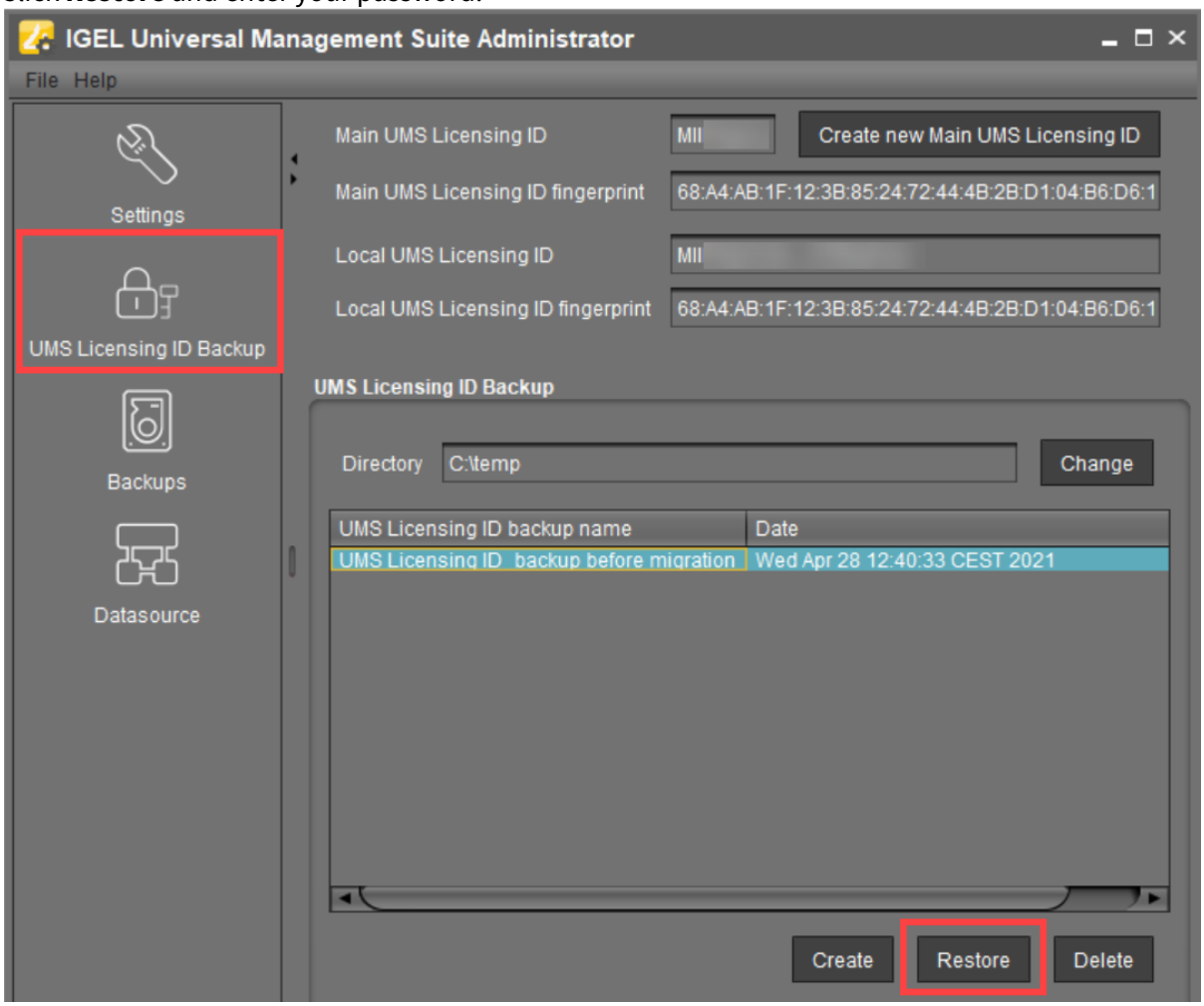


5. In your file explorer, go to the specified folder (in this case `C:\temp`).
6. Copy the UMS Licensing ID file (in this case `UMS Licensing ID_backup before migration.ksbak`) to a directory of your new UMS Server environment.

New Server: Restore the UMS Licensing ID to the New Server

1. Open the **UMS Administrator** of the new server and go to **UMS Licensing ID Backup**.
2. Click **Change** behind the **Directory** field to choose the directory where you stored the UMS Licensing ID.
   The file with the UMS Licensing ID will be listed.

3. Click **Restore** and enter your password.



The UMS Licensing ID is now stored in the new UMS environment.

Registering the New UMS Licensing ID in the IGEL License Portal (ILP)

1. Log in to the IGEL License Portal (ILP) at https://activation.igel.com[5]. If you have not registered yet, you must register first.
   Your dashboard is shown.
2. Select **UMS Licensing ID**.
   The page **UMS Licensing ID** is shown.
3. Click **Register UMS Licensing ID**.
   The dialog **Register UMS Licensing ID** opens.
4. Under **UMS Licensing ID Name**, enter a name for the UMS Licensing ID.

5 https://activation.igel.com/

5. Upload the certificate file you have exported in the UMS (see Obtaining Your UMS ID) and click **OK**. The UMS Licensing ID is registered. If this is the first UMS Licensing ID you registered, or if you just defined it as the default UMS Licensing ID, the dialog **Assign loose Product Packs** is shown.
6. If the dialog **Assign loose Product Packs** is shown, click **OK** to assign Product Packs and continue with Assigning a Product Pack to the UMS ID.

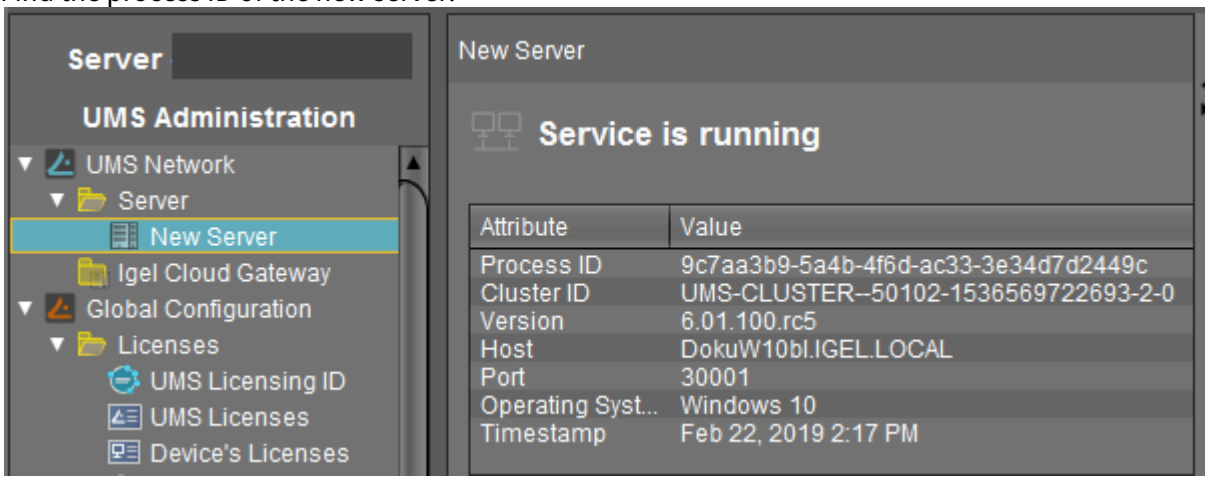
For a detailed instruction with screenshots, see Registering Your UMS ID.

Updating Host Assignment for Job Execution

Job execution in the UMS uses a device to UMS Server mapping to avoid multiple executions of one job with the same device. If a UMS Server is migrated, this mapping needs to be adjusted.

> The mapping is relevant for HA installations only. In standard (single instance) installations, the host assignments do not need to be adjusted. In HA installations, follow the steps below.

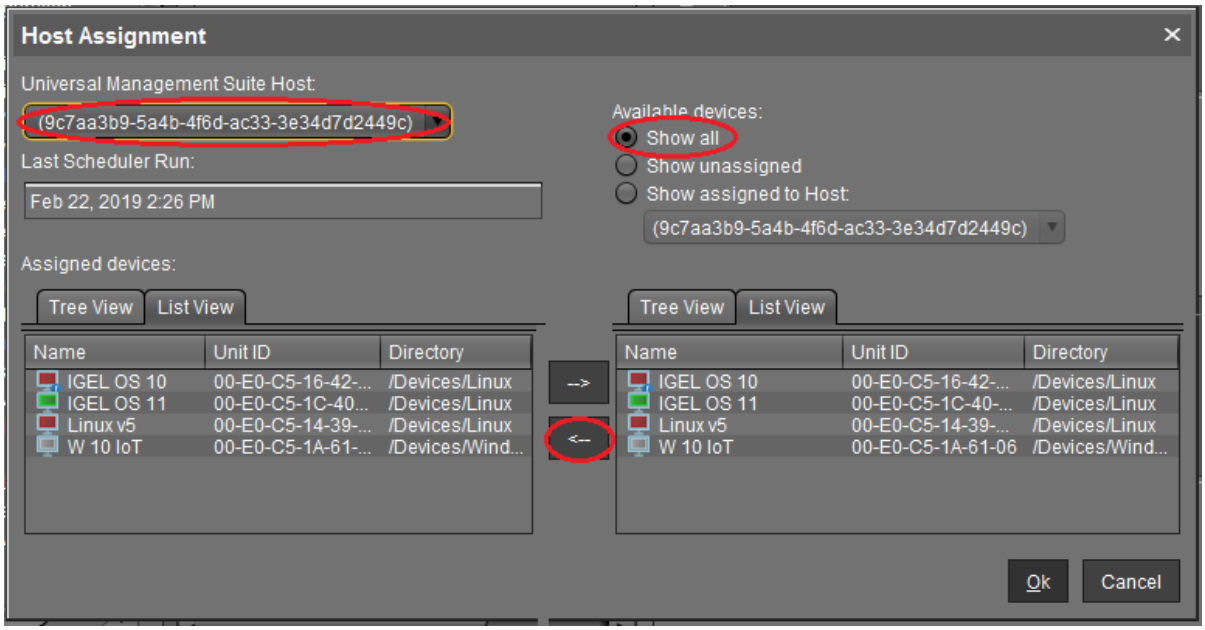
1. In the UMS Console, go to **UMS Administration > UMS Network > Server >** [new server].
2. Find the process ID of the new server.



3. In the menu bar of the UMS Console, select **Misc > Scheduled Jobs > Host Assignment**.
4. Select the new server and check the process ID.
5. Under **Available devices**, activate **Show all**.
6. In **List View** on the right side, select all devices.

   > To select all devices, set the focus in the list and press [Ctrl+a].

7. Click the left arrow to assign the devices to the new host.


Host Assignment
Universal Management Suite Host:
(9c7aa3b9-5a4b-4f6d-ac33-3e34d7d2449c)
Last Scheduler Run:
Feb 22, 2019 2:26 PM
Available devices:
Show all
Show unassigned
Show assigned to Host:
(9c7aa3b9-5a4b-4f6d-ac33-3e34d7d2449c)
Assigned devices:
Tree View
List View
Name
Unit ID
Directory
IGEL OS 10 00-E0-C5-16-42-... /Devices/Linux
IGEL OS 11 00-E0-C5-1C-40... /Devices/Linux
Linux v5 00-E0-C5-14-39-... /Devices/Linux
W 10 IoT 00-E0-C5-1A-61-... /Devices/Wind...
-->
<--
Tree View
List View
Name
Unit ID
Directory
IGEL OS 10 00-E0-C5-16-42-... /Devices/Linux
IGEL OS 11 00-E0-C5-1C-40-... /Devices/Linux
Linux v5 00-E0-C5-14-39-... /Devices/Linux
W 10 IoT 00-E0-C5-1A-61-06 /Devices/Wind...
Ok
Cancel

Migrating a UMS Database From Embedded DB to Microsoft SQL Server

This document describes how to migrate the database of a *Universal Management Suite (UMS)* installation from *Embedded DB* to a *Microsoft SQL Server*.

This is an exemplary representation. If you want to integrate the other way round or integrate other databases, the same steps are always performed. You can always use this description as a guide.

IGEL Demos Channel

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=_200UQppobw

Setting Up the SQL Database

⚠ The UMS supports only those standard sortings of Microsoft SQL Server which are case insensitive ("CI"). Therefore, make sure that the parameter **Collation** in MS SQL Server is set appropriately.

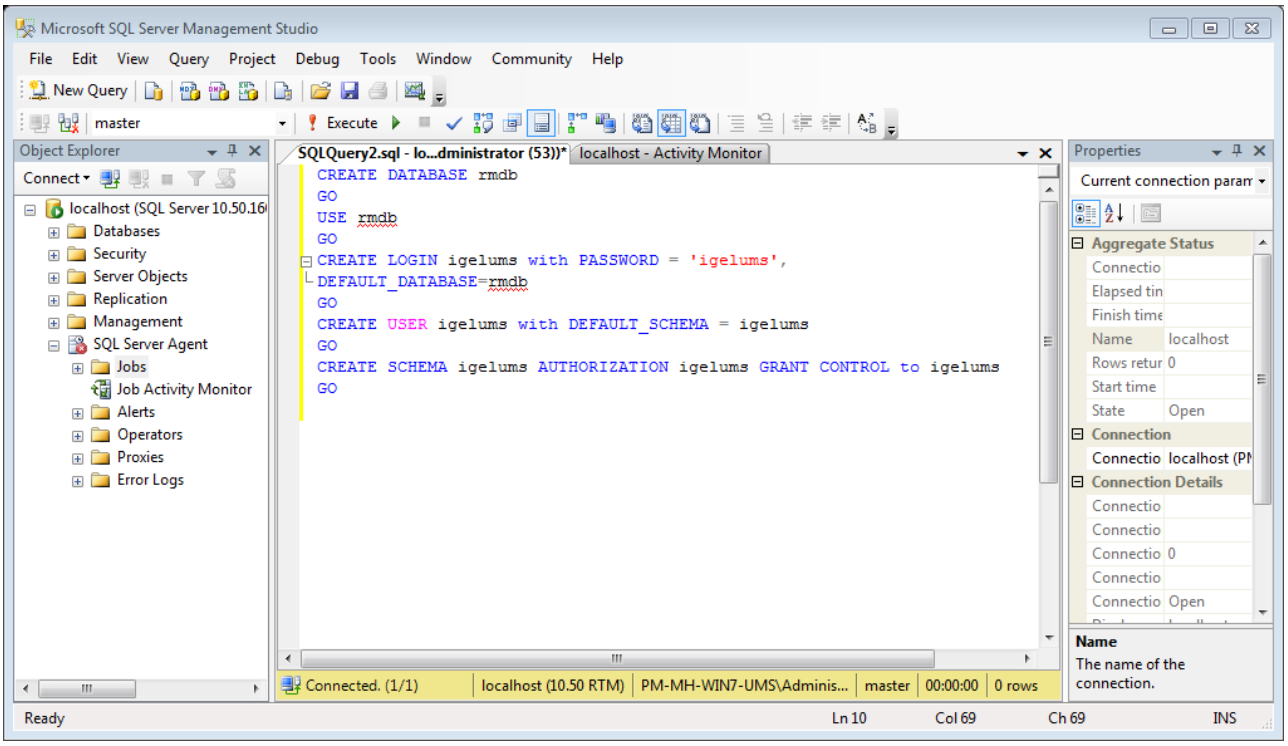
▶ Execute the following SQL script on the *Microsoft SQL Server* in order to create database, login, user and schema. Replace the placeholders such as `[databasename]` with settings of your choice. `[sql-user]` has to be an SQL account, not a Windows domain account. The script uses the same string for login, user and schema in order to simplify *UMS* setup.

ⓘ The **user name** for the external database may only be created with the following properties:

- it consists only of **lower case** letters or **upper case** letters.
- the **low-cut character** ("_") is the only special character, which is allowed.

Do not mix upper and lower case letters. Don't use points, spaces, minus, or @ sign!

```
CREATE DATABASE [databasename]
GO
USE [databasename]
GO
CREATE LOGIN [sql-user] with PASSWORD = '[password]',
DEFAULT_DATABASE=[databasename]
GO
CREATE USER [sql-user] with DEFAULT_SCHEMA = [sql-user]
GO
CREATE SCHEMA [sql-user] AUTHORIZATION [sql-user] GRANT CONTROL to [sql-user]
GO
```

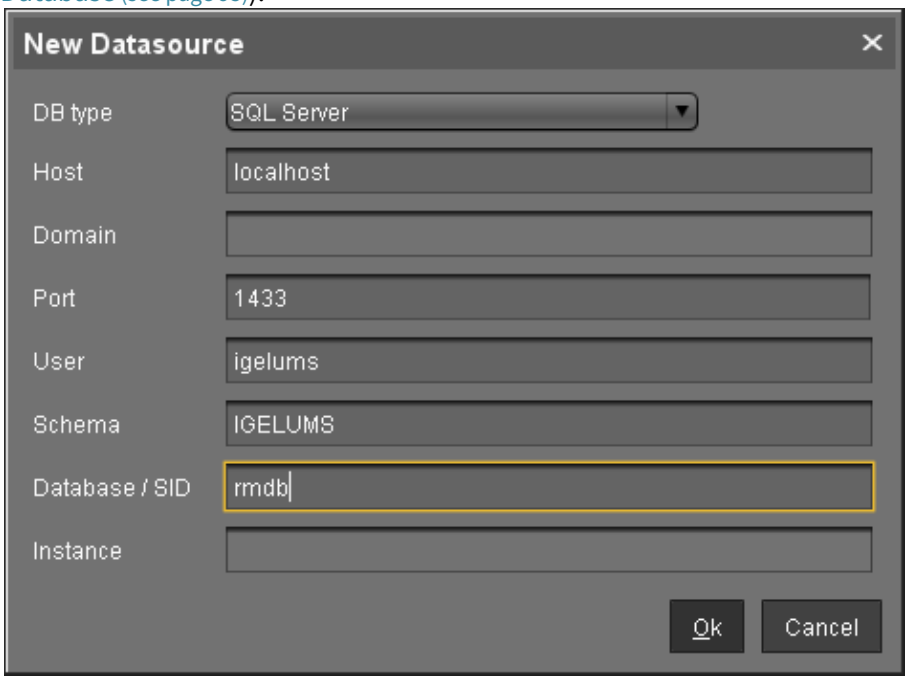

Microsoft SQL Server Management Studio
File Edit View Query Project Debug Tools Window Community Help
New Query
master
Execute
Object Explorer
Connect
localhost (SQL Server 10.50.16
Databases
Security
Server Objects
Replication
Management
SQL Server Agent
Jobs
Job Activity Monitor
Alerts
Operators
Proxies
Error Logs
SQLQuery2.sql - lo...dministrator (53))*
localhost - Activity Monitor
CREATE DATABASE rmdb
GO
USE rmdb
GO
CREATE LOGIN igelums with PASSWORD = 'igelums',
DEFAULT_DATABASE=rmdb
GO
CREATE USER igelums with DEFAULT_SCHEMA = igelums
GO
CREATE SCHEMA igelums AUTHORIZATION igelums GRANT CONTROL to igelums
GO
Properties
Current connection param
Aggregate Status
Connectio
Elapsed tin
Finish time
Name localhost
Rows retur 0
Start time
State Open
Connection
Connectio localhost (PM
Connection Details
Connectio
Connectio
Connectio 0
Connectio
Connectio Open
Name
The name of the connection.
Connected. (1/1)
localhost (10.50 RTM)
PM-MH-WIN7-UMS\Adminis...
master
00:00:00
0 rows
Ready
Ln 10
Col 69
Ch 69
INS

Copying Database Contents

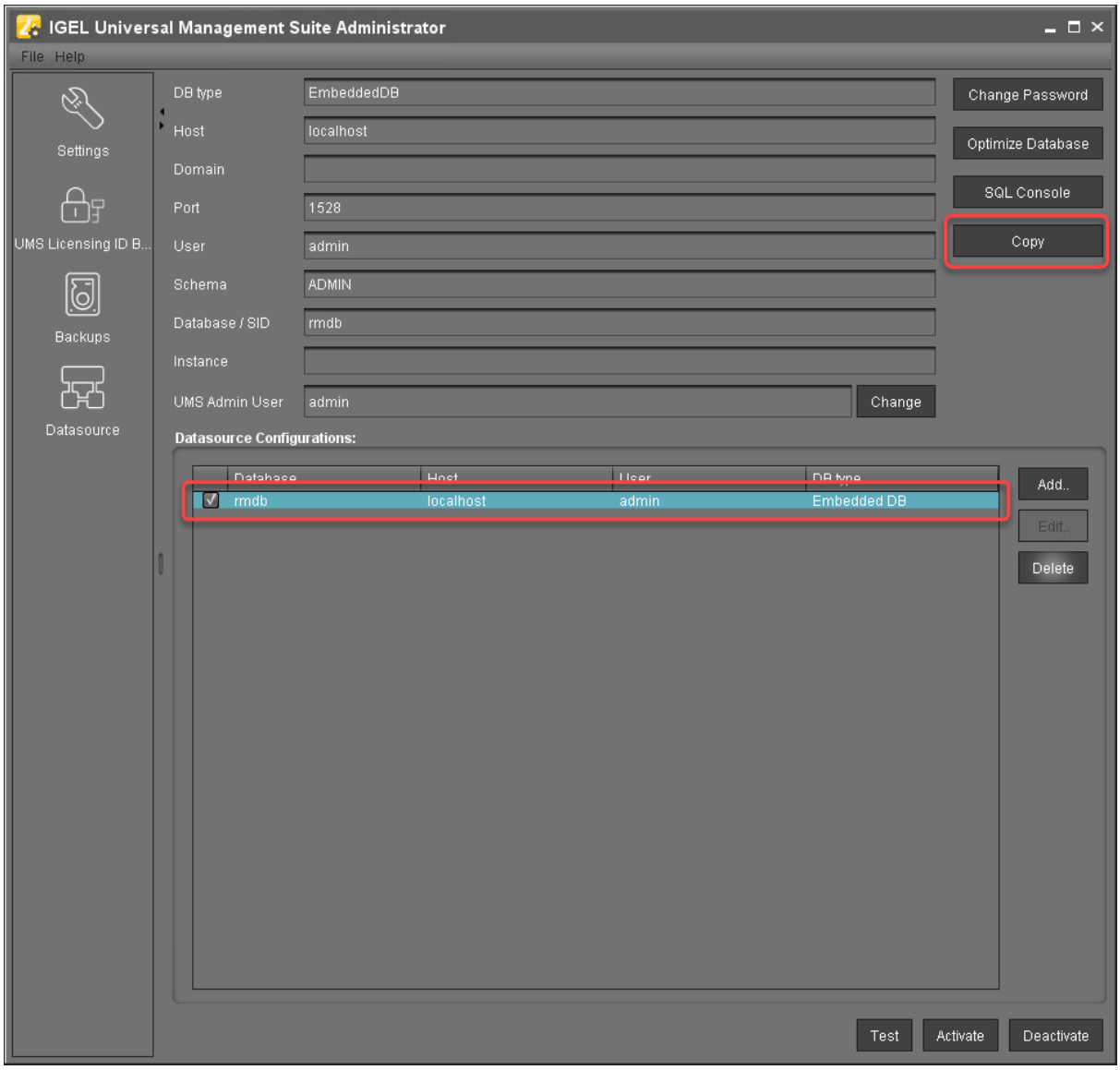
1. Start IGEL Universal Management Suite Administrator.

   > Default path to the UMS Administrator:
   > Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
   > Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
   > The IGEL UMS Administrator application can only be started on the UMS Server.

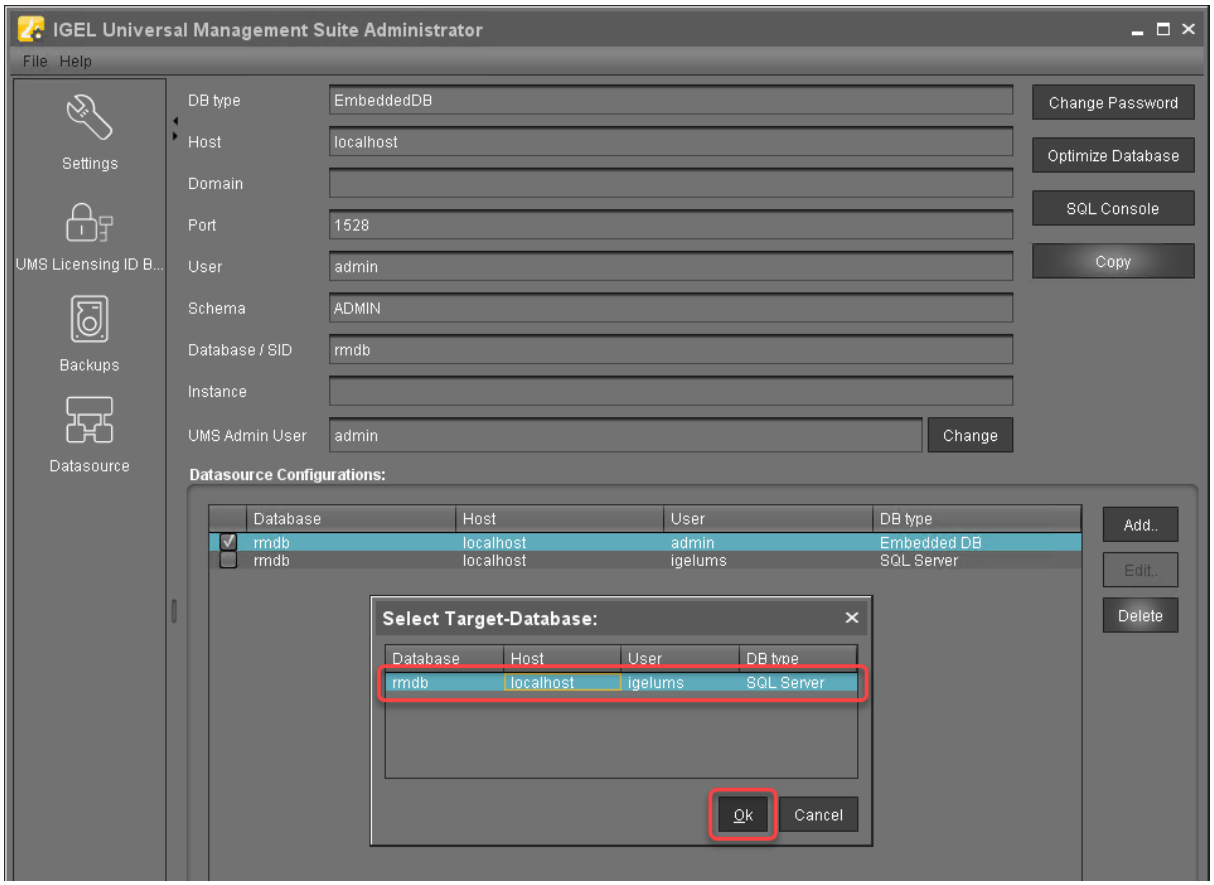
2. Go to **Datasource > Add...** to create a new SQL Server data source; use exactly the same database name and settings you have defined while setting up the SQL Database (see Setting Up the SQL Database (see page 95)).



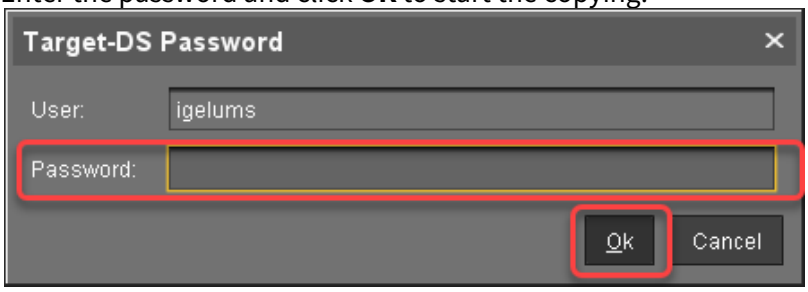
3. Select the **Embedded DB** entry and click **Copy.**



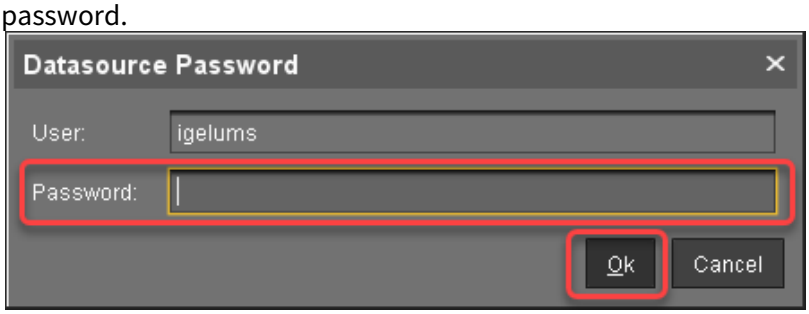
4. Select the newly created SQL Server entry as the target and click **OK.**



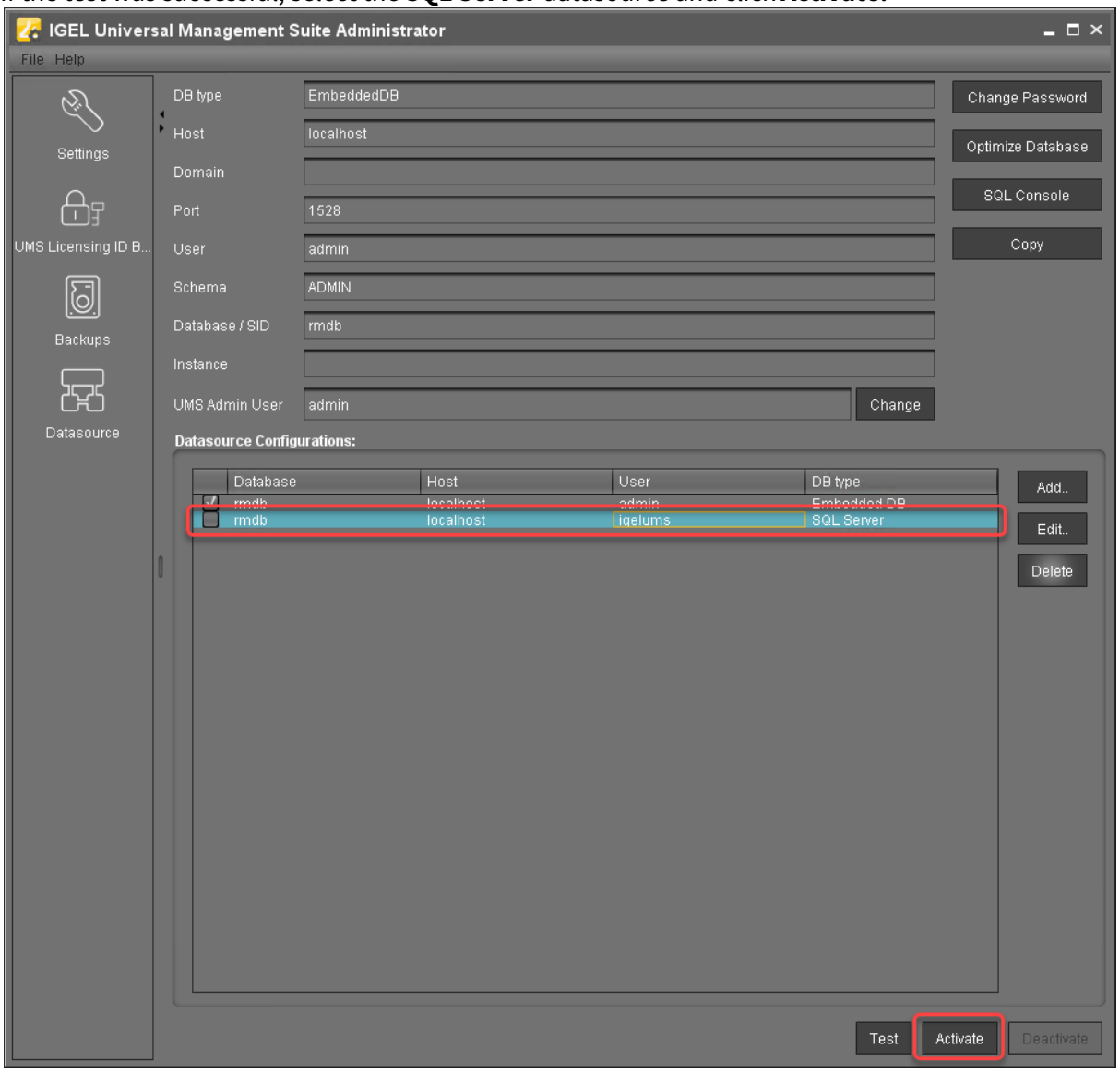
5. Enter the password and click **OK** to start the copying.



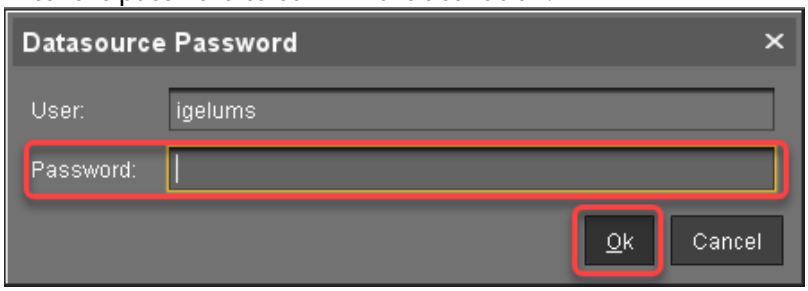
6. When the copying has completed, test the database connection by clicking **Test** and entering the password.



7. If the test was successful, select the **SQL Server** datasource and click **Activate.**



8. Enter the password to confirm the activation.



Now the Microsoft SQL Server is set up as the datasource. From now on, back up the SQL Server in order to back up UMS data.

The same way you can go back to the embedded database, if you need.

Restore and Recover Corrupted UMS Embedded DB

Environment

- UMS 6 on Windows or Linux

If the embedded database of UMS* is corrupted, try the following measures to resolve the issue.

*The underlying technology of the embedded database is Apache Derby.

Restoring a Database Backup Made with the UMS Administrator

If a backup of the embedded database is available (see Creating a Backup (see page 546)), just restore the backup, see Restoring a Backup (see page 550).

Restoring a File-Based Backup

If an uncorrupted copy of the database files located under `C:\Program Files...\IGEL\RemoteManager\db\rmdb` (default installation path on Windows) and/or `/opt/IGEL/RemoteManager/db/rmdb/` (default installation path on Linux) is available, you can restore the file copy. In the remainder of this how-to, the aforementioned possible paths will be referred to as `RMDB_PATH.`

To restore the backup, perform the following steps:

1. Open the UMS Administrator, and go to **Datasource** in the menu on the left.

   > Default path to the UMS Administrator:
   > Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
   > Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
   > The IGEL UMS Administrator application can only be started on the UMS Server.

2. In the **Datasource** area, delete the corrupted Derby DB.
3. Create a new embedded DB with exactly the same user name and password as you used for the deleted DB.
4. Deactivate the newly created DB.
5. Stop the UMS Server service. For details on how you can stop it, see HA Services and Processes (see page 592).
6. Erase all files contained in the folder at `RMDB_PATH` .
7. Copy your previously backed-up files to `RMDB_PATH` .
8. Activate the DB with the UMS Administrator under **Datasource**.
9. Wait 1 - 2 minutes, then log in to the UMS Console.

ICG Reinstallation after the Migration of the UMS Server

Situation

The UMS has been migrated to a new server. The corresponding ICG must be reinstalled.

Question

What happens to the clients connected to the old ICG installation?

Answer

After the reinstallation, the previously bound devices can be managed via the new ICG and do not have to be re-registered

- The ICG must not move to a new server and must be reachable as before.
- The same root certificate must also be used for the installation.

.

Wake on LAN

Deploying a Wake on LAN Proxy for Distributed Environments

Problem

The UMS is residing outside the network which contains your devices, so it cannot wake up your devices by Wake on LAN.

Goal

You want the UMS to wake up your devices from outside their network.

Solution

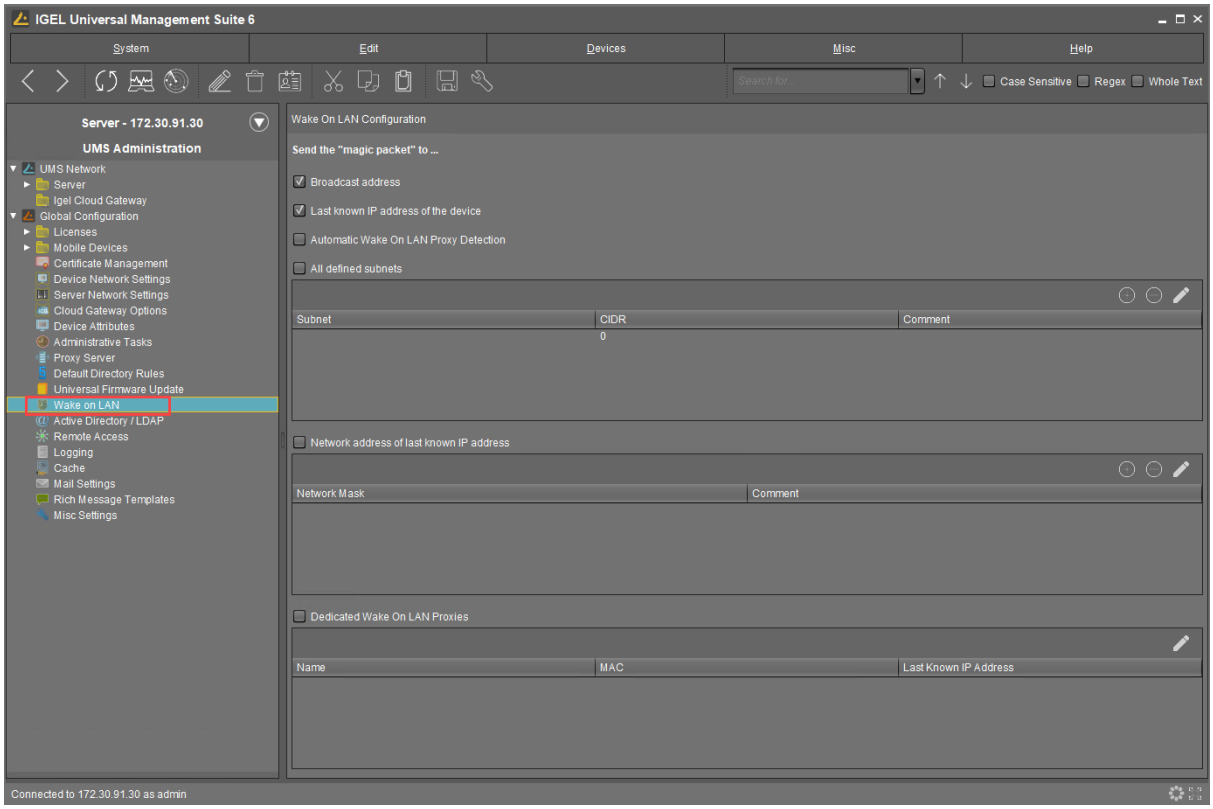
If you are using UMS version 5.02.100 or higher and devices running Linux version 5.09.100 or higher, you can make a device act as a proxy which sends the Wake on LAN packets on behalf of the UMS.

Defining Devices as Wake on LAN Proxy

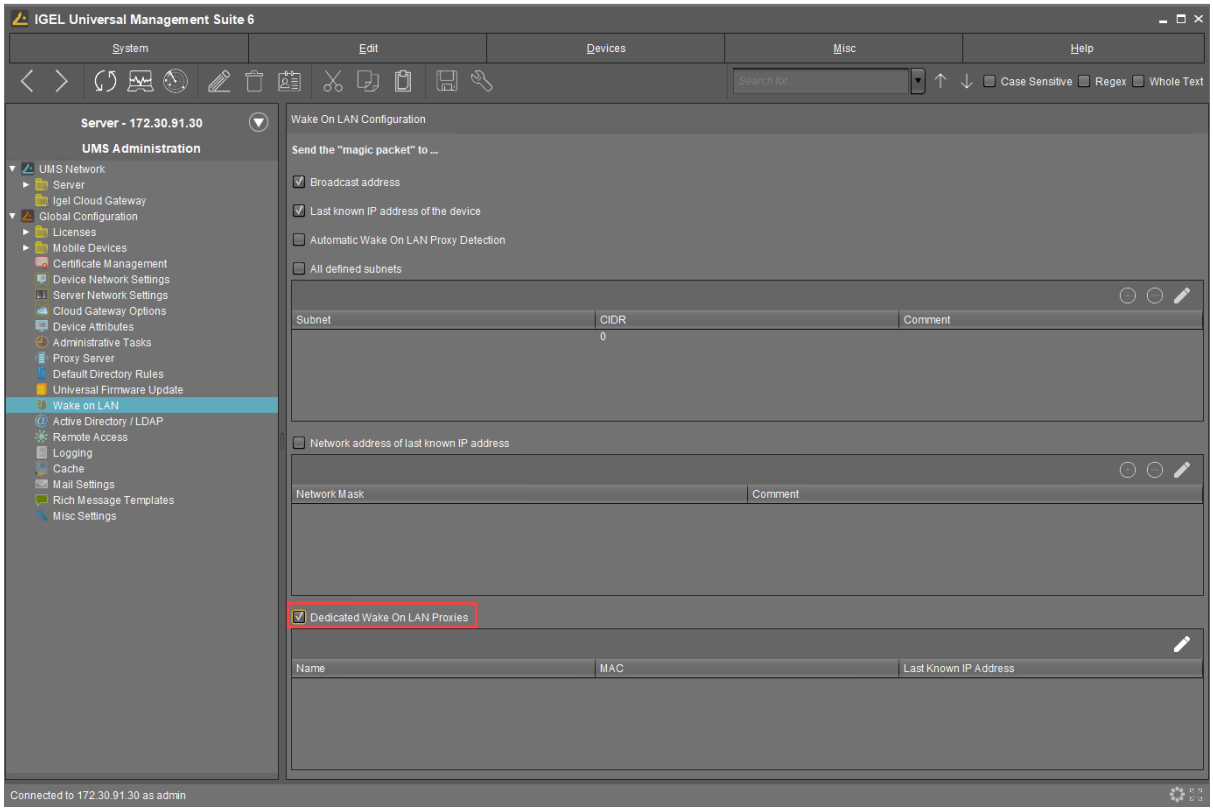
You can define one or more devices as a Wake on LAN proxy.

To define a device as a Wake on LAN proxy:

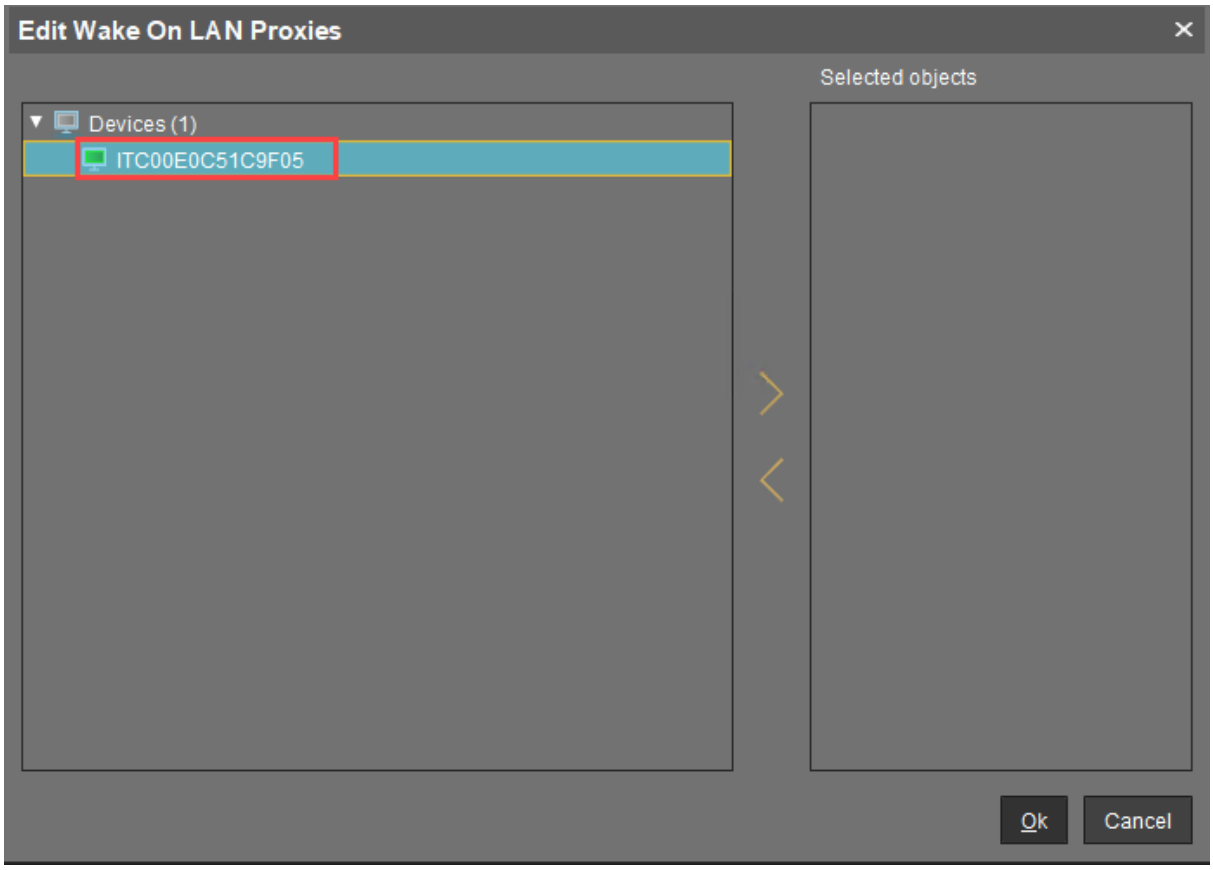
1. Logon to the UMS console.
2. Go to **UMS Administration**.
3. Select **Wake on LAN**.



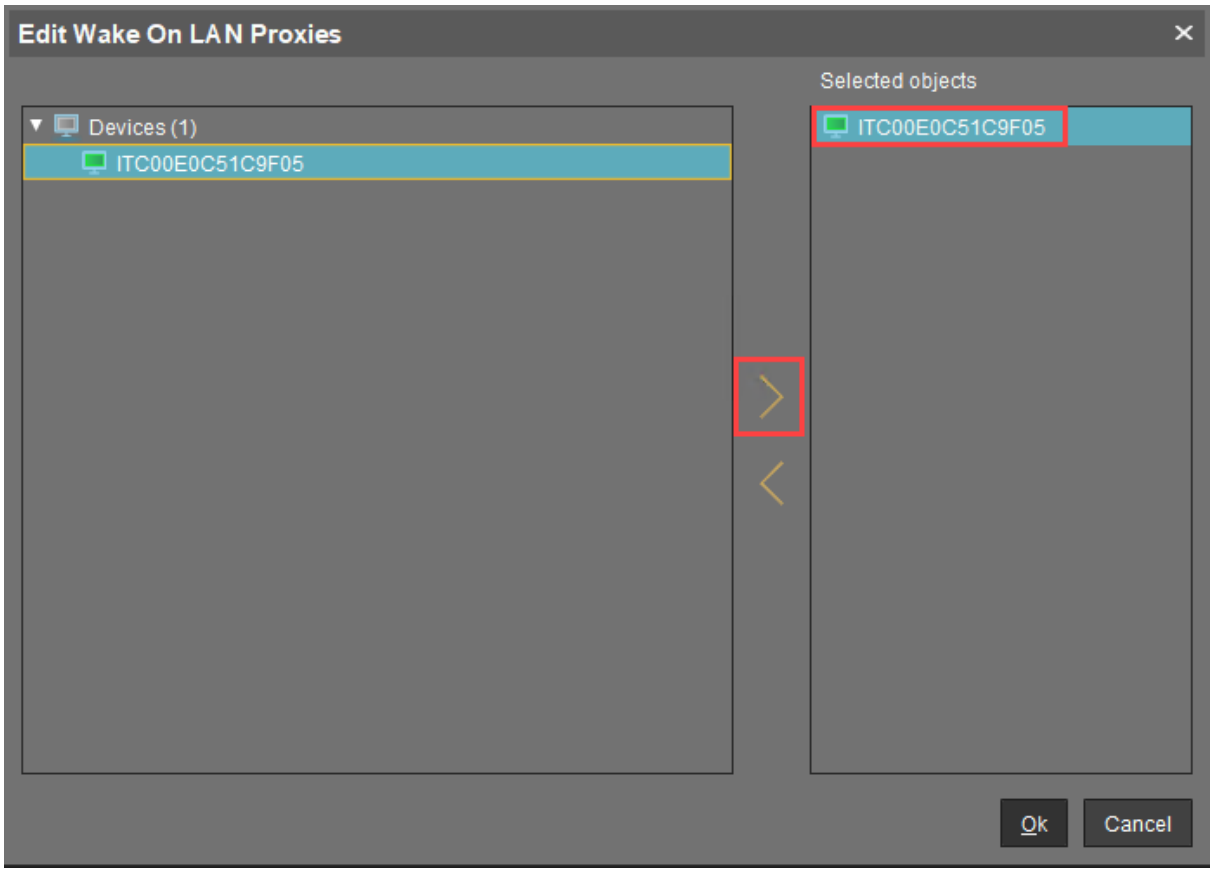
4. Activate **Dedicated Wake on LAN Proxies**.



5. Click  .
   The dialog **Edit Wake ON LAN Proxies** opens.
6. Select the device you want to use as a Wake on LAN proxy.



7. Click .
   The selected device is listed under **Selected objects**.



8. Click **Ok**.
   The selected device is configured as a Wake on LAN proxy. In the device's registry, the **parameter** `system.remotemanager.wol_proxy.enabled` is set to true.

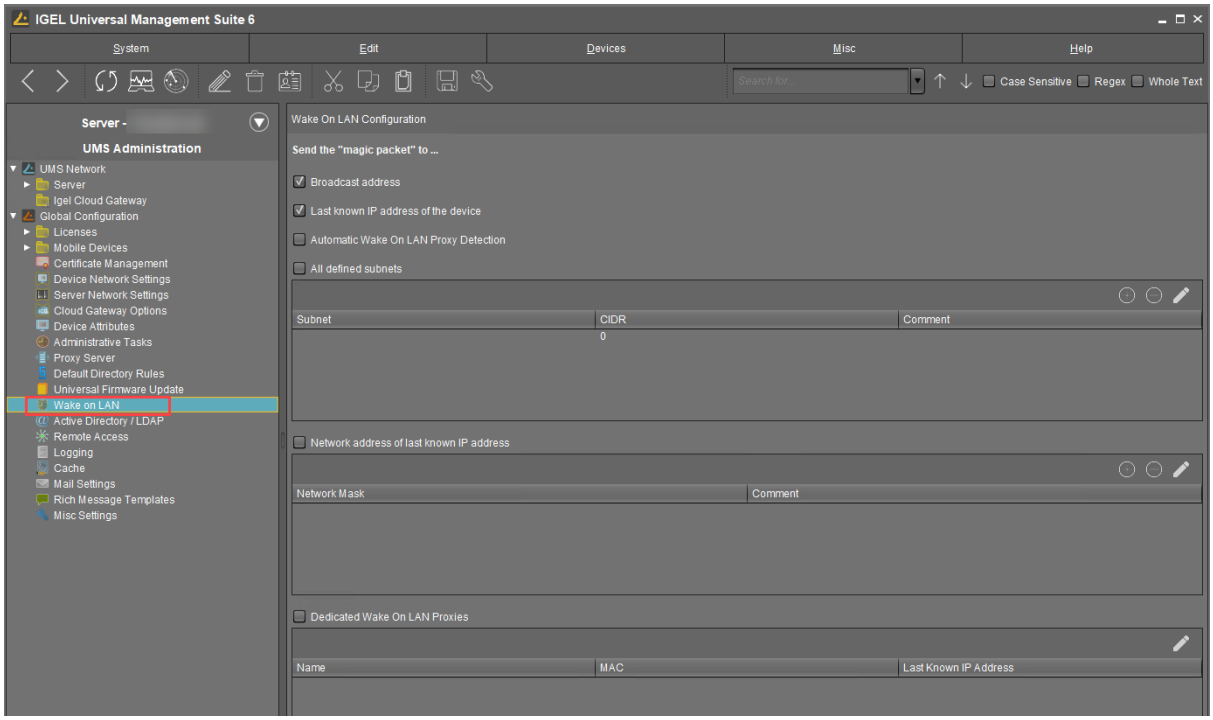
> A device that is configured as a Wake on LAN proxy cannot be set to standby or shut down. This lock is in effect as soon as the device has received its settings from the UMS.

Removing a Wake on LAN proxy

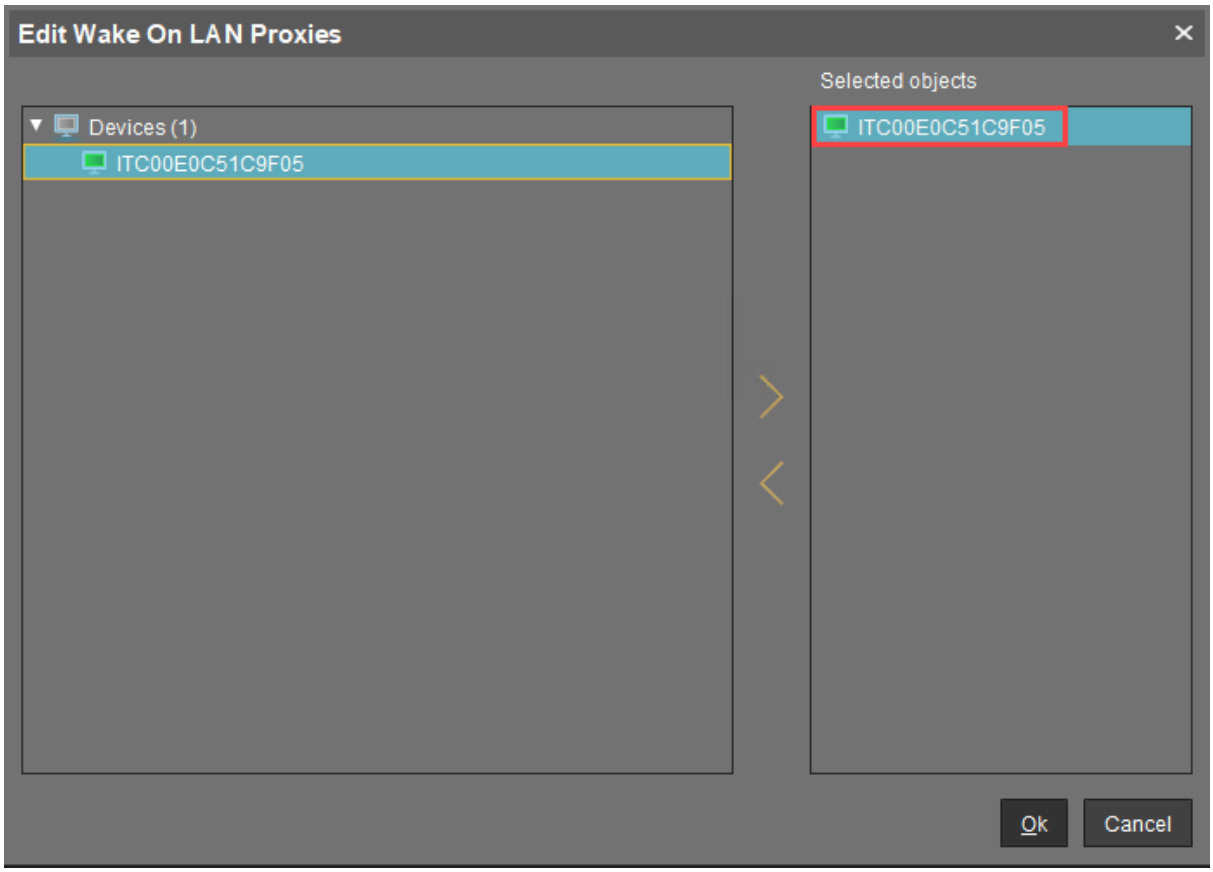
You can remove the Wake on LAN proxy function from a device.

To define one or more devices as Wake on LAN Proxy:

1. Log in to the UMS Console.
2. Go to **UMS Administration**.
3. Select **Wake on LAN**.



4. Click  .
   The dialog **Edit Wake ON LAN Proxies** opens.
5. Select the device you do not want to use as Wake on LAN proxy.



6. Click .
7. Click **Ok**.
   The selected device is no longer configured as a Wake on LAN proxy. As soon as the device has received its settings from the UMS, it can be set to standby and shut down as normal. In the device's registry, the parameter **system > remotemanager > wol_proxy > enabled** is set to "false".

Distributing Wake on LAN Packets

IGEL UMS sends the magic packets as UDP datagrams to port 9. In order to work for different subnets, this has to be supported by the routers involved.

Wake on LAN settings can be configured in **UMS Console** under **UMS Administration > Global Configuration > Wake on LAN**.

UMS supports sending Wake on LAN magic packets to

- the broadcast address
- the last known IP address of the device
- all defined subnets
- the network address of the last known device IP address (define one or more network masks to be applied)
- a dedicated Wake on LAN proxy to wake up thin clients in another network; see Use a WoL Proxy for Waking up Devices (see page 113)

Use a WoL Proxy for Waking up Devices

You have the possibility to wake up devices even if they live in a different network that does not allow broadcast packets from the WAN. The trick is to set up one or more devices as Wake-on-LAN proxy. A device acting as a Wake-on-LAN proxy will never fall asleep itself, as its job is to listen to a special wake-up call from the UMS. This wake-up call tells the Wake-on-LAN proxy to send magic packets to all devices or a selection of devices in its network. To support this functionality, the Wake-on-LAN proxy device must have IGEL Linux version 5.09.100 or higher.

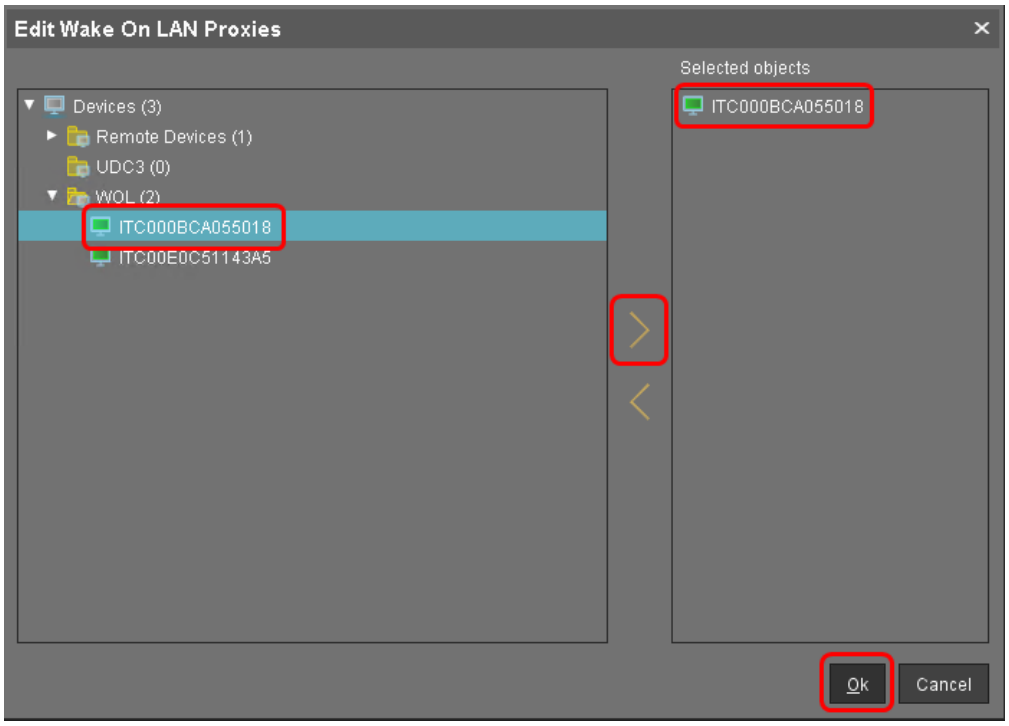
You can define a dedicated Wake-on-LAN proxy, or, alternatively, set the UMS to determine a Wake-on-LAN proxy automatically. However, the latter option cannot guarantee that a Wake-on-LAN proxy can be defined, as this depends on an appropriate device being online in the relevant subnet.

For detailed information, see the Wake-on-LAN (see page 496) chapter in the manual.

To define a dedicated Wake-on-LAN proxy:

1. Go to **UMS Administration > Global Configuration > Wake On LAN**.
2. Under **Send the "magic packet to ..."**, choose the adress(es) to which the Wake-on-LAN proxies should send their wake-up calls.
3. Activate **Dedicated Wake On LAN Proxies**.

4. In the area below **Dedicated Wake On LAN Proxies**, click on  .
5. Highlight the desired device in the left-hand column.
6. Click on  to select the device.
7. Click on **OK**.



The device will now function as a Wake-on-LAN proxy.

> A device that is configured as a Wake-on-LAN proxy can no longer be put on standby or shut down. This restriction applies as soon as the device receives the settings from the UMS.

> As an alternative or parallel one can also use the **Automatic WoL Proxy Detection**. However, you cannot be sure that this proxy is always running, while the **Dedicated WoL Proxy** is always running.

Using an HTTP Proxy for Firmware Updates in UMS

Symptom

You want UMS to download firmware updates from the Internet.

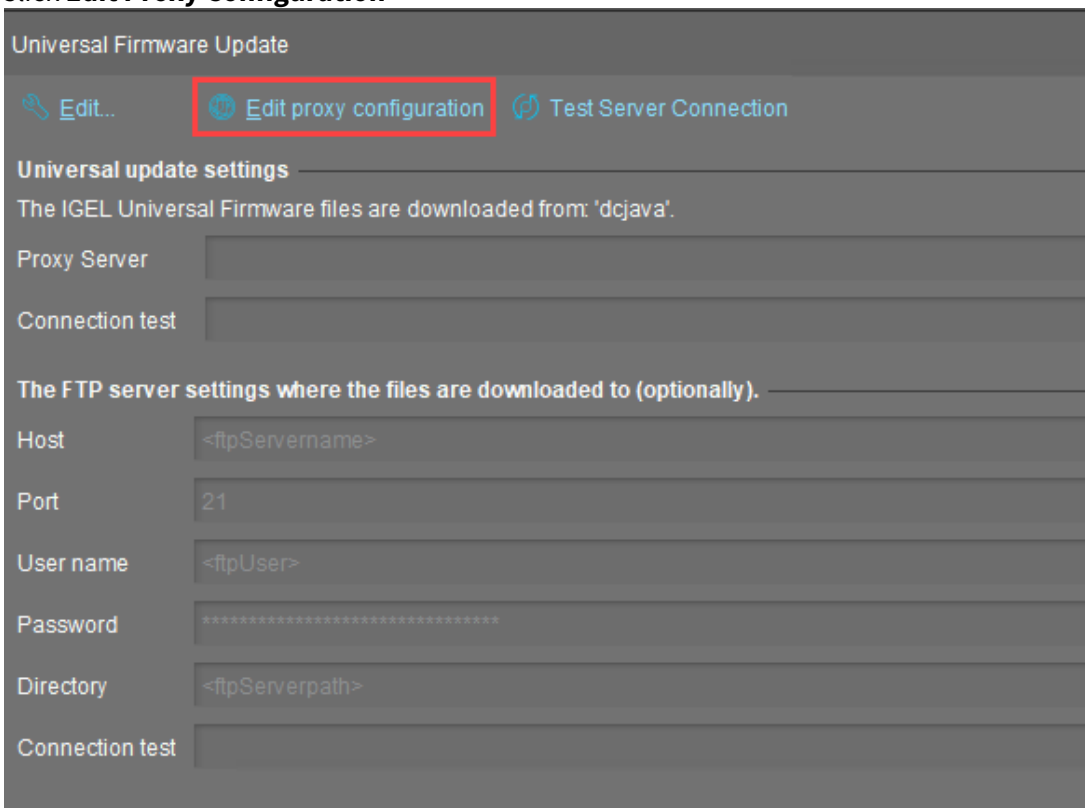
Problem

Internet access is only available via an HTTP proxy in your environment.

Solution

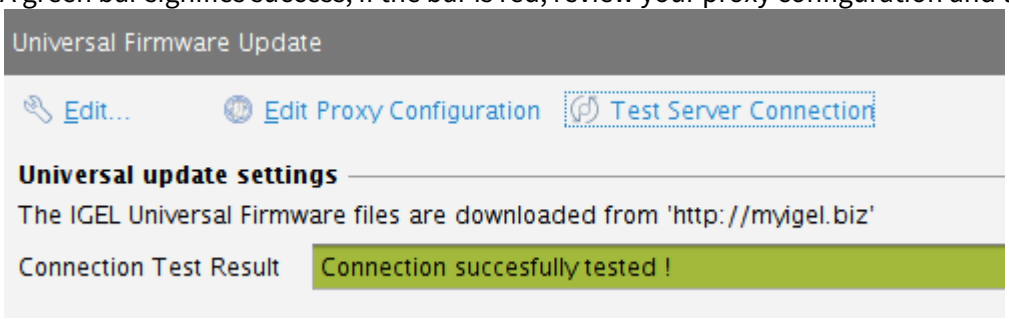
Configure an HTTP proxy for firmware downloads in UMS:

1. In UMS Console, go to **UMS Administration > Global Configuration > Universal Firmware Update**
2. Click **Edit Proxy Configuration**



   The **Edit Proxy Configuration** dialog opens.
3. Check **Use proxy for HTTP connection to firmware update server**.
4. Enter the **Proxy-Host** name or IP address.
5. Enter the proxy host **Port**.

6. Enter the proxy **User**.
7. Enter the proxy **Password**.
8. Click **Save**.
   The dialog closes.
9. To test the connection via the proxy, click **Test Server Connection**.
   A green bar signifies success, if the bar is red, review your proxy configuration and test again.



High Availability

New Installation of an HA Network

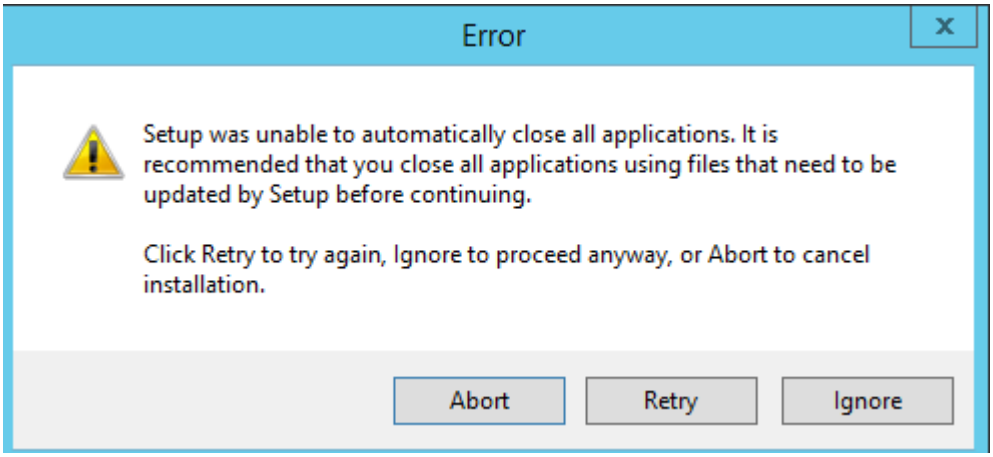
For installation requirements and details on how to install the High Availability Extension, see HA Installation (see page 564).

⚠ This page is due for deletion. Please check the above link and use it in the future.

Load Balancer Is Not Stopping during the Update of the HA Installation

Symptom

When updating the High Availability (HA) installation, an error message appears saying that not all applications could be closed before the update. A retry does not solve the problem.

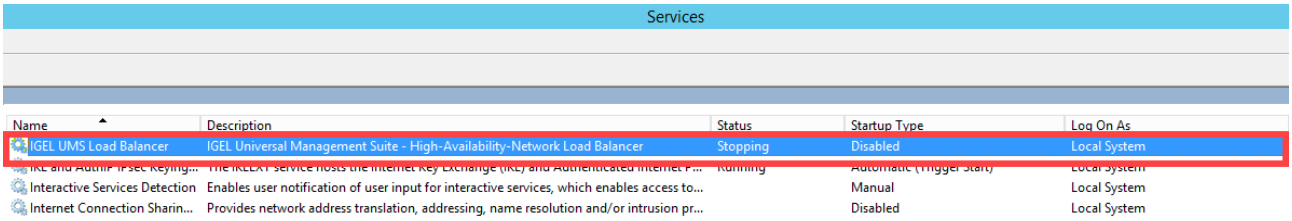


Environment

- UMS HA installation

Problem

The load balancer does not stop and stays in the "Stopping" mode:



Solution

▶ Stop the load balancer manually and proceed with the update. For information regarding stopping the HA services, see HA Services and Processes (see page 592).

How to Detect Which Files Are Synchronized Automatically

Prerequisites

A HA environment with UMS 5.08.120 or newer, with 2 servers and 2 load balancers.

Description

When a user creates a new file object on Server A, it is automatically synchronized with Server B every 30 minutes.

But this synchronization is only a synchronization of the file system. It does not refresh the view in any UMS console other than the one in which the file was created.

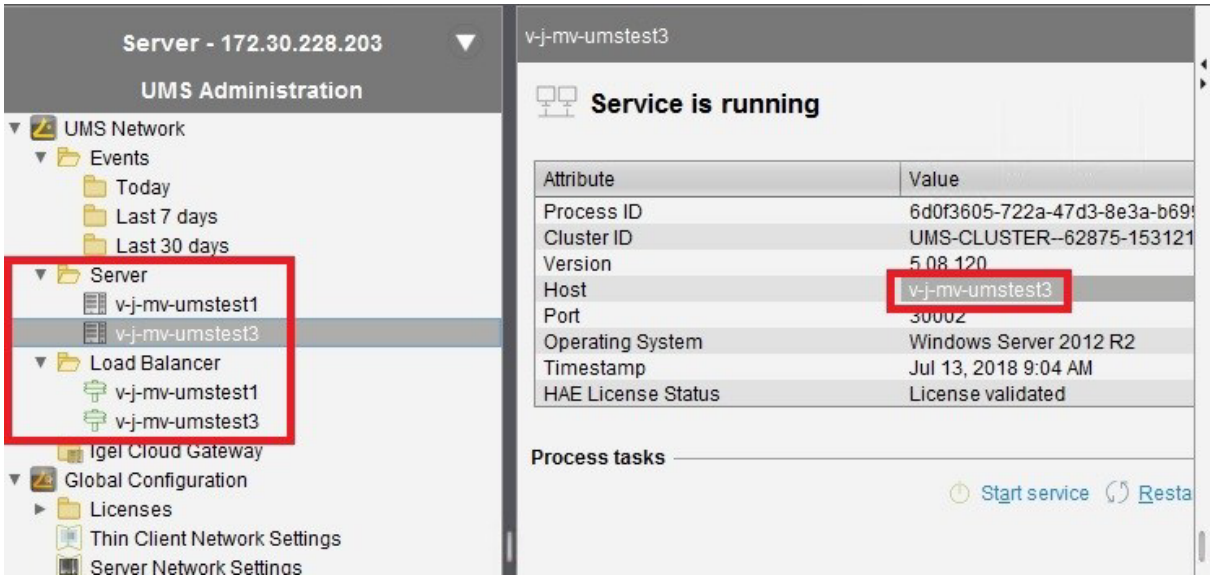
> Files that are not created as file objects in UMS, but are only stored in the file system in `ums_filetransfer`, are NOT synchronized.

> Note that Universal Firmware Updates (see page 415) are NOT synchronized. You have to either download them to all HA nodes or configure an external (FTP) server used as an update source.

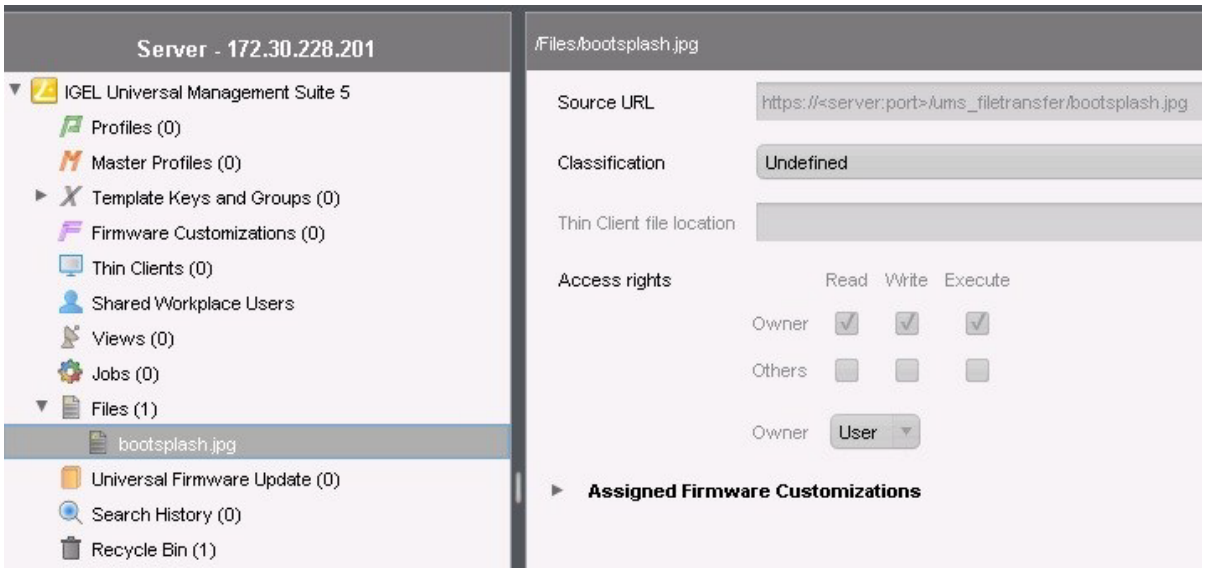
> To avoid problems with your HA installation, make sure that the time on the servers of the HA network does not differ by more than one minute. After each manual time reset, the HA services on the relevant server must be restarted.

In Detail

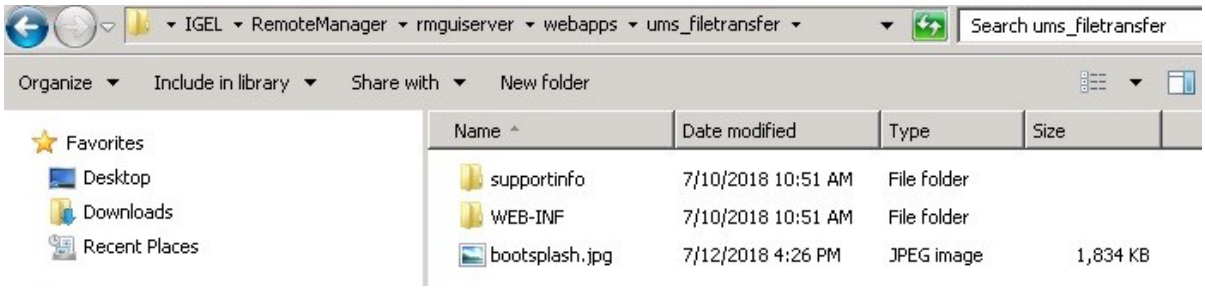
1. The system consists of server A (`v-j-mv-umstest1`) and server B (`v-j-mv-umstest3`).



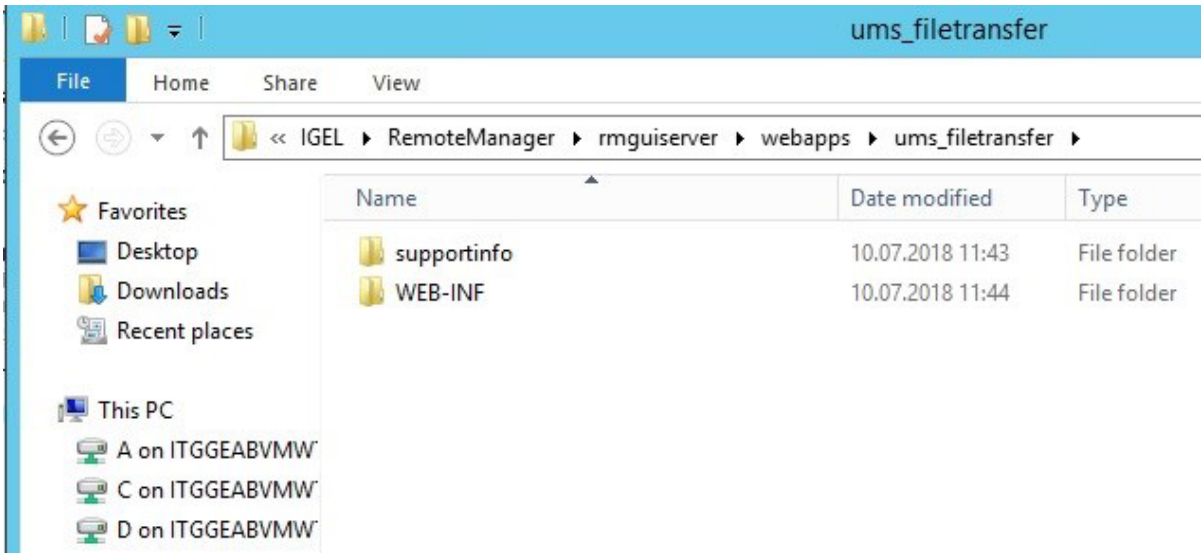
2. The user creates a file object called `bootsplash.jpg` on server A, that is, `v-j-mv-umstest1`:



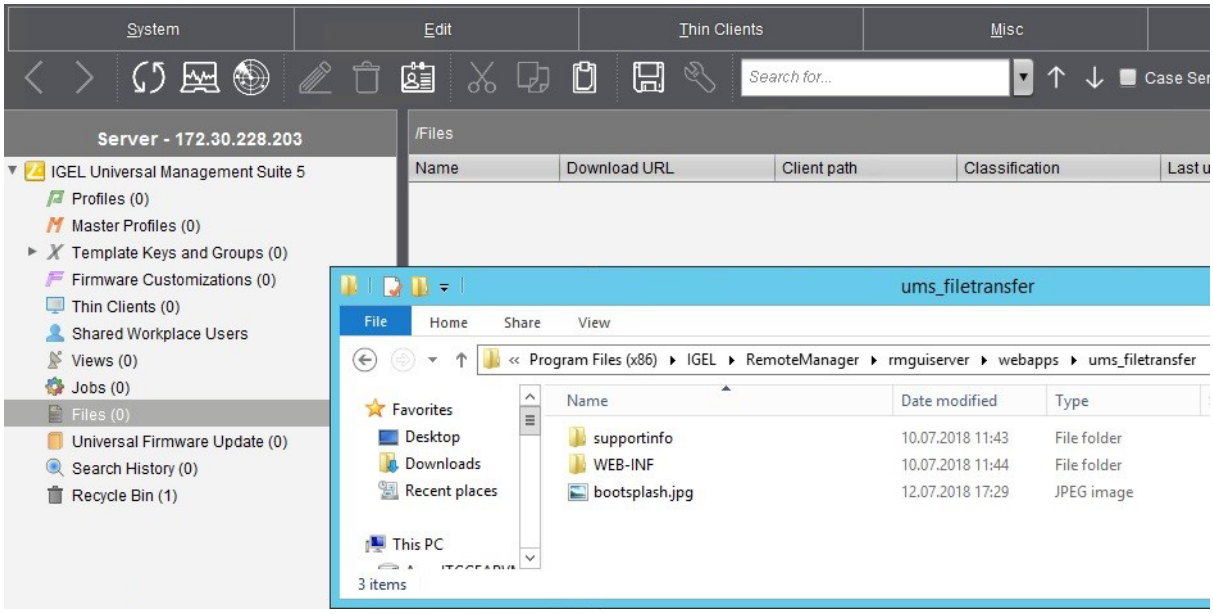
3. After the file object has been created on server A (`v-j-mv-umstest1`), the file `bootsplash.jpg` is present on the file system.



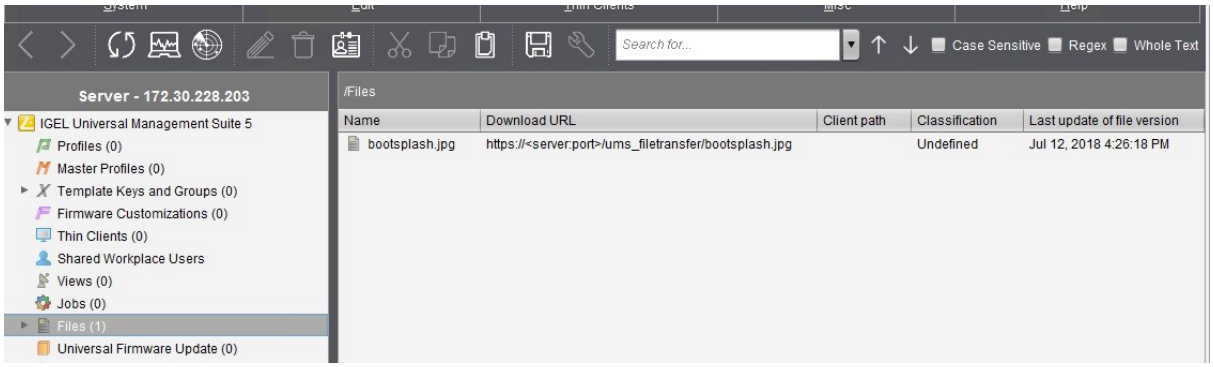
4. Before synchronization, the new file is not present on the file system of server B (`v-j-mv-umstest3`).



5. After file synchronization, the file is present on the file system of server B (`v-j-mv-umstest3`), but the file object is not visible yet on the UMS console connected to server B.



6. After pressing [F5] or selecting the refresh button, the UMS console connected to server B (`v-j-mv-umstest3`), shows the file object.



On server A (`v-j-mv-umstest1`), on which the file object was created by the user, the following new entry is added to the log file `Catalina.log` :

```
2018-07-12 16:30:00,184 INFO[Thread-888]
UMSEprSynchronizeWebDavServiceImpl: File https://v-jmv-umstest1:8443/
ums_filetransfer/boototsplash.jpg was successfully downloaded.
```

This is the URL from which server B attempts to download this file to its own file path.
If the download does not work, an error message is added. Possible causes, for instance: The file is currently in use and cannot be accessed, or the user has manually deleted the file in the file system.
A separate log entry is created for each file.

Load Distribution with a Number of Load Balancers

If a UMS Server and Load Balancer are installed on a shared computer, the UMS Server communicates with the endpoint devices via port 30002, otherwise via port 30001 as is customary with a single server installation. The Load Balancer always communicates with the devices via port 30001.

Load distribution to the load balancers can be performed as follows. When booting, the devices attempt to establish contact with the UMS Server in this order:

- Name `igelrmserver` in the DNS (*Record Type A*)
- DHCP tag 224
- Local list of **Remote Management Servers** (in the specified order)

In a UMS High Availability network, the load balancers are automatically specified in the list of remote management servers in the local device configuration.

If the DNS entry `igelrmserver` or DHCP tag 224 is used in an HA network, the IP of a load balancer must be entered.

If neither this DNS entry nor the DHCP tag 224 is used, endpoint devices always connect to the first load balancer in the setup list, i.e. all devices are communicating with a single load balancer. The other load balancers are merely stand-bys and will be used only if the first load balancer in the list is not available.

To achieve load distribution between the load balancers, you can however use the DNS entry `igelrmserver` with a *Round Robin DNS*. To do this, the IP addresses of all load balancers are recorded in the DNS as a *Resource Record Set* for the `igelrmserver` entry (cf. https://en.wikipedia.org/wiki/Round-robin_DNS). The devices then connect randomly to one of the available load balancers, thus distributing the query load of all devices.

License Error Because HA Servers Are out of Sync

> **Solution Based on Experience from the Field**
>
> This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

Symptom

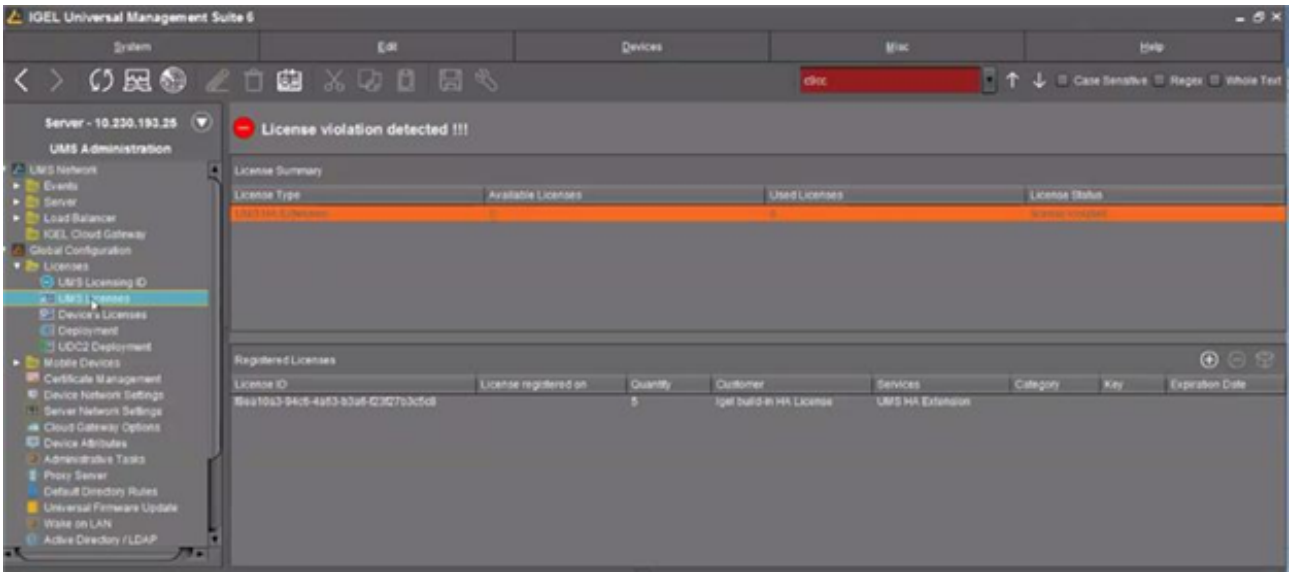
HA servers are out of sync preventing devices from registering in the UMS and throwing a license error.

Environment

- High Availability (HA) environment
- Firmware version: any
- UMS version: 6.01 or higher

Problem

Devices are not able to register in the UMS. Licenses are applied correctly. 2 servers appear in sync and another one is out of sync.



Solution

Issue is related to the UMS Licensing ID. A workaround / solution is to back up the UMS Licensing ID from the UMS Administrator and restore it to the out-of-sync server. See Manual Synchronization of the UMS Licensing ID (see page 127).

Manual Synchronization of the UMS Licensing ID

Overview

When the main UMS Licensing ID is not synchronized between the UMS Servers, **UMS Licensing ID status** under **UMS Administration > Global Configuration > Licenses** reads "Not in sync, please restart server", see UMS Licensing ID (see page 431). However, even when you restart the UMS Server, the UMS Licensing ID sometimes remains unsynchronized. In this case, the manual synchronization is required.

Environment

- UMS 6.01.100 or higher
- High Availability (HA) environment

Instructions

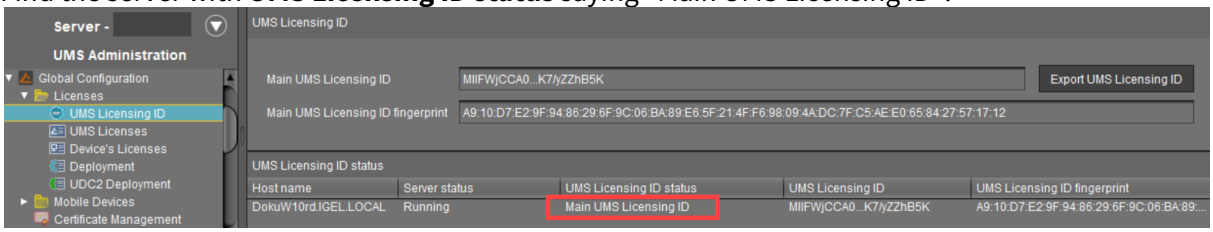
The manual synchronization of the UMS Licensing ID includes the following steps:

1. Locating the server holding the main UMS Licensing ID (see page 127)
2. Creating a backup of the UMS Licensing ID (see page 127) on that server
3. Restoring the created backup on all servers with the UMS Licensing ID unsynchronized (see page 130) and restarting all servers

Locating the Server Holding the Main UMS Licensing ID

To find out which server of the HA installation holds the **Main UMS Licensing ID**:

1. Open **UMS Console** and navigate to **UMS Administration > Global Configuration > Licenses > UMS Licensing ID**.
2. Find the server with **UMS Licensing ID status** saying "Main UMS Licensing ID".



Creating a Backup of the UMS Licensing ID

1. Open the UMS Administrator (see page 539) on the server with the main UMS Licensing ID you located in the previous step.

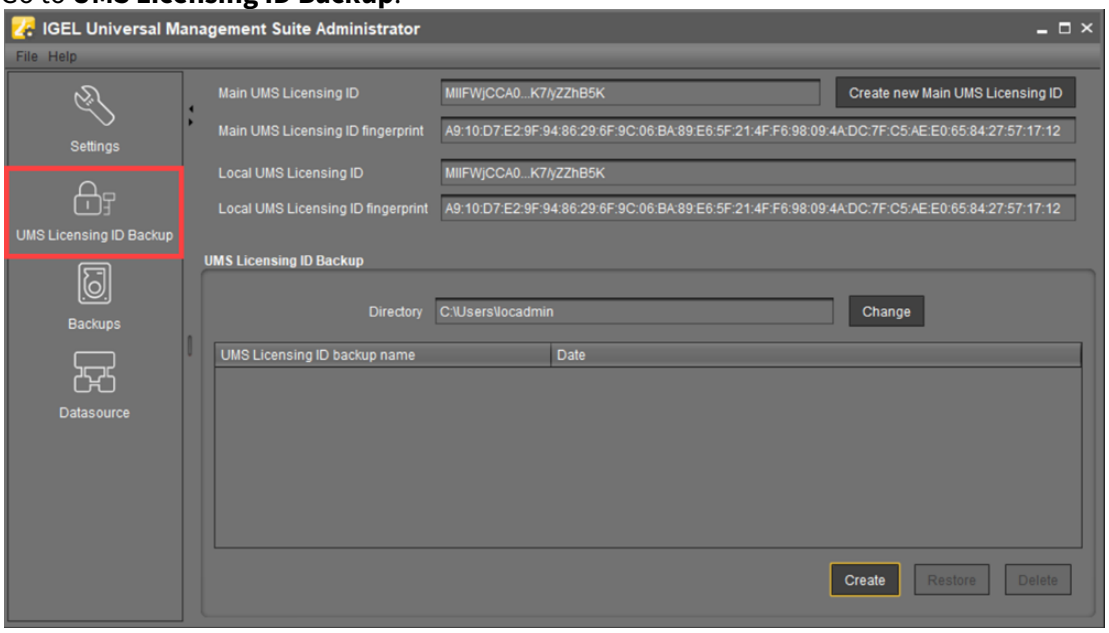
   Default path to the UMS Administrator:

Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`

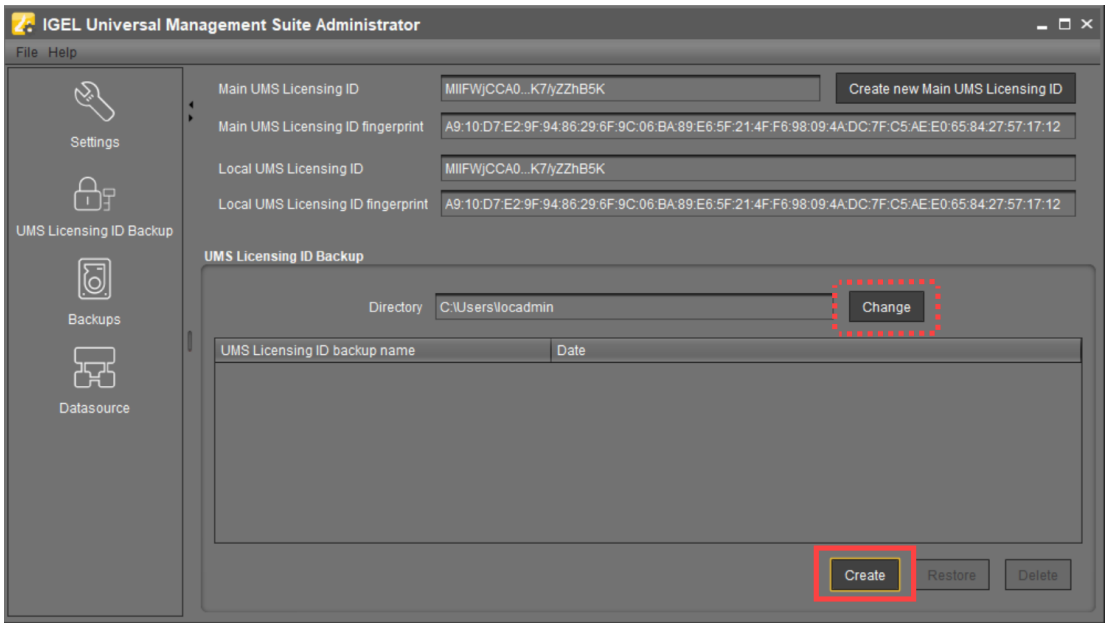
Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`

The IGEL UMS Administrator application can only be started on the UMS Server.

2. Go to **UMS Licensing ID Backup**.



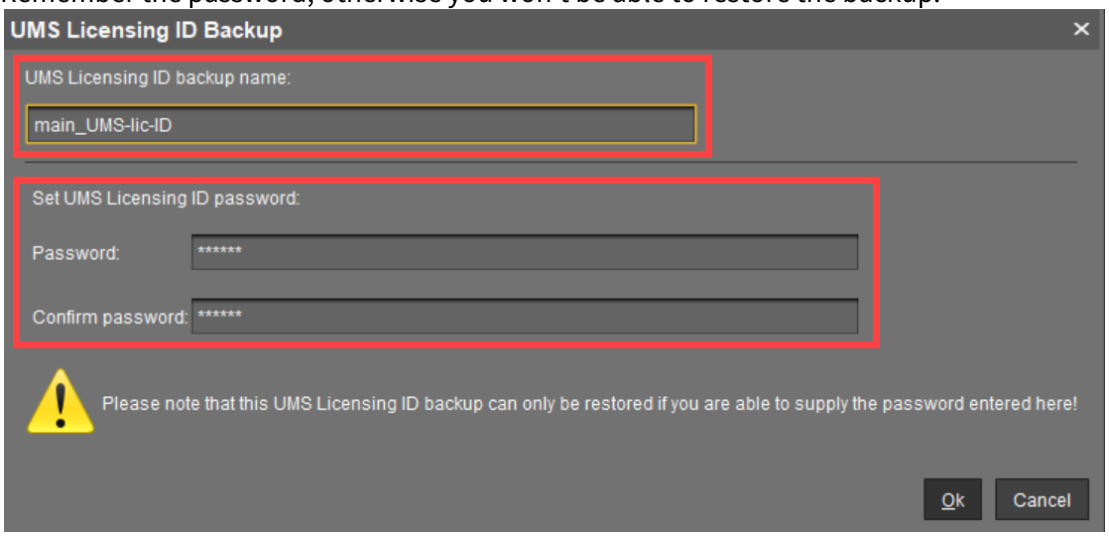
3. Click **Change** if you want to change the directory for storing the backup.
4. Click **Create**.



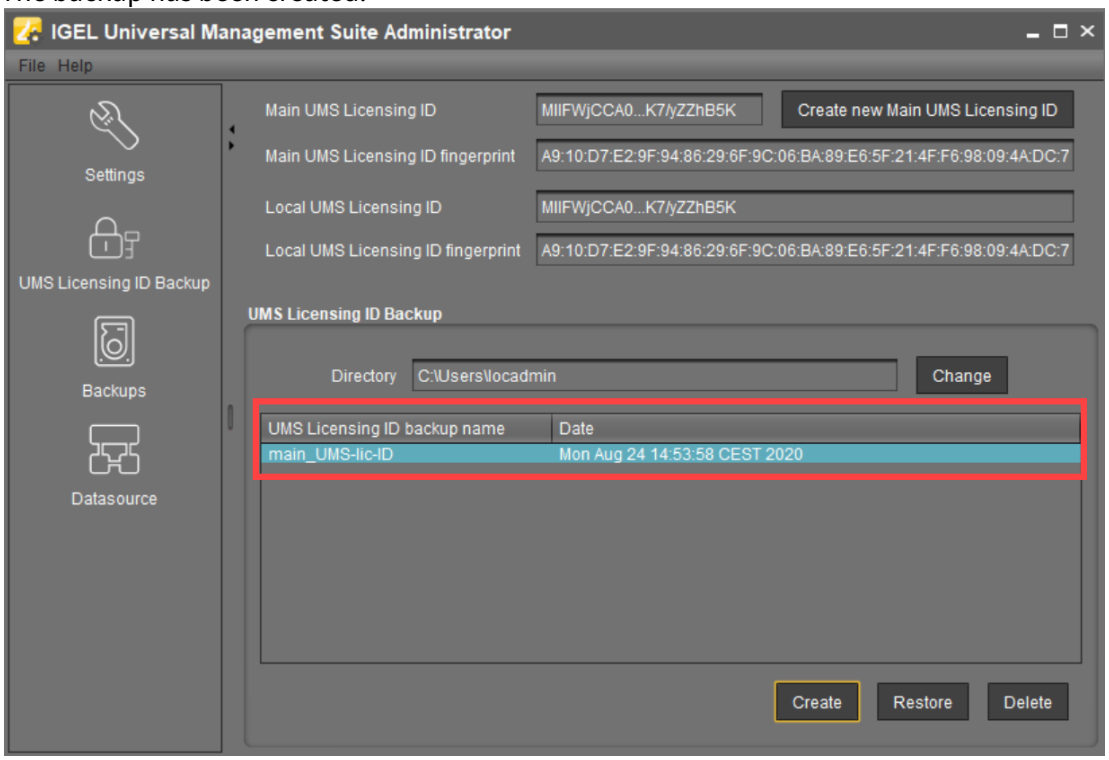
The **UMS Licensing ID Backup** dialog opens.

5. Under **UMS Licensing ID backup name**, specify a name for the backup.

6. Under **Set UMS Licensing ID password**, specify a password for the backup and confirm it. Remember the password, otherwise you won't be able to restore the backup.



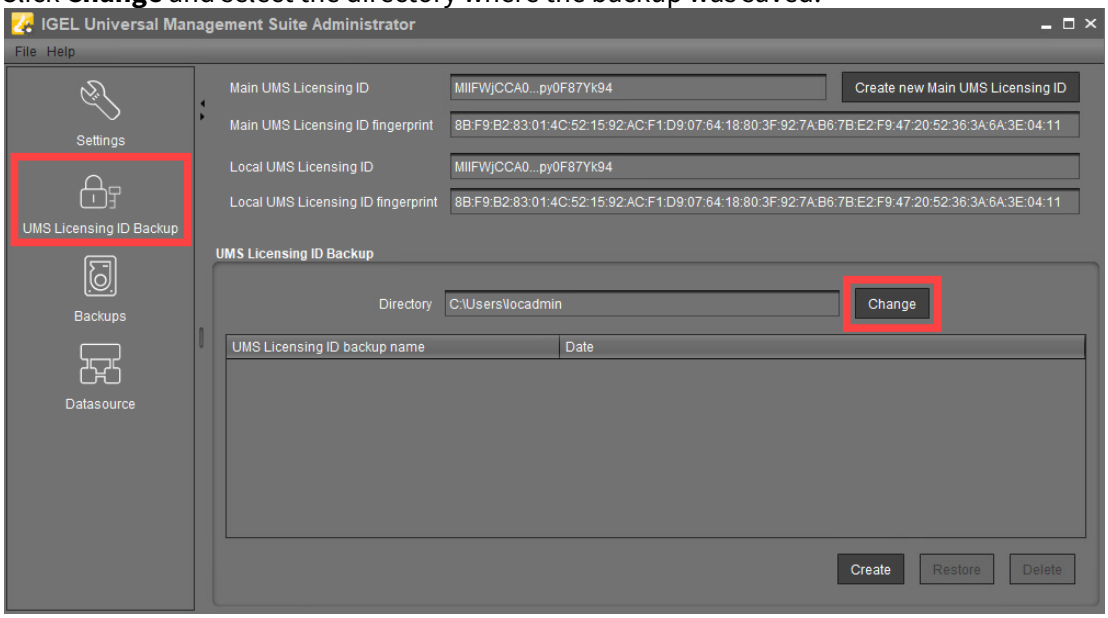
7. Click **Ok**.
The backup has been created.



8. Transfer the created backup to every server where the UMS Licensing ID is not in sync.

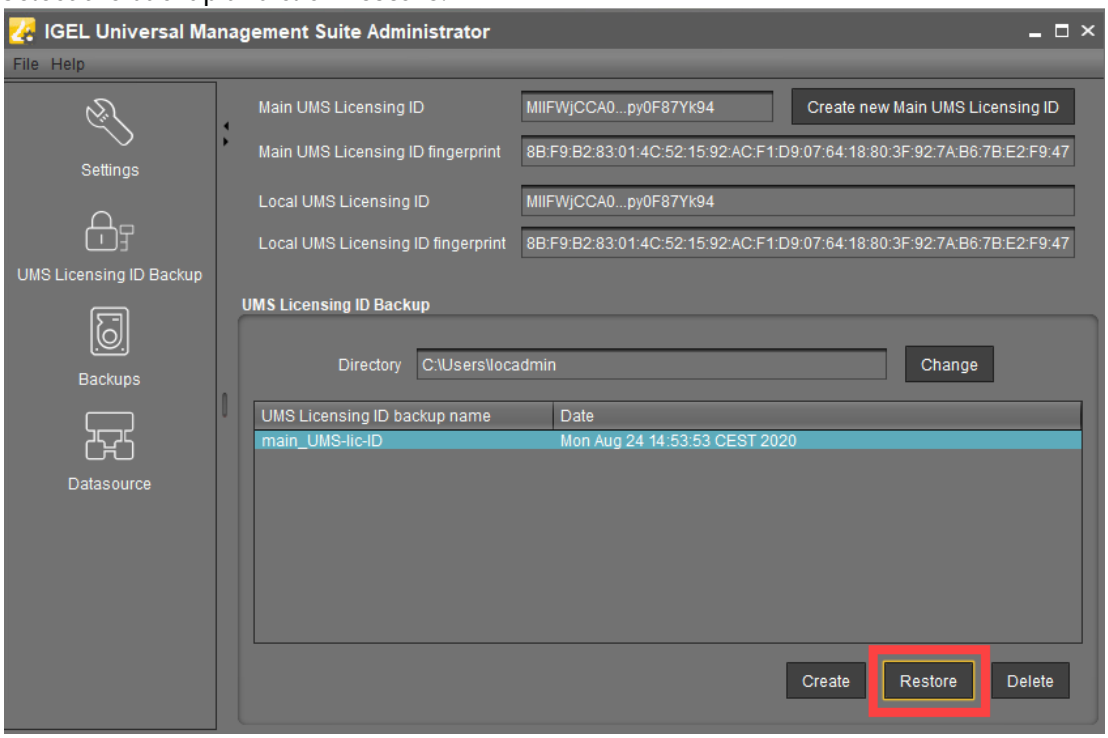
Restoring the Backup on All Servers with the UMS Licensing ID Unsynchronized

1. Open the UMS Administrator **> UMS Licensing ID Backup** on every server where the UMS Licensing ID is not in sync.
2. Click **Change** and select the directory where the backup was saved.



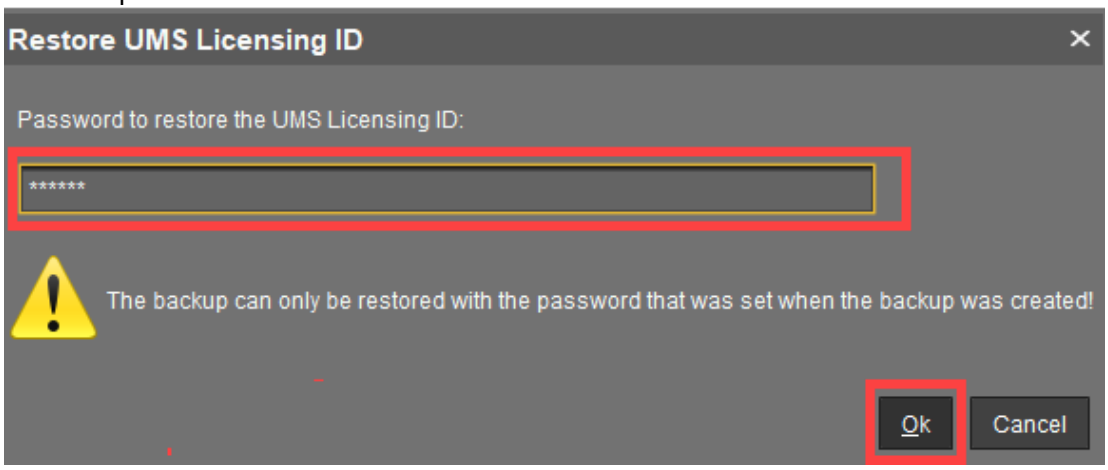
The backup appears in the list of the available UMS Licensing ID backups.

3. Select the backup and click **Restore**.

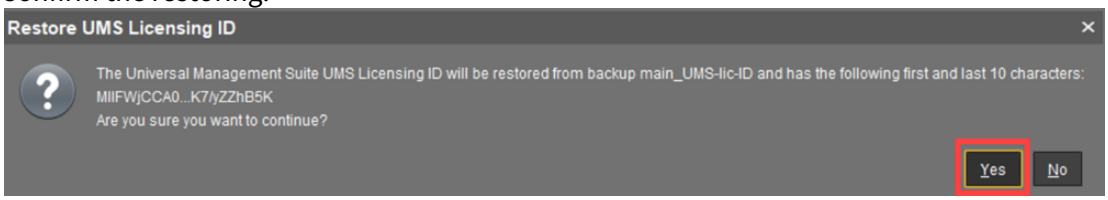


The **Restore UMS Licensing ID** dialog opens.

4. Enter the password and click **OK**.



5. Confirm the restoring.



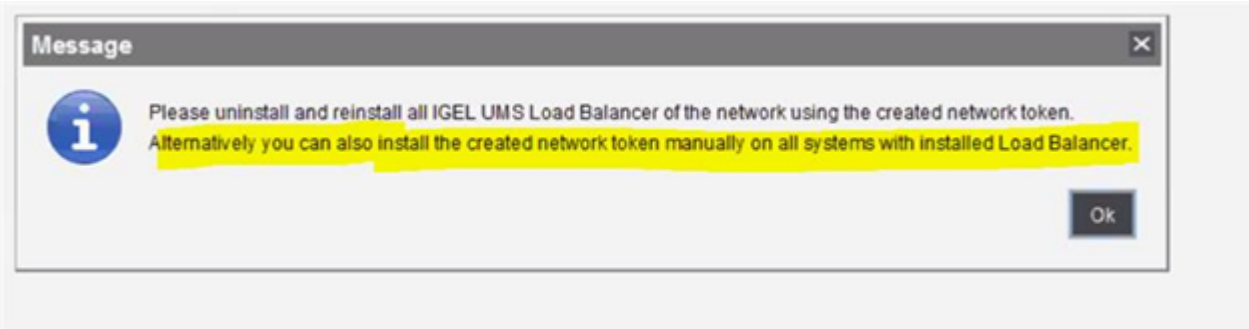
6. Repeat the procedure for all servers with the UMS Licensing ID unsynchronized.
7. When the backup restoring procedure is complete, restart all servers if you have not yet done so. In the UMS Console, the **UMS Licensing ID status** under **UMS Administration > Global Configuration > Licenses > UMS Licensing ID** should show that the UMS Licensing ID is now synchronized on all servers.

Error Message When Switching Back from an Externally Signed CA to the Internal CA

> **Solution Based on Experience from the Field**
>
> This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

Symptom

After testing externally signed CA, if switch back to the internal one, an error message will come up:



Environment

- UMS HA; UMS version: any

Solution

1. Run the installer again.
2. Choose **Repair**.
3. Point to the HA 'token' / certificate and install it that way.

Device

Device Scan or Online Check fails

Symptom

Although a device responds to a ping command, it does not appear in the UMS Console's list of scanned devices, can not be registered or shows up as offline (red) in the UMS Console's navigation tree.

Problem

The packets for scanning the devices or checking their online status are getting blocked within the network, e.g. by a firewall or VPN.

Solution

Make sure UDP packets on port 30005 are not blocked within your network. Those packets are used for both, scanning for devices as well as checking the status of the clients.

See also UMS Communication Ports.

Registration of a Device in the IGEL UMS Fails

The following article explains the possible reasons and solutions for device registration failure in the IGEL Universal Management Suite (UMS).

Symptom

Although a device can be scanned from the UMS Console, it cannot be registered on the UMS Server. One of the following error messages will appear in the UMS Console:

- `Cannot connect to remote management server`
- `Protocol state invalid`
- `Certificate invalid`

Problem

This may be caused by

- the server's firewall blocking the process
- an already existing UMS certificate on the device
- some database service hanging
- network transfer delays or losses affecting the registration process
- not correct time / date on the device or the UMS Server

Solution

Solving the Firewall Problem

1. On your system running the UMS Console and UMS Server, add the following port to the Windows firewall as an exception:
   - **Name** = `IGEL RMGUIServer`
   - **TCP Port** = `30001`

   > If you have changed the standard port 30001 in the UMS Administrator, open the firewall accordingly for this port. For more details on ports, see UMS Communication Ports (see page 26).

2. Make sure no other firewall within the network is blocking ports 30001 and 30005.
3. Try to import the device again.

> It can also be useful to check the network firewall for SSL inspection.

Solving the Certificate Problem

▶ Delete the `server.crt` certificate from `/wfs/` folder on the device. Try to register the device again.

OR

▶ Reset the device to factory defaults and try to register the device again. For how to reset the IGEL OS device to factory defaults, see Reset to Factory Defaults.

OR

▶ If you know from which UMS Server exactly the device has received the certificate and have access to this UMS Server, you can remove the certificate as described under Removing a Certificate (see page 176).

Solving the Database Problem

▶ In the **UMS Administrator** > **Datasource**, disable the currently active data source and re-activate it again. Try to register the device again.

For details on the UMS Administrator, see The IGEL UMS Administrator (see page 539).

Checking the Network

▶ Check if the network is fine by sending pings from the device console to your UMS Server:

```
ping -s  -c 10 -M do
```

Start with SIZE =1500 and decrease the size of packages until all packages got transferred without fragmentation or package loss. 1440 / 1400 / 1350 / 1300 are good values to test with.

> For "pinging" the UMS Server on a device with IGEL OS, you can use the built-in network tools (by default, **Start menu > System > Network Tools**; see Network Tools).

Checking Time and Date

▶ Check if the time and date are set correctly on the device (see Time and Date) and on the UMS Server.

> **Tip**
> If you have problems with device registration in the UMS, it is generally recommended to check

- if the registration directly from the endpoint device functions, see UMS Registration. If not, it is usually a sign of some network problems.
- if there is another UMS on the network, and the DHCP and/or DNS server configuration points to the "wrong" UMS.

Related Topics

Thin Client Registration fails with Error Message "Unexpected end of input stream" (see page 138)

Device Registration Behind SonicWall Firewall Fails (see page 139)

Device Scan or Online Check fails (see page 134)

Device Registration fails with Error Message: Unexpected end of input stream

Symptom

UMS console shows an error message like "Unexpected end of input stream found at ..." during registration of devices.

Problem

Devices cannot register with UMS over a remote link via VPN gateway, router, firewall or other networking device due to issues with large packets.

The error may occur even if there is no NAT used and the networking device seems to be configured correctly so e.g. pinging is successful in both directions.

Solution

Please consult the documentation for your network device and look up the options for handling large packets. In the case of SonicWall devices the solution is setting the `Ignore Don't Fragment Bit` option.

Device Registration Behind SonicWall Firewall Fails

Symptom

The devices are detected by the UMS during a scan, but registration fails. UMS console shows an error message like "Unexpected end of input stream found at ...".

Possible Causes

The following causes have been reported with firewalls by SonicWall;

- Large packets: See Thin Client Registration fails with Error Message "Unexpected end of input stream" (see page 138).
- SonicWall DPI-SSL replaces the UMS certificate: If SonicWall DPI-SSL is enabled, it functions as intermediate CA and sends its own certificate to the devices instead of the original UMS certificate. As a consequence, the devices refuse to register because they would only accept the original UMS certificate.

Solution

1. In SonicWall, under **DPI-SSL Status**, add the IP address of the UMS server to the list of DPI-SSL exclusions.
2. Restart the VPN tunnel.

Changing the Hostname of an Endpoint Device via UMS

There are two different ways to change the hostname of an endpoint device via UMS:

Option 1:

If **Adjust UMS-internal name if network name has been changed** is checked under **UMS Administration > Global Configuration > Device Network Settings***:*

1. Right-click the device within the UMS structure tree.
2. Choose **Edit Configuration**.
3. Go to **Network > LAN Interfaces**.
4. Change **Terminal name**.
5. Click **Save**.
6. Select that you want the settings to be applied **Now**.
7. Click the **Refresh** button in the UMS in order to see the changed hostname.
8. Reboot the device.

Option 2:

If **Adjust network name if UMS-internal name has been changed** is checked under **UMS Administration > Global Configuration > Device Network Settings**:

1. Right-click the device within the UMS structure tree.
2. Choose **Rename**.
3. Change the name.
4. Click **OK**.
5. Right-click the device.
6. Choose **Other commands > Settings UMS -> Device**.
7. Reboot the device.

Start of the UMS Console / Web App

Starting UMS Console Crashes NX Session

Symptom

When you are connected to an Ubuntu host via NX, starting the UMS Console on the Ubuntu host crashes the NX session.

Solution

1. Become **Root** on the Ubuntu host.
2. Open the configuration file `/opt/IGEL/RemoteManager/rmclient/RemoteManager.bin.config` in a text editor.
3. Add the line `vmparam -Dsun.java2d.xrender=false` to the file.
4. Save the file.
5. Become a regular user.
6. Start the UMS Console.

UMS Console doesn't start on Linux System without X11

Symptom

IGEL UMS doesn't start on Linux system without X11.

Problem

The UMS console application needs X11 to run.

Solution

- Install X Window System (X11) to run IGEL UMS.

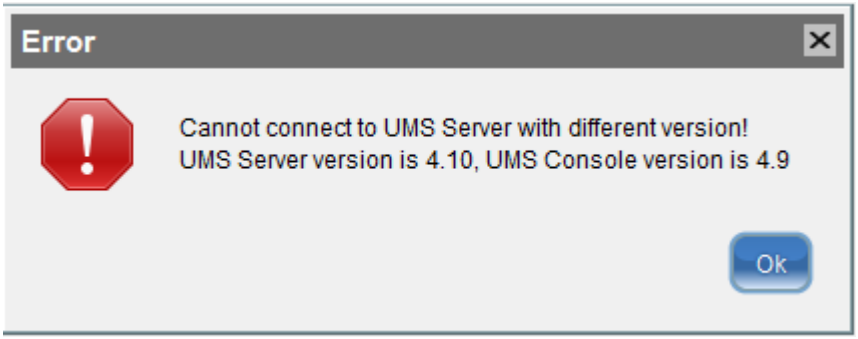
Logon failures

UMS Console Logon fails

Symptom

When you try to log on to the console you get the error message **Unable to load tree**.

More recent UMS versions show the following error message:



Problem

Problems with the connection between the UMS console and the UMS server may be caused by a difference in software versions, e.g. if the UMS server was updated but the console still uses an old version.

Solution

Check the version status:

1. Check the version of the console by selecting **Help > Info** from the UMS console menu.
2. Check the version of the server by selecting **Help > Info** from the UMS administrator menu.
3. If necessary, update the UMS console to the same version as the server or newer.

UMS Console Login with AD User Account fails

Symptom

UMS console login fails for Active Directory user.

Problem

1. Open catalina log file `C:\Program Files\IGEL\RemoteManager\rmguiserver\logs\catalina.log`
2. Check the log for message `KDC has no support for encryption type (14)`

Solution

If this happens, the following things needs to be done/checked:

1. Have a look at http://technet.microsoft.com/en-us/library/cc733991.aspx.
2. Disable **DES encryption** for the AD user account, this can be done in the account setup of the Windows user administration > Account options.
3. Follow http://docs.oracle.com/javase/6/docs/technotes/guides/security/jgss/tutorials/Troubleshooting.html.

Login to the UMS Fails after the Update

Symptom

You cannot log in to the UMS after an update or the installation of the UMS Server.

An error message with the URL `https://[ums_server_host]:8443/info` appears:

Problem

The IGEL RMGUI Server Service has not fully started yet.

Solution

Wait for a few minutes more. After that, try to log in again.

Active Directory / LDAP

Integrating Active Directory

Problem

Instead of creating and organizing UMS administrators manually you are looking for an easy way of importing them from your existing Active Directory.

Reason

You would like to import users and user groups from the Active Directory to the UMS, using the same AD group assignments and credentials as already defined in the AD.

Solution

In this paper we explain the best way of importing users from the Active Directory as UMS administrator accounts.

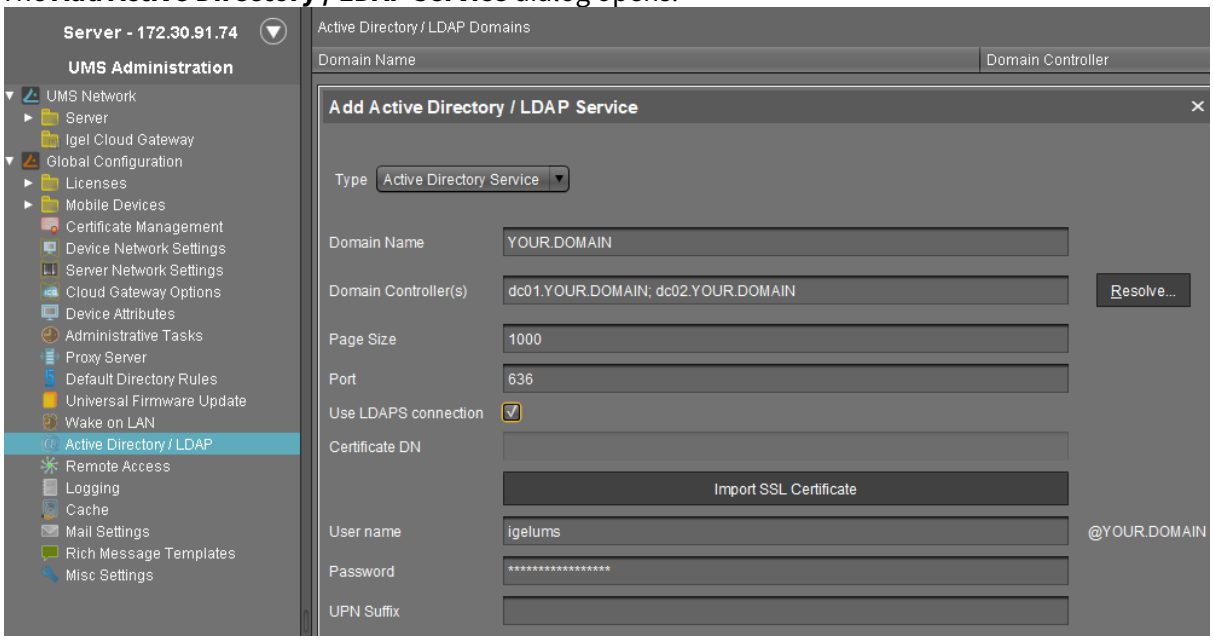
We will import users from the Active Directory to the UMS console in three steps by:

- Configuring the connection to the Active Directory
- Selecting the users to be imported and starting the import
- Assigning permissions

Configuring an AD Connection

Perform the following steps to set up the connection between the UMS and the Active Directory of your company:

1. Click **Add (+)** under UMS console > **UMS Administration > Global Configuration > Active Directory / LDAP**.
   The **Add Active Directory / LDAP Service** dialog opens.



2. Select **Active Directory Service** as **Type.**
3. Enter the **Domain Name**.

   > Several Active Directories can be linked. You should therefore ensure that you provide the correct domain when logging in (e.g. to the UMS console).

4. Enter the **Domain Controller(s)** manually or click **Resolve...** for the automatic search.
   To separate domain controllers, use a semicolon.

   > If the option **Use LDAPS connection** (see below) is enabled, make sure that a fully qualified name of the **Domain Controller** has been entered. See Problems When Configuring an Active Directory with LDAP over SSL (see page 161).

5. Enter **Page Size**.
   The **Page Size** property sets the maximum number of items in each page of results that will be returned by a search. It affects query performance, but not the number of overall results. The standard value is "1000". Change this value in line with your server configuration.
6. Activate **Use LDAPS connection** to secure the connection with the provided certificate.
   The **Port** changes automatically to default "636".
7. Click **Import SSL Certificate** to configure the certificate and to verify the **Certificate DN**.

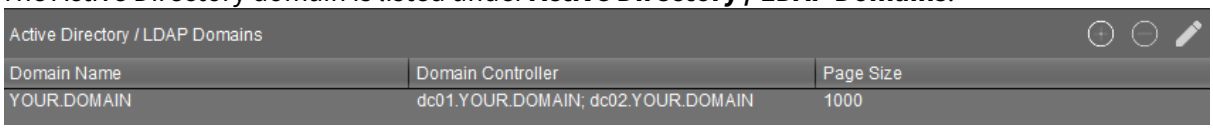
> Since the name of the **Domain Controller** is checked against the certificate, they must correspond. If more than one domain controller is used, the root certificate of the domain must be configured. See Problems When Configuring an Active Directory with LDAP over SSL (see page 161).

> The supported certificate formats are `.cer`, `.pem` and `.der`

8. Under **User name** and **Password**, enter your user credentials.
9. Enter **UPN Suffixes** (aliases) if you have defined any (semicolon separated list). Example: `domain.local;test.local`

   > The settings must correspond to the configuration of the Active Directory. If there are registered UPN suffixes in the AD, they should be known also by the UMS.

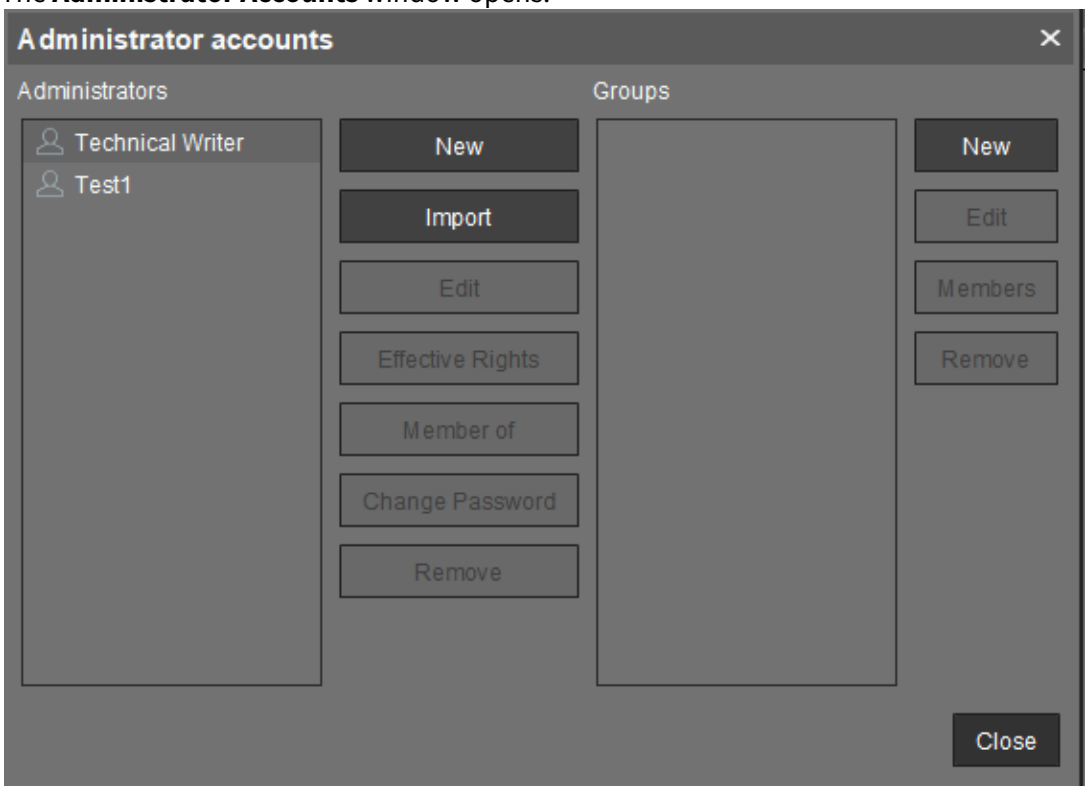
10. Click on **Test Connection** to check that you have entered a valid configuration.
11. Click **Ok** to confirm your settings.
    The Active Directory domain is listed under **Active Directory / LDAP Domains**.



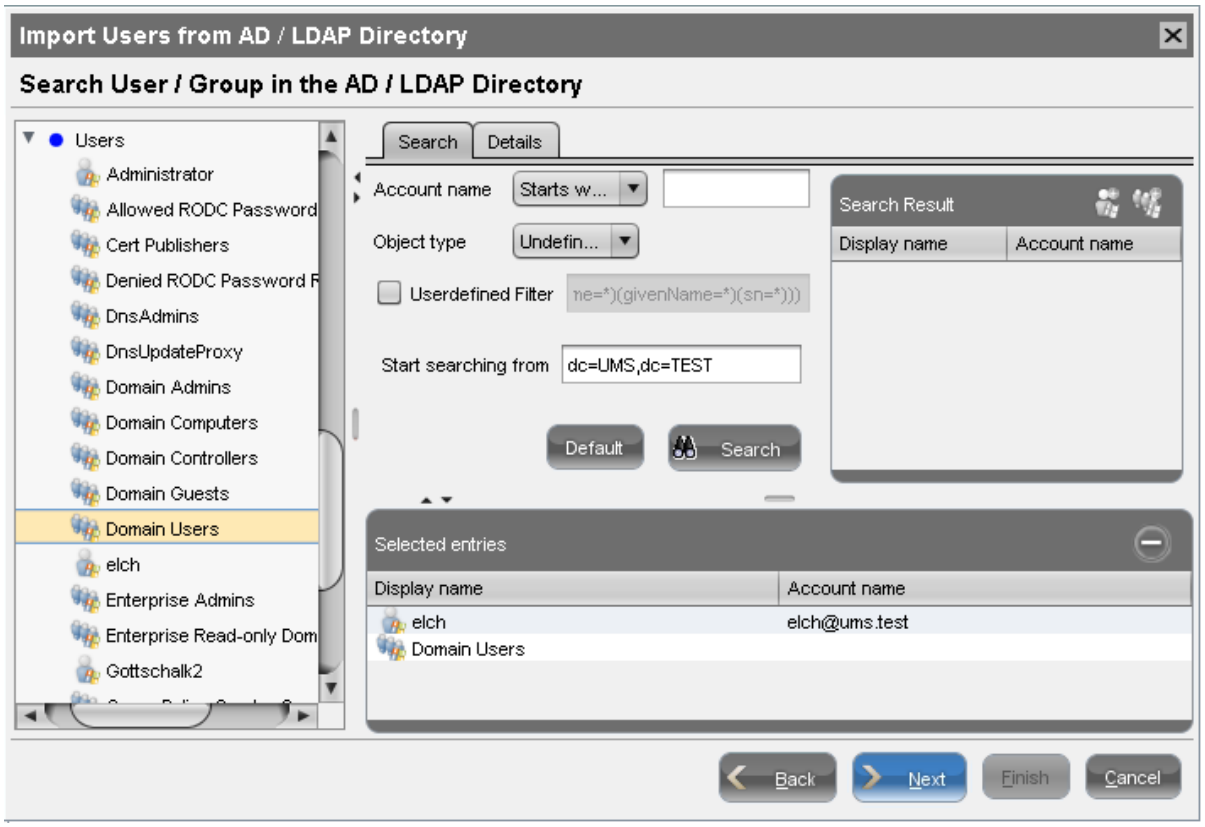
Importing Users from AD to UMS

After connecting the Active Directory you can import users or user groups to the UMS:

1. Click **System > Administrator Accounts**.
   The **Administrator Accounts** window opens:



2. Click **Import** to log in to the AD/LDAP service.
3. Select the domain and enter your credentials, if not already defined.
4. Click **Next** to open the Active Directory browser.
5. Select individual users or groups from the structure tree of your AD.
6. Use drag and drop to add your selection to the **Selected Entries** list.



As an alternative to navigating in the structure tree, you can also add users or groups to your selection using the Search function.

7. Click **Next** and confirm to start the import.
   A result list of imported accounts opens.

8. Click **Finish** to complete the import.

If the result list is either empty or some accounts are missing from the list, see Import of Administrator Accounts from Active Directory Fails (see page 162).

> A UMS administrator set up by mistake must be deleted manually using the dialog 'Administrator accounts'. The IGEL UMS uses the 'User logon name' from the AD as the name of the imported user.

Assigning Permissions

After the AD users have been imported, they can access the UMS with their Active Directory credentials.

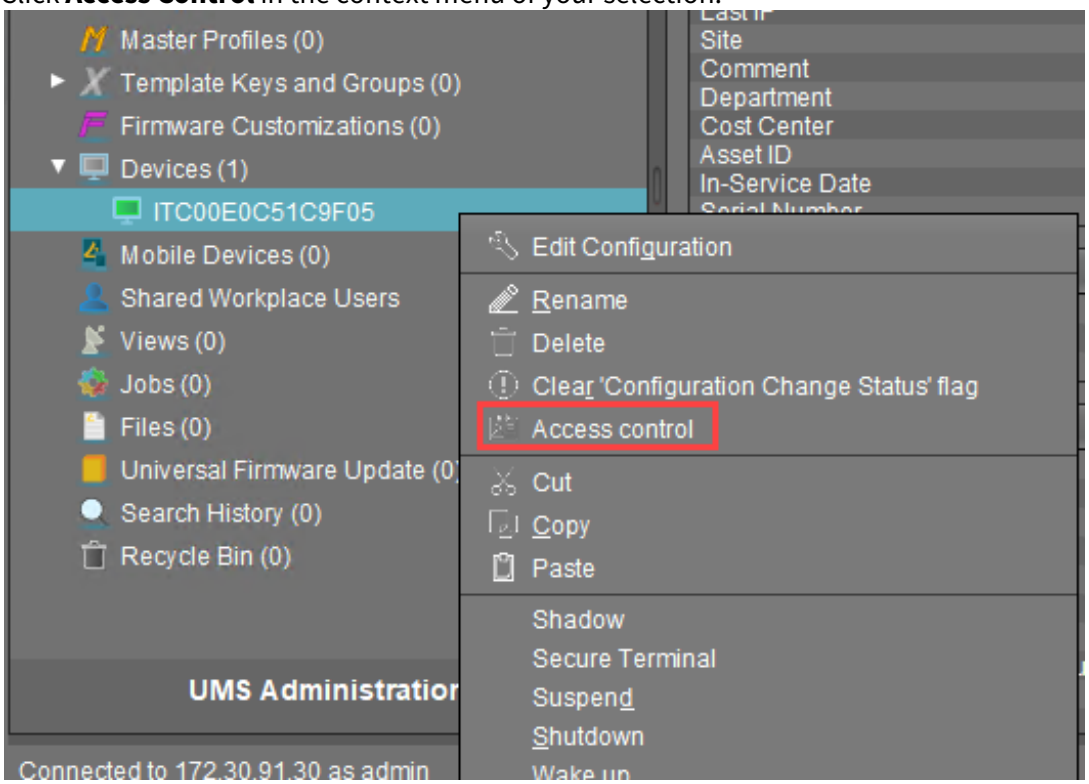
As UMS administrators, the users still need individual access rights.

> The logon to the UMS is not possible via the 'pre Windows 2000 logon name' ('DOMAIN\logon name'), but only via the format 'logon name@DOMAIN'.

> For example, in order to be able to change the configuration of a thin client, a user requires authorization to browse the thin client's directory path and configure the thin client itself.

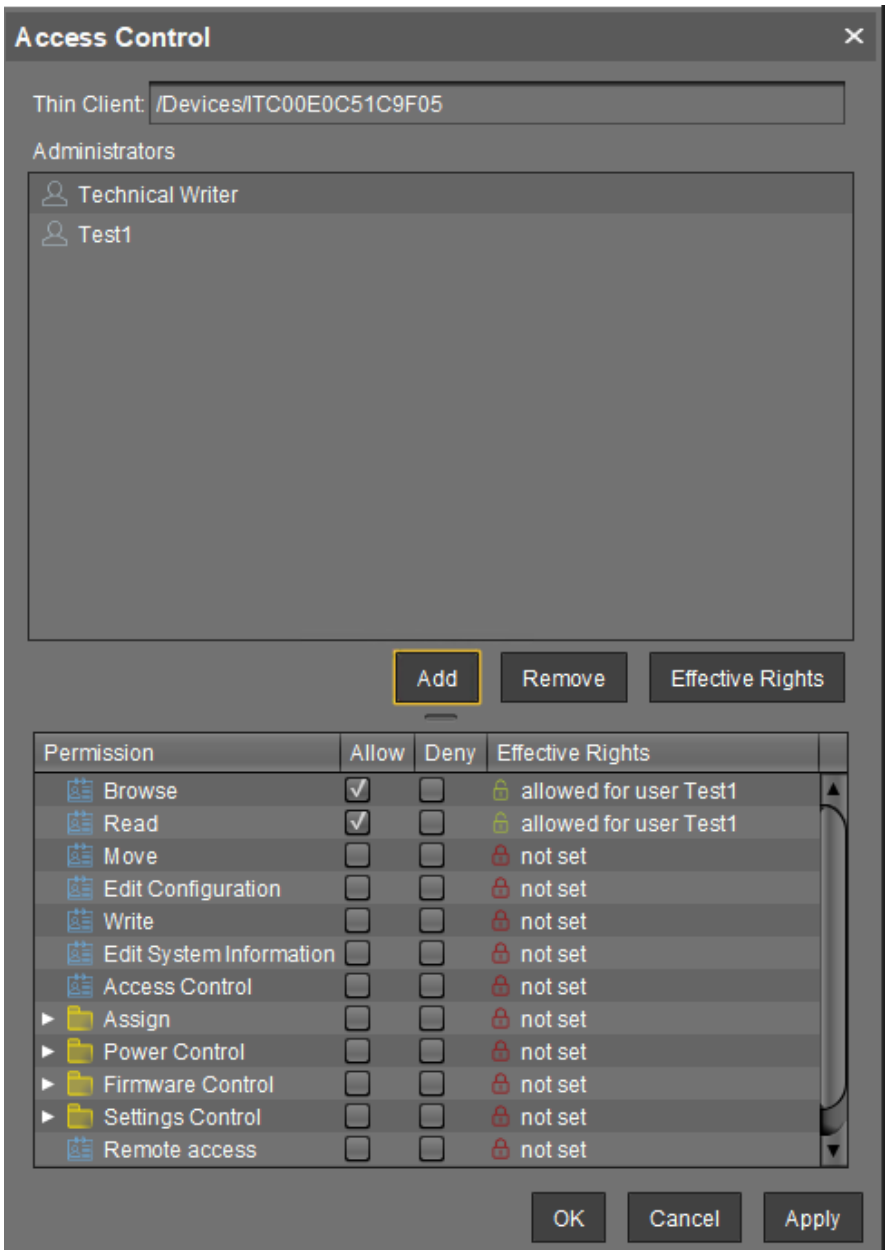
To assign these rights, proceed as follows:

1. In the structure tree of the UMS console choose the **Devices** node or a subgroup of devices or a single client.
2. Click **Access Control** in the context menu of your selection.



3. The **Access Control** window opens.

4. Click **Add** to select your new user/group.
5. The corresponding **Effective Rights** will be listed in the lower part of the mask.



6. **Allow** or **Deny** the rights of the selected group or user for access to the selected devices
7. Confirm the settings with **OK**.

8. Click the **Refresh** button of the console to apply the changes in the UMS.

> If you have changed the rights of registered users they only take effect after a refresh.

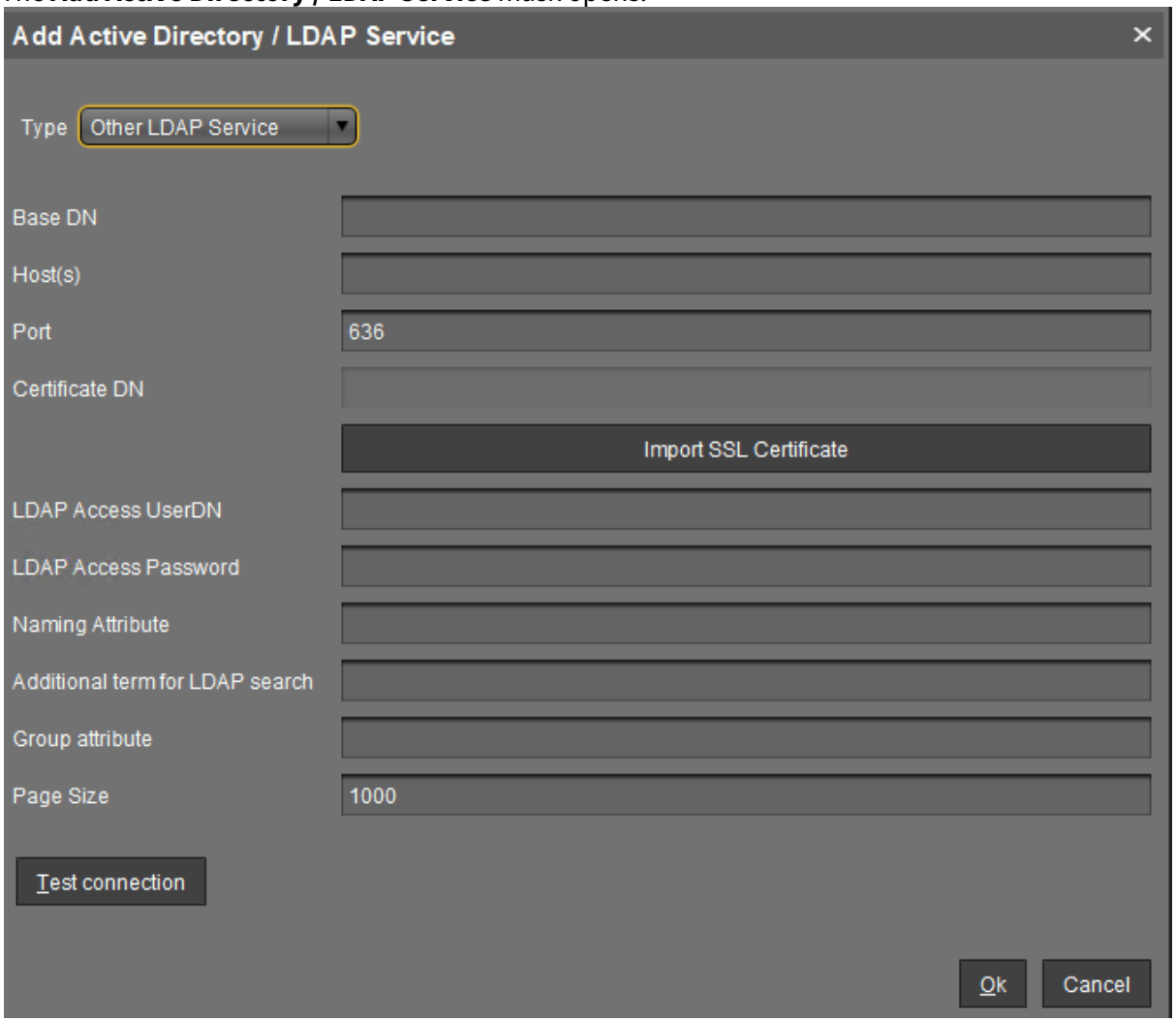
For further details about authorization rules see our How-To IGEL UMS: User Authorization Rules (see page 61).

Access rights to objects or actions within the IGEL UMS are attached to the administrator accounts and groups. The rights of the database user account cannot be restricted. They are created during installation or when setting up the data source. The account always has full access rights in the UMS.

Configuring an LDAP Connection

As a variant you may connect other LDAP directory services, i.e. Novell eDirectory and OpenLDAP, to the UMS:

1. Click **Active Directory / LDAP** in the **UMS Administration** area of the UMS console.
2. Click **Add (+)** in the **Active Directory / LDAP Domains** mask.
3. The **Add Active Directory / LDAP Service** mask opens.



4. Select **Other LDAP Service** as **Type**.
5. Enter the **Base DN** and the **LDAP Access UserDN** in accordance with the LDAP Data Interchange Format.
6. Enter the IP of your device in the **Host(s)** field; for more devices, use a comma separated list.
7. The default **Port** for LDAP over SSL is 636.

> For security reason UMS supports secure LDAP connections only.

8. Under **LDAP Acess UserDN/Password** enter the credentials of the LDAP Service access. The user needs to have read rights on the whole directory service, because it will be used for the determination of the structure in the directory service.
9. Under **Naming Attribute** enter the name of the LDAP attributes, which contains the distinct user account name.
10. Optionally, you can add an **Additional term for LDAP search**, which will be attached to the search for users. This way, performance can be optimized.
11. As **Group attribute** enter the name of the LDAP attribute, which contains the group membership of a user.
12. Define the **Page Size**. This property sets the maximum number of items in each page of results that will be returned by a search. It affects query performance, but NOT the number of overall results. The standard value is 1000. Change this value in line with your server configuration.
13. Click **Import SSL Certificate** to verify the **Certificate DN**.

Problems When Configuring an Active Directory with LDAP over SSL

Symptom

You cannot configure an AD Connection under **Active Directory / LDAP** with the option **Use LDAPS connection** activated. When testing the connection, one of the following types of error messages appears:

- "`The connection to the LDAP service failed! Check the certificate and server name`";
- "`simple bind failed`".
  The log file looks like:
- "`2019-05-23 14:13:38,512 ERROR [https-jsse-nio-8443-exec-151] dec: simple bind failed: QA-DC01:636 javax.naming.CommunicationException: simple bind failed: QA-DC01:636 [Root exception is javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: No subject alternative DNS name matching QA-DC01 found.]`"
  or
- "`javax.naming.CommunicationException: simple bind failed: dc01.your.domain:636 [Root exception is javax.net.ssl.SSLHandshakeException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target]`"

Problem

The **Domain Controller(s)** name and the certificate configured under **Import SSL Certificate** do not match.

Solution

1. Check that a *fully qualified name of the domain controller* has been entered, e.g. "dc01.your.domain". An IP address or a short name such as "dc01" will not be accepted when the domain controller name is checked against the certificate.
2. If several domain controllers are used, make sure that the *root certificate* has been configured.

Import of Administrator Accounts from Active Directory Fails

Symptom

The import of UMS administrators from an Active Directory fails, the result list of imported accounts is either empty or some accounts are missing on the list.

Problem

Active Directory user accounts may have an empty User Principal Name (UPN). This occurs when updating an older Active Directory (e.g. on Windows NT 4.0) to a new one migrating the AD user accounts to the new AD.

Solution

1. Set the UPN of each AD account to be imported.
2. Retry the import of AD users in IGEL UMS.

Profiles

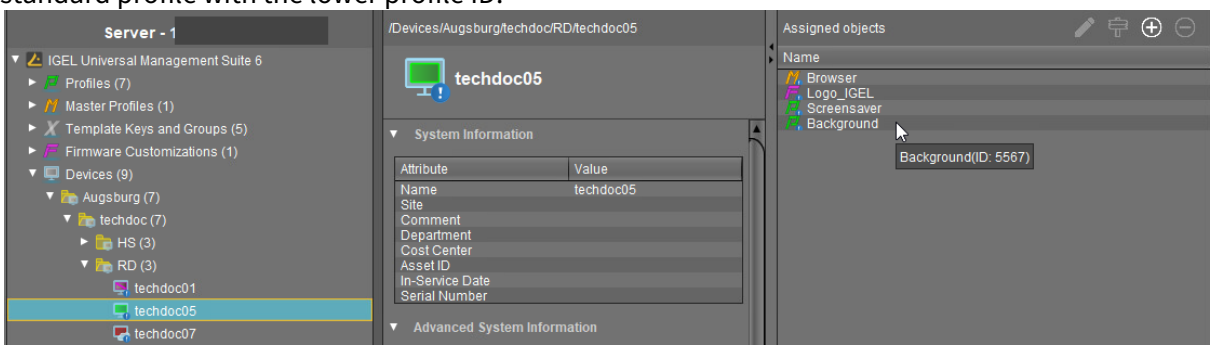
Find Out a Profile's Priority

Using profiles is a very powerful method to manage and configure one, ten, or thousands of endpoint devices with the IGEL UMS (Universal Management Suite). However, when you are deploying a great number of profiles, things can get confusing. Some profiles may have overlapping scopes and thus try to set different values for one specific parameter on a device. One profile will always win, but which one is it? Luckily, the UMS can show the order of priorities at a glance.

For a comprehensive reference of profiles, see the Profiles Chapter (see page 276) in the UMS Manual; the prioritization is covered in Prioritization of Profiles (see page 304).

The following example shows how to find out a profile's priority:

1. In the structure tree, select the device for which you want to see the order of profile priorities.
2. Take a look at the **Assigned objects** area. All profiles that are assigned to the device are listed by priority, in descending order. The profile with the highest priority is listed first, and so on.
   In the following screenshot, the profile with the highest priority is a master profile. It is followed by a firmware customization, which has in turn higher priority than a standard profile, see Firmware Customizations (see page 339). And at the bottom, the object with the lowest priority is displayed – a standard profile with the lower profile ID.



Precedence of Profiles and Universal Firmware Updates

This article explains which firmware update settings will be effective when several concurring settings are assigned to your devices. Firmware update settings can be defined locally on the device, by one or more profiles, or by one or more Universal Firmware Update.

General Order of Priority

Generally, the order of priority is as follows, from highest to lowest priority:

- Universal Firmware Update
- Profile
- Local settings

For details, see the following sections.

Universal Firmware Update vs. Profile

If both a Universal Firmware Update and a profile that contains update settings are assigned to your device, the Universal Firmware Update has priority over the profile. This is also valid if the profile is a master profile; for further information, see Prioritization of Profiles (see page 304).

The following settings under **System > Update > Firmware Update** are overwritten by the Universal Firmware Update:

- **Protocol**
- **Server name**
- **Port**
- **Server path**
- **User**
- **Password**

Profile vs. Local Settings

The settings of a profile always overwrite the local settings.

Universal Firmware Update vs. Universal Firmware Update

If several Universal Firmware Updates are assigned to one device, the rules described below apply.

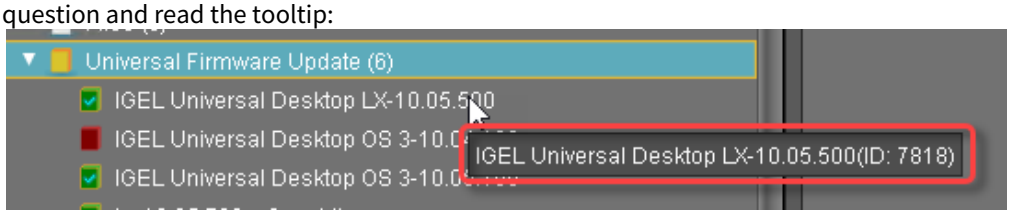
Assignment to Different Levels in a Hierarchical Order of Folders

If several Universal Firmware Updates are assigned to a device via different folders and subfolders, the one that is closest to the device has priority over all others.
Example: A Universal Firmware Update for IGEL OS 10.05.100 is assigned to a folder named "devices", which contains our device. Another Universal Firmware Update which contains IGEL 10.06.100 is assigned to a folder named "teamA". The folder "teamA", on this part, contains the folder "devices". As a result, the devices will be

updated to IGEL OS 10.05.100 (or keep IGEL OS 10.05.100) because the Universal Firmware Update for IGEL OS 10.05.100 is closer to the device in the folder hierarchy.

Assignment on the Same Level

If several Universal Firmware Updates are assigned to a device on the same hierarchical level, the one with the highest ID has priority over the others.
To find the ID of a Universal Firmware Update, move the mouse pointer over the Universal Firmware Update in question and read the tooltip:



In this example, the ID is 7818.

Compatibility

Only those Universal Firmware Updates are effective which are compatible with the device.

Assigning Profiles to Devices filtered by Views or Search

Valid for UMS version 5.02.100 and higher.

If you need to assign a profile to a group of devices which meet a certain criterion, you can proceed in the following way:

1. Define a view which filters the clients with a certain criterion (e. g. all devices which contain a USB storage hotplug).
2. Right-click the view to open the context menu.
3. Click **Assign profiles to the thin clients of the view**.
   The **Assign profiles** window opens.
4. Select the relevant profile (e. g. the profile which allows USB storage hotplug).
5. Click  to move it from the left to the right column.
6. Confirm the setting with **OK**.

In the same way you can assign profiles to devices of a search result:

1. Right-click the search result to open the context menu.
2. Click **Assign profiles to the thin clients of the search**.
   The **Assign profiles** window opens.
3. Select the relevant profiles and click  to move them from the left to the right column.
4. Confirm the setting with **OK**.

▶ To cancel the profile assignment, click **Detach profiles from the device of the view** or **search**.

> ⓘ You can also assign profiles to views or search results automatically and regularly as an administrative task.

Java Web Start

UMS Console via Java Web Start

Requirements

Java 1.8.0_40 or newer

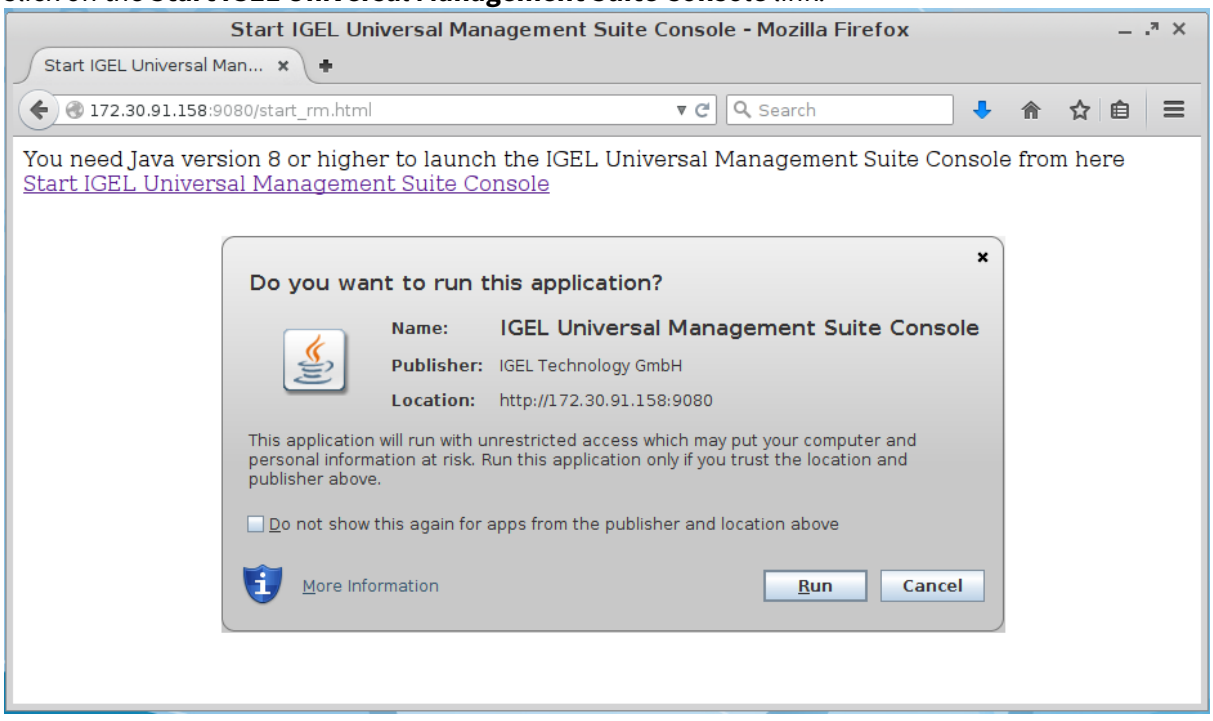
Starting the UMS Console via Java Web Start

To start the UMS Console via Java Web Start, proceed as follows:

1. In a web browser, open the address
   - `http://[UMS-Server]:9080/start_rm.html` if you want to use the HTTP port
   or
   - `https://[UMS-Server]:8443/start_rm.html` if you want to use the HTTPS port.

   > If **UMS Administrator > Settings > Allow connection via SSL only** is activated, the HTTP port, 9080, will be disabled. See also Settings (see page 540).

2. Click on the **Start IGEL Universal Management Suite Console** link.



3. Confirm that the downloaded JNLP file will be opened with the **Java Web Start Launcher**. The application will be downloaded.

4. Allow the application signed by IGEL Technology GmbH to be executed.
   The UMS Console will start, and the login window (see page 228) will appear.

   > Starting the UMS Console via Java Web Start ensures that the version of the UMS Console matches the version of the UMS Server.

Error when connecting to UMS via Java Web Start: "received fatal alert: handshake_failure"

Symptom

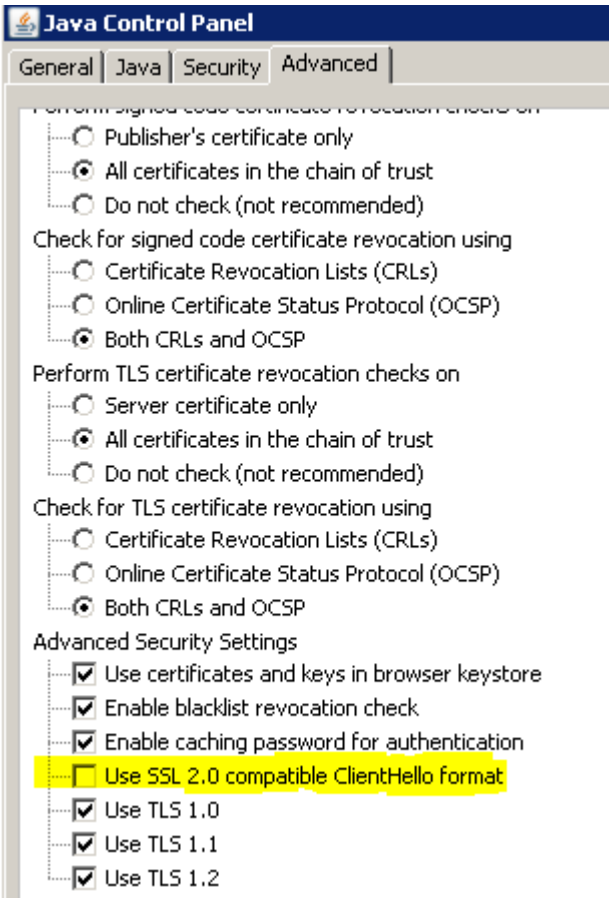
When trying to connect to *UMS* via *Java Web Start*, the connection fails with the error message "`received fatal alert: handshake_failure`".

Problem

The old Java Feature "SSL 2.0 compatible ClientHello format" is outdated and not accepted by UMS versions 4.09.100 or newer.

Solution

Disable **Use SSL 2.0 compatible ClientHello format** in the **Advanced Settings** menu of the **Java Control Panel**.



VNC Connection Error with Java Web Start Console and external VNC Viewer

Symptom

You are using IGEL UMS Java Web Start Console with Java SE Runtime Environment 7 or 8 (Java 7 or 8) and you have defined an external VNC viewer program in IGEL UMS Java Web Start Console.

When shadowing a thin client the error message appears: **Cannot run program "": CreateProcess error=2, system cannot find the file.**

Problem

The VNC viewer program's path definition is not correct. Java 6 did accept the path without quotes but Java 7 or 8 will not find the program without quotation. So this problem will most likely occur after upgrading the Java Environment.

Solution

Check the VNC viewer program's path in your UMS Console:

1. Go to **Misc > Settings**
2. Select your **External VNC viewer** program
3. Make sure the path is enclosed in double quotes (`"C:\program files\path\program.exe"`)
4. Save your settings with **OK**

Misc

Clearing up the UMS

Problem

You have several firmware versions in the UMS. Your collection of clients and profiles has become large and confusing. You are losing track of assignments and connections between these elements.

Goal

You want to minimize the variety of firmware and profiles to simplify processes. You just want to see what you need.

The firmware, clients, and profiles are interdependent. So, what is the best way to proceed?

Solution

> We advise making a back-up of the UMS before deleting any components. You can also use the UMS recycle bin for the deleted objects.

The following are the main steps for reorganizing the UMS:

1. Download the new firmware.
2. Move clients to the new firmware.
3. Move profiles to the new firmware.
4. Delete old firmware, clients, and profiles that are no longer required.

Downloading the new Firmware

1. Check our download server[6] to see whether there are new updates that are relevant for your applications.
2. Download the relevant update files. Install an update directory for the files on the UMS server or on your FTP server.

Moving Clients to the New Firmware

Find out how many different firmware versions you really need.

Upgrading all clients to the same firmware:

1. Create a new **View** to search for all clients using a firmware version older than the current version. Example:
   View Name: Show all UD LX devices with old firmware
   Rule: Product name is like (!reg!)(?i).*Universal Desktop LX.* AND Firmware version is less than 5.04.100
2. Assign the update directory to these devices.

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

3. Start the update process.

Moving Profiles to New Firmware

Examine your profiles and decide which of them are relevant for the new firmware. You have three possibilities you can do now:

- Adjust the firmware version the profiles are based on, to be sure that they will work with the new firmware.
- Leave the profile settings as they are.
  If the parameters of the new firmware match the parameters of the old version, a profile will work anyway. If they do not match, these parameters will be ignored.
- Create new profiles.

For more information see UMS Manual: Creating Profiles.

Deleting old Firmware, Clients and Profiles that are no longer required

To finally clear up the UMS you now should delete obsolete objects.

- Use again Views to select the clients, which are no longer required.
  For more Information see UMS Manual: Creating a New View (see page 391).
- Select the obsolete profiles. You can do this manually or by using the search option: **Misc > Search > Profiles > Product&Firmware**.
- Delete old firmware which is not assigned any longer to a client or profile: **Misc > Remove Unused Fimwares**.

Do you have also obsolete **Views**, **Jobs**, **Template Keys**? Delete them as well.

For **Template Keys** the **Profile Relation** is shown in the setting mask.

Removing a Certificate

UMS also allows you to remove the certificate from devices. This may be necessary

- in order to prepare for moving a device from the test environment to the productive environment
- in order to prepare for replacing the server certificate.

To remove the certificate, proceed as follows:

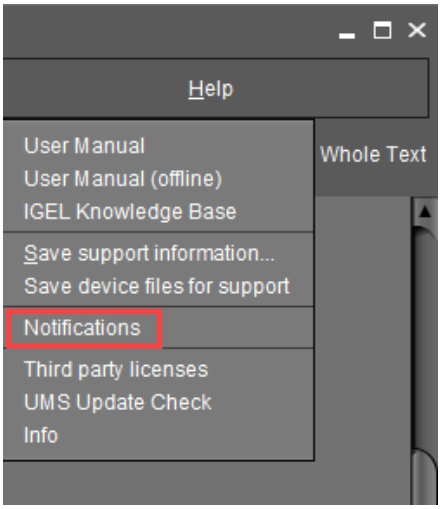
▶ Select **Remove UMS Certificate** under **Devices > Commands > Other device commands**.
Each *IGEL* UMS Server can now access the device configuration until one of the servers registers the client.

Notifications - Always Be Informed

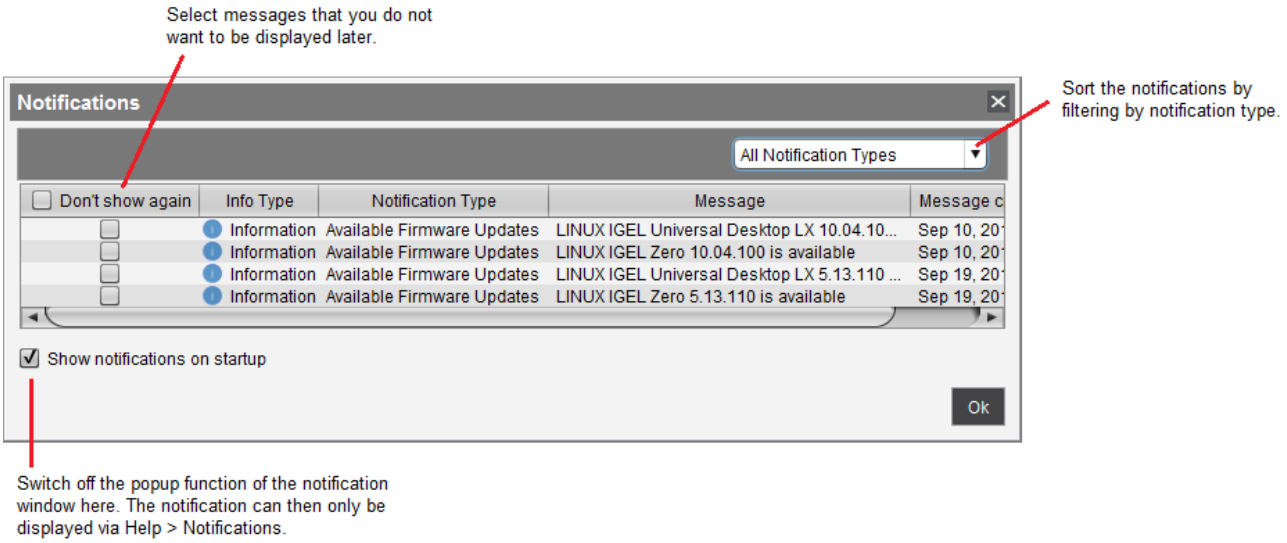
As of UMS 5.09.100, you can get notifications about newly available firmware updates, device licenses, etc. By default, notifications are enabled and pop up when you start the UMS Console. In this article, you will learn how to adapt this feature to your needs.

About Notifications

Basically, all users with read permission can see the notifications. The notifications are displayed after starting the UMS Console. When the dialog is closed, the notifications can still be viewed anytime under **Help > Notifications**.



The Notification Window



Enabling the Notification Function

1. Go to **UMS Administration > Misc Settings**.
2. Activate **Enable notifications**.

The notification feature is active. The notifications can be viewed under **Help > Notifications**.

Exporting Notification and Sending It by Email

The disk usage notifications can be exported and sent via email: **UMS Administration > Administrative Tasks > add > Action: "Send notification information via email"**.

- Configuring the Notifications Pop-Up (see page 179)
- Disk Usage (see page 180)
- Global Notifications (see page 181)
- Admin Tasks (see page 182)

Configuring the Notifications Pop-Up

To configure the notifications pop-up:

1. Go to **Misc > Settings > Notifications**.
2. Enable **Show notifications on startup** to display the notification window as a pop-up every time the UMS Console is started.
3. Select **Show custom** under **Show following notification for the current user or group**.
4. Specify which content should be displayed in the notification.
   Possible options:
   - **Device Licenses:** Informs about the expiration of device licences.
   - **Universal Management Licenses:** Informs about the expiration of UMS licences.
   - **Universal Firmware Updates:** Informs about the latest firmware updates.
   - **Disk Usage:** Informs about a critical value of free disc space. For more details, see Disk Usage (see page 180).
   - **Global Notifications**: Informs about important news like maintenance times and bugfixes. For more details, see Global Notifications (see page 181).
   - **Admin Tasks**: Automatically informs in a set of cases if no administrative task has been defined. For more details, see Admin Tasks (see page 182).
5. Confirm the settings with **Ok**.

Disk Usage

Menu path: **Misc > Settings > Notifications > Disk Usage**

This notification informs the user when there is not enough free drive space anymore.

> The notifications are generated on a daily base. Therefore it might take up to 24 hours until you get a notification after your available disk space has fallen below the configured value.

The individual critical drive space value can be set under **UMS Administration > Global Configuration > Misc Settings > Notifications**.

Types of disk usage notifications:

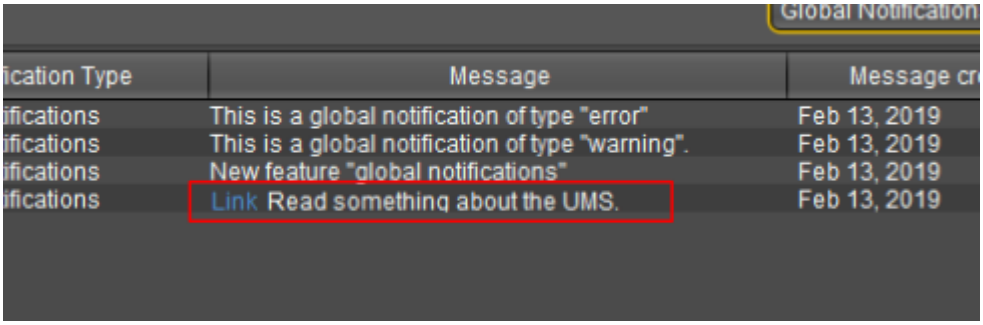
- Specific notification for each connected server: The server hostname and the available drive space will be shown in the notification message.
- Installation path and database path are on different file systems: Two notifications for each file system will be shown.

Global Notifications

Menu path: **Misc > Settings > Notifications** > **Global Notifications**

This notification type informs the user about important news, like maintenance times and bugfixes.

Global Notifications can include an additional web link that can provide more information. The web link is displayed as a blue link button next to the global notification.



- Click the link to open the web page in the standard browser.
- Move the mouse over the link to display the URL.

Admin Tasks

Menu path: **Misc > Settings > Notifications > Admin Tasks**

Admin Tasks: Informs automatically in the following cases if no administrative task has been set:

- enabled **Logging**;
- a new **Scheduled Job** has been set;
- the embedded database is active.

Exporting Notification and Sending It by Email

The disk usage notifications can be exported and sent via email: **UMS Administration > Global Configuration > Administrative tasks > Add > Action: Send notification information via email**.

> Each server executes an administrative task every 6 hours to check the available space on the drive and deliver the disk usage information to the notification system. Disk usage admin tasks older than 24 hours are considered expired. In order to display the notification, the server must have been running continuously for up to 6 hours within the last 24 hours.

Updating Timezone Information (Daylight Saving Time, DST)

Symptom

The device is showing an incorrect time of day for your location, although you have set the correct time zone.

Problem

The time zone or the regulation for Daylight Saving Time (DST) for your location has changed.

Solution

Update the time zone information files via IGEL Universal Management Suite (UMS). This is known to work for

- IGEL Linux version 10.01.100 or newer
- IGEL Linux version 5.04.100 or newer
- IGEL Linux version 4.14.100 or newer
- IGEL Linux ARM version 1.09.100 or newer.

Retrieving current time zone information files:

On Windows

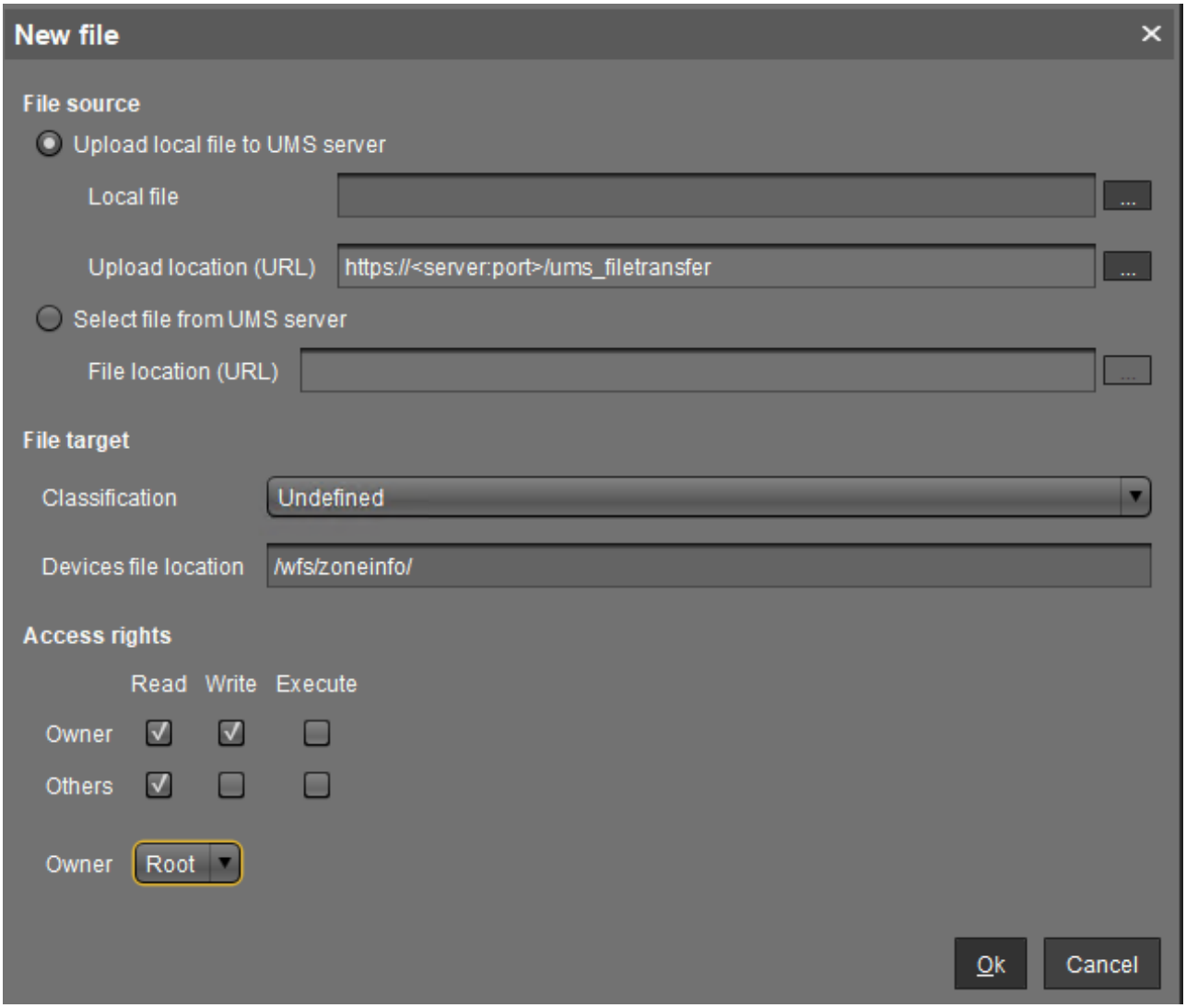
- Use your web browser to download the following package files:
  - http://packages.ubuntu.com/xenial-updates/all/tzdata/download for *IGEL Linux* version 10.x
  - http://packages.ubuntu.com/trusty-updates/all/tzdata/download (for *IGEL Linux* version 5.x)
  - http://packages.ubuntu.com/precise-updates/all/tzdata/download (for *IGEL Linux* version 4.x)
- Extract the package contents using the program 7-Zip (freely available from http://www.7-zip.org).
- Find the file for your location in the extracted directory in `usr/share/zoneinfo/` , e.g. `usr/share/zoneinfo/Africa/Casablanca` for Morocco.

On Linux

- Update your system time zone information with these commands: `sudo apt-get update` `sudo apt-get install tzdata`
- Find the file for your location in the system directory `/usr/share/zoneinfo/` , e.g. `/usr/share/zoneinfo/Africa/Casablanca` for Morocco.

Distributing the files from IGEL Universal Management Suite

- Select **System > New > New File** from the UMS Console menu bar or go to **Files** in the tree structure and select **New File** from the context menu.
- Select the time zone file for your location under **Local File**.
- Select **Undefined** under **Classification**.
- Specify `/wfs/zoneinfo/` as the **Devices file location**.
- Set the **Access rights** to Read and Write for the Owner, and to Read for Others.
- Select Root as the **Owner**.
- Click **OK** to confirm the settings.



On a device, you can verify the transfer and activation of the new time zone information files:

- In the **Local Terminal**, enter `grep 'timezone_config' /var/log/messages`

> On *IGEL Linux version 10.x*, use: `journalctl | grep 'timezone_config'`

- The output should look like the following:
  `Feb 27 11:28:13 (none) timezone_config: loading /wfs/zoneinfo/Casablanca to /usr/share/zoneinfo/Africa/Casablanca`
  `Feb 27 11:28:13 (none) timezone_config: loading /wfs/zoneinfo/Casablanca to /usr/share/zoneinfo/posix/Africa/Casablanca`
  `Feb 27 11:28:13 (none) timezone_config: configure timezone Africa/Casablanca`

E-Mail Settings for Gmail Accounts

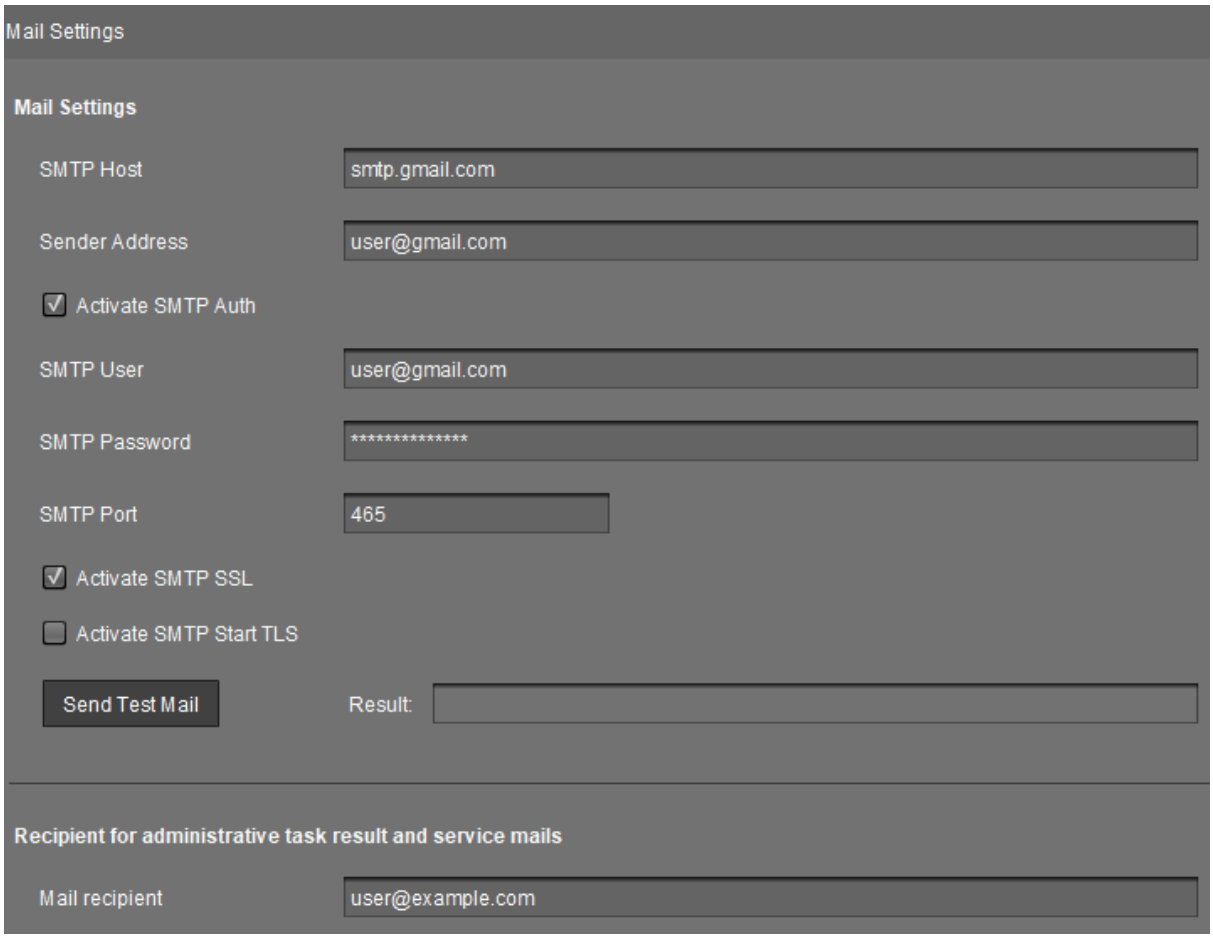
Purpose

You want to send views from the IGEL Universal Management Suite by email using a Gmail account.

Solution

> In order to allow the UMS to send emails via Gmail, you have to make the following setting in your Google account:
>
> - Log in to Google.
> - Go to **My Account > Sign-in & security > Connected apps & sites**.
> - Set **Allow less secure apps** to `ON`.

1. Go to **UMS Administration > Global Configuration > Mail Settings**.
2. Enter `smtp.gmail.com` as the **SMTP Host**.
3. Enter your Gmail address under **Sender Address**.
4. Enable **Activate SMTP Auth.**
5. Enter your Gmail address under **SMTP User**.
6. Enter your Gmail password under **SMTP Password**.
7. Enter `465` under **SMTP Port**.
8. Enable **Activate SMTP SSL**.
9. Under **Mail recipient**, enter the email address you want administrative emails from the UMS to be sent to.



10. Click **Send Test Mail** to test your settings.

Additional Information

https://support.google.com/a/answer/176600?hl=en

Searching With Regular Expressions in UMS

Universal Management Suite (UMS) can help you manage large thin client installations. Often you will want to search or filter for objects with certain properties, and UMS offers a wide selection. For advanced searches, however, you might need Regular Expressions, a powerful feature built into UMS.

You can use them in:

- Quick Search
- **Misc > Search**
- **Views > New View**
- **Edit > Edit Configuration > System > Registry > Search parameter ...**
- **UMS Administration > Global Configuration >Default Directory Rules**

UMS uses Java Regular Expressions. These are different from the globbing patterns that you may know from the DOS/Windows Command Prompt or the Linux commandline. For example, instead of using `*` to match any number of characters, in UMS you use:

```
.*
```

Here the `.` matches any character. The `*` acts as a quantifier, stating how often the preceding pattern may occur, in this case zero or more times.

So, if you want to find something that begins with IGEL, use:

```
IGEL.*
```

Something begining with IGEL and ending with 12:

```
IGEL.*12
```

If you want to find something ending with IGEL:

```
*.IGEL
```

Find out more about Java Regular Expressions in Oracle's documentation (see page 188).

Copy Sessions in Setup or UMS

Sometimes you want to create a session that differs from another only in a few details. *IGEL* Linux *version 5.10.100* or newer and UMS *version 5.02.100* or newer let you copy complete sessions. Once the session is copied, you can easily adapt the required settings.

Copying is available in the **Sessions** section of *IGEL* Setup (and occasionally in some other sections) as well as in the **Edit Configuration** function in UMS.

To copy a session, proceed as follows:

1. In the setup, open the menu path **Sessions > [Session Type] > [Session Type] Sessions**.
   Example: **Sessions > RDP > RDP Sessions**
   The existing sessions are shown.
2. Highlight the session that you want to copy.
3. Click  .
   A copy of the session will be created within the same folder.

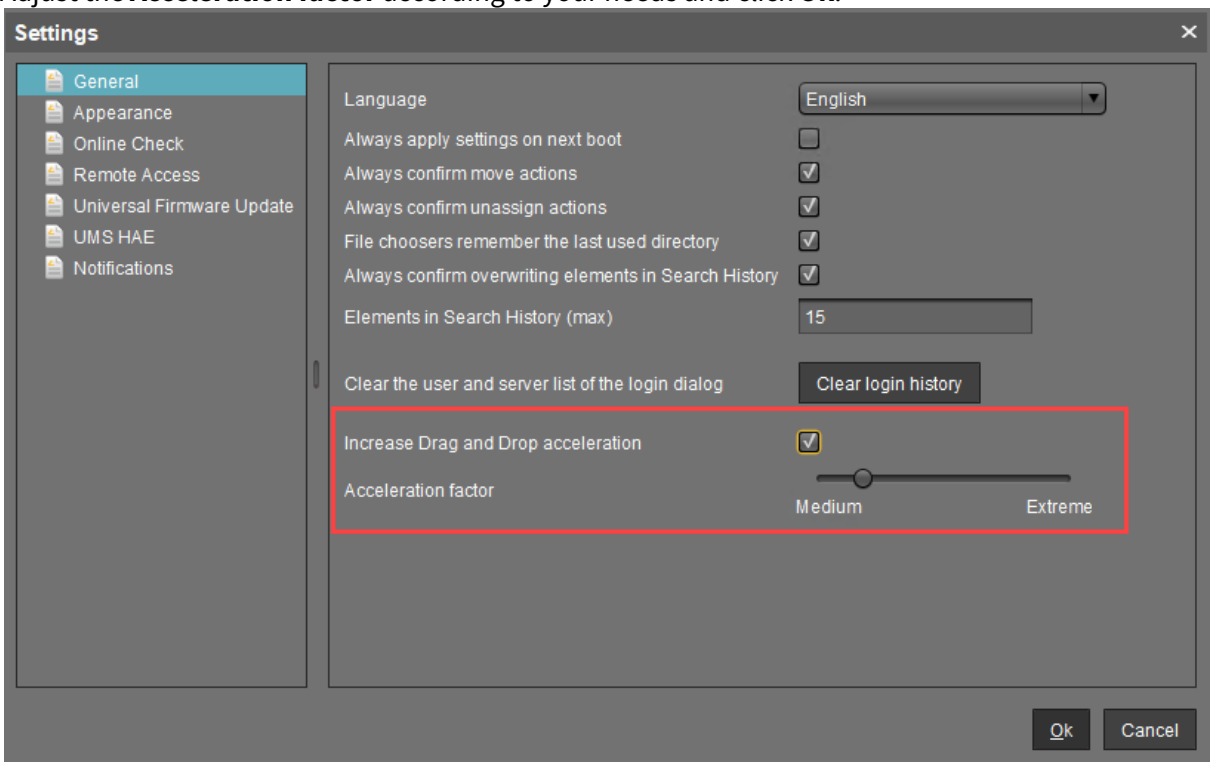
Drag & Drop Acceleration for Large Structure Trees

If you have a really large number of objects in your IGEL UMS (Universal Management Suite), it can be tedious to drag and drop an object to a new position if the new position is quite far away from the current position.

But with UMS version 5.03.100 or newer, you can increase your scrolling speed. As soon as the object you are moving touches the bottom edge of the structure tree window, the acceleration starts.

To enable drag and drop acceleration:

1. Open the UMS and go to **Misc > Settings > General**.
2. Activate **Increase Drag and Drop acceleration.**
3. Adjust the **Acceleration factor** according to your needs and click **Ok**.



Drag & drop acceleration is ready.

Which UMS Directories Should Be Scanned for Viruses, Which Can Be Excluded?

Question

Which UMS directories can be excluded from antivirus scanning, which directories should be scanned?

Environment

This article is valid for the following environment:

- UMS 5.08 or higher
- UMS is installed on Microsoft Windows server

Answer

Everything in `C:\<Program Files>\IGEL\RemoteManager\` can be excluded.

If your UMS also manages Windows devices, the downloadable files in `C:\<Program Files>\IGEL\RemoteManager\rmguiserver\webapps\ums_filetransfer\` should be scanned.

Licensing with Smartcard fails

Symptom

You can not create licenses from smartcard in IGEL UMS (**License Management**) although valid licenses are stored on the SIM / smartcard and the smartcard reader's driver is installed to your system.

- The smardcard reader shows a problem in the Windows Hardware Manager [**!**].

Problem

Another smartcard reader (eg. built-in cardreader) overrides the access.

Solution

Deactivate or deinstall all other smartcard readers in the Windows Hardware Manager.

UMS Reference Manual

What Is New in 6.02.100?

You will find the release notes for the IGEL Universal Management Suite 6.02.100 both as a text file in the same folder as the installation programs on our download server[7] and in the Knowledge Base article Notes for Release 6.02.100 (see page 775).

New View Criterion "Device License"

You can now use a view to collect unlicensed devices, or devices whose license is about to expire, or devices whose license has already expired. For a list of criteria, see Possible Search Criteria (see page 393); for instructions, see Finding Devices Which Need Licenses.

LDAP over SSL Support for Active Directory Configuration Added

You can now deploy the option "Use LDAPS connection" when configuring an AD connection, see Active Directory / LDAP (see page 499).

New Notification Types in UMS

Three new notification types have been added to the notification system (UMS menu bar **> Misc > Settings > Notifications**), see Disk Usage (see page 180), Global Notifications (see page 181), Admin Tasks. (see page 182) See also Configuring the Notifications Pop-Up (see page 179).

Profile Dialog Simplified

The option to define advanced settings by creating a new profile has been moved to the "Expert mode", thus making the creation of a new profile more user-friendly, see Creating Profiles. (see page 282)

7 https://www.igel.com/software-downloads/igel-universal-management-suite/

Overview

With the IGEL Universal Management Suite (UMS), you can remotely configure and control IGEL devices.

The UMS supports not only various operating systems but also databases and directory services such as Microsoft® Active Directory.

> Each IGEL device comes with a free version of the IGEL Universal Management Suite.

For an overview of devices supported by the IGEL UMS, see Devices Supported by IGEL Universal Management Suite (UMS) (see page 25).

Typical Areas of Use

- Setting up devices automatically;
- Configuring devices, software clients, tools and local protocols;
- Distributing updates and firmware images;
- Diagnostics and support.

- Attributes of the IGEL UMS (see page 196)
- IGEL UMS Components (see page 198)

Attributes of the IGEL UMS

Quick installation:

A wizard helps you during the installation procedure. You can connect external database systems as an alternative to the integrated database.

Straightforward management at the click of a mouse:

Most hardware and software settings can be changed with just a few clicks.

Standardized user interface:

The UMS user interface is similar to that for local device configuration. The additional remote management functions give the administrator complete control in the familiar, proven environment.

No scripting:

Although scripting is supported, you will only need it for managing the device configuration in the most exceptional circumstances.

Asset management:

Automatic capturing of all your hardware information, licensed features and installed hotfixes.

Commentary fields:

For various customer-specific information such as location, installation date and inventory number.

Support for numerous operating systems:

The UMS server can run on many common versions of Microsoft® Windows® Server and Linux, see Installation Requirements (see page 203).

Access independent of the operating system:

The UMS console runs on any device with the Java Runtime Environment. You can also use the UMS console with Java Web Start without a local installation, *see* Installation Requirements (see page 203).

Encrypted communication:

Certificate-based TLS/SSL-encrypted communication between remote management servers and clients to prevent unauthorized reconfiguration of the devices.

Failsafe update function:

If a device fails while the update is in progress, e. g. as a result of a power outage or loss of the network connection, it will still remain usable. The update process will then be completed when the device next boots.

Based on standard communication protocols:

There is no need to reconfigure routers and firewalls because the *UMS* uses the standard HTTP and FTP protocols.

Support for extensive environments:

The IGEL Universal Management Suite can be scaled to accommodate several thousand devices.

Group and profile-based administration:

The devices within a given organizational unit can be administered easily via profiles. If members of staff move to another department, the administrator can change the settings with a simple drag-and-drop procedure.

Trouble-free rollout:

IGEL devices can be automatically assigned to a group on the basis of either the relevant subnet or a list of MAC addresses provided by *IGEL*. They then automatically receive the configuration settings for the group.

Comprehensive support for all configuration parameters:

Most IGEL device settings, e. g. device or session configurations, can be changed via the *UMS* user interface.

Transferral of administrative rights:

Large organizations can authorize a number of system administrators for different control and authorization areas. These administrative accounts can be imported from an Active Directory.

Planning tasks:

Maintenance tasks can be scheduled to take place during the night so that day-to-day operations are not disrupted.

VNC shadowing:

Members of the IT support team have remote access to devicescreens, enabling them to rapidly identify problems and demonstrate solutions directly to users.

IGEL UMS Components

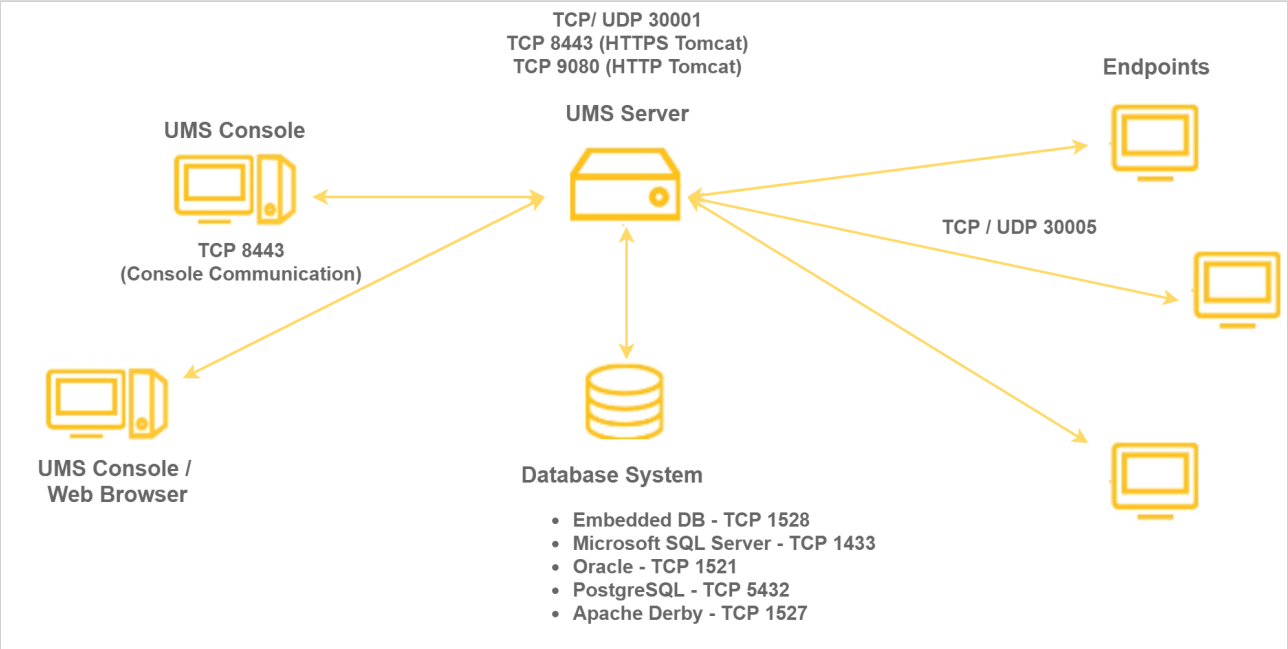
The IGEL Universal Management Suite program (referred to below as the UMS) comprises the following three components:

- UMS Server (see page 199)
- UMS Administrator (see page 200)
- UMS Console (see page 201)

UMS Server

The UMS Server is a server application which requires a database management system (RDBMS). Information regarding supported database management systems can be found under Installation Requirements (see page 203). The database can be installed on the server itself or on a remote host.

The UMS Server communicates internally with the database and externally with the registered devices and the UMS Console:



Typically, the UMS Console and UMS Server are installed on different computers. Data transmission between the UMS Server and devices as well as between the UMS Server and Console is encrypted.

All configurations for the managed devices are saved in the database. Changes to a configuration are made in the database and are transferred to the device if necessary. The device can retrieve the information from the database during the booting procedure or you can send the new configuration to the device manually. A scheduled configuration update is also possible.

UMS Administrator

The UMS Administrator is one of the UMS Server's administrative components.

The key parts of the UMS Administrator are as follows:

- Network configuration (ports, WebDAV resources)
- Database configuration (data sources, backups)

Further information regarding the UMS Administrator can be found under The IGEL UMS Administrator (see page 539).

UMS Console

The UMS Console is the user interface to the UMS Server. The devices and their configuration are administered via the GUI of the UMS Console.

The key tasks of the UMS Console are as follows:

- Displaying the devices' configuration parameters
- Setting up profiles and scheduled jobs
- Administering firmware updates

You will find further information regarding the UMS Console under UMS Console User Interface (see page 245).

UMS Installation and Update

This chapter describes the requirements for installing the UMS. The standard installation with the embedded database is explained with an example for Windows (see page 212) and for Linux (see page 206). You are also told what you need to bear in mind when performing an update and where you can connect external database systems.

- Installation Requirements (see page 203)
- Installing a UMS Server (see page 205)
- Updating UMS (see page 215)
- Connecting External Database Systems (see page 220)

TechChannel

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=3YJnFiE7y5w

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=p52CxtB_0ok

Installation Requirements

You can run the IGEL UMS with Windows and Linux 64-bit systems (x86_64).

> For the supported operating systems, see the "Supported Environment" section of the release notes (see page 649).

Your hardware and software must meet the following minimum requirements:

UMS Complete Installation

- At least 4 GB of RAM (6 GB recommended)
- At least 1 GB of free disk space (plus database system)

Individual Console Installation

- At least 1.5 GB of RAM (2 GB recommended)
- At least 250 MB of free disk space

> Under Linux, an X11 system is required. It is required by the UMS Administrator application which can only be launched on the same machine as the UMS Server.

> As an alternative to a local console installation, you can execute the UMS Console as a Java Web Start application too. The console does not need to be installed here. If necessary, it can be downloaded from the UMS Server and executed. Further information can be found under UMS Console via Java Web Start (see page 169).

> Do not install the UMS Server on a domain controller system!

> Manually modifying the Java runtime environment on the UMS Server is not recommended.

> Running additional Apache Tomcat web servers together with the UMS Server is likewise not recommended.

Database Systems (DBMS)

> For details on the supported database systems, see the "Supported Environment" section of the release notes (see page 649). Details of the requirements when installing and operating the database can be found in the documentation for the particular DBMS.

High Availability

For installation requirements for High Availability (see page 560), see Installation Requirements (see page 565).

The embedded database cannot be used for a High Availability network. You can use the embedded database only for a dedicated test installation with only a single server for the UMS Server and Load Balancer.

All UMS Servers and UMS Load Balancers must reside on the same VLAN. Network traffic must be allowed over UDP broadcast port 6155, and TCP traffic and UDP broadcast traffic over port 61616. For more information on UMS ports, see UMS Communication Ports (see page 26).
Note: IGEL UMS Server HA is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks.

Installing a UMS Server

This example describes the complete procedure for installing a UMS Server with an embedded database. If your required installation differs, you can select individual components, e.g. for an individual console installation.

- Installation under Linux (see page 206)
- Installation under Windows (see page 212)

If you want to install UMS High Availability (HA) Extension (see page 560), see HA Installation (see page 564).

If you already have a standard UMS installation and want to switch to the UMS HA, see Switching from a Standard UMS Installation to an HA Installation (see page 581).

Installation under Linux

For the supported operating systems, see the "Supported Environment" section of the release notes (see page 649).

The procedure for installing the IGEL Universal Management Suite under Linux is as follows:

1. Download the current version of the IGEL Universal Management Suite from the IGEL Download Server[8].
2. Open a terminal emulator such as xterm and switch to the directory in which the installation file `setup-igel-ums-linux-[Version].bin` is located.
3. Check whether the file is executable. If not, it can be made executable using the following command:
   `chmod u+x setup*.bin`

   You will need `root/sudo` rights to carry out the installation.
4. Execute the installation file as `root` or with `sudo`:
   `sudo ./setup-igel-ums-linux-[Version].bin`
   This unzips the files into the `/tmp` directory, starts the Java Virtual Machine contained and removes the temporary files after the installation procedure.
5. Start the installation procedure by pressing **Enter**.

   You can cancel the installation at any time by pressing the [Esc] key twice.
6. Read and confirm the license agreement.
7. Decide whether the installer will automatically install the required dependencies:
   - **Now**: Installs the necessary dependencies automatically.
   - **Manual**: Skips the installation. You will have to install the required dependencies manually if this has not already been done.
   - **Cancel installer**: Aborts the installation procedure.
8. Under **Destination directory**, select the directory in which the UMS is to be installed. (Default: `/opt/IGEL/RemoteManager`)
9. If you update an existing UMS installation: Under **Database backup**, select a file for the backup of the embedded database as well as licenses and certificates. If you have already created a backup, you can also select **No (continue)** in order to skip this step. See also Updating under Linux (see page 217).
10. Under **Installation type**, select the scope of installation:
    - Complete: UMS Server and UMS Console
    - Client only: UMS Console only
    - HA net: High Availability configuration

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

> Freely selectable directories for file transfers are no longer supported. After completing the installation, move the existing files to the `ums_filetransfer/` directory and use the **Files** and **Firmware Update** points in the UMS Console to make them available online again. You may also need to amend download addresses in the device configurations and profiles.

11. Under **Data directory**, select the directory in which Universal Firmware Updates and files are to be saved. (Default: `/opt/IGEL/RemoteManager`)
12. Select the **run levels** in which the UMS Server is to run.
13. Under **Database**, select the desired database system.
    - Internal: The internal database (embedded database)
    - Other: An external database server

    > The embedded database is suitable for most purposes. It is included in the standard installation. If you have to manage a large network of devices and a dedicated database system is already in use in your company, it is advisable to use this system. The same applies if the High Availability solution is used.
14. Enter a **user name** and **password** for database access.
15. Specify whether you would like to create **shortcuts** for the UMS Console and UMS Administrator in the menu.
16. Check the summary of the installation settings and start the procedure by selecting **Start installation**.
    If you have selected the standard installation, the UMS Server along with the internal database will be installed and started.
17. Once the installation procedure is complete, open the UMS Console via the menu or with the command `/opt/IGEL/RemoteManager/RemoteManager.sh`
18. Connect the UMS Console to the UMS Server by entering the login data for the database that you specified during installation.

- Installing UMS on Red Hat Enterprise Linux (RHEL) 7.3 (see page 208)
- Installing UMS on Oracle Linux Server (see page 210)

Installing UMS on Red Hat Enterprise Linux (RHEL) 7.3

You want to install the UMS on the 64-bit version of Red Hat Enterprise Linux (RHEL) 7.3.

From UMS 5.09

From UMS Version 5.09, the installation of 32-bit libraries is no longer required. The necessary dependencies are automatically installed if the corresponding option has been chosen during the UMS installation procedure.

1. Adjust the RHEL Server firewall settings to allow the network ports used by the UMS, see UMS Communication Ports (see page 26).
2. Complete the installation as described in Installation under Linux (see page 206).

From UMS 5.07.100

From UMS Version 5.07.100, the required 32-bit libraries can automatically be installed by the UMS installer if the corresponding option is chosen during the UMS installation procedure.

1. Adjust the RHEL Server firewall settings to allow the network ports used by the UMS, see UMS Communication Ports (see page 26).
2. Complete the installation as described in Installation under Linux (see page 206).

Before UMS 5.07.100

To install the UMS on the 64-bit version of RHEL 7.3, proceed as follows:

1. As `root`, update your 64-bit packages to the latest version:
   ```
   yum update
   ```
2. Install libraries for 32-bit support:
   ```
   yum install \
   glibc.i686 \
   libzip.i686 \
   ncurses-libs.i686 \
   bzip2-libs.i686 \
   libXtst.i686 \
   libXinerama.i686 \
   libXi.i686 \
   libXext.i686 \
   libXrender.i686 \
   libgcc.i686
   ```
3. Reboot.
4. Adjust the RHEL Server firewall settings to allow the network ports used by the UMS, see UMS Communication Ports (see page 26).

5. Complete the installation as described in Installation under Linux (see page 206).

> There is a bug/glitch on Red Hat Enterprise Linux (RHEL) 7.3 with GNOME desktop version 3.14, when running UMS Console. The main window of the UMS Console is displayed as an empty grey rectangle, because the GUI is rendered incorrectly. As a workaround, the window can be resized by dragging the windows edges or by double-clicking near the top edge (maximizing) where the title bar would be. This triggers a repaint, and the UMS Console window is then displayed correctly. Alternatively, use the KDE desktop environment on RHEL 7.3.

Installing UMS on Oracle Linux Server

Oracle

For the proper operation of the UMS with Oracle databases, particularly for the upgrade process, the number of `open_cursors` for the database must be adjusted. `open_cursors` is a system setting.

1. To get the actual value, log in to the database as `SYSDBA` and execute:
   `SQL> select name, value from v$parameter where name = 'open_cursors';`
2. The recommended value for `open_cursors` is "3000". To set the value, issue the following command as `SYSDBA` :
   `SQL> alter system set open_cursors = 3000 scope=both;`
3. The same command should be added to the `SPFILE` of the Oracle system in order for the changes to persist on the next reboot.

You want to install the UMS on the 64-bit version of Oracle Linux Server.

From UMS 5.09

From UMS Version 5.09, the installation of 32-bit libraries is no longer required. The necessary dependencies are automatically installed if the corresponding option has been chosen during the UMS installation procedure. See Installation under Linux (see page 206).

1. Adjust the Oracle Linux Server firewall settings to allow the network ports used by the UMS, see UMS Communication Ports (see page 26).
2. Complete the installation as described in Installation under Linux (see page 206).

From UMS 5.07.100

From UMS Version 5.07.100, the required 32-bit libraries can automatically be installed by the UMS installer if the corresponding option is chosen during the UMS installation procedure.

1. Adjust the Oracle Linux Server firewall settings to allow the network ports used by the UMS, see UMS Communication Ports (see page 26).
2. Complete the installation as described in Installation under Linux (see page 206).

Before UMS 5.07.100

To install the UMS on the 64-bit version of Oracle Linux Server, proceed as follows:

1. As `root` , update your 64-bit packages to the latest version:
   `yum update`
2. Install libraries for 32-bit support:
   `yum install \`

```
glibc.i686 \
libzip.i686 \
ncurses-libs.i686 \
bzip2-libs.i686 \
libXtst.i686 \
libXinerama.i686 \
libXi.i686 \
libXext.i686 \
libXrender.i686 \
libgcc.i686
```

3. Reboot.
4. Adjust the Oracle Linux Server firewall settings to allow the network ports used by the UMS, see UMS Communication Ports (see page 26).
5. Complete the installation as described in Installation under Linux (see page 206).

Installation under Windows

Standard Installation

To install the IGEL Universal Management Suite under Windows, proceed as follows:

1. Download the current version of the IGEL Universal Management Suite from the IGEL Download Server[9].
2. Launch the installer.

   > You will need administrator rights in order to install the UMS.

3. Read and confirm the **License Agreement**.
4. Read the **Information** regarding the installation process and click **Next**.
5. Select the folder for the installation under **Select Destination Location**. (Default: `C:\Program Files\IGEL\RemoteManager`)
6. If you already have a UMS installation, select the file name for the **backup** of your embedded database. If you do not choose a file name and click on **Next**, no backup will be created. See also Updating under Windows (see page 219).
7. Choose the components to be installed under **Select Components.**
   - **Standard UMS**
     - **with UMS Console**
     - **with Embedded Database**
   - **Only UMS Console**
   - **UMS High Availability Network**
     - **UMS Server**
     - **UMS Load Balancer**

     > The embedded database is suitable for most purposes. If not disabled, the embedded database will automatically be installed if you select **Standard UMS**. The use of an external database system is recommended in the following cases:
     > - You manage a large network of devices.
     > - A dedicated database system is already in use in your company.
     > - You integrate the High Availability solution.

8. Select the **UMS data directory**. (Default: `\RemoteManager`)
9. Under **User Credentials for DB-connect**, enter a user name and password for the database connection.
10. Choose a folder name under **Select Start Menu Folder**.
11. Read the summary and start the installation process.
    The installer will install the UMS, create entries in the Windows software directory and in the start menu and will place a shortcut for the UMS Console on the desktop.
12. Close the program after completing the installation by clicking on **Finish**.
    If you have chosen the standard installation, the UMS Server will run with the embedded database.

9 https://www.igel.com/software-downloads/workspace-edition/

13. Start the UMS Console.
14. Connect the UMS Console to the UMS Server using the access data for the database that you entered during the installation.
    You will find information regarding the use of the UMS with external databases under Connecting External Database Systems (see page 220).

Silent Installation of the UMS Console

You can carry out the installation silently by first creating an `.inf` file and then launching the installation using a command line.

> Silent installation is only possible for the UMS Console. It is not possible for the UMS Administrator and the UMS Server.

For further information, see Unattended/Silent Installation of UMS Console (see page 214).

Unattended/Silent Installation of UMS Console

Issue

After a UMS Server update, an update of the UMS Console on client machines is needed.

Solution

Perform the following steps for an unattended/silent installation of the UMS Console:

1. Create a config file:
   In `cmd` or `powershell`:
   `C:\[download directory]\setup-igel-ums-windows_x.y.z.exe /saveinf="[config-file]"`
2. Use the wizard displayed to complete the installation while recording it to the config file.
3. Install:
   `C:\[download-directory]\setup-igel-ums-windows_x.y.z.exe /loadinf="[config-file]" /silent`
   An installer window prompting the user may appear, but the installation will complete in the background, regardless.

This applies only to the UMS installer for Windows.

Silent installation is only possible for the UMS Console. It is not possible for the UMS Administrator and the UMS Server.

Updating UMS

Here you will find how to update a UMS installation under Windows or Linux.
Update instructions for the UMS High Availability (HA) installation can be found under Updating the Installation of an HA Network (see page 576).
If you want to switch to the UMS HA from the standard UMS installation, see Switching from a Standard UMS Installation to an HA Installation (see page 581).

- Updating under Linux (see page 217)
- Updating under Windows (see page 219)

⚠ Before the installation, check that your hardware and software fulfill the installation requirements (see page 203). See also Devices Supported by IGEL Universal Management Suite (see page 25).

⚠ Create a backup of the database before updating a previously installed version of the UMS. Otherwise, you risk losing all database content. See Backups (see page 545) and Creating a Backup (see page 546).

✔ We recommend that you install the new version of the UMS on a test system before installing it on the productive system. Once you have checked the functions of the new version on the test system, you can install the new version on the productive system. This also applies to hotfixes, patches etc. for the server system and database.

⚠ Installing a version of the UMS which is older than the one currently used is only possible if you have a backup of the database with the corresponding older schema. You can only switch from an older database schema to a newer one, not the other way around. You should therefore create a backup of your existing system before you start the update.
Since the version of the database schema always corresponds to the current major.minor version of the UMS (i.e. 6.10 for all 6.10.x releases, 6.08 for all 6.08.x. releases), the downgrades are only possible within a major.minor version. Example: you can downgrade from 6.10.140 to 6.10.120, but not from 6.10.140 to 6.09.120.

⚠ If the version of the UMS Console is older than the version of the UMS Server, you will not be able to establish a connection to the UMS Server (`Unable to load tree` error message). In this case, you will need to update the installation of the UMS Console.

✔ If you use an older version of the IGEL Remote Manager with *SAP DB*, we recommend that you switch to the embedded database before updating the UMS. For a more detailed description of this switch, please contact IGEL Support[10].

10 https://www.igel.com/submit-a-ticket/

From UMS 5.01.100, you can only use the directory `ums_filetransfer` or subdirectories created in it for WebDAV downloads. The installer offers you the option of moving existing directories to this new default folder.

During a UMS upgrade, e.g. from 6.01 to 6.02, the database schema is changed by the installer. With large production databases, this process can last up to 2 hours. Do not abort the installation during this time.

Updating under Linux

To perform an update under Linux, proceed as follows:

> Create a backup of the database (see page 545) before updating a previously installed version of the UMS. Otherwise, you risk losing all database content.

> **Oracle**
>
> For the proper operation of the UMS with Oracle databases, particularly for the upgrade process, the number of `open_cursors` for the database must be adjusted. `open_cursors` is a system setting.
>
> 1. To get the actual value, log in to the database as `SYSDBA` and execute:
>
>    ```
>    SQL> select name, value from v$parameter where name =
>    'open_cursors';
>    ```
> 2. The recommended value for `open_cursors` is "3000". To set the value, issue the following command as `SYSDBA` :
>
>    ```
>    SQL> alter system set open_cursors = 3000 scope=both;
>    ```
> 3. The same command should be added to the `SPFILE` of the Oracle system in order for the changes to persist on the next reboot.

1. Download the current version of the IGEL Universal Management Suite from the IGEL Download Server[11].
2. Log in as `root`.
3. Open a terminal emulator such as xterm and switch to the directory in which the installation file `setup-igel-ums-linux-[Version].bin` is located.
4. Check whether the installation file is executable. If not, it can be made executable with the following command:
   ```
   chmod u+x setup*.bin
   ```
5. Execute the installation file.
   The installer unzips the files into the `/tmp` directory, starts the included Java Virtual Machine and removes the temporary files once the installation has been completed.

   > You can cancel the installation at any time by pressing the [Esc] key twice.
6. Read and confirm the license agreement.
7. Read the explanation of the installation process.
8. Under **Destination directory**, select the directory in which the UMS is to be installed. (Default: `/opt/IGEL/RemoteManager`)

11 https://www.igel.com/software-downloads/workspace-edition/

9. Under **Database backup**, select a file for the backup of the existing embedded database. If you have already created a backup, you can select **No (continue)** in order to skip this step.
10. Under **Installation type**, select the scope of installation:
    - Complete: UMS Server and UMS Console
    - Client only: UMS Console only
    - HA net: High Availability configuration
11. Select the **Runlevels** in which the UMS server is to run.
12. Specify whether you would like to create **shortcuts** for the UMS Console and UMS Administrator in the menu.
13. Check the summary of the installation settings and start the procedure by selecting **Start installation**.

    > During a UMS upgrade, e.g. from 6.01 to 6.02, the database schema is changed by the installer. With large production databases, this process can last up to 2 hours. Do not abort the installation during this time.

14. Once the installation procedure is complete, open the UMS Console via the menu or with the command `/opt/IGEL/RemoteManager/RemoteManager.sh`
15. Connect the UMS Console to the UMS Server with the help of the existing access data.

Updating under Windows

> Create a backup of the database (see page 545) before updating a previously installed version of the UMS. Otherwise, you risk losing all database content.

To perform an update under Windows, proceed as follows:

1. Download the current version of the IGEL Universal Management Suite from the IGEL Download Server[12].
2. Close any other applications and launch the installer.

   > You will need administrator rights in order to install the UMS.

3. Read and confirm the **License Agreement**.
4. Read the **Information** regarding the installation process and click **Next**.
5. Under **Database backup**, select a file for the backup of the existing embedded database. If you do not choose a file name and click on **Next**, no backup will be created.
6. Choose the components to be installed under **Select Components.**
   - **Standard UMS**
     - **with UMS Console**
     - **with Embedded Database**
   - **Only UMS Console**
   - **UMS High Availability Network**
     - **UMS Server**
     - **UMS Load Balancer**
7. Choose a folder name under **Select Start Menu Folder**.
8. Read the summary and start the installation process.
   The installer will install a new version of the UMS, create entries in the Windows software directory and in the start menu and will place a shortcut for the UMS Console on the desktop.

   > During a UMS upgrade, e.g. from 6.01 to 6.02, the database schema is changed by the installer. With large production databases, this process can last up to 2 hours. Do not abort the installation during this time.

9. Close the program once the installation is complete by clicking on **Finish**.
10. Start the UMS Console.
11. Connect the UMS Console to the UMS Server with the help of the existing access data.

12 https://www.igel.com/software-downloads/workspace-edition/

Connecting External Database Systems

The use of an external database system is recommended in the following cases:

- You manage a large network of devices.
- A dedicated database system is already in use in your company.
- You integrate the High Availability (see page 560) solution.

In other cases, the use of the embedded database is suitable. It is included in the standard UMS installation, see Installation under Windows (see page 212) or Installation under Linux (see page 206).

For details on the supported database systems, see the "Supported Environment" section of the release notes (see page 649). Details of the requirements when installing and operating the database can be found in the documentation for the particular DBMS.

- To configure the database, use the relevant DBMS management program.
- To configure the data source and to connect the UMS to the database, use the UMS Administrator (see page 539) > Datasource (see page 554).

Be aware not to use special characters in your schema name or database user name!

All UMS Servers must work with the same database.

For large High Availability environments, cluster databases are recommended.

For the backup procedure for UMS installations with the external database, see Creating a Backup (see page 546).

See also Migrating a UMS Database From Embedded DB to Microsoft SQL Server (see page 94).

Oracle

To integrate Oracle, proceed as follows:

1. Set up a new database user with `Resource` role in the Oracle Database Administration.

> A number of Oracle versions set up the `Resource` role without `Create View` authorization. Please ensure that this authorization is set for the role.

> **Oracle**
>
> For the proper operation of the UMS with Oracle databases, particularly for the upgrade process, the number of `open_cursors` for the database must be adjusted. `open_cursors` is a system setting.
>
> 1. To get the actual value, log in to the database as `SYSDBA` and execute:
>
>    ```
>    SQL> select name, value from v$parameter where name =
>    'open_cursors';
>    ```
>
> 2. The recommended value for `open_cursors` is "3000". To set the value, issue the following command as `SYSDBA` :
>
>    ```
>    SQL> alter system set open_cursors = 3000 scope=both;
>    ```
>
> 3. The same command should be added to the `SPFILE` of the Oracle system in order for the changes to persist on the next reboot.

2. In the UMS Administrator (see page 539), set up a new **Oracle** type data source.

Oracle RAC

1. Set up a new database user with `Resource` role in the Oracle Database Administration.

> A number of Oracle versions set up the `Resource` role without `Create View` authorization. Please ensure that this authorization is set for the role.

> **Oracle**
>
> For the proper operation of the UMS with Oracle databases, particularly for the upgrade process, the number of `open_cursors` for the database must be adjusted. `open_cursors` is a system setting.
>
> 1. To get the actual value, log in to the database as `SYSDBA` and execute:
>
>    ```
>    SQL> select name, value from v$parameter where name =
>    'open_cursors';
>    ```
>
> 2. The recommended value for `open_cursors` is "3000". To set the value, issue the following command as `SYSDBA` :
>
>    ```
>    SQL> alter system set open_cursors = 3000 scope=both;
>    ```
>
> 3. The same command should be added to the `SPFILE` of the Oracle system in order for the changes to persist on the next reboot.

2. Use the UMS Administrator (see page 539) to set up a new **Oracle RAC** type data source for each server.

Microsoft SQL Server

To connect the Microsoft SQL Server, proceed as follows:

1. Open the SQL Console of the SQL Server by selecting "New Query" in SQL Server Management Studio.
2. Use the following script as a template, customize it (password), and then execute it.

   > To avoid problems when enabling the data source, ensure that `LOGIN`, `USER`, and `SCHEMA` have the same name.

   ```
   CREATE DATABASE rmdb
   GO
   USE rmdb
   GO
   CREATE LOGIN igelums with PASSWORD = 'setyourpasswordhere',
   DEFAULT_DATABASE=rmdb
   GO
   CREATE USER igelums with DEFAULT_SCHEMA = igelums
   GO
   CREATE SCHEMA igelums AUTHORIZATION igelums GRANT CONTROL to
   igelums
   GO
   ```

3. In the UMS Administrator (see page 539), set up a new **SQL Server** type data source.
4. Ensure that the **port** of the SQL Server in the data source is configured correctly. (Default: 1433)

> The Microsoft SQL Server should allow Windows and SQL authentication.

> If you deploy MS SQL Server Always On Availability Groups, use **SQL Server** as a **DB type** and specify under **Host** the domain name of the Always On Availability Group listener.

Microsoft SQL Server Cluster

1. Open the SQL console of the SQL server by selecting "New Query" in SQL Server Management Studio.
2. Use the following script as a template, customize it (password) and execute it.

   > To avoid problems when activating the data source, ensure that `LOGIN`, `USER`, and `SCHEMA` have the same name.

   ```
   CREATE DATABASE rmdb
   GO
   USE rmdb
   GO
   CREATE LOGIN igelums with PASSWORD = 'setyourpasswordhere',
   DEFAULT_DATABASE=rmdb
   GO
   CREATE USER igelums with DEFAULT_SCHEMA = igelums
   GO
   CREATE SCHEMA igelums AUTHORIZATION igelums GRANT CONTROL to
   igelums
   GO
   ```

3. Use the UMS Administrator (see page 539) to set up a new **SQL Server Cluster** type data source for each server.

   > The Microsoft SQL Server Cluster should allow Windows and SQL authentication.

PostgreSQL

> For details on the supported database systems, see the "Supported Environment" section of the release notes (see page 649). Details of the requirements when installing and operating the database can be found in the documentation for the particular DBMS.

When installing a new instance of the PostgreSQL database, set the following parameters:

1. Install the database cluster with `UTF-8` **coding.**
2. Accept the conditions for all **addresses**, not just `localhost.`
3. Activate **Procedural Language** `PL/pgsql` in the default database.

For further information regarding installation of the PostgreSQL database, see http://www.postgresql.org[13].

Once installation is complete, carry out the following configuration procedure:

1. Change the server parameters: The parameter `listen_addresses` in the file `postgresql.conf` must contain the host name of the IGEL UMS Server or `'*'` in order to allow connections to each host.
2. Set up a `host` parameter in the file `pg_hba.conf` in order to give the UMS Server the authorization to log in using the user data defined there.

   > If the IGEL UMS Server is installed on the same machine as the PostgreSQL Server, no changes to these files are needed.
3. Launch the administration tool pgAdmin.
4. Create a new login role with the name `rmlogin.`
5. Create a new database with
   name = `rmdb`
   owner = `rmlogin`
   encoding = `UTF-8`
6. Set up a new schema within the rmdb database with
   name = `rmlogin`
7. Check whether the language plpgsql is available in the rmdb database.
   If not, set it up.
8. In the UMS Administrator (see page 539), create a new data source with the following parameters:
   DB type: `PostgreSQL`
   Host: Name of the PostgreSQL Server
   Port: Port of the PostgreSQL Server. (Default: 5432)

13 http://www.postgresql.org/

User: `rmlogin`
Database / SID: `rmdb`

Apache Derby

> For details on the supported database systems, see the "Supported Environment" section of the release notes (see page 649). Details of the requirements when installing and operating the database can be found in the documentation for the particular DBMS.

As with other external databases, we recommend that you create a new database instance for use by the IGEL UMS.

Perform the following steps to create a new database instance and define the instance as a data source in the **UMS Administrator**:

1. For security purposes, enable **User Authentication** in the Derby DB.
2. Launch the *ij Utility* (in `[derby-installation-dir]/bin`).
3. To create the *rmdb* instance, execute the following command:
   ```
   connect 'jdbc:derby://localhost:1527/
   rmdb;user=dbm;password=dbmpw;create=true';
   ```
4. Create the schema `rmlogin` using the following command:
   ```
   create schema rmlogin;
   ```
5. Define the UMS database user `rmlogin` with the password `rmpassword`:
   ```
   CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.user.rmlogin',
   'rmpassword');
   ```
6. Exit *ij* and launch the *Derby Network Server*.
7. In the UMS Administrator (see page 539), create a new data source with the following parameters:
   DB type: `Derby`
   Host: Name of the Derby Server
   Port: Port of the Derby Server. (Default: 1527)
   User: `rmlogin`
   Database / SID: `rmdb`

For further information regarding installation of the Derby database, see http://db.apache.org/derby.

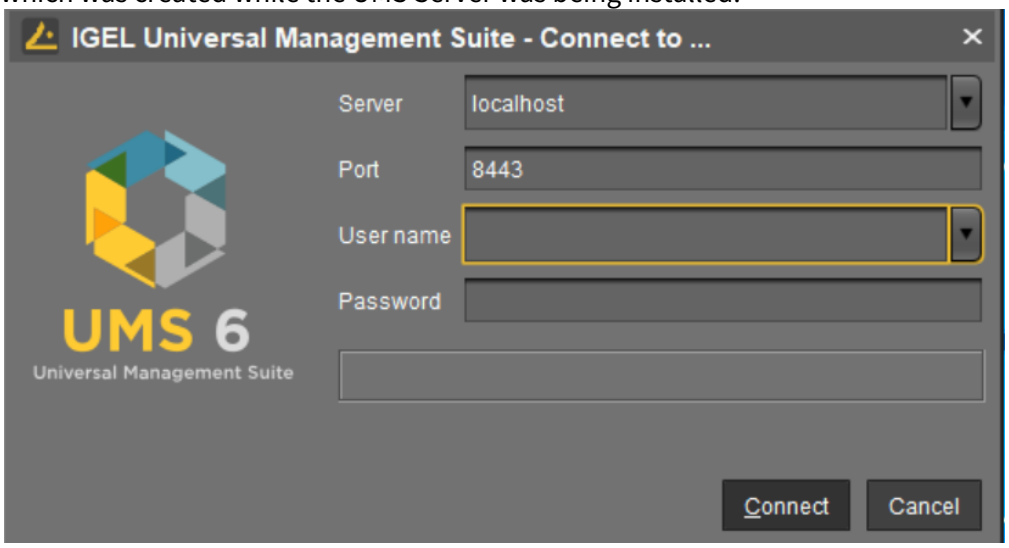
Connecting the UMS Console to the IGEL UMS Server

The following article describes the procedure for connecting the IGEL Universal Management Suite (UMS) Console to the UMS Server.

To establish a connection to the UMS Server, proceed as follows:

1. Start the UMS Console.

2. Enter the access data:
   - **Server**: Host name or IP address of the UMS Server. If you are logging in to the local UMS Console of the server, enter `localhost` or leave the field empty.
   - **Port**: Port on which the GUI server of the UMS receives UMS Console queries (Default: 8443). You can change the port using the UMS Administrator, see Settings (see page 540).
   - **User name**: User name for the connection between the UMS Console and database. When setting up the UMS for the first time, this is the user name of the database user account which was created while the UMS Server was being installed. If you belong to a domain configured in the UMS, enter `@`.
   - **Password**: Password for the connection between the UMS Console and database. When setting up the UMS for the first time, this is the password of the database user account which was created while the UMS Server was being installed.



3. Click on **Connect**.

The data entered under **Server**, **Port**, and **User name** will be saved for subsequent connection procedures. The next time you establish a connection, you will only need to enter the password. The server and user information last used is also stored. You can delete stored logon data under **Misc** > **Settings** > **General** > **Clear login history**.

Registering IGEL OS Devices on the UMS Server

The following article provides a short overview of possible methods for registering endpoint devices on the IGEL Universal Management Suite (UMS) Server. Depending on the number of devices to be registered, physical availability of devices in the network, etc., you can select the method that best suits your needs.

Device Registration Methods

> If you deploy IGEL Cloud Gateway (ICG), it is not necessary to register the device in the UMS since this process is performed when you set up the ICG connection on the device in the IGEL Setup Assistant (see Setup Assistant for IGEL OS) or the ICG Agent Setup (see Using ICG Agent Setup).

You can register devices on the UMS Server in the following ways:

- Scanning the network for devices and registering the found devices (see page 231)
  In this case, the devices must be physically available in the network and switched on. This method is usually used if not so many devices are to be registered; for the initial mass rollout, the automatic registration of devices is preferred.

- Automatic registration (see page 242)
  If you enable automatic registration and configure the DHCP tag and/or the DNS alias `igelrmserver` with the IP or FQDN of the UMS Server, all devices on the server's network will be automatically registered at startup.

  > IGEL recommends automatic registration when registering new devices for the first time during the rollout.
  > Disable automatic registration as soon as all devices have been registered, so that no unknown devices can obtain sensitive settings.

- Importing devices (see page 236)
  Here, you import the devices' data from a CSV file, so this method can only be used if you already know which devices exactly are to be registered. This approach allows you to make devices known to the UMS before the devices are physically available in the network. With this method, you can also specify editable device attributes such as site, department, or cost center.

- Creating a device entry manually (see page 244)
  In this case, you create a database entry for a device manually. This method is not appropriate for the initial setup of the UMS since the firmware for the devices must already be in the database. It is rather suitable for registering only a small number of devices.

- Using the UMS Registration function on the device
  In this case, you start the **UMS Registration** function directly on the device and manually enter the data of the required UMS Server.

Video

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube-nocookie.com/embed/1XMWDpv2wDI?autoplay=1

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube-nocookie.com/embed/_evv-Vlixwg?autoplay=1

Scanning the Network for Devices and Registering Devices on the IGEL UMS

In the following article, you will learn how to register devices on the IGEL Universal Management Suite (UMS) using the **Scan for devices** function.

For an overview of device registration methods, see Registering IGEL OS Devices on the UMS Server (see page 229).

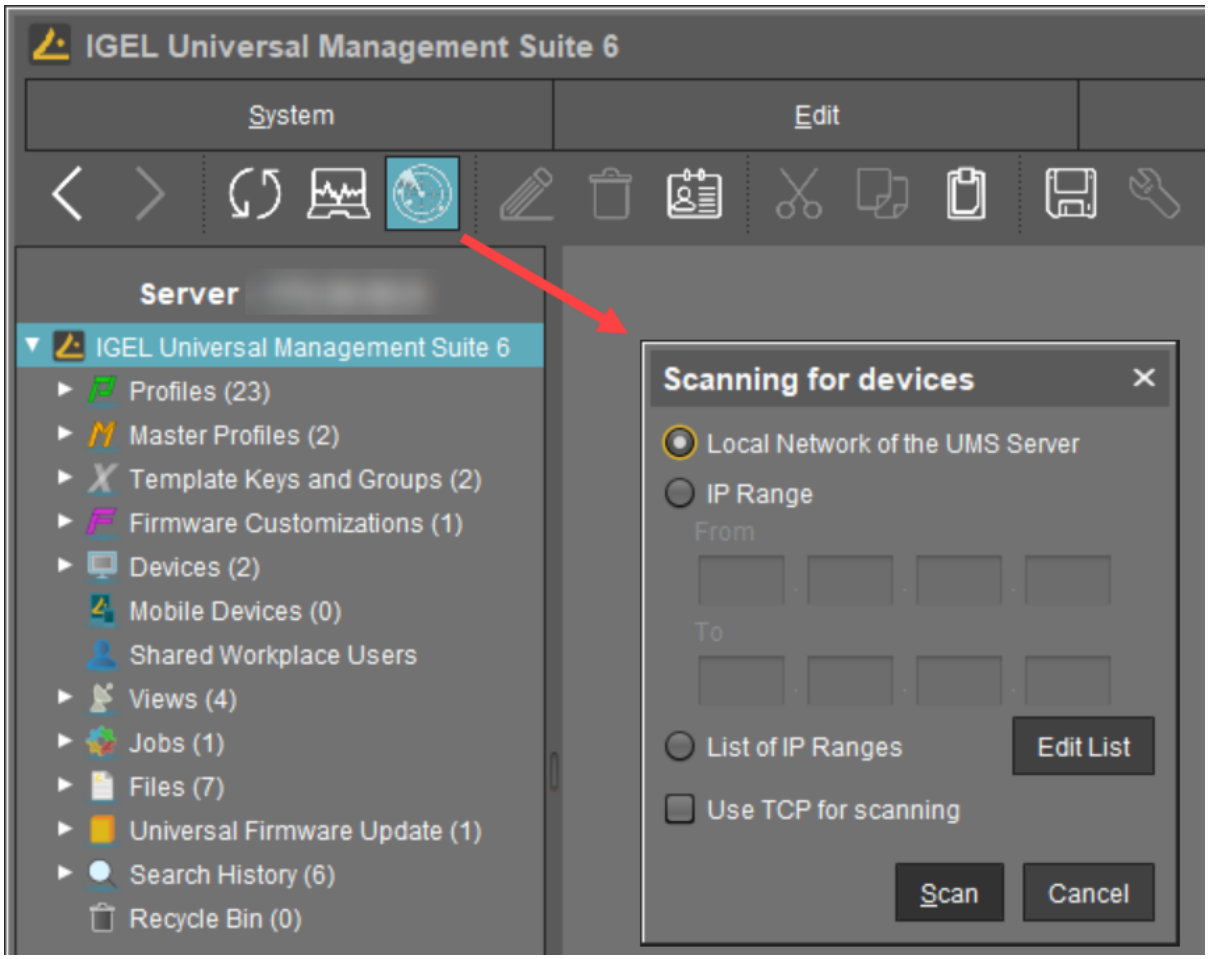
Searching for Devices

In order to find devices in the network, the following requirements must be met:

- The devices must be switched on and functioning.
- The firmware for the devices must support the UMS. This is the case with the following devices:
  - IGEL devices with original firmware
  - Devices converted with IGEL OS Creator (OSC)
  - Devices on which IGEL OS was booted via a UD Pocket
  - Devices on which IGEL OS was installed using IGEL Universal Desktop Converter 2/3 (UDC2/UDC3)
  - Devices on which the UMA (Universal Management Agent) is running

To search for devices in the network and register them in the UMS, proceed as follows:

1. Log in to the UMS Console.
2. Click on  .
   The **Scanning for devices** window will open.



3. Specify the search area:
   - **Local Network of the UMS Server**: The UMS Server will send a broadcast message to the network.

     > If there are a number of network interfaces, you should bear in mind that the broadcast message is only sent via the first network interface. If you use Windows, this is under the first item in the list of network connections.

   - **IP Range**: The UMS Server contacts each device in the given range.
   - **List of IP Ranges**: With **Edit list**, you can specify the IP ranges in which the UMS will search for devices.
   - **Use TCP for scanning**: If this option is enabled, communication with the devices will take place via TCP. If this option is disabled, UDP will be used.

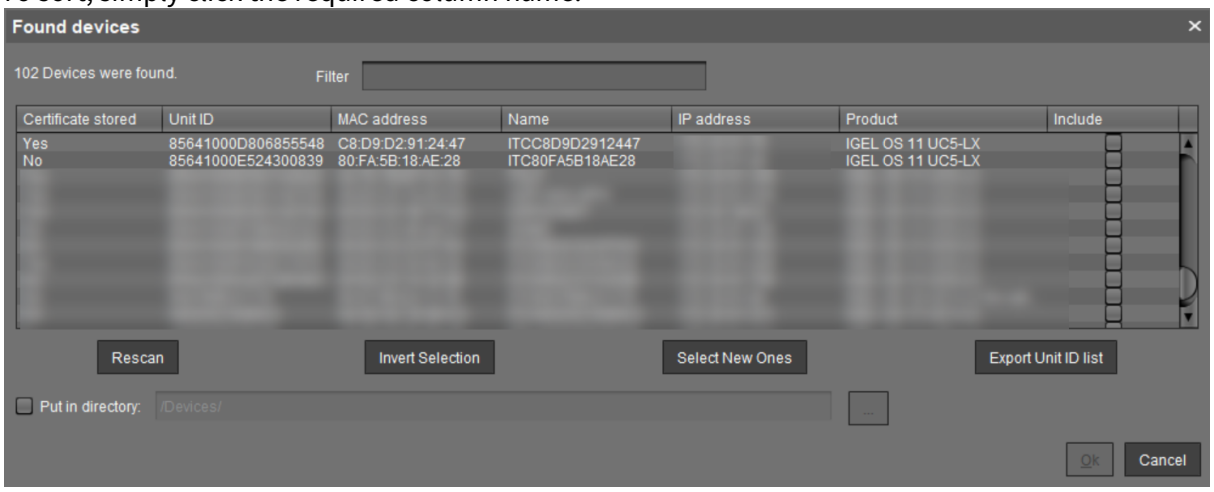
     > If TCP is used for searching, the search procedure will take longer; the scan results can be more reliable, however.

4. Click **Scan**.
   The search results will be shown in the **Found devices** window. The devices can now be registered.

Registering Devices

As soon as you have obtained the search result, you can register new devices.

1. If you only want to see devices with a specific feature in the **Certificate stored**, **Unit ID**, **MAC Address**, **Name**, **IP Address**, or **Product** column, enter the corresponding character string in the **Filter** field.
   To sort, simply click the required column name.



> You won't be able to register a device with **Certificate stored** = "Yes" unless the UMS has the same certificate.
> "Yes" for **Certificate stored** indicates that the device has already a server certificate from some UMS, i.e.
> - the device has already been registered on the current UMS. In this case, the device is simply re-registered since the UMS and the device share the same certificate. You can, however, preliminarily search for the device if you want to verify that it is registered on this UMS, and not some other UMS, see Search for Objects in the UMS (see page 273).
>   OR
> - the device has already been registered on some other UMS. In this case, see Registration of a Device in the IGEL UMS Fails (see page 135).

2. Select the devices that are to be registered. You have the following options:
   - Manual selection: In the **Include** column, highlight the devices that are to be registered.
   - Selecting all devices that are not yet registered: Click on **Select New Ones**. This will highlight all devices that have not yet received a server certificate from the UMS.

3. Click **OK**.
   The devices will now be registered in the UMS database. This may take some time.

   > During registration, the UMS Server certificate is saved on the device. Further access to the device will now be validated on the basis of this certificate. Only the owner of the certificate can manage the device.

   The result of the procedure and any error messages will be displayed in a new window.

   The devices will be placed in the **Devices** directory in the structure tree if no other directory was specified under **Put in directory**.

Registering Devices

For details on how to register devices using the **Scan for devices** function, see Scanning the Network for Devices and Registering Devices on the IGEL UMS (see page 231).

⚠ This page is due for deletion. Please check the above link and use it in the future.

Importing Devices

You can make devices known to the UMS before the devices are physically available in the network. This allows you to specify editable attributes such as department or cost center. To do this, import the devices' data from a CSV file.

> In order for devices to be registered fully, the devices' firmware data must be available in the UMS. Further information can be found under Import Firmwares (see page 371).

To import devices, proceed as follows:

1. Configure your DHCP and DNS server as described in Registering Devices Automatically on the IGEL UMS (see page 242), step 2.
2. Select **System** > **Import** > **Import Devices**.
3. Click on **Open File** and select the file.
4. Select the relevant format, i.e. the format of the data.
   - **Short Format**: See Import with Short Format (see page 237)
   - **Long Format**: See Import with Long Format (see page 238)
   - **IGEL Serial Number Format**: See Import with IGEL Serial Number (see page 240)
5. If entries are flagged as erroneous, click on **Clear** to delete all messages from the window.
6. Click on **Import devices** to launch the import procedure.

To correct erroneous entries, proceed as follows:

▶ Change the entries highlighted in red with the following editing functions:

- [Ctrl-C] and [Ctrl-V] for copying and pasting a highlighted row
- [Del/Ctrl-X] for deleting a highlighted row
- [Return/Enter] inserts an additional row under a field.

Import with Short Format

The short format provides the information required for the import and assignment to a profile:

- **MAC Address**: MAC address of the device.
- **Name**: Device name.

  - The maximal length of the device name is restricted to 15 characters if **Adjust network name if UMS-internal name has been changed** is enabled under UMS Console **> UMS Administration > Global Configuration > Device Network Settings**.
  - The length of the device name is not restricted if **Adjust network name if UMS-internal name has been changed** and **Naming Convention** are not activated under **UMS Administration > Global Configuration > Device Network Settings**.
  - Each device name will be automatically overwritten in compliance with the naming convention, even if **Adjust network name if UMS-internal name has been changed** is enabled, in case **Enable naming convention** is activated under **UMS Administration > Global Configuration > Device Network Settings**.

  See also Device Network Settings (see page 444).

- **Firmware ID**: ID of the firmware installed on the device.

  The ID of a firmware version already registered can be found via **Misc** > **Firmware Statistics**.

- **Profile Assignments**: ID of the assigned profile or a list of IDs separated by commas if a number of profiles are to be assigned to the device.

  You can remove a profile assignment already made by placing an exclamation mark in front of the profile ID. Example: `!12`

  The ID of a profile is shown in the **description data** and in the **tooltip** for the profile.

Code Example

```
00E0C5540B8B;IGEL-Office15-2;111;26
00E0C5540B8C;IGEL-Office15-3;111;12,26,27
00E0C5540B8D;IGEL-Office16-1;111;12
```

Import with Long Format

Unlike the short format, the long format also allows further data, e.g. the storage directory in the UMS structure tree, serial number, site etc. to be imported. You will see what information can be imported after selecting the long format in the import dialog.

The long format provides the following data:

- **Directory**: Storage directory in the UMS structure tree
- **MAC Address**: MAC address of the device
- **Product and Version**: Product name and firmware version of the device (separated with a semicolon)
- **Name**: Device name

  - The maximal length of the device name is restricted to 15 characters if **Adjust network name if UMS-internal name has been changed** is enabled under UMS Console **> UMS Administration > Global Configuration > Device Network Settings**.
  - The length of the device name is not restricted if **Adjust network name if UMS-internal name has been changed** and **Naming Convention** are not activated under **UMS Administration > Global Configuration > Device Network Settings**.
  - Each device name will be automatically overwritten in compliance with the naming convention, even if **Adjust network name if UMS-internal name has been changed** is enabled, in case **Enable naming convention** is activated under **UMS Administration > Global Configuration > Device Network Settings**.

  See also Device Network Settings (see page 444).

- **Site**: Location of the device
- **Department**: Department to which the device is assigned
- **Comment**: Comment regarding the device
- **Asset ID**: Inventory number of the device
- **In-Service Date**: Date on which the device was commissioned
- **Serial Number**: Serial number of the device
- **Profile Assignments**: ID of the assigned profile or a list of IDs separated by commas if a number of profiles are to be assigned to the device

  You can remove a profile assignment already made by placing an exclamation mark in front of the profile ID. Example: `!12`

  The ID of a profile is shown in the description data and in the tooltip for the profile.

- **Cost Center**: Cost center to which the device is assigned

Code example

```
/Import;00E0C5540B9A;IGEL OS 11;11.01.100.01;IGEL-1;Büro1;EDV;Meier;0815;01.06.2019;F44M;26;01
/Import;00E0C5540B9B;IGEL OS 11;11.01.100.01;IGEL-2;Büro2;EDV;Müller;4711;01.06.2019;F45M;26;01
/Import;00E0C5540B9C;IGEL OS 11;11.01.100.01;IGEL-2;Büro3;EDV;Schulz;42;01.06.2019;F46M;26;01
```

A slash "/" means that the devices will be placed in the root directory. In the above examples, the devices are thus placed in the folder "Import" under root (the folder "Import" must exist).

Import with IGEL Serial Number

When ordering your IGEL devices, you can request an import file from IGEL. Alternatively, you can create your own import file using an alternative format. Both formats are based on CSV.

> This import method works only for IGEL UD devices.

Both the format of an import file that is sent by IGEL and the alternative format specify the fields **Serial Number** and **MAC Address**.

Serial Number Format as Sent by IGEL

In an import file that is sent by IGEL, the serial number format consists of 5 fields. However, only the **Serial Number** (2nd field) and **MAC Address** (3rd field) are specified in the file.

Example:

```
;14D3F5002B290902DD ;00E0C521B4E4 ; ;
;14D3F5002B29090441 ;00E0C521B648 ; ;
;14D3F5002B2909056F ;00E0C521B776 ; ;
;14D3F5002B29090648 ;00E0C521B84F ; ;
;14D3F5002B2909070B ;00E0C521B912 ; ;
```

Alternative Serial Number Format

The alternative format has 2 fields. The field sequence is random.

Example:

Sequence MAC address - serial number:

```
00E0C51B37F8;14D3D3C03B174120D0
```

Sequence serial number - MAC address:

```
14D3D3C03B174120D0;00E0C51B37F8
```

Import Fields

For both import formats, the UMS fills in the fields **Name** and **Version** by itself. In the following, all fields predefined for imported devices are described.

MAC Address: MAC address of the device.

Name: Device name.

> The maximal length of the device name is restricted to 15 characters if **Adjust network name if UMS-internal name has been changed** is enabled under UMS Console **> UMS Administration > Global Configuration > Device Network Settings**.

The length of the device name is not restricted if **Adjust network name if UMS-internal name has been changed** and **Naming Convention** are not activated under **UMS Administration > Global Configuration > Device Network Settings**.
Each device name will be automatically overwritten in compliance with the naming convention, even if **Adjust network name if UMS-internal name has been changed** is enabled, in case **Enable naming convention** is activated under **UMS Administration > Global Configuration > Device Network Settings**.
See also Device Network Settings (see page 444).

Version: Firmware version of the device, assigned by the UMS. The firmware with the highest ID will be assigned to the device. The IDs for firmware versions already registered can be found via **Misc** > **Firmware Statistics**.

Serial Number: Serial number of the device.

Registering Devices Automatically on the IGEL UMS

In the following article, you will learn how to configure the automatic registration of endpoint devices on the IGEL Universal Management Suite (UMS). To learn more about automating the rollout with Zero Touch Deployment, see Automating the Rollout Process in the IGEL UMS (see page 65).

For an overview of device registration methods, see Registering IGEL OS Devices on the UMS Server (see page 229).

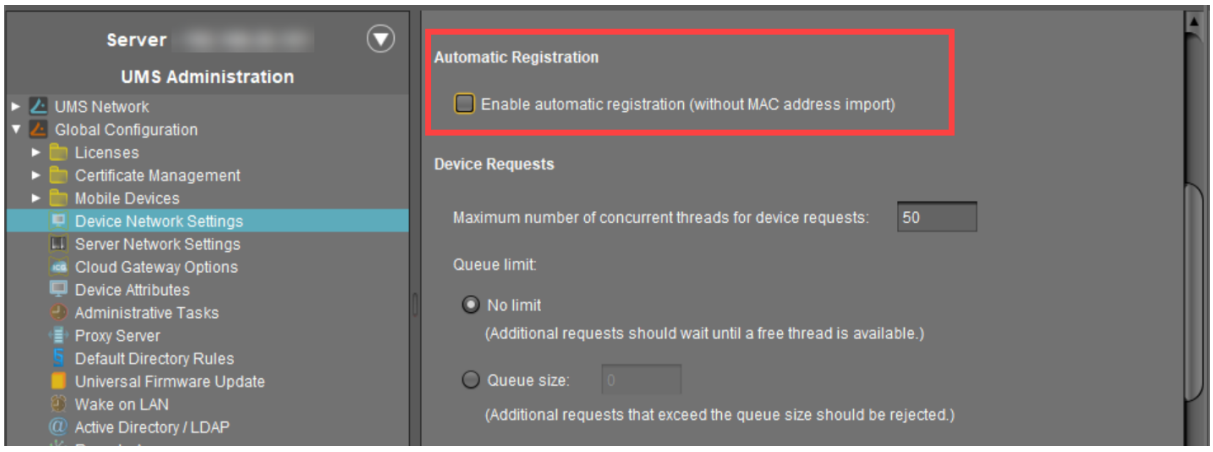
You can configure the UMS Server so that all IGEL OS devices on the server's network are automatically registered at startup. To do this, the devices must be given the address of the UMS Server via **DHCP or DNS**.

> ⓘ We recommend automatic registration when registering new devices for the first time during the rollout. Disable automatic registration as soon as all devices have been registered, so that no unknown devices can obtain sensitive settings.

To configure UMS Servers and devices for automatic registration, proceed as follows:

1. In the UMS Console, go to **UMS Administration** > **Global Configuration** > **Device Network Settings** and select the **Enable automatic registration (without MAC address import)** checkbox.

   > ⓘ If this option is enabled, each device without a UMS certificate (is distributed to the clients during registration) in the network will be added to the UMS database. If you reset a device to the factory settings and reboot it, it will immediately be registered on the server again.

2. Configuration of the network environment for an automatic UMS registration:
   - **Via DNS**:
     Create a DNS entry `igelrmserver` (entry type A) on your DNS server which points to the UMS Server.

- **Via DHCP**:
  Change the DHCP server configuration depending on the IGEL OS version of your endpoints as follows:
  - **IGEL OS 11.03.500 or lower**: Set `igelrmserver` as DHCP option 224. Set the DHCP option 224 as a string - not as a DWORD - to the IP address of the server. For the default Linux DHCP server, add the following in the `dhcpd.conf` file in the appropriate section, e.g. in the global section: `option igelrmserver code 224 = text` `option igelrmserver ""`
  - **IGEL OS 11.04.100 or higher**: Alternatively you can use DHCP option 43 (vendor-specific options) to send DHCP option 224 (name: `igelrmserver`) to the correct endpoints. An end device with IGEL OS 11.04.100 or higher sends the option 60 (vendor class identifier) with `igel-dhcp-1` as value.

    > An IGEL-specific DHCP option that is sent in DHCP option 43 overrides a corresponding DHCP option that is sent in the global namespace. The DHCP options 1, 224, and 226 can be embedded in option 43.
    > You can prevent a DHCP option 224 that has been sent in the global namespace from being interpreted. To achieve this, you must add option 1 (called "exclusive", type Byte, value 1) to DHCP option 43.

Setting up Devices Manually

You can create the data sets for devices manually.

> The firmware for the devices must be available in the database. To ensure that this is the case, it can be imported or provided by devices that have already been registered. This method is therefore not always appropriate when setting up the UMS for the first time.

To create an entry for a device in the database manually, proceed as follows:

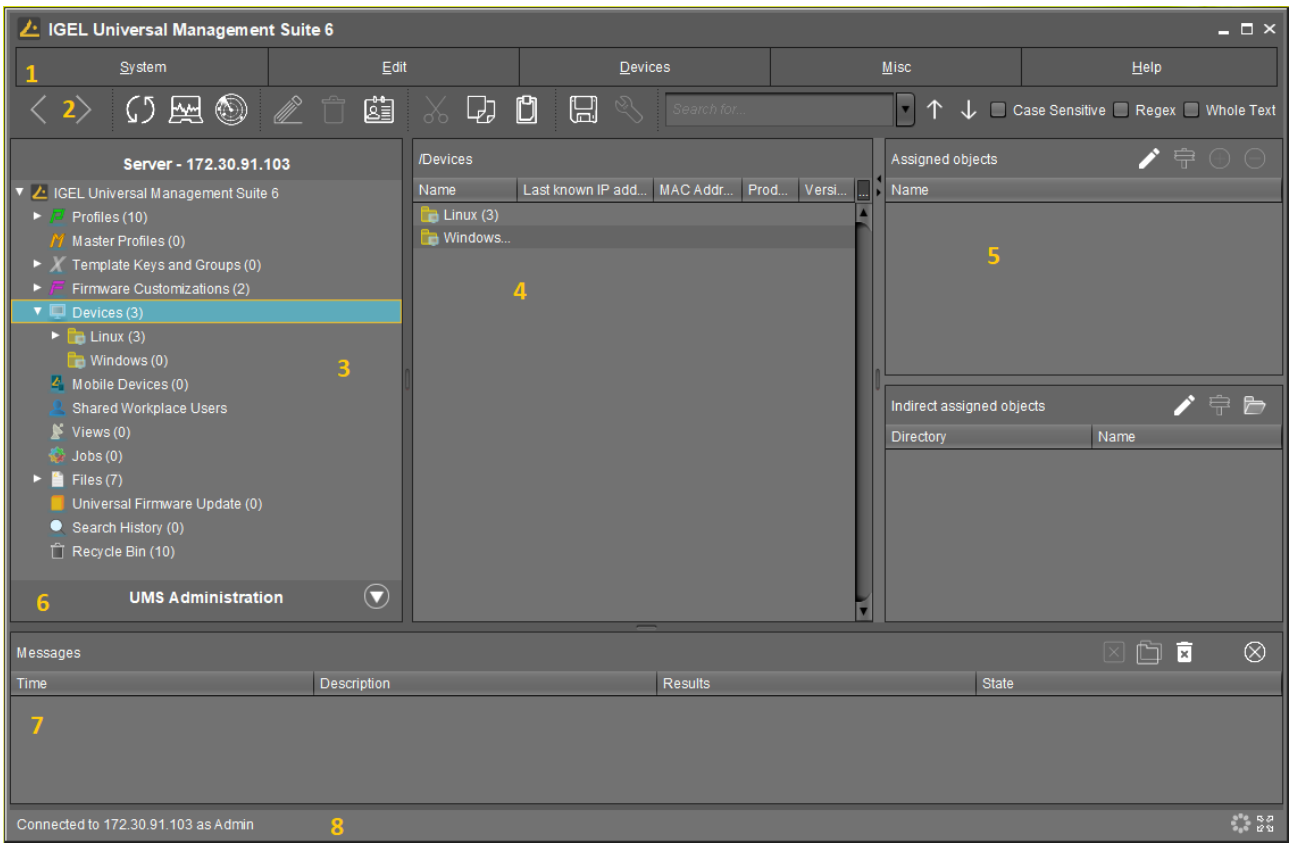
1. In the context menu of a device directory, select the **New Device** option.
2. Give the **MAC address**, the **name** and the **firmware** of the device and, optionally, select a **directory** for the device.
3. Enter the following data:
    - **MAC address**: MAC address of the device
    - **Version**: Firmware version of the device
    - **Name**: Device name (A maximum of 15 characters is allowed.)
    - **Directory** (optional): Directory in which the device is to be displayed

UMS Console User Interface

The program's graphical user interface and the tools available are described in detail below.

The Console Window

The UMS Console contains the following areas:



1	Menu Bar	All commands and actions can be executed from the menu. You can use shortcuts ([Alt] + underlined character in the menu element) to access the menu bar via the keyboard.
2	Symbol Bar (see page 265)	Frequently used commands relating to objects in the navigation tree.
3	Structure Tree (see page 264)	Provides access to all UMS Objects such as devices registered on the UMS Server, Directories, Profiles, Views, Scheduled tasks etc.
4	Content Panel	Information regarding the selected object. Many entry fields can be edited directly.
5	Assigned Objects	Objects assigned to the devices or folders.

6	UMS Administration (see page 268)	Administrative tasks, e. g. configuring domains, Universal Firmware Updates and the scheduled backup of the UMS Database (only Embedded DB)
7	Messages	Messages regarding actions launched in the UMS Console. Messages regarding successful procedures will be shown in green. Messages regarding problems when executing procedures will be shown in red.
8	Status row	Status messages from the console, e. g. the server currently connected and the user name.

You can change the vertical and horizontal limits between the navigation tree/UMS Administration, content panel and messages in order to adjust the size of the areas to suit your needs. From UMS Version 5.02.100, the changes are saved so that they will be available again the next time that you log on.

Menu Bar

The menu bar comprises the following menus:

- System (see page 249)
- Edit (see page 250)
- Devices (see page 251)
- Misc (see page 253)
- Help (see page 263)

System

Menu path: **Menu Bar > System**

In this menu, you will find options for actions relating to the UMS:

- **Connect to:** Allows you to establish the UMS server connection
  - **Server**: IP or host name of the UMS server
  - **Port**: Port number, default: 8443
  - **User name**: User name, "@'" for LDAP users
  - **Password**: User password
- **Refresh:** Allows you to refresh the view
- **Disconnect:** Allows you to disconnect the UMS server connection
- **New:** Allows you to create new UMS objects such as directories, profiles, tasks etc.
- **Import**: Allows you to import objects such as firmware, profiles, devices
- **Export**: Allows you to export objects such as firmware, profiles, devices
- **Administrator accounts**: Allows you to set up and manage UMS user accounts and user groups
- **Logging**: Allows you to display and export recordings of messages, events and VNC log entries.
- **License management**: Allows you to create and assign firmware licenses to devices and export device lists.

  > From UMS Version 5.07.100, the license management for device licenses can be found under **UMS Administration > Global Configuration >** Device Licenses (see page 434).

- **VNC viewer**: Allows you to shadow a device
- **Open Customization Builder**: if licensed: Allows you to launch the Universal Customization Builder (UCB), see the UCB manual.
- **Exit**: Allows you to close the UMS console application

Edit

Menu path: **Menu bar > Edit**

In this menu, you will find options for editing highlighted objects:

- **Save description**: Allows you to save changes to the data in the content panel
- **Edit Configuration**: Allows you to edit configuration parameters for the selected device or profile
- **Rename**: Allows you to rename an object in the navigation tree
- **Delete**: Allows you to delete an object in the navigation tree
- **Access control**: Allows you to manage user and group rights for the selected object
- **Cut**: Allows you to cut a data object and copy it to the clipboard.
- **Copy**: Allows you to copy data objects to the clipboard.
- **Paste**: Allows you to paste data objects from the clipboard.

Devices

Menu path: Menu Bar > **Devices**

At the top of this menu, you will find all commands that can be sent to selected devices at the top.

Suspend: Puts the highlighted devices into suspend mode.

Shut down: Shuts down the highlighted devices.

Wake up: Starts the highlighted devices via the network (Wake-on-LAN).

Reboot: Restarts the highlighted devices.

Update: Carries out a firmware update on the highlighted IGEL OS devices.

Update when shutting down: Updates the firmware when the highlighted IGEL OS devices are shut down.

Download firmware snapshot: Downloads the firmware snapshot for the highlighted Windows clients.

Partial update: Carries out a partial update on the highlighted Windows clients.

Create firmware snapshot: Creates a firmware snapshot on the highlighted Windows clients.

Reset to factory defaults: Resets the highlighted devices to the factory defaults.

See also Reset to Factory Defaults (IGEL OS) or Reset to Factory Defaults (Windows).

Send message: Sends a message to the highlighted devices.

Other device commands:

- **Reset to factory defaults**: Resets the highlighted devices to the factory defaults.
- **Settings UMS ->Device**: Sends the configuration of the UMS to the highlighted devices.
- **Settings Device ->UMS**: Reads the local configuration of the highlighted devices to the UMS.
- **Update desktop customization**: Updates the set desktop background and the boot logo on the highlighted IGEL OS devices.
- **File UMS ->Device**: Defines a file which is sent to the highlighted devices.
- **Device File ->UMS**: Defines a file which is sent from the highlighted devices to the UMS.
- **Delete file from device**: Defines a file which is deleted from the highlighted devices.
- **Download Flash Player**: Downloads the Flash Player plugin for Firefox on the highlighted IGEL OS devices.
- **Remove Flash Player**: Removes the Flash Player plugin for Firefox from the highlighted IGEL OS devices.
- **Store UMS certificate**: Stores the UMS certificate on highlighted devices.
- **Remove UMS certificate**: Removes the UMS certificate from the highlighted devices.
- **Refresh license information**: The license information will be refreshed.
- **Refresh system information**: The system information will be refreshed.
- **Refresh asset inventory data**: Asset inventory data will be refreshed.

Specific device command: Executes the following commands:

- **Deploy Jabra Xpress package**: Installs a Jabra Xpress package (IGEL OS).

Take over settings from...: Sends profile settings to the device on a one-off basis.

Clear 'Configuration Change Status' flag: Resets configuration change flags (blue dot next to the symbols for the devices).

Check template definitions: Checks the assignment of template values.

Scan for devices: Searches for devices in the network of the UMS Server.

Misc

Menu path: Menu Bar **> Misc**

Search: Allows you to search for objects - the search is listed in the structure tree under **Search History** and can be changed again there.

Scheduled Jobs: Allows you to manage public holiday lists and assign tasks to hosts.

- **Host Assignment**: Allows you to assign virtual hosts to selected devices.
  - **Universal Management Suite Host**: Host name of the UMS.
  - **Last Scheduler Run**: Date and time when the Scheduler last ran.
  - **Available devices**: Restricts the available devices displayed.
  - **Assigned devices**: Tree or list view of the available clients on the selected host.
- **Manage Public Holidays**: Allows you to establish public holiday lists which you can use when creating new tasks.
  - **Date lists**: Allows you to set up lists for public holidays.
  - **Days**: Allows you to specify the date of the public holidays in a public holiday list.

Change Password: Allows the password of a logged-in user to be changed.

SQL Console: Direct access to the database with SQL commands.

> The SQL console is intended solely for administrative purposes. You can destroy the database through operations on the SQL console.

Firmware Statistics: A list of firmware versions registered in the database with filter function.

Remove Unused Firmwares: Opens a dialog which lists unused firmwares and allows you to delete them individually or collectively.

Cache Management: Allows you to view, refresh and empty the UMS Server cache.

Settings (see page 254): Allows you to change configuration parameters such as language and appearance of the UMS Console, types of notifications, etc.

———

- Settings (see page 254)

Settings

Menu path: **Menu Bar > Misc > Settings**

Here you can change the following parameters:

- General (see page 255)
- Appearance (see page 256)
- Online Check (see page 258)
- Remote Access (see page 259)
- Universal Firmware Update (see page 260)
- UMS HAE (see page 261)
- Notifications (see page 262)

General

Menu path: Menu Bar > **Misc > Settings > General**

Language: Language selection for the graphical user interface. For the changes to be applied, you must close the UMS Console and start it again.

☐ **Always apply settings on next boot** (Default)

☑ **Always confirm move actions** (Default)

☑ **Always confirm unassign actions** (Default)

☑ **File choosers remember the last used directory** (Default)

☑ **Always confirm overwriting of elements in Search History** (Default)

Elements in Search History (max): Maximum number of elements that the search history will show. (Default: 15)

Clear the user and server list of the login dialog: Allows you to clear the login history.

☐ **Increase Drag and Drop acceleration** (Default)

Acceleration factor: Can only be set if the checkbox above has been enabled.

Appearance

Menu path: Menu Bar **> Misc > Settings > Appearance**

Skin: Selection of possible themes/color combinations in which the GUI is displayed.

Possible options:

- "Workspace"
- "Smart contrast"
- "Pewter"
- "Cinder grey"
- "Ocean"

Device commands always in background

☑ In the background. (Default)

☐ Not in the background

Open message area automatically on new messages

☑ The message area in the lower part of the UMS Console window will open automatically when incoming messages are received. (Default)

☐ Will not open automatically

Show content amount of directories

☑ Will be shown. (Default)

☐ Will not be shown

Load collapsed/uncollapsed tree status at login

☑ The structure tree will be restored to how it was at the last login. (Default)

☐ Will not be restored

Show category root icon

☑ Show icons as symbols for the main categories in the structure tree. (Default)

☐ Show folder symbols for the main categories in the structure tree.

Use Advanced Health Status Icons

☑ Icons displaying the status of the device will be shown in the UMS Console; see Devices (see page 351). (Default)

☐ The status icons will not be shown.

Directory tooltip contains directory tree path

☑ Will be shown. (Default)

☐ Will not be shown

Directory tooltip contains directory and content amount

☑ The number of directories and the objects in the directory will be shown in the tooltip. (Default)

☐ The number of directories and the objects in the directory will not be shown in the tooltip.

Online Check

Menu path: Menu Bar > **Misc > Settings > Online Check**

Here you can define how often the UMS polls the devices to check if they are online.

Every: The online check is executed in the given interval in milliseconds. (Default: 3000)

Never: No check is executed.

Check now: The online check is executed when this button is clicked.

Remote Access

Menu path: Menu Bar **> Misc > Settings > Remote Access**

External VNC viewer: Allows you to configure an external VNC viewer by entering or selecting the path to the executable file.

External terminal client: Allows you to select an external terminal client by entering or selecting the path to the executable file (currently supported: Putty).

Show end dialog if two or more sessions are open

☑ The end dialog will be shown. (Default)

Show warning dialog for sessions that end unexpectedly

☑ The warning dialog will be shown. (Default)

Universal Firmware Update

Menu path: Menu Bar **> Misc > Settings > Universal Firmware Update**

Activate automatic status refresh

☑ The registration status of the firmware update will be refreshed automatically. (Default)

Automatic status refresh interval: Interval in seconds.

UMS HAE

Menu path: Menu Bar **> Misc > Settings > UMS HAE**

Here you can configure the High Availability Extension status update.

Activate automatic process status refresh

☑ The process status will be refreshed automatically. (Default)

Automatic process status refresh interval: Interval in seconds. (Default: 30)

> ⓘ You will see the status in the content panel if you click on a server or load balancer under **UMS Administrator > Server**.

Notifications

Menu path: Menu Bar > **Misc > Settings > Notifications**

Show notifications on startup

☑ The notification will pop up automatically on each connection to the UMS Console.

☐ The notification will not pop up automatically. To see the notification, go to **Help > Notifications**.

Show following notifications for the current user or group
Possible options:

- "Show all"
- "Show nothing"
- "Show custom"
  - "Device Licenses"
  - "Universal Management Licenses"
  - "Universal Firmware Updates"
  - "Disk Usage (see page 180)"
  - "Global Notifications (see page 181)"
  - "Admin Tasks (see page 182)"

Help

Menu path: **Menu Bar > Help**

In this area, you will find information which may help you when using the UMS.

- **User Manual:** Link to the manual on kb.igel.com
- **User Manual (offline):** Open the user manual in PDF format.
- **IGEL Knowledge Base:** Link to further online documentation on kb.igel.com
- **Save support information...:** Saves log files from the *UMS S*erver and *UMS* Console as well as profiles and associated firmware information for the selected devices in a ZIP file. If the IGEL Management Interface (IMI) extension is being used, its API log file will be saved too. Further information can be found under Support Wizard (see page 536).
- **Save device files for support:** Saves log and configuration files for a device, for example `setup.ini` and `group.ini`, in a ZIP file.
- **Notifications**: List of all notifications
- **Third party licenses:** A list of licenses for third-party software and libraries used in the *UMS*.
- **UMS Update Check**: Checks whether a newer version of the UMS is available for downloading
- **Info:** Shows details of the current version of the *UMS* Console and *Java* environment as well as the logged-in user

Structure Tree

You can highlight or select objects in the structure tree by clicking on them. Multiple selections are possible using the [Shift] or [Ctrl] key.

From UMS Version 5.01.100, you can specify whether the UMS Console should remember the open areas in the structure tree and show them open the next time that it starts. With extensive structures, however, this can result in longer starting times. You will find the **Load collapsed/uncollapsed tree status at login** setting under **Misc** > **Settings** > **Appearance**.

From UMS Version 5.03.100, you can increase the speed when scrolling for drag & drop actions. Acceleration starts as soon as the object moved touches the bottom edge of the structure tree window. Acceleration is helpful if the structure tree contains a very large number of objects. To change the scroll speed, enable **Extras > Settings > General > Increase drag and drop acceleration** and set the **Acceleration factor** to a suitable value.

The number of elements contained including elements in sub-folders is shown after each folder. You can change this setting under **Misc** > **Settings** > **Appearance** > **Show content amount of directories**.

The structure tree is subdivided into the following areas:

- Profiles (see page 276)**:** Create and organize standard profiles.
- Master Profiles (see page 319)**:** Create and organize master profiles.
- Template Keys and Groups (see page 321)**:** Keys and values for use in template profiles.
- Firmware Customizations (see page 339): Customize the user interface to suit your corporate design.
- Devices (see page 351)**:** Organize managed devices.
- Mobile Devices (see page 439): Organize managed mobile devices.
- **Shared Workplace users** (see page 389)**:** Assign specific profiles to AD users.
- Views (see page 390)**:** Create configurable list views for devices.
- Jobs (see page 401)**:** Define scheduled tasks, e.g. firmware updates.
- Files (see page 409)**:** Registering Files for transfer to devices.
- Universal Firmware Update (see page 415)**:** Allows you to download the current firmware versions for distribution to devices.
- Search History (see page 419)**:** Saved search queries.
- Recycle Bin (see page 421)**:** Deleted and restorable objects.

Symbol Bar

In the **symbol bar**, you will find buttons for frequently used commands:

	Navigate one step forwards or backwards in the console history. This only relates to the view; actions cannot be undone.
	Refresh the view and status of the devices
	Online check of the devices
	Search for devices within the network
	Change object names in the structure tree
	Delete objects in the structure tree
	Specify access rights for selected objects
	Cut a tree element
	Copy a tree element into the clipboard
	Paste a tree element from the clipboard
	Save the edited description data for devices or profiles
	Edit configuration parameters for devices or profiles
	Finds objects in the structure tree using a name, MAC, IP, or ID. Regular expressions (**Regex**) can be used, the user's last 20 search queries are saved.
	Navigate one step forwards or backwards in the search results

Case sensitive	Specify whether upper and lowercase letters are taken into account when searching
Regex	Specify whether regular expressions are used when searching
Whole text	Specify whether the search expression needs to match the entire text or only part of it

Content Panel

The **content panel** shows the properties of the particular object highlighted in the structure tree. This can be the contents of a directory, e.g. the profiles, devices, sub-folders, tasks etc. contained therein, or detailed information relating to an object such as a device's system information, the basic data for a profile, the hit list for a view etc.

These details are shown for example in the content panel for the following objects:

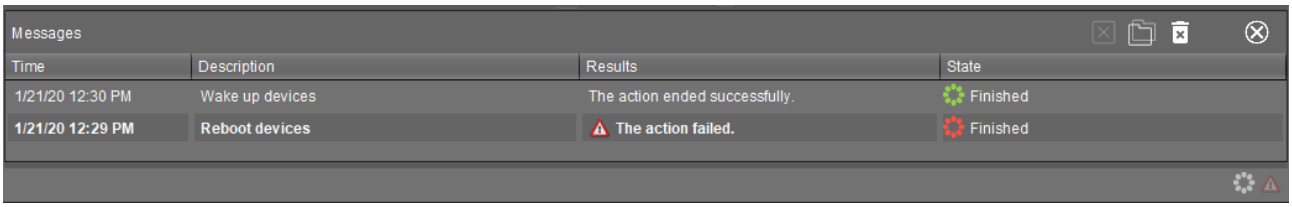
- **Directory**: Elements subordinate to the directory
- **Profiles**: Name, description, profile ID
- **Devices**: System information, license and monitor information, features
- **Views**: Name, description, rule, matching devices
- **Jobs**: Details, options, job info, schedule,execution results
- **Files**: Source URL, classification, device file location, access rights
- **Search History**: Name, rule, search type, matching devices
- **Server**: Information regarding the service executed, requests, failed and waiting requests
- **Licenses**: License summary, registered licenses
- **Device Attributes**: Device attributes
- **Administrative Tasks**: List with tasks, execution history
- **Universal Firmware Update**: Settings for the Universal Firmware Update, settings for the FTP servers to which the files are copied (optional)
- **Wake-on-LAN**: Wake-on-LAN configuration
- **Active Directory / LDAP**: Active Directory / LDAP domains
- **Remote Access**: Secure VNC connection, graphics settings
- **Logging**: Message log setting, logging event settings
- **Cache**: Cache configuration
- **Mail Settings**: Mail settings, recipient for administrative task result and service mails
- **Misc Settings**: Recycle bin, template profiles, master profiles

UMS Administration

Messages

The **Messages** window area contains information regarding the successful or unsuccessful execution of commands.

An unsuccessfully executed command will be marked in the message list with a warning symbol and a red **State** symbol. A warning symbol will also flash in the status bar of the UMS Console until the user selects the message.

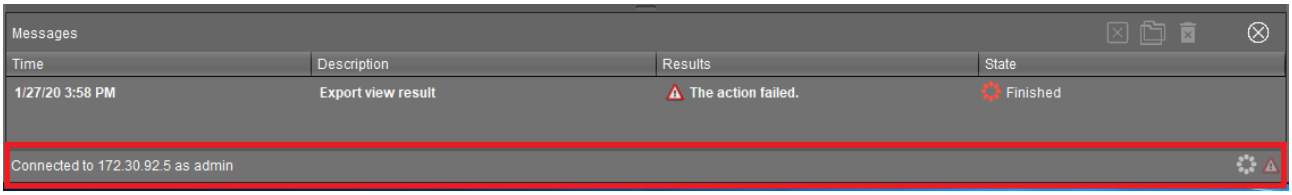


- Click or double-click the message in order to view the relevant details.
- Click to delete messages you have already dealt with or wait until the message window is automatically reset when you close the UMS Console.
- You can change the size of the message window using the middle slider or hide it altogether with a button.

To open the **Messages** window area again, click in the status bar of the UMS Console (or if messages about the unsuccessful command execution have not yet been selected).

Status Bar

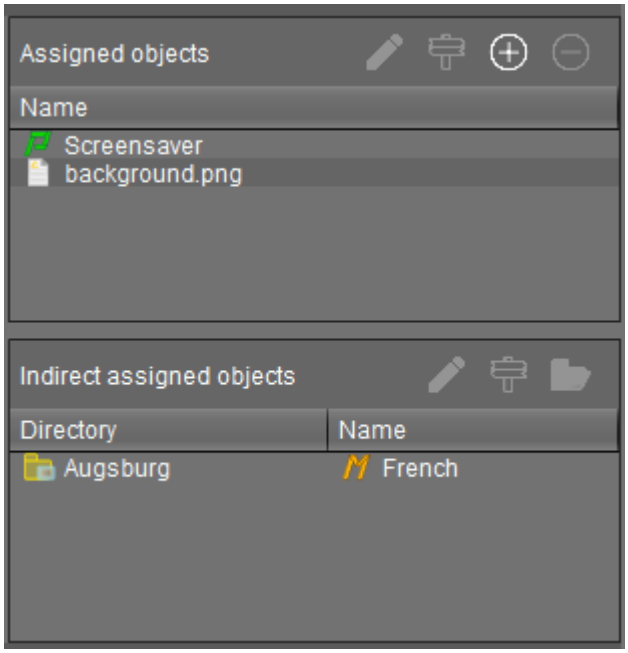
The **status bar** shows the name of the UMS Server currently connected and the user who is logged in to the UMS Console. The symbol at the bottom right indicates the status of the message window. For example, it signals when new warning messages are present. These can be seen here even if the message area is hidden.



Assigned Objects

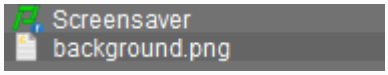
To ensure that you can quickly tell directly and indirectly assigned objects apart, the **Assigned objects** area is subdivided into two parts:

- Directly assigned objects have been assigned to an individual device, folder or profile.
- Indirectly assigned objects have been "inherited" via the file structure.



▶ Double-click an object in the assignment area in order to directly edit it.

Assigned objects with configuration changes not yet transferred to the device are marked with an exclamation mark:



Context Menu

You will be given an object-dependent **context menu** by right-clicking on the corresponding object. Depending on your selection, actions for folders, devices, Shared Workplace users etc. will be available. The chosen command will be carried out for all objects previously marked in the tree.

Certain commands can only be executed for individual objects, not for directories with objects. These options are then disabled in the menu. Example: The command **File Device> UMS** can only be executed for an individual device. In contrast, the command **File UMS > Device** can be executed for all devices in a directory.

Device Commands

You can send a command to a device not only via the context menu, but also via Menu bar > **Devices** (see page 248).

Search for Objects in the UMS

Objects within the UMS structure tree can be found using the following functions:

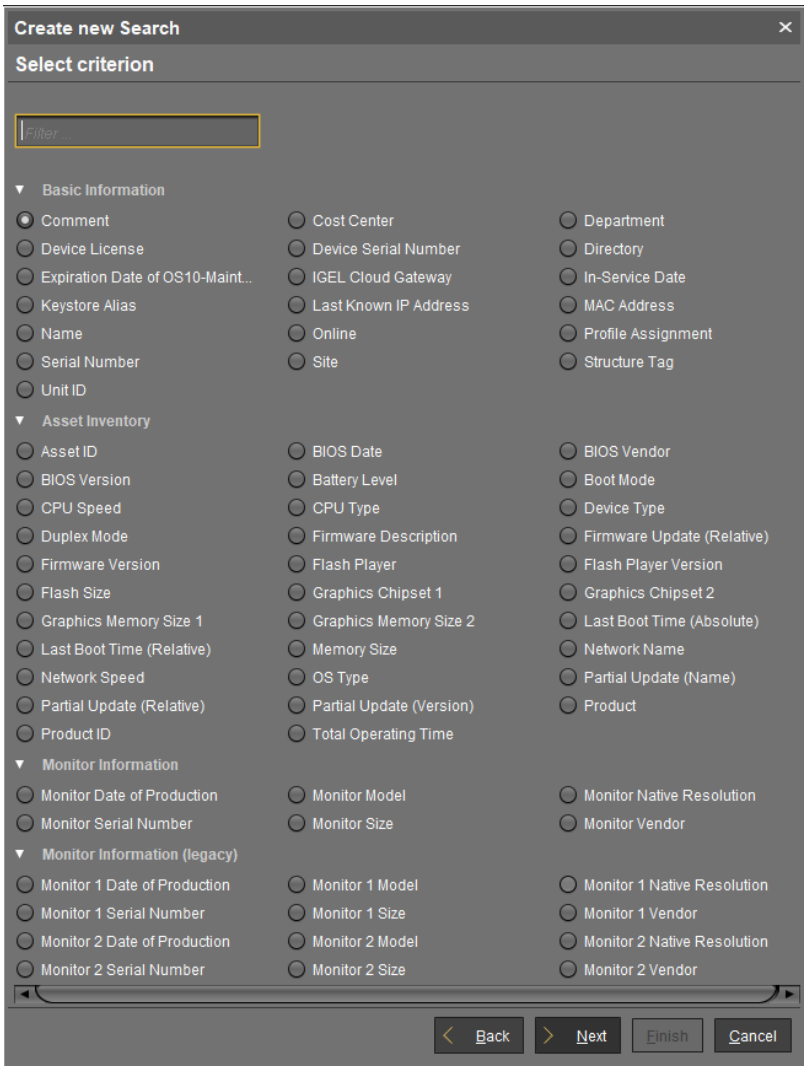
- **Quick Search**
- **Search function**
- **View**

Quick Search

The **Quick Search**  in the symbol bar (see page 265) provides the quickest access to the search function. The entry mask is always visible in the console window. The key combination [Shift-Ctrl-F] places the cursor in the entry field. The **Quick Search** search queries are restricted to a small number of object properties, e.g. object name, object ID, MAC address, and IP address. These data are buffered locally when the UMS Console is launched and can therefore be searched very quickly without having to access the database. The user's last 20 search queries are saved to allow quick access. They are saved in the console user's system user data (Windows Registry) rather than in the UMS database.

Search Function

The normal UMS search function (**Misc > Search** or [Ctrl-F] key combination) provides additional options for searching the UMS database. In addition to the Quick Search data (see above), all other device, profile or view data can be selected here, e.g. an individual inventory number or the monitor model connected. Various criteria can be logically linked (AND / OR). The user's search queries are recorded under Search History (see page 419) in the structure tree and can therefore be processed or reused easily.



Views

Views (see page 390) function very similarly to search queries. Here too, various criteria can be linked and the query saved. In contrast to search queries, however, views are available to all UMS administrators together – depending on their authorizations. Views can also be taken into account when defining scheduled tasks (see page 401).

From UMS Version 5.02.100, both search results and views can be assigned to profiles. See also Assigning Objects to a View (see page 400) and Assign Objects to the Devices of Views (see page 476).

Deleting Objects in UMS / Recycle Bin

In the IGEL Universal Management Suite, you can move objects to the **Recycle Bin** instead of permanently deleting them straight away. The Recycle Bin is enabled or disabled globally for all UMS users.

▶ Enable the Recycle Bin in the administration area under **Misc Settings > Enable Recycle Bin**.

If an object in the structure tree is deleted (**Delete** function in the symbol bar, in the context menu or the [Del] key), it will be moved to the Recycle Bin following confirmation.

> If the Recycle Bin is active, objects can also be deleted directly and permanently by pressing [Shift-Del].

Directories are moved to the Recycle Bin along with their sub-folders and all elements and can therefore be restored again as a complete structure. You will find the UMS Recycle Bin as the lowest node in the UMS Console structure tree. Elements in the Recycle Bin can be permanently deleted there or restored. To do this, bring up the context menu for an element in the Recycle Bin.

> If you cannot bring up the context menu for elements in the Recycle Bin, the Recycle Bin is probably inactive. Check the status of the Recycle Bin as described above.

Virtually all elements from the UMS structure tree can be moved to the Recycle Bin: devices, profiles, views, tasks, files, and their directories. Shared Workplace users cannot be deleted, while administrator accounts (in account management) and search history elements can only be deleted permanently (with [Shift-Del]). The highest nodes in the structure tree cannot be deleted either. However, this procedure will affect all deletable elements beneath this node!

- Objects in the Recycle Bin cannot be found via the search function or views and cannot be addressed by scheduled tasks.
- Devices in the Recycle Bin will not receive any new settings from the UMS but will remain registered in the UMS and can be restored again from the Recycle Bin along with all assigned profiles.
- The fact that profiles in the Recycle Bin are no longer effective means that the settings for devices may change. Profiles previously assigned to devices will be reactivated if they are restored again.
- Planned tasks, views and search queries in the Recycle Bin will not be executed.
- At the same time, assigned profiles, files, views, and firmware updates in the Recycle Bin are not active.

Profiles

Menu path: Structure tree **> Profiles**

In this area, you can manage profiles. **Profiles** are predefined configurations that can be assigned globally to managed devices via the Universal Management Suite.

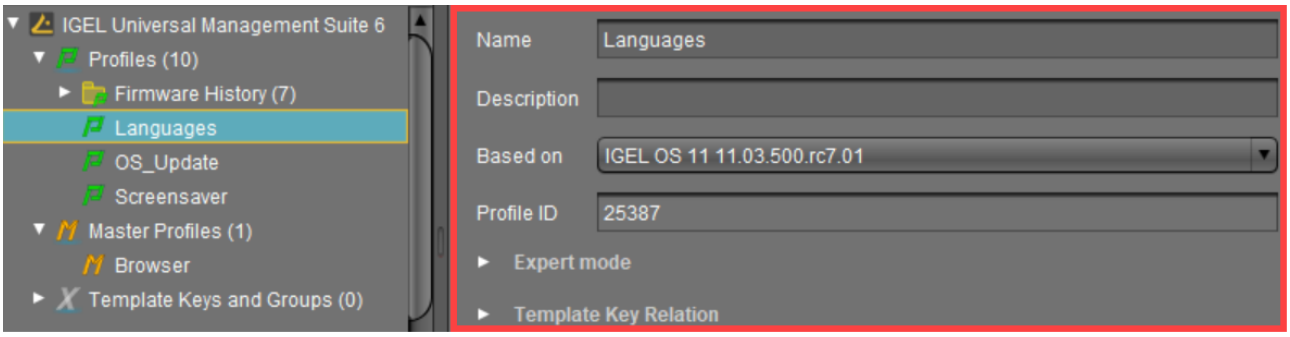
When Is It a Good Idea to Use Profiles?

You can achieve the following using profiles:

- Setting identical configurations for a number of devices
- Defining different usage scenarios for devices (or groups of devices) in an abstract manner.
- Significantly reducing administrative outlay.
- Reducing configuration options on the device.

You have the option of creating directories for saving profiles and can add, delete, and change the profiles in this part of the structure.

Information on a profile is shown in the content panel.



UMS profiles can be compared with policies in the structure of Microsoft Active Directory (AD). The directories that are grouped and managed via the devices correspond to the organizational units in the AD.

The following profile types exist:

Standard profiles can be assigned to devices **directly** or **indirectly** via directories. A device can receive its settings from a number of directly or indirectly assigned profiles. During the assignment process, the profile settings overwrite the settings configured directly on the device. See Effectiveness of Settings (see page 280).

If you use Shared Workplace (see page 594), you have the option of assigning profiles to users. Profiles assigned to users have a higher priority than profiles assigned to devices. See Order of Effectiveness of Profiles in Shared Workplace (see page 308) and Prioritization of Profiles (see page 304).

	**Template profiles** are profiles where one or more settings are set via variables. These values are determined dynamically. Standard and master profiles can thus be used and combined even more flexibly. See the Template Profiles (see page 321) chapter. If you deploy Shared Workplace (see page 594), notice that template profiles cannot be used.
	**Master profiles** can overwrite the settings of standard profiles and have their own authorizations, see Master Profiles (see page 319). The order of effectiveness is exactly the opposite of what it is for the standard profiles. See Order of Effectiveness of Master Profiles (see page 310).
	**Mobile-device profiles** are used for configuring mobile devices with the UMS add-on Mobile Device Management (see page 618) Essentials. See Creating Mobile Device Profiles (see page 645).

This chapter describes

- Choosing the Right Profile (see page 278)
- Configuration Levels (see page 279)
- Effectiveness of Settings (see page 280)
- Using Profiles (see page 281)
- Prioritization of Profiles (see page 304)

Managing Profiles

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=Ml522x3qqn0

Choosing the Right Profile

Standard Profiles

In most cases, **standard profiles** are sufficient to define configuration settings globally and transfer them to devices via profiles. You can use several profiles at the same time. With the help of the priority rule, the effectiveness of the parameter values specified by a profile can be managed.

In the Using profiles (see page 281) chapter, you can find out how to set up and assign profiles.

In the Template profiles (see page 321) chapter, you can also find out how to create profiles with variable values.

In the Prioritization of Profiles (see page 304) chapter, the priority rule is explained.

Master Profiles

The use of one or two **master profiles** can be helpful in a hierarchical structure with various administrators and complex rights management. With a master profile, a higher-ranking administrator can influence other administrators' profile settings without withdrawing their management rights.

Read the Master profiles (see page 319) chapter very carefully before you use this profile type.

> Use **master profiles** very sparingly and only in specific cases. If they are used incorrectly, you can unintentionally disable all other profiles.

User-Specific Profiles

When using *IGEL Shared Workplace (SWP)*, it is a good idea to manage user-specific configurations via profiles. User-specific SWP profiles differ from device profiles in terms of the way in which they work.

For more information, read IGEL Shared Workplace - Assigning a User Profile (see page 598).

Configuration Levels

Profiles allow you to globally manage configuration parameters on IGEL OS devices.

It is important to understand that there are parameters for different types of instances, normal parameters, and parameters for fixed and free instances.

Normal Parameters and Fixed Instances

Fixed instances refer to settings options which are fixed, i.e. integrated within the system. These fixed instances include language settings, monitor settings, firmware update settings, user interface settings, etc. These options cannot be added or deleted – only changed.

Parameter settings for fixed instances that are configured on the device itself can be overwritten if other values are specified in an assigned profile. If fixed instances are managed via various profiles, very specific priority rules (see page 304) apply.

Free Instances

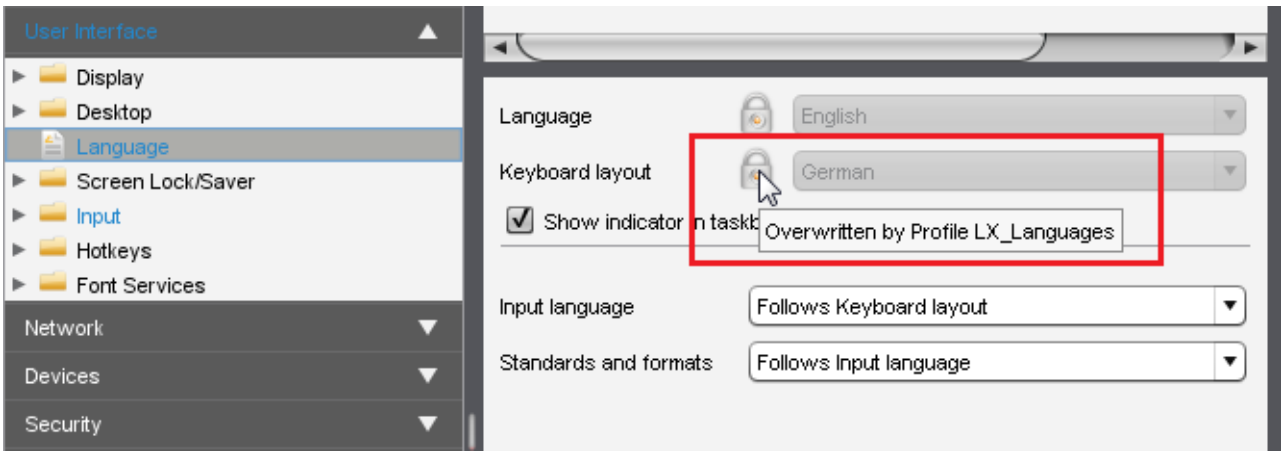
These are the instances that the user can add or delete via  . These include sessions, USB devices, printers, accessories, VPN connections, and everything that can be selected in device lists.

Parameter values of free instances cannot be overwritten. If several free instances (e.g. printers) are assigned to a device, they are added together. Therefore, there are no priorities for the parameter values of free instances.

> You can break this rule if you enable **Overwrite sessions** when setting up a profile, see Creating Profiles (see page 282).

Effectiveness of Settings

Parameters set via a profile are blocked in the configuration dialog and indicated by a lock symbol.



They can only be edited in the profile. The name of the profile responsible for the locked status will be shown if you move the mouse pointer over the lock symbol.

Each parameter has two value types:

- values determined by the device and
- value determined by the profiles.

These values exist alongside each other, although there is a rule whereby profile settings always take precedence.

> If you have set a value for a parameter in a profile and then remove the assignment to a device, the value of the parameter will be changed back to its previous device value. The profile value will not be copied to the device settings.

Using Profiles

In this chapter, you can learn the following:

Creating Profiles

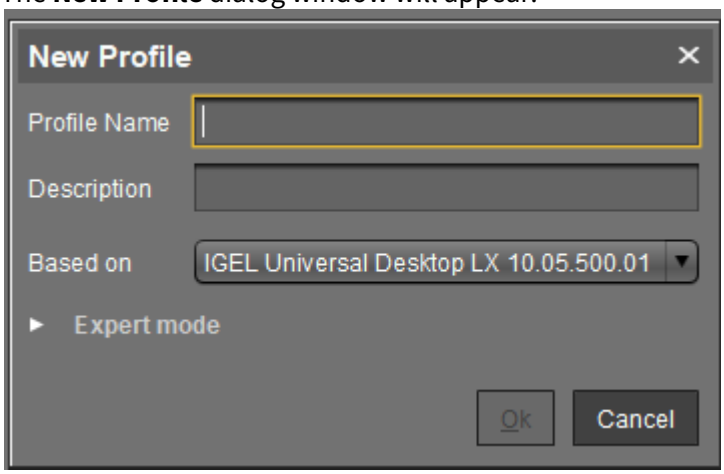
Menu path: Structure tree **> Profiles**

With the new knowledge about profiles, you can start to apply this feature.

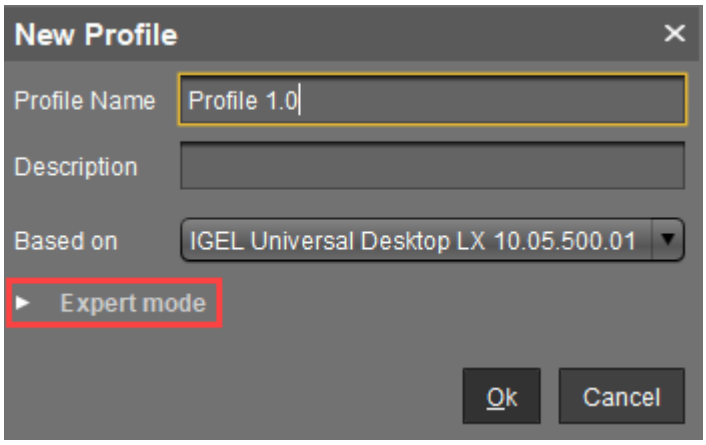
⚠ To ensure that you can use all new features of IGEL OS:
- Update your UMS to the current version.
- For all relevant profiles, set **Based on** to the appropriate firmware version.

To create a new profile in the UMS:

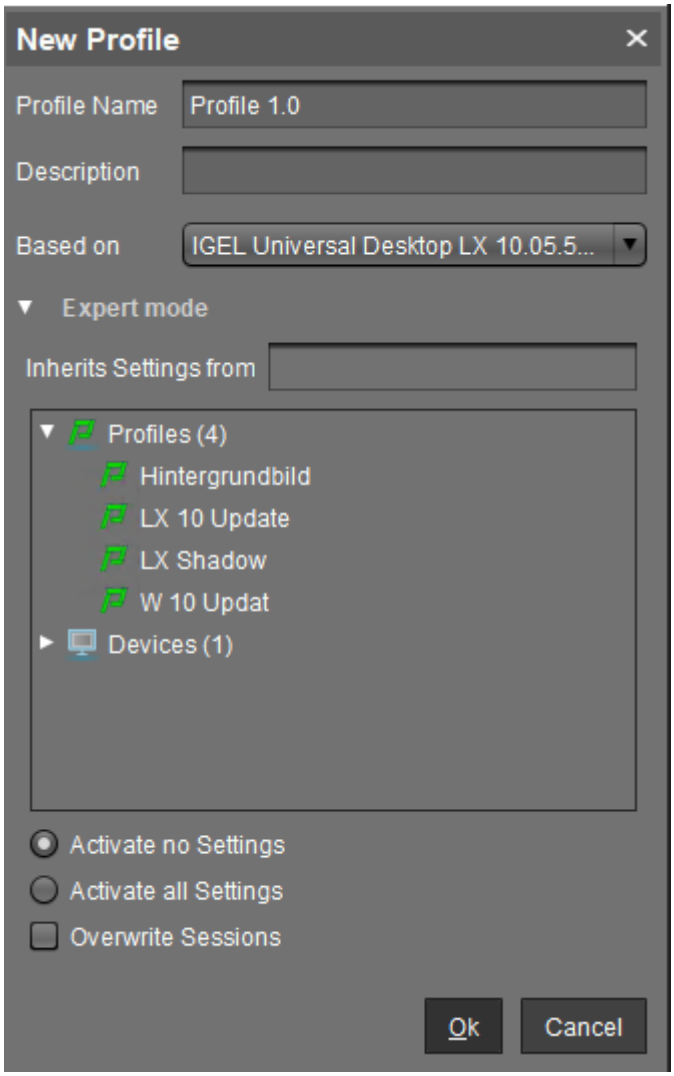
1. Select **New Profile** under **System > New** or in the context menu of the corresponding option in the structure tree
   OR
   import a previously created profile. See Exporting and Importing Profiles (see page 296).
   The **New Profile** dialog window will appear.



2. Enter a **Name** and a **Description** for the profile.
3. For an "empty" profile that will not use any existing settings, you must select a firmware version for the new profile.
4. Click **Expert mode** if you want to use a profile with existing settings.



5. Now you can specify whether the new profile **Inherits Settings from** an existing profile or device.



6. Select the appropriate firmware under **Based on**.
7. Select one of the possible options:
   - **Activate no settings:** Initially there are no active parameters.
   - **Activate all settings:** All available parameters of the profile will be active.
   - **Overwrite Sessions:** All free instances will be overwritten by the profile.

   > Attention! Before changing the default settings in this option, inform yourself about the consequences of other options in New Profile - Options (see page 285). Activating all settings will block all settings in the local setup! **Overwrite Sessions** should be activated only in exceptional cases. With this option, you can override free instances of all other profiles.
8. Click **OK** to set up and save the profile.

   > The new profile will be placed in the selected profile directory. If no directory is selected, the new profile will be put directly in the directory **Profiles**.
9. Make your settings.
10. Click **Apply** to save the settings without quitting the profile.
11. Click **Save** to save the settings and quit the profile.

    > For a better overview, it is recommended to organize profiles using subdirectories.

Video

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=Sc38mRv5Z1s

New Profile - Options

The options in the **New Profile** window have the following meanings:

- **Do not enable any settings:** No parameters are initially active.
- **Enable all settings:** All available parameters for the profile are enabled. Please note that all settings are locked on the device with a lock symbol. A profile with this setting prevents settings being changed locally on the device. This option makes sense only if you would like to have all settings for a device managed on the basis of this profile.

  > In many cases, profiles which contain all parameters for an item of firmware take up space in databases and backup files unnecessarily. You should therefore use this option only if it seems necessary. In the majority of cases, it is advisable to configure a device on the basis of several profiles with specific configuration parts.

- **Overwrite sessions:**

  ☑ Overwrites the free instances defined for the device or assigned via other other profiles with those of this profile.

  ☐ The free instances defined in the profile are added to the free instances that were defined previously on the device or by the assignment of other profiles.

  > In this case, **sessions** mean both the applications that can be selected via **Sessions** in the menu tree and all other **free instances** that can be created or deleted. See Parameter Levels.

  The **Overwrite sessions** option ensures that only the free instances for this profile are created on the device. Free instances created in other profiles or directly in the device configuration are disabled.
  If a number of profiles with the **Overwrite sessions** option enabled are assigned to a device (or Shared Workplace user), the profile with the highest priority is effective, i.e. only the free instances for this profile are available on the device.

  > Exception: If the profile is a standard profile and a master profile (see page 319) with session settings is also assigned to the device or user, the settings are added: The device receives all sessions for the standard profile and the master profile. Sessions in master profiles can only be overwritten by a master profile.

New Profile - Configuration

The properties of a profile consist of so-called description data and the profile configuration.
Description data consist of the name of the profile, a descriptive text, the firmware version and the overwrite flag for sessions.

Click on **Edit > Save Description Data** or in the toolbar in order to save these data.
The data are now updated in the database.

> When changing the firmware version, remember that profile settings will be lost if they are not supported in the new firmware.

To edit the profile configuration, proceed as follows:

1. Double-click on a profile or select a profile from the navigation tree.
2. Click on **Edit > Edit Configuration**.
   The setup will open.

   > Paths highlighted in blue in the configuration tree lead to settings that have already been set via the profile.

   > Keys in the Registry (settings) that have been set via a profile are highlighted with a color. The same colors as for highlighting paths in the configuration tree of the UMS are used.

3. To change settings, click on the activation symbol in front of the parameter until the desired function is active.

	The parameter is inactive and will not be configured by the profile.
	The parameter is active and will be configured by the profile. Template keys are inactive.
	The parameter is active and will be configured by the profile. Template keys are active.
	The parameter is active and will be configured by the profile using a template key.
	Reset to default value.

When saving the profile, you can determine when your changes will take effect:

1. Make the required changes.
2. Click on Save.
3. Decide whether the new settings are to take effect immediately or when the relevant devices next boot.

> Bear in mind that users who are working may be disturbed if changes take effect immediately.

Assigned profiles with configuration changes not yet transferred to the device are flagged with an exclamation mark in the list of Assigned Objects.

How to Allocate IGEL UMS Profiles

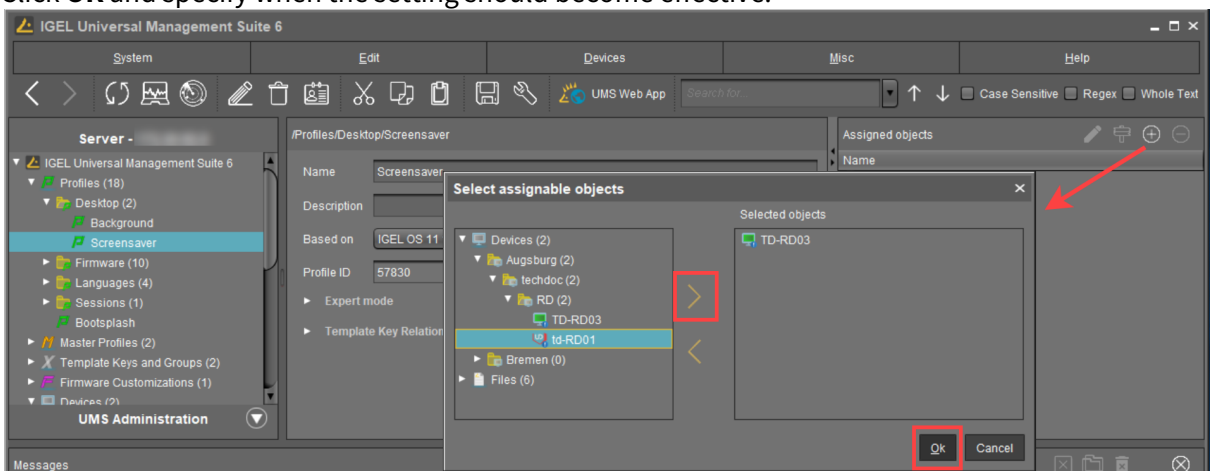
In the IGEL Universal Management Suite (UMS), you can assign a profile to a device or a device directory.

> **Direct and Indirect Assignment of Objects in the IGEL UMS**
> Objects in the IGEL UMS can be assigned directly or indirectly:
> - Directly assigned objects have been assigned to an individual device or directory.
> - Indirectly assigned objects have been "inherited" via the directory structure.
>
> Whether a profile is assigned directly or indirectly influences the priority of a profile, see Order of Effectiveness of Profiles (see page 305).
> Note also the following:
> - If you assign a profile to a directory, it is **indirectly** assigned to each device in this directory including the subdirectories.
> - If you subsequently move a device to this directory, the directory profiles will affect this device too.
> - If you remove a device from this directory, the profile will no longer influence this device and the local settings for the device will be restored.

You can assign a profile to a device or a device directory per drag & drop or under **Assigned objects** in the **Profiles** or **Devices** tree nodes.

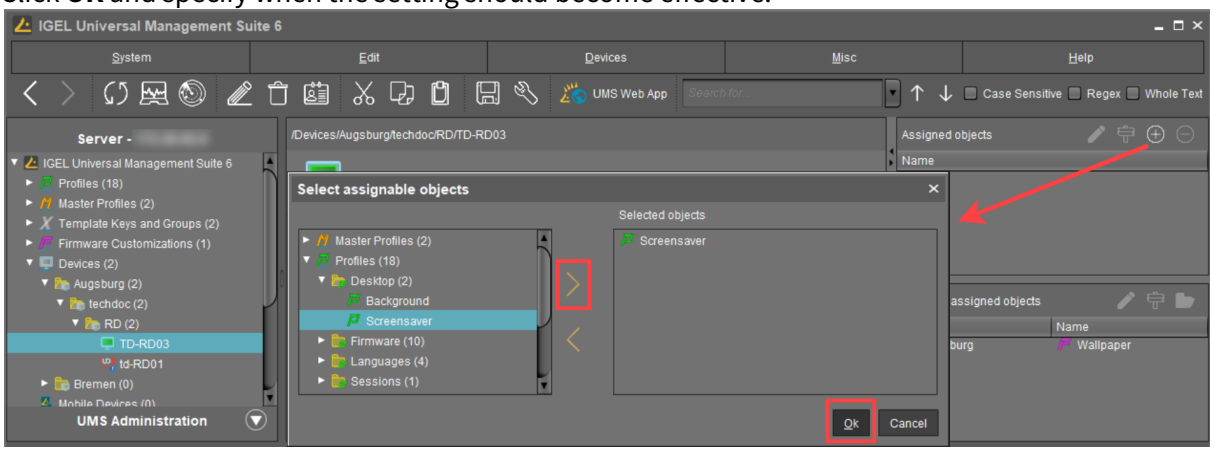
How to Assign a Profile: Starting from the Profile

1. In the UMS Console, go to **Profiles** and select the required profile.
2. Under **Assigned objects**, click  .
   The **Select assignable objects** window will open.
3. Highlight the required device or device directory and click  .
4. Click **OK** and specify when the setting should become effective.



How to Assign a Profile: Starting from the Device / Device Directory

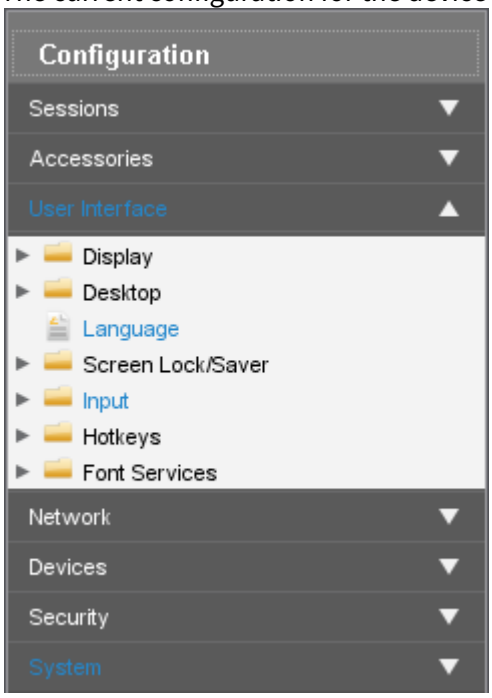
1. In the UMS Console, go to **Devices** and select the required device or device directory.
2. Under **Assigned objects**, click ⊕.
   The **Select assignable objects** window will open.
3. Highlight the required profile and click ›.
4. Click **OK** and specify when the setting should become effective.



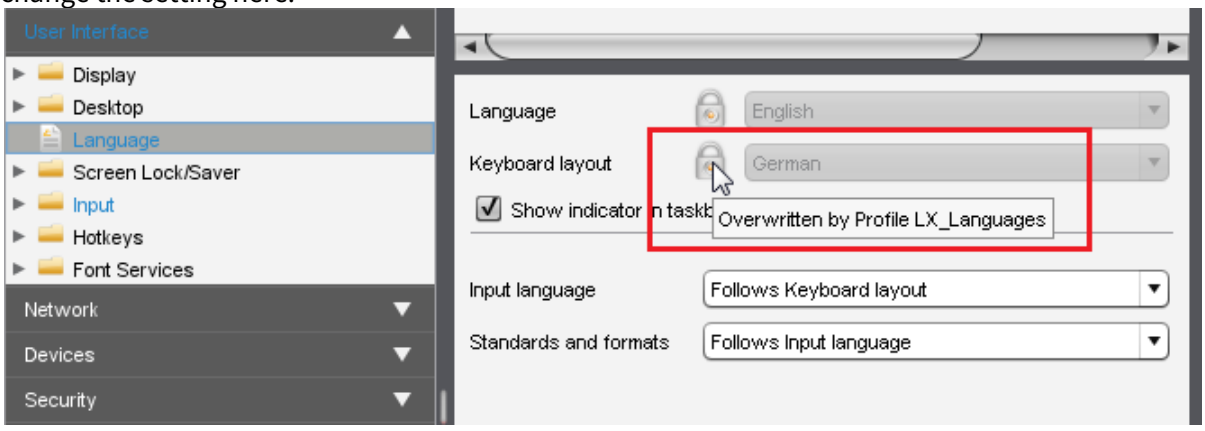
Checking Profiles

If you have assigned a profile to a device, check the results:

1. Select a device and click **Edit >Edit Configuration**.
   The current configuration for the device will be displayed.



   A lock symbol will be shown in front of each overwritten setting, i.e. in front of an active setting for an assigned profile. The value that you have specified in the profile will be shown. You cannot change the setting here.



2. Move the mouse over the lock symbol  .
   A tooltip will show the profile from which the parameter value was taken. This is useful if you have

assigned more than one profile to the device. If a setting is active in a number of assigned profiles, the value in the most up-to-date profile will apply.

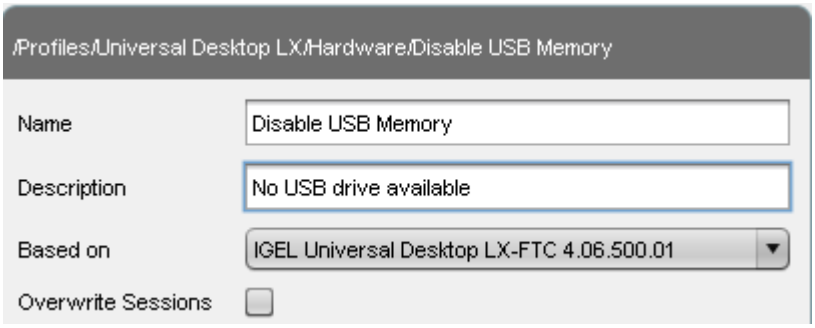
In the **Assigned Objects** area, you can navigate to an assigned device, profile or assigned file, or edit the configuration.

- Select an object.
- Click  to edit the object.
- Click  to navigate to this object in the tree structure.
- Double-click an assigned object to jump straight to it.

Editing profiles

The properties of a profile consist of so-called description data and the profile configuration.

Description data consist of the name of the profile, a descriptive text, the firmware version and the overwrite flag for sessions. Example:



▶ Click on **Edit > Save Description Data** or  in the toolbar in order to save these data.
The data are now updated in the database.

> When changing the firmware version, remember that profile settings will be lost if they are not supported in the new firmware.

To edit the **profile configuration**, proceed as follows:

1. Double-click on a **profile** or select a profile from the navigation tree.
2. Click on **Edit > Edit Configuration**.
   The set up will open.

   > Paths highlighted in blue in the configuration tree lead to settings that have already been set via the profile.

3. To change settings, click on the activation symbol in front of the parameter until the desired function is active.

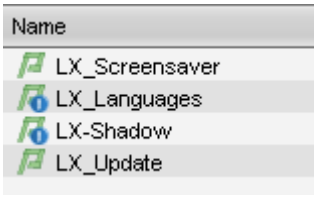
		The parameter is inactive and will not be configured by the profile.
		The parameter is active and the set value will be configured by the profile.

When saving the profile, you can determine when your changes will take effect:

1. Make the required changes.
2. Click on **Save**.
3. Decide whether the new settings are to take effect immediately or when the relevant devices next boot.

> Bear in mind that users who are working may be disturbed if changes take effect immediately.

Assigned profiles with configuration changes not yet transferred to the device are flagged with an exclamation mark in the list of **Assigned Objects**:



Removing Assigned Profiles from a Device

You can remove assigned profiles from a device or a device directory:

Starting from the profile

1. Select a profile in the navigation tree.
2. Select an object in the **Assigned Objects** area.
3. Click  .

Starting from the device

1. Select a device or a device directory in the navigation tree.
2. Select an assigned profile from the list in the **Assigned Objects** area.
3. Click  .

This profile will now no longer affect the individual device(s) in the directory. The overwritten value for the settings is reset to the value which was valid before the profile was assigned.

> Only directly assigned profiles can be removed. Indirectly assigned profiles can only be removed where they are assigned directly, that is the directory.

Deleting Profiles

If you would like to delete a profile, select it in the UMS navigation tree and perform one of the following options:

- In the symbol bar, click on **Delete**  .
- Press the [Del] button on your keyboard.
- Right-click on the profile and select the **Delete** option from the context menu.

The same applies to directories too. These are deleted along with all sub-directories and profiles.

> If you delete a profile, it will be removed for every device or every device directory to which it was assigned. The profile values no longer affect the device settings. In addition, all settings for the profile from the database will be deleted.

If the recycle bin is active, the deleted profile will be stored there and you may recover it if you need to.

Exporting and Importing Profiles

Profiles can be exported from the database together with their directory structure. This can be helpful for backup purposes or when importing the profile data from one *UMS* installation to another.

Alternatively, device settings can be imported as profiles; see Importing devices as profiles (see page 373).

Exporting a Profile and Firmware

To export an individual profile, proceed as follows:

1. Right-click the profile.
2. Select the command **Export Profile.**

To export a number of profiles in one file (ZIP archive), proceed as follows:

1. Highlight the desired profiles using the [Ctrl] and [Shift] keys.
2. Select **System>Export>Export Profile.**
   The **Export Profiles** window will open.

3. Select the requested profiles in the column **Include**.
4. Confirm by clicking **OK**.
5. Select the destination file.

The firmware information can be exported to an archive along with the profile data. This allows importing to a *UMS* installation without the relevant firmware being registered. This can now be imported together with the profile.

> The profiles are converted into the XML format. Make sure that you do not make these files public if the source profiles contain passwords or other confidential data!

Importing a Profile and Firmware

To import an individual profile, proceed as follows:

1. Click **System > Import > Import Profiles**.
2. Select the `XML` file or archive containing your profile(s).
   The **Import Profiles** dialog window will appear. This shows the name and firmware version of each profile configuration contained in the file you have selected.
3. Uncheck one of the boxes in the left row of the table to exclude the relevant profile from the import process.

   > During the import, you can retain the original directory path of the profile. Alternatively, the profile can be placed in the main directory.

   A dialog window shows whether all the selected profiles were imported.
   An item of firmware from an archive which was previously not present in the database will automatically be imported together with the corresponding profile.

- Importing Profiles with Unknown Firmware (see page 299)

Importing Profiles with Unknown Firmware

Profiles whose underlying firmware is not contained in the database or the import file cannot be imported and will be highlighted in red in the import view.

Such profiles can contain settings which do not feature in any of the registered firmware versions.

To import profiles with unknown firmware, proceed as follows:

1. Click the firmware field that is highlighted in red.
2. Select any firmware version that is known to the system.
3. Import the profile.

If you select an item of firmware that is known to the system, the version will be implicitly converted. Normally, this has only a negligible effect on the profile settings if you select a similar firmware version or a newer version of the same model. However, unknown firmware settings will be lost in the process.

Copy Profile

Menu path: Navigation Tree **> Profiles >** [Name of the profile] > Context Menu **> Copy**

You can copy a profile and paste it in any profile directory.

> Copying and pasting are also possible between standard profile directories and master profile directories. If you copy a standard profile and paste it into a master profile directory, the copy of the standard profile will be defined as a master profile. If you copy a master profile and paste it into a standard profile directory, the copy will be defined as a standard profile. Information regarding master profiles can be found in the Master Profiles (see page 319) chapter.

To copy a profile, proceed as follows:

1. Click on the profile that you want to copy.
2. Open the context menu for the profile and select **Copy**.
3. Click on the profile directory in which you would like to paste the copy of the profile. This can also be the directory of the original profile.
4. Open the context menu for the directory and select **Paste**.
   A new profile which has the same name and settings as the original profile will be created. The new profile is not yet assigned to a device, irrespective of the assignments of the original profile.

Copy Profile Directory

Menu path: Navigation Tree **> Profiles >** [Name of the profile directory] > Context Menu **> Copy**

You can copy a profile directory and paste it in any directory.

> Copying and pasting are also possible between standard profile directories and master profile directories. If you copy a standard profile directory and paste it into a master profile directory, the copies of the standard profiles will be defined as master profiles. If you copy a master profile directory and paste it into a standard profile directory, the copies of the master profiles will be defined as standard profiles. Information regarding master profiles can be found in the Master Profiles (see page 319) chapter.

To copy a profile directory, proceed as follows:

1. Click on the profile directory that you want to copy.
2. Open the context menu for the profile directory and select **Copy**.
3. Click on the directory in which you would like to paste the copy of the profile directory. This can also be the directory in which the original profile directory is located.
4. Open the context menu for the directory and select **Paste**.
   A new profile directory which has the same name as the original profile directory will be created. The new profile directory will contain newly created copies of the profiles contained in the original profile directory as well as copies of the sub-directories. The copies of the profiles are not yet assigned to a device, irrespective of the assignments of the original profiles.

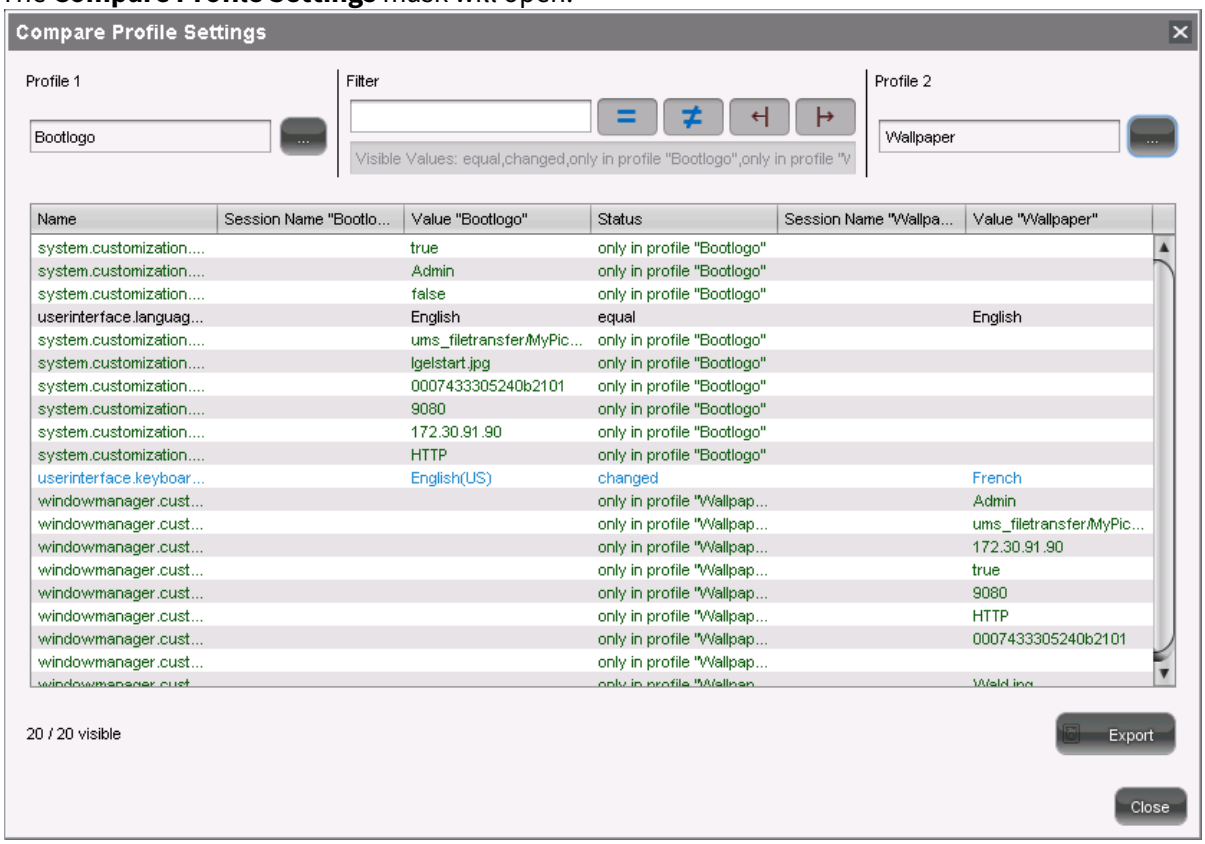
Comparing Profiles in the IGEL UMS

In the IGEL Universal Management Suite (UMS), you can use a function which makes it easy to compare profiles with each other.

Menu path: **UMS Console > Profiles**

To compare two profiles, proceed as follows:

1. Highlight two profiles using the [Ctrl] key.
2. Right-click on one of these profiles.
3. Select **Compare Profile Settings...** from the context menu.
   The **Compare Profile Settings** mask will open.



All settings configured in the two profiles are listed one after another in the standard view. You can use specific comparative operators by clicking on the following buttons:

		Settings that are the same in both profiles are shown or hidden.
		Settings that are different in the profiles are shown or hidden.
		Settings that are only found in profile 1 are shown or hidden.
		Settings that are only found in profile 2 are shown or hidden.

- Click on one of these buttons in order to disable the relevant comparative operator.
- Click on it again to enable the operator once more.

inactive active

- Enable or disable a number of comparative operators.
- Click on **Export** to save the comparison list locally as a csv, html or xml file.

Prioritization of Profiles

Profiles can be assigned to devices directly or indirectly via directories. A device can receive its settings from a number of directly or indirectly assigned profiles. During the assignment process, the profile settings overwrite the settings configured directly on the device.

If you use *Shared Workplace*, you have the option of assigning profiles to users. Profiles assigned to users have more weight than those assigned to devices. See Order of effectiveness of profiles in Shared Workplace (see page 308).

The procedure for setting up and configuring profiles is described in Use profiles (see page 281). This chapter mainly looks at priorities - which profile overrides which one and when.

Order of Effectiveness

The priority of profiles is symbolized by "LEDs" below:

The more red lights, the higher the priority of the profile.

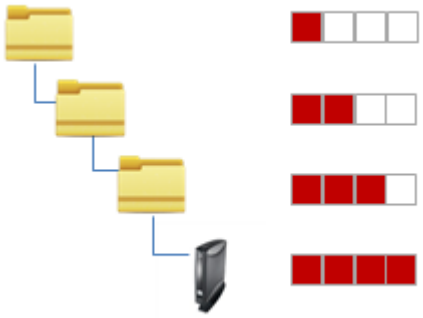
Order of Effectiveness of Profiles

In order to be able to manage the effectiveness of different profile types, you need to understand the order of priority. Various profiles that overlap like stencils can be assigned to a device. What happens if two profiles specify a different value for a setting? Which one has more weight?

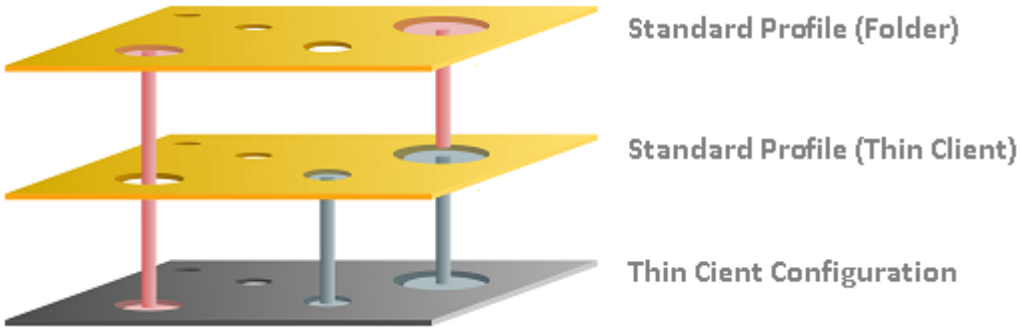
> Avoid competing settings in a number of profiles. If possible, set up one profile per setting, e.g. a profile for language settings, one for a left-handed mouse, etc.

The following rules apply to competing settings in various profiles:

Rule: The closer the standard profile is to the device in the directory tree, the higher its priority.



The priority rule only plays a role if the same parameter value is different in two profiles. The following graphic shows that there are specified values in both profiles which have an effect on the device. Only the parameter on the right is set by both profiles. In this case, the value of the bottom profile has priority because it is closer to the device.



Rule: In the event that the same settings are specified a number of times, the profiles with higher priority override other profiles. The effectiveness of settings which are specified in one profile only does not change.

See the following example (see page 307).

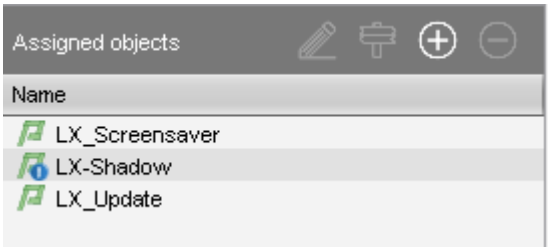
Rule: If several profiles are assigned on an equal basis, the newer profile with the higher profile ID has priority.

In order to read out the ID of a profile, point to a profile in the list of assigned profiles with the mouse pointer. A tooltip with the profile ID will be shown.

Rule: The priority rule only applies to general settings. If a number of sessions are set up, they will not be overridden. They will exist alongside each other because free instances are added.

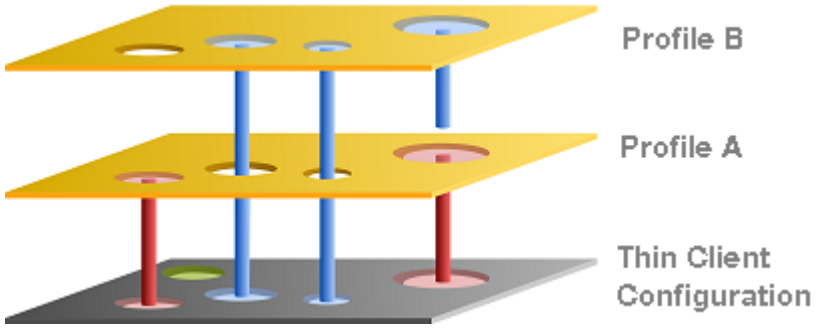
The lists of directly or indirectly assigned profiles are sorted according to the order of priority. Within a directory level, the profile which is higher up in the list thus has a higher priority.

In this example, the "screen saver" profile has the highest priority.



Example – Standard Profiles

We will create three profiles which we assign directly and indirectly to a device:



- **Device Configuration**: You specify the mouse settings on the device itself. In this case (green), the left-handed mouse is specified.
- **Profile A**: You assign to the device a language profile in which (red) the language and the keyboard layout are set to German.
- **Profile B**: You assign to a higher-level directory a profile with screen configuration. This specifies the resolution and the dual screen settings and the language is set to English (blue).

The settings that arrive at the device are:

- Green: Left-handed mouse (device configuration)
- Red: Language and keyboard German (Profile A)
- Blue: Resolution and dual screen setting (Profile B)

The "English" language setting from Profile B has no effect on the device because Profile A has set the language parameter to German. Because Profile A is closer to the device, it has priority.

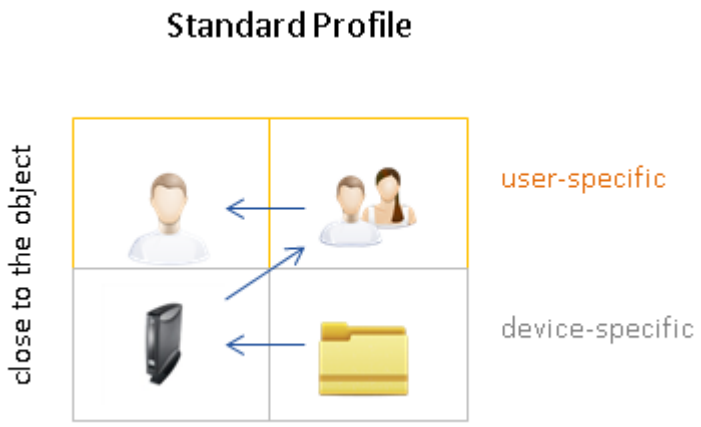
Order of Effectiveness of Profiles in Shared Workplace

In IGEL Shared Workplace (see page 594), you can use profiles to configure user settings. For further information, see the guide IGEL Shared Workplace - Assigning a User Profile (see page 598).

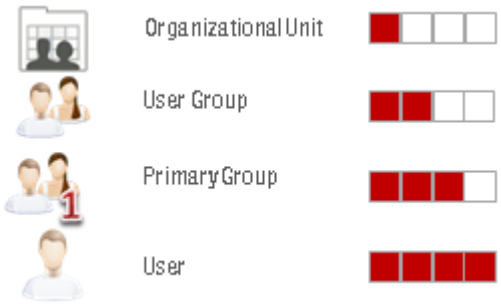
⚠ Template profiles and template keys (see page 321) cannot be used if Shared Workplace is deployed.

Rule: Profiles that are assigned to users have a higher priority than those that are assigned to devices. This applies to standard profiles and master profiles.

If you allocate a number of profiles, it may be that specific user or client settings are made a number of times. In this case, the following **priority of standard profiles** applies:



Higher priority	than...
user-specific profiles	device-specific profiles
closer to the user/device	further away from the user/device



Higher priority	than...
primary groups	other groups
other groups	organizational unit

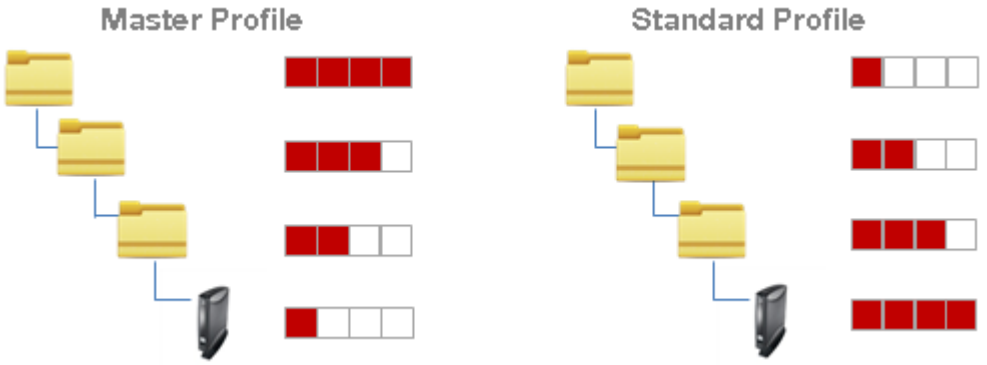
Rule: Profiles that are assigned to an object are prioritized in descending order according to profile ID (highest ID = highest priority).

Rule: Groups within a level are prioritized in alphabetical order.

Order of Effectiveness of Master Profiles

Master profiles allow more flexible access rights within the *IGEL UMS* as they can override the settings for standard profiles and have their own authorizations.

Master profiles are prioritized **the other way around** compared to the standard profiles. This means that a competing profile setting has higher priority the further away from the object the profile is:

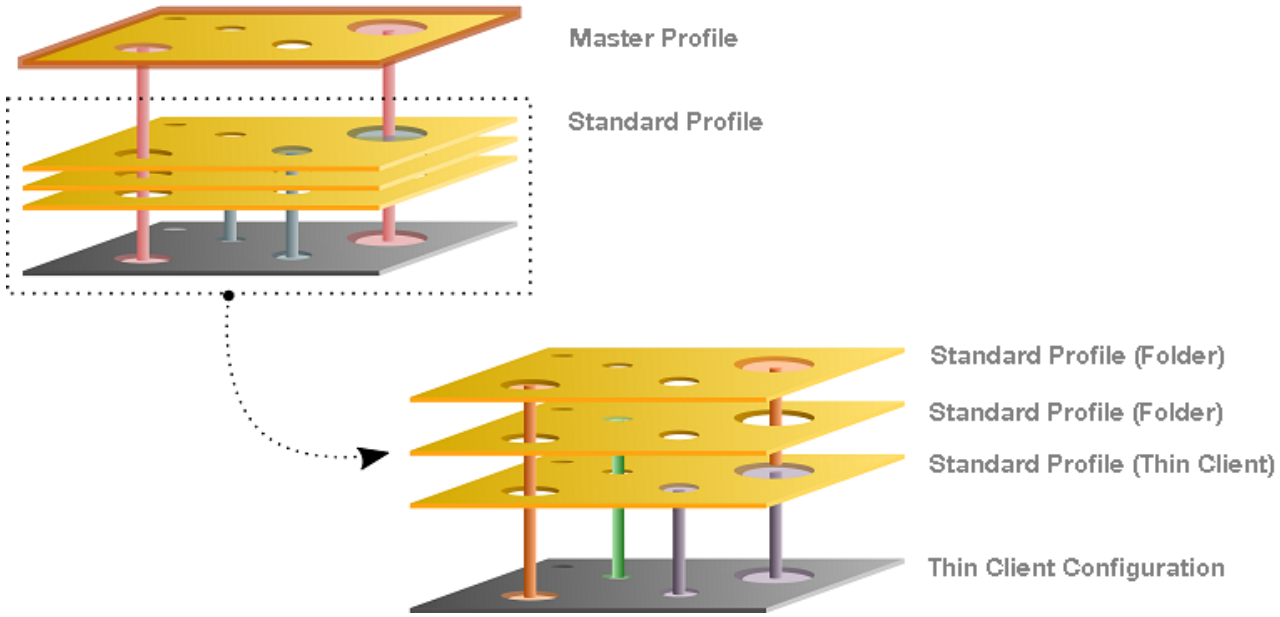


The following applies to master profiles:

Higher priority	than...
further away from the device	closer to the device
higher-level directory	sub-directory

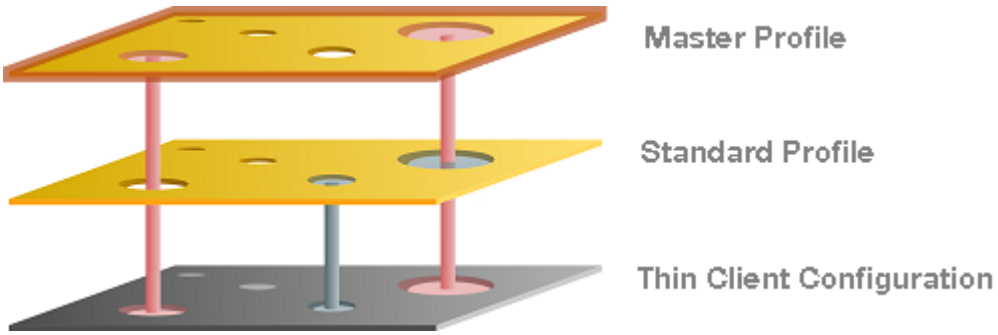
Rule: Master profiles override all standard profiles.

The following graphic shows that the master profile setting overrides that of the standard profiles if the same parameter is pre-populated. Settings that are not double-populated are effective without restriction.



Example – Master Profiles

We will create a standard profile and a master profile which we assign to a device.

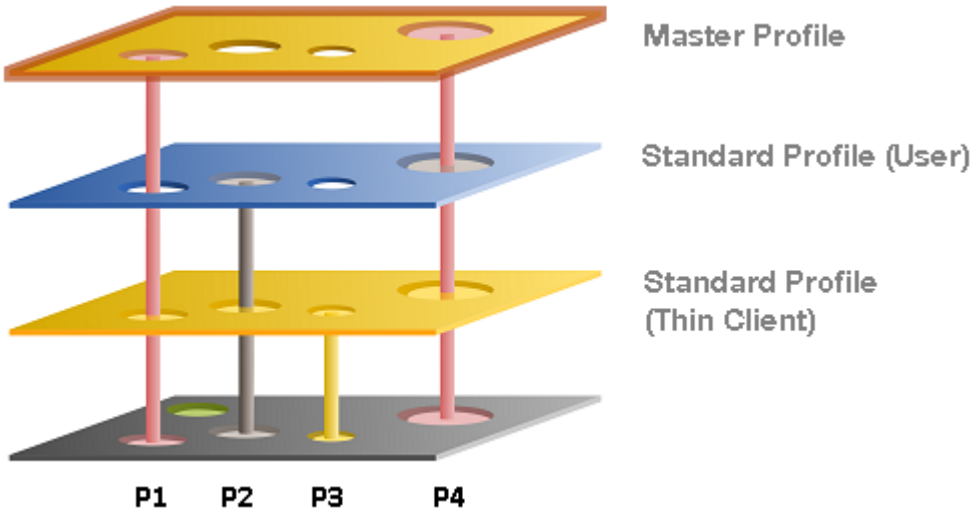


- **Standard profile**: You assign to the devide a standard profile in which (gray) the language and the keyboard layout are set to German.
- **Master profile**: You assign to a higher-level directory a master profile. This specifies the background image and the language is set to English (red).
  The settings that arrive at the client are:
  - Gray: Keyboard German (standard profile)
  - Red: Background image and language setting English (master profile)

  The "German" language setting from the standard profile has no effect on the device because the master profile has set the language parameter to English. If the parameter settings are the same, the master profile overwrites the values of standard profiles.

Example – Master and Various Standard Profiles

We will create a master profile, a user-specific standard profile and a device-specific standard profile.

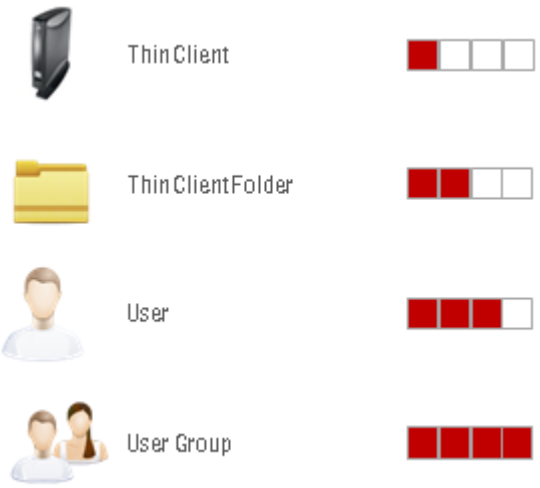


- **Standard profile (device)**: You assign to the device a standard profile with which you define the mouse settings. In this case the left-handed mouse (**P2**) is specified, the speed of the mouse pointer (**P4**) is set to slow, the double-click interval (**P1**) is set to slow and the keyboard layout is set to German (**P3**).
- **Standard profile (User)**: You assign to a higher-level directory a user-specific standard profile in which the right-handed mouse (**P2**) is specified and the mouse speed (**P4**) is set to quick.
- **Master Profile**: You assign to a higher-level directory a master profile. In this case, the mouse pointer speed (**P4**) and the double-click interval (**P1**) are set to medium.
  The settings that arrive at the client are:
  - Yellow: (**P3**) Keyboard layout German (standard profile green)
  - Grey: (**P2**) Right-handed mouse (standard profile blue)
  - Red: (**P4**, **P1**) Mouse speed and double-click interval (master profile)

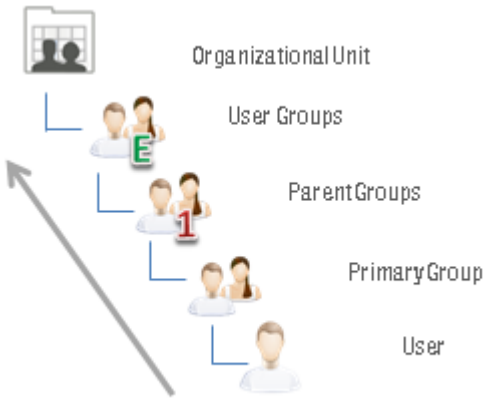
Master Profiles in Shared Workplace

Profiles assigned to users have a higher priority than profiles assigned to devices. In the case of the master profiles, the relevant group rather than the individual client or user is prioritized. This means:

Rule: Master profiles assigned to user groups have a higher priority than those assigned to individual users. These have higher priority than master profiles assigned to device directories. Master profiles assigned to an individual client have the lowest priority.

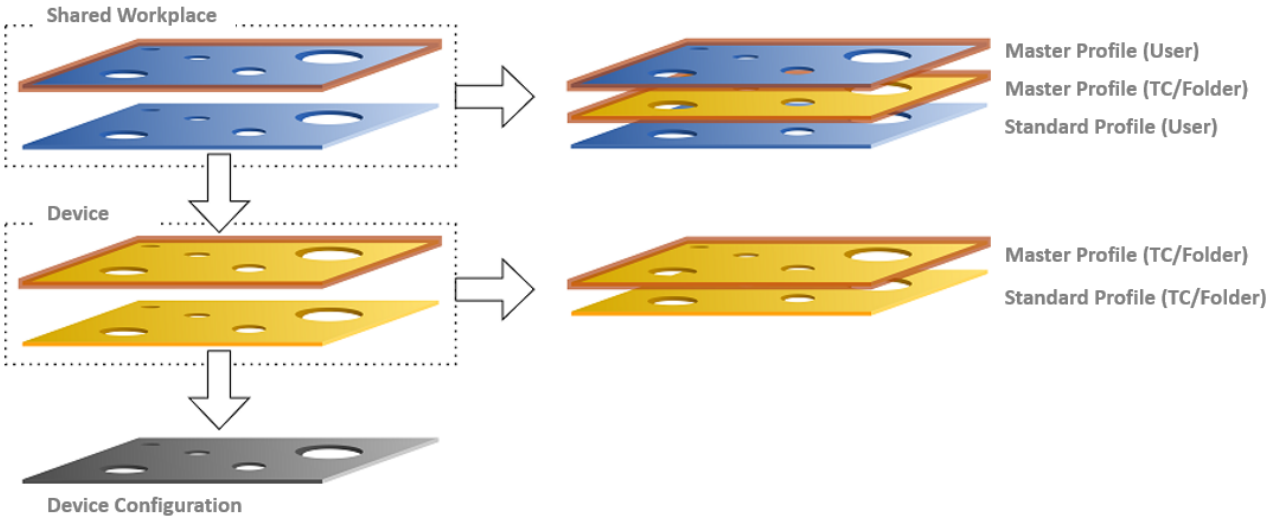


Higher priority	than...
user-specific profiles	device-specific profiles
further away from the user/device	closer to the user/device



Higher priority	than...
organizational unit	other groups
other groups	primary group

Order of Effectiveness of All Profiles



Parameters on the profile level (device and Shared Workplace)

- are specified by profiles or master profiles,
- can be configured exclusively via the UMS,
- overwrite parameter values that were configured on the device itself,
- take effect through assignment to a device or directories,
- can be enabled individually.

Parameters for the device configuration

- can be configured on the device itself or via the UMS,
- always contain ALL parameters,
- ALWAYS exist, even without the UMS.

Summary

The following overview summarizes all rules relating to the priority of profiles:

A - Basic rule

- In the event that the same settings are specified a number of times, the profiles with higher priority override other profiles. See the graphic in the example (see page 307).
- Settings which are specified in one profile only are not overridden.
- The priority rule only applies to general settings and fixed instances. If for example a number of free instances (see page 279) are set up, they will not be overridden – they will exist alongside each other.
- If several profiles are assigned on an equal basis, the newer profile with the higher profile ID has priority.

B - Standard profiles

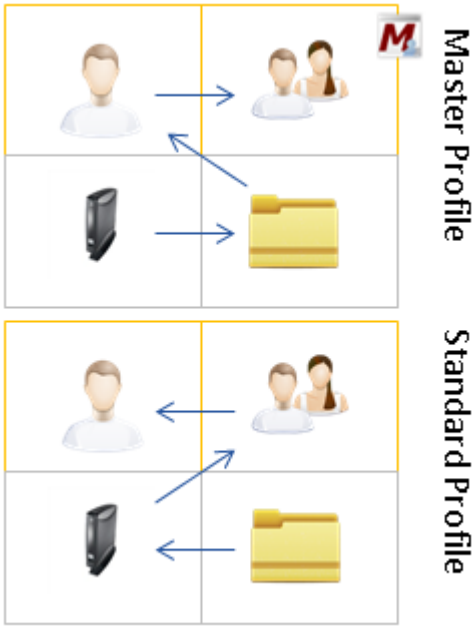
- The closer the standard profile is to the device, the higher its priority.

C - Shared Workplace

- The closer the standard profile is to the user, the higher its priority.
- Profiles assigned to users have a higher priority than profiles assigned to devices.
- Groups within a level are prioritized in alphabetical order.

D - Master profiles

- Master profiles override all standard profiles.
- Settings in master profiles can only be overwritten by master profiles.
- Master profiles are prioritized the other way around compared to the standard profiles.
- Master profiles which are closer to the object have lower priority.
- Master profiles assigned to user groups have a higher priority than those assigned to individual users. These have higher priority than master profiles assigned to device directories. Master profiles assigned to an individual client have the lowest priority.


Master Profile
Standard Profile

Master Profiles

Menu path: Structure tree > **Master Profiles**

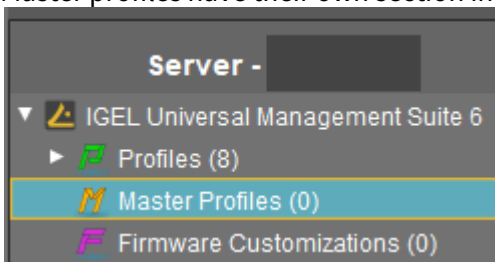
> Master profiles have to be first enabled under **UMS Administration > Global Configuration > Misc Settings**, see Enabling Master Profiles (see page 320).

The aim of introducing master profiles is to be able to reproduce the more complex system of rights management for UMS administrators in very large or distributed environments.

Important profile configurations can now be assigned to all registered devices on a priority basis without having to revoke the rights of other administrators to manage other settings or profiles.

Most Important Features of Master Profiles

- Master profiles are identical to standard profiles in terms of their effects, but are prioritized differently. For more information, see Order of Effectiveness of Master Profiles (see page 310).
- Master profiles are profiles whose settings override all standard profiles.
- Master profiles cannot be overwritten by standard profiles.
- Master profiles have their own section in the IGEL UMS structure tree.



IGEL TechChannel

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=FZFPpdSe0lM

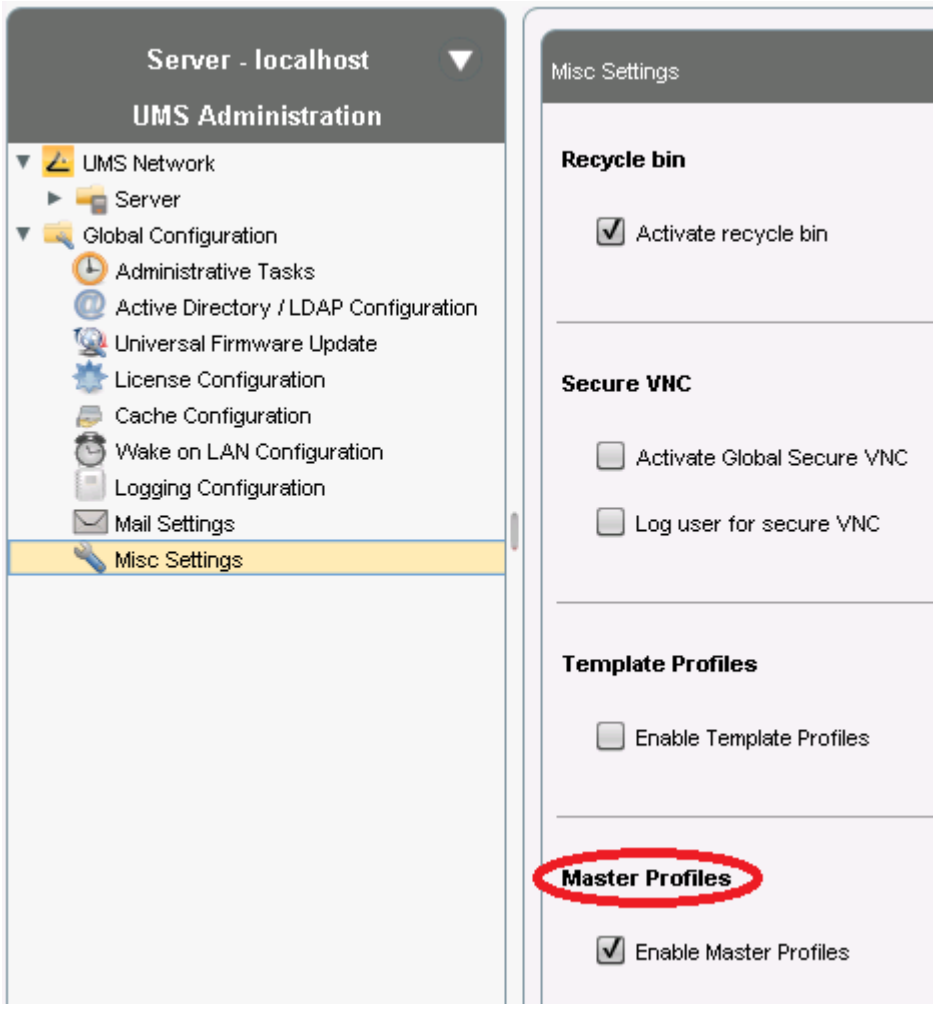
- Enabling Master Profiles (see page 320)

Enabling Master Profiles

You can specify whether or not you would like to use master profiles. By default, they are disabled.

To enable the master profiles function, proceed as follows:

1. In the UMS structure tree, select **UMS Administration > Global Configuration > Misc Settings**.
2. Activate **Enable Master Profiles**.



The node **Master Profiles** appears in the structure tree.

Template Profiles

Menu path: Structure tree **> Template Profiles**

> Template profiles have to be enabled first under **UMS Administration > Global Configuration > Misc Settings**, see Activating Template Profiles (see page 323).

A template profile allows you to add variables for individual parameters in the profile and to assign their values to objects.

> Both **standard profiles** and **master profiles** can become template profiles through the use of variables.

Template profiles are used if you would like to avoid having to set up numerous sessions which differ only in terms of a few points.

> Template profiles and template keys cannot be used if Shared Workplace (see page 594) is deployed.

Example

A company's devices are spread across a number of sites. All devices are to receive a browser session with the same settings via a profile, but a different start page is to be configured in the global settings for each site. It should also be possible to choose an individual session name for each site.

Previous Solution

A dedicated profile with global settings and session data was created for each site.

Problem

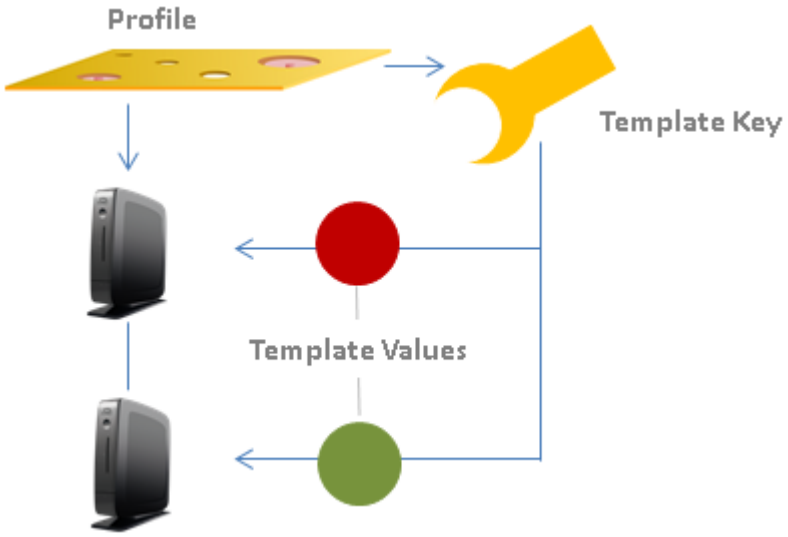
In many cases, the desired settings cannot be combined via various profiles, see free instances (see page 279). The unnecessarily large number of profiles is also difficult to manage in the long term.

Solution

The use of a single template profile offers greater flexibility. This contains all data for the browser session which are common to the devices as well as placeholders, so-called template keys (see page 324). The template keys contain parameters that are to receive divergent values for different devices at different sites. In addition, there are static template keys that receive their values from the device.

The template profile is assigned to all devices. The site-relevant template values are assigned to the particular devices that are to receive this value.

The device thus receives a profile whose settings are made up of fixed parameter values updated in the profile and the template values assigned to it that are referenced by template keys in the profile.



Rules:

- Template keys are used in one or more profiles.
- A template key has a number of values.
- The template profile is assigned directly or indirectly to a number of devices.
- A value from the key can be assigned to one or more devices directly or indirectly.

A device thus receives not only general profile settings but also the template value assigned to it for the configuration parameter which is represented in the profile by the associated template key as a placeholder.

IGEL TechChannel

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

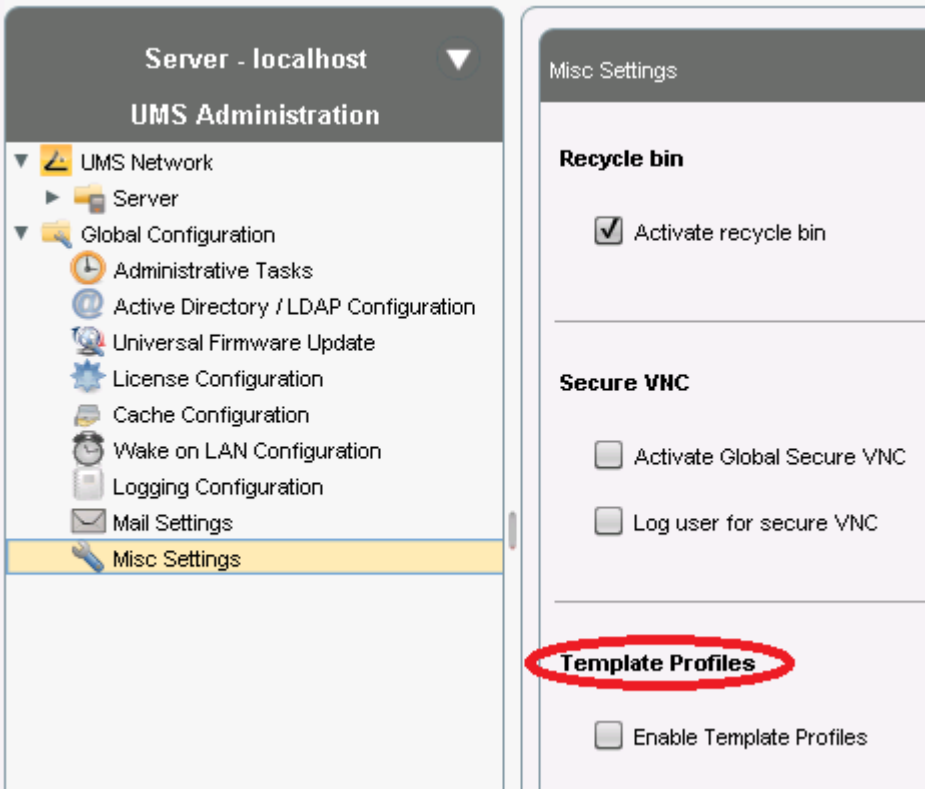
https://www.youtube.com/watch?v=uJnIK5u688c

- Activating Template Profiles (see page 323)
- Creating Template Keys and Values (see page 324)
- Using Template Keys in Profiles (see page 330)
- Assigning Template Profiles and Values to the Devices (see page 332)
- Value Groups (see page 334)
- Export Template Keys and Value Groups (see page 336)
- Import Template Keys and Value Groups (see page 337)

Activating Template Profiles

If you would like to use the template profiles function, you must enable it first:

1. In the UMS Console, go to **UMS Administration > Global Configuration > Misc Settings**.
2. Activate **Enable Template Profiles**.

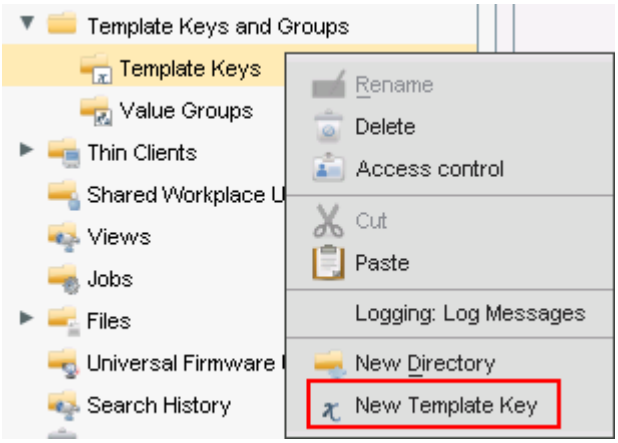


The **Template Keys and Groups** node appears in the UMS structure tree.

Creating Template Keys and Values

To create template keys and values, proceed as follows:

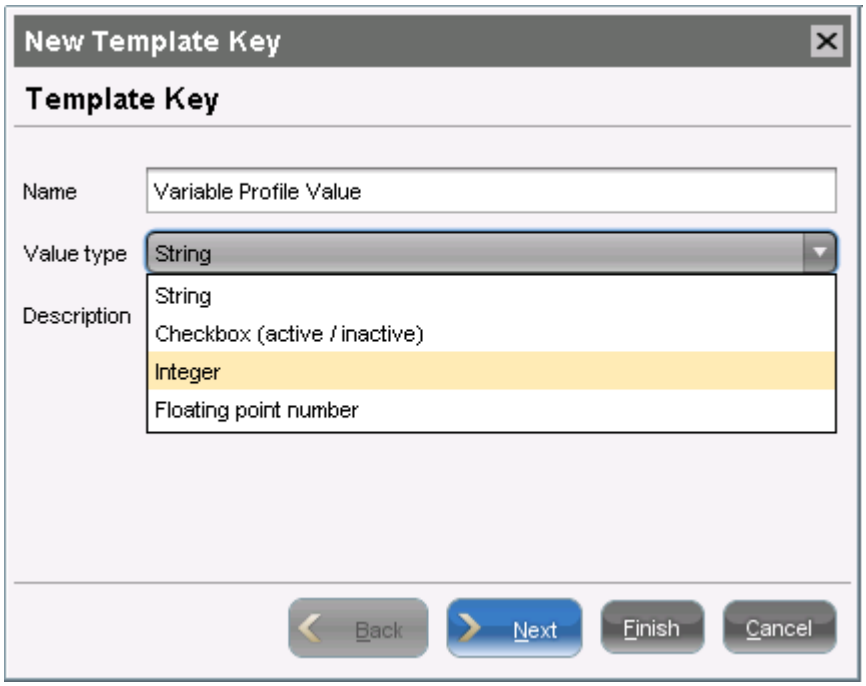
1. Open the context menu for the **Template Keys** folder.
2. Click on **New Template Key**.



> Alternatively, this function is also accessible via the menu **System>New>New Template Key**, the focus must be on the **Template Keys** node.

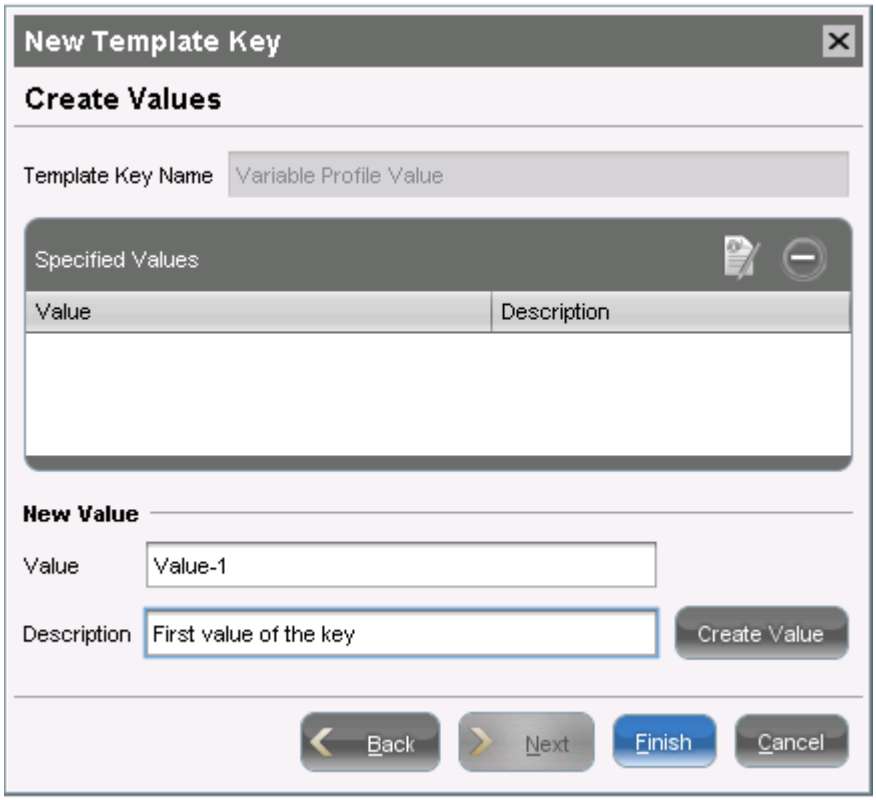
An assistant will guide you through the steps for creating a new template key:

3. Define a **name** for the key.
4. Select a **value type** for the key (String, Checkbox, Integer or Floating point number).
5. Optionally, give a **description** of the key.
6. Click on **Next**.



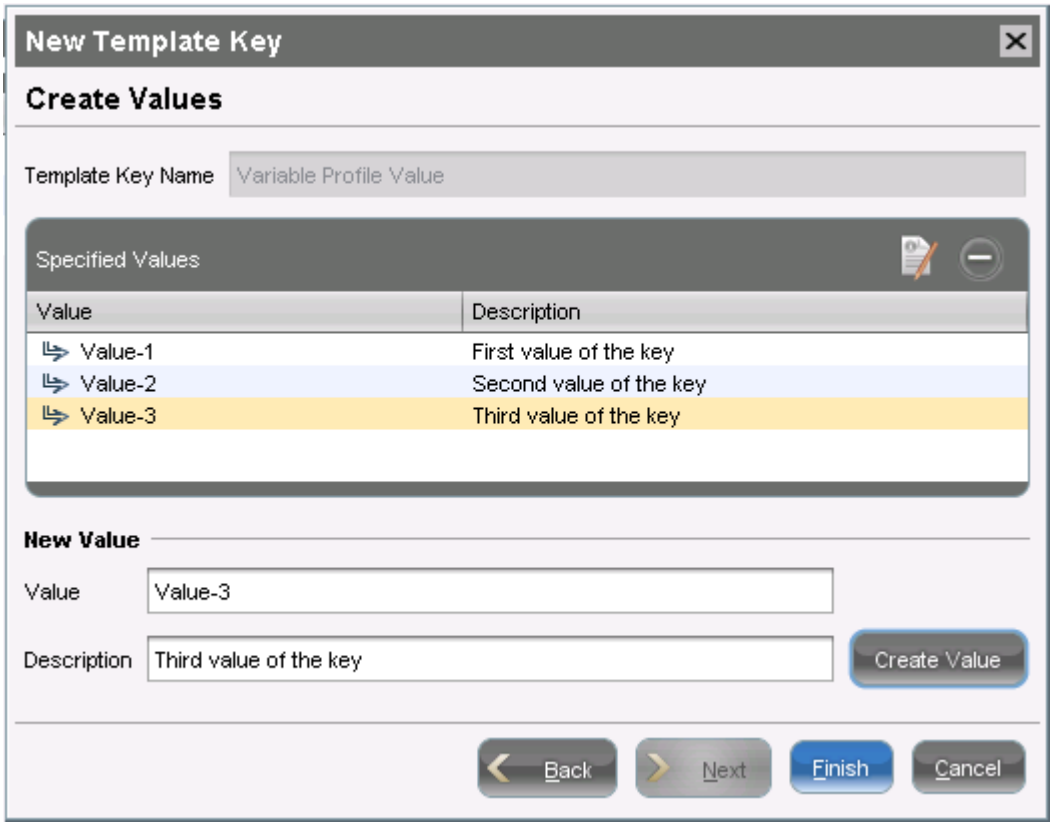
To specify the first value of the key, proceed as follows:

1. Enter the desired parameter value in the **Value** field.
2. Optionally, add a **description** of the value.
3. Click on **Create Value**.

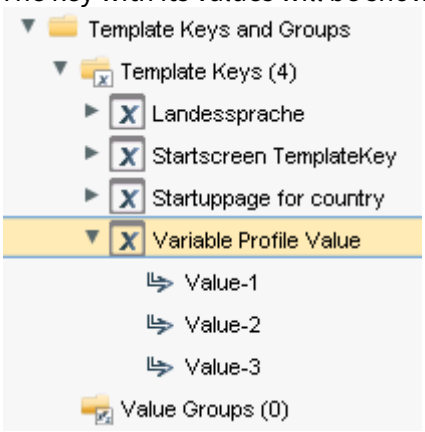


To specify further values for the key, proceed as follows:

1. Change the entries under **Value** and **Description**.
2. Click again on **Create Value**.
3. Click on **Finish** to save the key with its values once you have created all desired values.



The key with its values will be shown in the tree:



The recommended workflow is to create template keys and values from the profile configuration (see page 328).

Creating Keys and Values in the Profile

In profiles, specific parameters with a template key can be configured. To do this, combine the following steps to form a workflow:

- Create template keys and values
- Use template keys in profiles

To use template keys when configuring a profile, proceed as follows:

1. Open an existing profile or create a new profile.
2. Click on **Edit Configuration** in order to bring up the parameters to be updated.
3. Select a parameter which is to obtain a client-specific value from a template key.
4. Click the activation symbol in front of the parameter until the desired function is active (here: ):

		The parameter is inactive and will not be configured by the profile.
		The parameter is active and the set value will be configured by the profile, template keys are not available for the parameter.
		The parameter is active and the set value will be configured by the profile, template keys are available for the parameter.
		Template keys are active for this parameter, the profile receives a value from the key later on.

> Certain parameters cannot be configured with template keys and only offer the option *inactive* or *active*. This applies for example to passwords or parameters which depend on other configuration settings.

5. Click on the **selection symbol**  in order to select a template key.
6. Click on **Add**  to create a new template key.
   An assistant will guide you through the steps for creating a new template key:
7. Give a **name** for the key.

> The **value type** for the key is stipulated by the parameter.

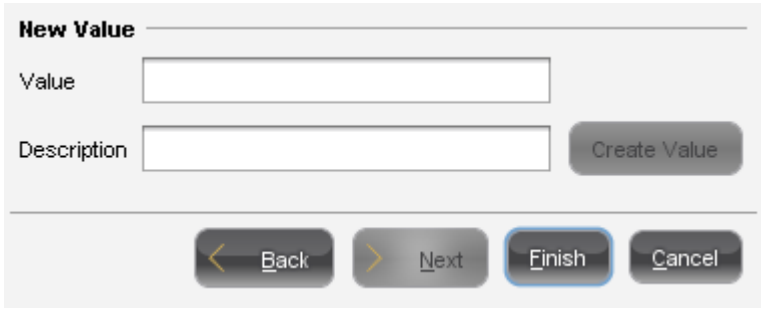
8. Optionally, give a **description** of the key.

9. Click on **Next**.

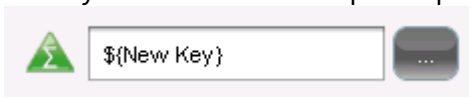
To enter the first value of the key, proceed as follows:

1. Define the desired parameter value in the **Value** field.
2. Optionally, add a **description** of the value.
3. Click on **Create Value**.

> In the case of parameters with a fixed value range such as selection menu or checkbox, the available options will be provided for selection. Click on **Add all** to create values for each entry in the value range or **Create Value** to add selected entries only.



4. Click on **Finish** to save the key with its values.
5. Click on **OK** to return to the profile.
   The key will be shown in the profile parameter:



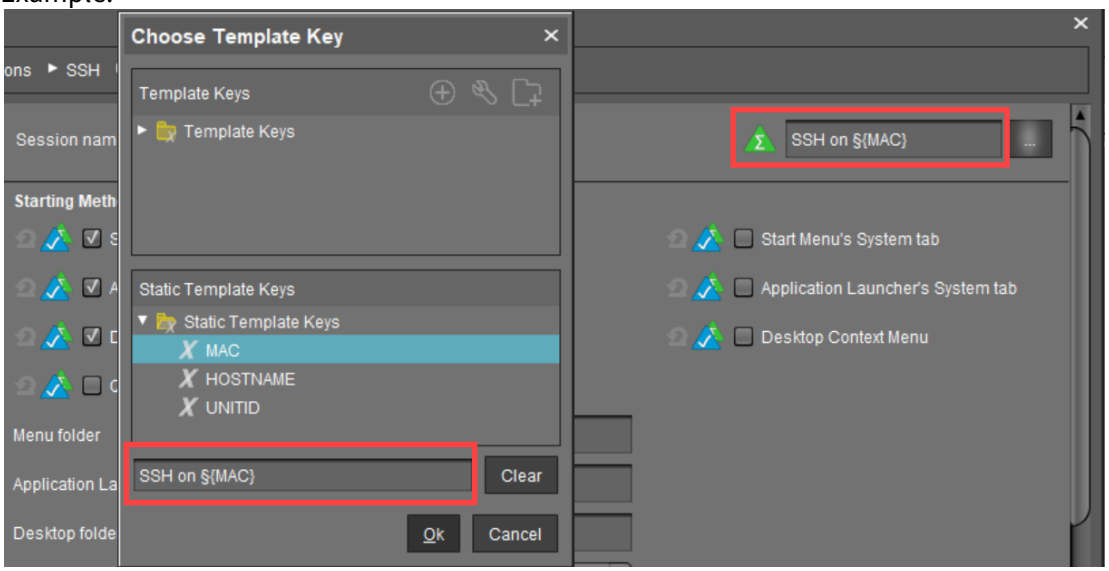
6. **Save** the template profile.
   Profiles which use at least one template key in the configuration are labeled with a special symbol in the navigation tree:  .

Using Template Keys in Profiles

Template keys are listed in the **Template Keys and Groups / Template Keys** node in the structure tree. They can be moved to their own sub-folders.

Static template keys are not visible in the structure tree; their values are received directly from the device. Static template keys are marked with the § symbol. The following static template keys are available:

- **MAC**: MAC address of the device
- **HOSTNAME**: Host name of the device
- **UNITID**: Unit ID of the device
  Example:



To use a template key in the profile, proceed as follows:

1. Open an existing **profile** or create a new profile.
2. In the profile configuration, bring up the parameters to be updated.
3. Now select a parameter which is to be supplied with client-specific values from a **template key**.
4. Click the **activation symbol** in front of the parameter until the desired function is active –  :

	The parameter is inactive and will not be configured by the profile.
	The parameter is active and the set value will be configured by the profile, template keys are not available for the parameter.
	The parameter is active and the set value will be configured by the profile, template keys are available for the parameter.

	Template keys are active for this parameter, the profile receives a value from the key later on.
	Reset to the default value.

> Certain parameters cannot be configured with template keys and only offer the option *inactive* or *active*. This applies for example to passwords or parameters which depend on other configuration settings.

5. Click on the selection symbol  to choose a template key.
6. Double-click on the desired template key or static template key. Alternatively, you can create a new key, see Create template keys and values in the profile (see page 328).
7. Click on **OK**.
8. **Save** the template profile.
9. You can also combine template keys:

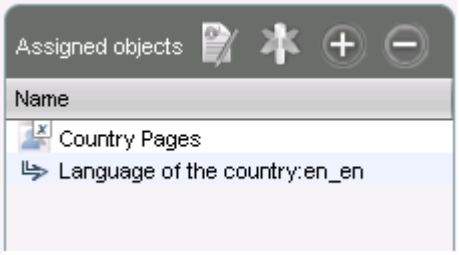
Profiles which use at least one template key in the configuration are labeled with a special symbol in the structure tree:  .

Assigning Template Profiles and Values to the Devices

Once you have created the **template keys** and **values** and configured **profiles** using the template keys, you will need to bring together the keys and values again on the device.

To assign to a device a template profile and the values needed to replace the keys, proceed as follows:

1. Select a **template profile** and assign it in the usual manner to a group of devices or a device directory.
2. Select a **value** for each **template key** used in the profile.
3. Assign the relevant values to the corresponding devices.



4. Assign further key values to further devices. Several values for various keys can also be assigned collectively ([Shift]and [Ctrl] keys).

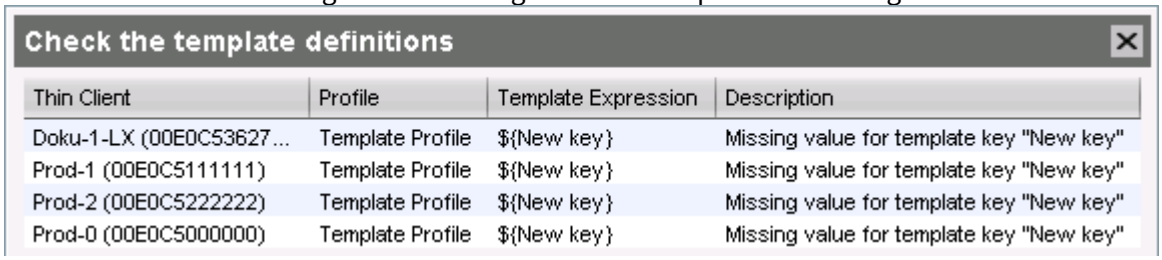
> Each device must then have an assigned value for each key in the assigned profiles.

To check that template profiles and values have been assigned correctly, proceed as follows:

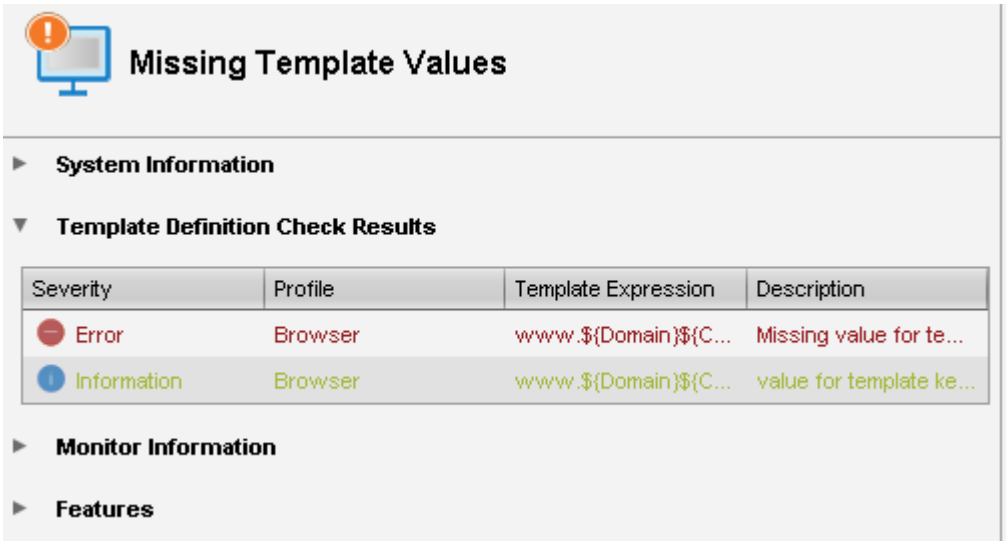
1. Click on **Devices** in the top menu bar.
2. Select **Check the Template Definitions**.
   The selected and checked devices are flagged according to the result:

	all template keys are defined
	missing template keys

3. Double-click on the message in the message window to open the error log for the check function:



   Or click on a device and the results of the check will be shown immediately:



As soon as the devices receive their updated profile settings (e.g. automatically after restarting the devices), the keys contained in the profile for each device will be replaced by the corresponding value from their assignment to the device and then transferred to the device. The local device setup thus receives only the usual parameter values and no more keys.

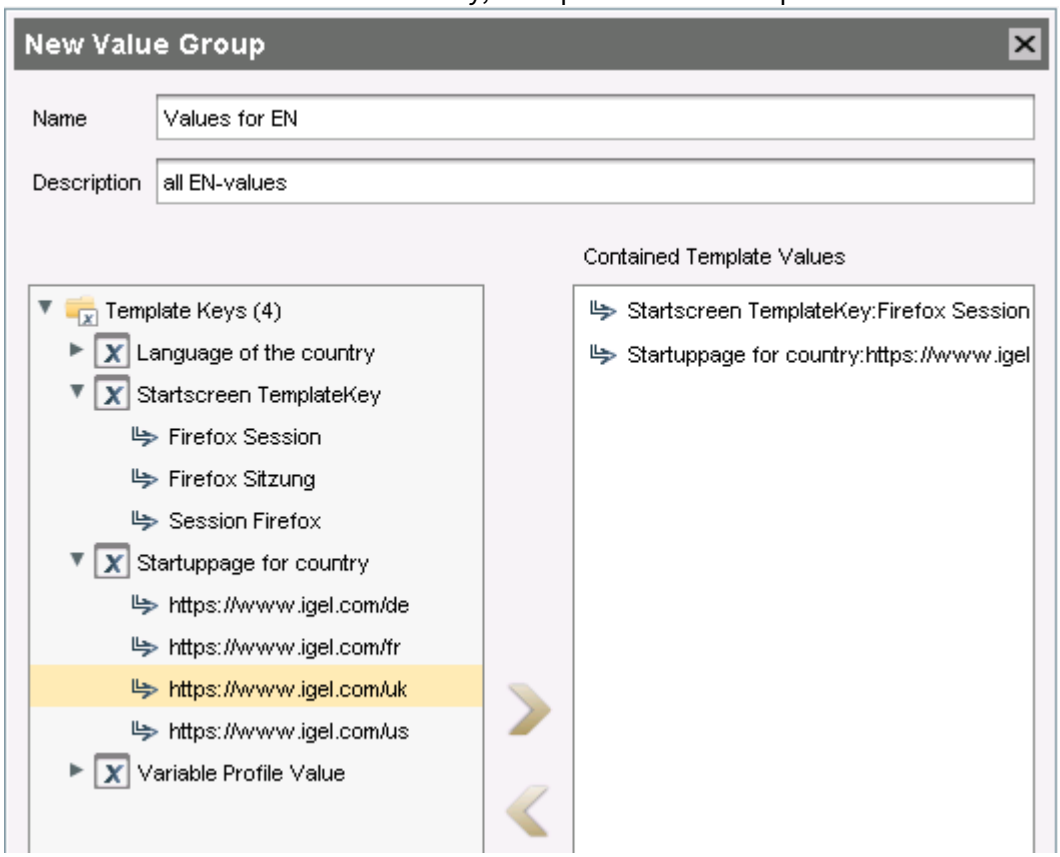
Value Groups

In value groups, logically associated values from various template keys can be brought together and assigned together to devices.

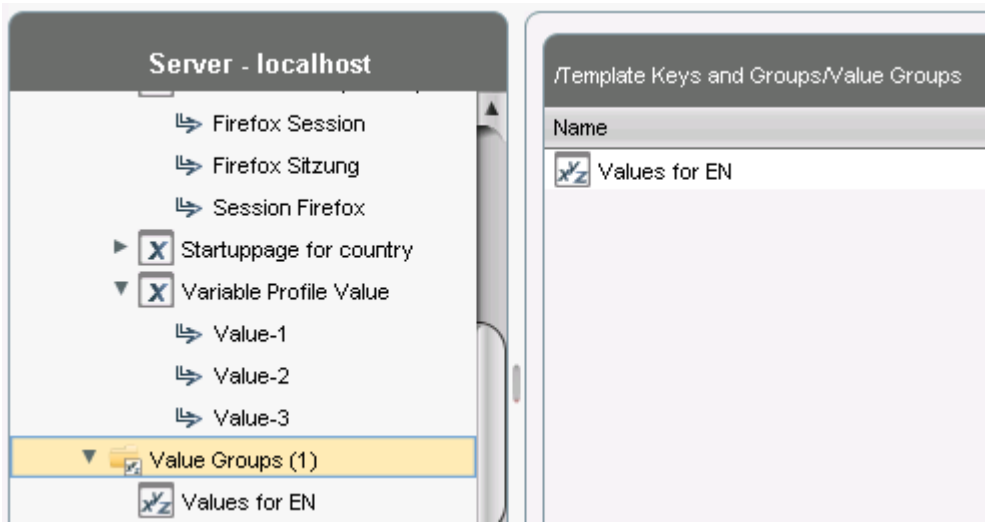
If for example you have various profiles which are to receive country-specific settings via template keys and value assignments, all values for a country / a language can be grouped in a value group. When such a group is assigned, a device also receives all values for its country / its language contained in it.

To create a group, proceed as follows:

1. Create a **template profile** with keys and values.
2. Click on **System>New>New Value Group** in order to create a new value group.
3. Enter a **name** and description for the group.
4. Select the desired values from each key, multiple selections are possible.



5. Confirm your settings by clicking on **OK**.
6. Create further groups.



7. Assign the template profile to all devices.
8. Assign the appropriate group in each case to the devices.
9. Highlight the **Devices** tree node.
10. Click on **Devices>Check the Template Definitions** in order to check the definitions.
    The result is shown in the message window.

After the next restart or a manual transfer, the devices will receive the new session data with shared and country-specific profile settings.

> The advantage of this method is that you only need to add further key values to the relevant value group in the future in order to assign these to the site's devices. In addition, a better overview is possible if there are a large number of template keys and values.

Export Template Keys and Value Groups

Menu path: **System > Export > Export Template Keys and Value Groups**

You can export template keys and value groups in the UMS database in order to import them to another UMS installation.

To export template keys and value groups, proceed as follows:

1. If you would like to preselect template keys, value groups or directories, highlight the desired items in the navigation tree.
2. Go to **System** > **Export** > **Export Template Keys and Groups**.
   In the **Export Template Keys and Groups** window, the template keys and value groups previously selected or all available template keys and value groups will be shown.
3. In the **Export** column, select the template keys and value groups that you want to export.
4. Click on **Next** and select a save location.
5. Click on **Done**.
   The template keys and value groups will be saved in a ZIP archive.

Import Template Keys and Value Groups

Menu path: **System > Export > Import Template Keys and Value Groups**

You can import template keys and value groups. In order for this to be possible, the template keys which are to be imported must not yet exist in the UMS database. Each template key has a unique name which may only be used once in a UMS database.

To import template keys and value groups, proceed as follows:

1. In the navigation tree, highlight the directory in which the template keys and value groups are to be placed.

   > ⓘ If you would like to import template keys and value groups in a single step, please note the following: If a directory below **Template Keys** is selected, the template keys will be placed in the selected directory and the value groups in the **Value Groups** directory. If a directory below **Value Groups** is selected, the value groups will be placed in the selected directory and the template keys in the **Template Keys** directory.

2. Go to **System** > **Import** > **Import Template Keys and roups**.
3. Select the file with the template keys and value groups and click on **Open**.
   The **Template keys and value groups** window will open.
4. In the **Import** column, select the template keys and value groups that are to be imported.
5. With the **Create path relative to the directory currently selected** option, specify whether the directory structure of the imported template keys and value groups is to be retained:
   ☑ The directory structure of the imported template keys and value groups will be retained, i.e. the exported subdirectories will be restored. (default)
   ☐ The directory structure of the imported template keys and value groups will be ignored, i.e. all template keys and value groups will be placed on the highest directory level.
6. Click on **OK**.
   Once all template keys and value groups have been imported, a confirmation will be shown.
   If not all template keys and value groups could be imported, the template keys and value groups for which the import failed will be shown.

Mobile-Device Profiles

With UMS 5.09.100, as part of the UMS extension IGEL Mobile Device Management Essentials (MDM), **mobile-device profiles** were introduced, see the MDM Manual (see page 621) for detailed information on this profile type.

Firmware Customizations

Menu path: **Structure Tree > Firmware Customizations**

From UMS *Version 5.05.100*, you can customize the user interface of your IGEL OS devices to suit your CD (corporate design) through firmware customization. The configuration takes place in a dedicated wizard; for a minimal configuration, only a name and a file object need to be specified.

Mode of Action

A firmware customization can be assigned to a device or a directory.

Firmware customizations override normal profiles but in turn can be overridden by master profiles. They are therefore between master profiles and standard profiles in terms of their priority.

Further information regarding the prioritization of profiles can be found under Prioritization of Profiles (see page 304).

If several applications cases of the same type are assigned to a device, e.g. a background image, only the Use case with the highest priority will be effective. The priority is determined by how direct or indirect the assignment to the device is: A firmware customization assigned directly to the device has a higher priority than one which is assigned to the directory of the device. If both firmware customizations have the same priority, the firmware customization with the higher ID will be effective.

> In order to obtain the ID of a firmware customization, move the mouse pointer over the relevant object in the structure tree.

_____

Create Firmware Customization

To create a **Firmware Customization**, proceed as follows:

1. Move the cursor to **Firmware Customization** in the structure tree.
2. Select **Create New Firmware Customization** in the context menu.
   The **Firmware Customization Details** dialog window will appear.
3. Give a **Name** for this firmware customization.
4. Select an **Use case**. The following can be selected:
   - Start Button (see page 341)
   - Start Menu (see page 342)
   - Taskbar Background (see page 343)
   - Screensaver (see page 344)
   - Screensaver (Custom Partition) (see page 345)
   - Bootsplash (see page 347)
   - Background Image (see page 348)
5. Click on **Next**.
   The **Firmware customization assignment** dialog window will appear.
6. Highlight one or more directories or devices and click on  in order to assign the firmware customization.
7. Click on **Done**.

The firmware customizations created are listed in the structure tree under the **Firmware customizations** node. If you click on a firmware customization, the associated files and assigned objects will be shown.

The files used in a firmware customization are marked with a  .

> If you want to delete a file marked with  , you must first remove it from the associated firmware customization.

The settings for an Use case can be enabled or disabled for a firmware customization as you will already know from the profiles:

	The parameter is inactive and will not be configured by the firmware customization.
	The parameter is active and the set value will be configured by the firmware customization.

> Exception: The file path for screensaver (custom partition) cannot be disabled.

Start Button

Firmware Customization Details

- **Name**: Name of the firmware customization
- **Use case**: “Start button”
- **Image**: Name of the selected image file
- **Choose file**: All files registered in the UMS in a suitable format (*.png, *ico) and for which your have authorizations are shown here.
- **Upload file**: Select a file from a local directory or from the UMS Server.
- **Clear**: Deletes the image file shown under **Image**.

Firmware Customization Assignments

Assignment of the devices for which the customizations are to apply.

Start Menu

Firmware Customization Details

- **Name**: Name of the firmware customization
- **Use case**: “Start menu”
- **Image**: Name of the selected image file
- **Select file**: All files registered in the UMS in a suitable format (*.jpg, *bmp, *png) and for which your have authorizations are shown here.
- **Upload file**: Select a file from a local directory or from the UMS server.
- **Delete**: Deletes the image file shown under **Image**.

Firmware Customization Assignment

Assignment of the devices for which the customizations are to apply.

Taskbar Background

Firmware Customization Details

- **Name**: Name of the firmware customization
- **Use case**: “Taskbar background”
- **Image**: Name of the selected image file
- **Choose file**: All files registered in the UMS in a suitable format (*.jpg, *bmp, *png) and for which your have authorizations are shown here.
- **Upload file**: Select a file from a local directory or from the UMS server.
- **Clear**: Deletes the image file shown under **Image**.

Firmware Customization Assignment

Assignment of the device for which the customizations are to apply.

Screensaver

Firmware Customization Details

- **Name**: Name of the firmware customization
- **Use case**: “Screensaver”
- **Image**: Name of the selected image files
- **Choose file**: All files registered in the UMS in a suitable format (*.jpg, *bmp, *png) and for which your have authorizations are shown here.
- **Upload file**: Select a file from a local directory or from the UMS server.
- **Clear**: Deletes the image file shown under **Image**.
- **Display mode**: Type of display.
  Possible options:
  - next to each other small
  - next to each other medium
  - centered in the middle
  - cut
- **Screen mode**:
  - One image per monitor
  - One image for all monitors (stretched if necessary)
- **Display time**: Time in seconds that an image is shown before it switches. (default: 10)
- **Start**
  Possible options:
  - Start screensaver automatically
  - Do not start screensaver automatically
- **Start time**: Time in minutes until the screensaver starts. (default: 5)
- **Background color**: (default: black)
  - **Choose color**: Color selection according to color spaces
    Possible color spaces:
    Swatches
    HSV
    HSL
    RGB
    CMYK

Firmware Customization Assignment

Assignment of the devices for which the customizations are to apply.

Screensaver (Custom Partition)

Firmware Customization Details

- **Name**: Name of the firmware customization
- **Use case**: “Screensaver (custom partition)”
- **Images**: Names of the selected image files
- **Choose file**: All files registered in the UMS in a suitable format (*.jpg, *bmp, *png) and for which your have authorizations are shown here. You can select a number of images here.
- **Upload file**: Select a file from a local directory or from the UMS server.
- **Clear**: Deletes the selected image files.

File path (custom partition + folder): File path of a folder on the custom partition (example: `/custom/screensaver`).

> The custom partition must be created beforehand so that the images can be added to it. If no custom partition has been created, the images will be saved in the RAM and will be reloaded each time that the system boots. The folder does not need to be created beforehand, it will be created if necessary. Ensure that the path begins with a `/`.

- **Display mode**: Type of display. The following can be selected:
  - Small, jumping
  - Medium, jumping
  - Filled
  - Fit in
- **Image mode**:
  - One image per monitor
  - One image for all monitors (stretched if necessary)
- **Display time**: Time in seconds that an image is shown before it switches. (default: 10)
- **Start**
  Possible options:
  - Start screensaver automatically
  - Do not start screensaver automatically
- **Start time**: Time in minutes until the screensaver starts. (default: 5)
- **Background color**: (default: black)
  - **Choose color**: Color selection according to color spaces
    Possible color spaces:
    Swatches
    HSV
    HSL
    RGB
    CMYK

Firmware Customization Assignment

Assignment of the devices for which the customizations are to apply.

Bootsplash

Firmware Customization Details

- **Name**: Name of the firmware customization
- **Use case**: "Bootsplash"
- **Image**: Name of the selected image file
- **Choose file**: All files registered in the UMS in a suitable format (*.jpg, *bmp, *png) and for which your have authorizations are shown here.
- **Upload file**: Select a file from a local directory or from the UMS server.

  > For the bootsplash, the device obtains the selected file from the UMS via HTTPS as soon as it is required.

- **Clear**: Deletes the image file shown under **Image**.
- **Horizontal position**: Horizontal position of the bootsplash. (default: 50%)
- **Vertical position**: Vertical position of the bootsplash. (default: 50%)
- **Progress horizontal position**: Horizontal position of the progress bar. (default: 90%)
- **Progress vertical position**: Vertical position of the progress bar. (default: 90%)

Firmware Customization Assignment

Assignment of the devices for which the customizations are to apply.

Background Image

Firmware Customization Details

- **Name**: “Background image”
- **Use case**: “Background image”
- **Background monitor 1-8**: Name of an image file for up to 8 monitors
- **Choose file**: All files registered in the UMS in a suitable format (*.jpg, *bmp, *png) and for which your have authorizations are shown here.
- **Upload file**: Select a file from a local directory or from the UMS server.

  > For the background image, the device obtains the selected file from the UMS via HTTPS as soon as it is required.

- **Clear**: Deletes the image file shown under **Background monitor 1-8**.

Firmware Customization Assignment

Assignment of the devices for which the customizations are to apply.

Export Firmware Customizations

Menu path: **System > Export > Export Firmware Customizations**

You can export firmware customizations. The data exported contain all necessary settings and files.

To export firmware customizations, proceed as follows:

1. If you would like to preselect firmware customizations, highlight the desired firmware customizations or directories in the navigation tree.
2. Go to **System** > **Export** > **Export Firmware Customizations**.
   In the **Export Firmware Customizations** window, the previously selected firmware customizations or all available firmware customizations will be shown.
3. In the **Export** column, select the firmware customizations that you want to export.
4. Click on **Next** and select a save location.
5. Click on **Finish**.
   The firmware data will be saved in a ZIP archive.

Import Firmware Customizations

Menu path: **System > Import > Import Firmware Customizations**

You can import firmware customizations. The imported data contain not only the settings but also all required files.

To import firmware customizations, proceed as follows:

1. Highlight the directory where the firmware customizations are to be placed.
2. Go to **System** > **Import** > **Import Firmware Customizations**.
3. Select the file with the firmware customizations and click on **Open**.
   The **Import firmware customizations** window will open.
4. In the **Import** column, select the firmware customizations that are to be imported.
5. With the **Create path relative to the directory currently selected** option, specify whether the directory structure of the imported firmware customizations is to be retained:
   ☑ The directory structure of the imported firmware customizations will be retained, i.e. the exported subdirectories will be restored. (default)
   ☐ The directory structure of the imported firmware customizations will be ignored, i.e. all firmware customizations will be placed on the highest directory level.
6. Click on **OK**.
   Once all firmware customizations have been imported, a confirmation will be shown.
   If not all firmware customizations could be imported, the firmware customizations for which the import failed will be shown.

Devices

Menu path: Structure tree **> Devices**

In the **Devices** area, you can manage end devices registered on the UMS Server. All devices registered on the UMS Server are shown.

The name of a device shown in the structure tree is used for identification in the UMS and does not need to be identical to the name of the device in the network. The name shown in the structure tree does not need to be unique and can be used a number of times.

The unit ID serves as a unique identifier. With IGEL devices, IGEL zero clients, devices with the IGEL UDC and devices with the IGEL UMA, the unit ID is assigned the MAC address of the device.

You can structure the **Devices** area by creating directories and, possibly, sub-directories. When doing so, you should bear in mind that each device can only be shown once in the structure tree. You can move a device by dragging and dropping it from one directory to another.

Icons for an IGEL Device

The following icons in the structure tree show the status of an IGEL device:

When the device is connected via IGEL Cloud Gateway (ICG), a cloud symbol icon  is added to the device.

	The device is online. Please note that **Misc > Settings > Online Check** must be activated for indicating the online status.
	The device is offline. Please note that **Misc > Settings > Online Check** must be activated for indicating the online status.
	Changes have not yet been transferred to the device (possible with all statuses).

As of IGEL OS 10.03.100, the following status displays are offered. In order to make them visible, the **Devices send updates** option must be enabled (default). To do this, go to **UMS Administration > Global Configuration > Device Network Settings > Advanced Device's Status Updates**.

	The device is showing the login screen (if configured).
	The device is being updated.
	The UMS has no license for the device.
	The device has never been registered.

The UMS monitors the status of the devices by regularly sending UDP packets. In accordance with the preset, this occurs every 3 seconds. You can specify the interval for the online check in the **Misc > Settings > Online Check** menu. You can also update the status manually.

Icons for a UD Pocket

The following icons in the structure tree show the status of a UD Pocket:

	The registered UD Pocket (no further information is available at the moment).
	The UD Pocket is online. Please note that **Misc > Settings > Online Check** must be activated for indicating the online status.
	The UD Pocket is offline. Please note that **Misc > Settings > Online Check** must be activated for indicating the online status.
	The UD Pocket is showing the login screen (if configured).
	The UD Pocket is being updated.
	The UD Pocket is not licensed.

- Device (see page 353)
- Managing Devices (see page 356)
- Configuring Devices (see page 366)
- Exporting and Importing Data (see page 369)
- Send Immediate Messages (see page 374)
- View Asset Information (see page 376)
- Secure Terminal (Secure Shell) (see page 379)
- Shadowing (VNC) (see page 383)

Device

Menu path: Structure Tree **> Devices >** [Directories] **> [Name of the device]**

This area shows up-to-date information regarding the selected device.

System Information

- **Name**
- **Last IP**
- **Location**
- **Comment**
- **Department**
- **Cost center**
- **Inventory number**
- **Setup and startup**
- **Serial number**
- **[custom attributes]**
- **Unit ID**
- **MAC address**
- **Product**
- **Product ID**
- **Version**
- **Firmware description**
- **IGEL Cloud Gateway**
- **Expiry date of the maintenance subscription**
- **Last start time**
- **Network name at last restart**
- **Runtime since last restart**
- **Runtime since setup and startup**
- Battery Level: The battery level is shown on mobile devices. The display can be updated by clicking on  . This function is available from IGEL OS 10.03.100. The frequency at which the device sends details of the current battery level to the UMS can be set via the setup; further information can be found under Battery Level Control.
- **CPU speed (MHz)**
- **CPU type**
- **Size of the flash memory (MB)**
- **Memory (MB)**
- **Network speed**
- **Duplex mode**
- **Graphic chipset 1**
- **Graphics memory 1 (MB)**
- **Graphic chipset 2**
- **Graphics memory 2 (MB)**
- **Device type**
- **Operating system type**

- **BIOS manufacturer**
- **BIOS version**
- **BIOS date**
- **Boot mode**
- **Serial number of the device**
- **Structure tag**

Template Definition Check Results

- **Type**
- **Profile**
- **Template expression**
- **Description**

Monitor Information

- **Monitor 1**
  - **Vendor**
  - **Model**
  - **Serial Number**
  - **Size**
  - **Native Resolution**
  - **Date of Manufacture**
- **Monitor 2**
  - **Vendor**
  - **Model**
  - **Serial Number**
  - **Size**
  - **Native Resolution**
  - **Date of Manufacture**
- Further monitors, if applicable...

Features

In this area, the features available on the device are listed.

Windows Updates and Hotfixes

In this area, the *Windows* updates and hotfixes installed on the device are listed.

Partial Updates

In this area, the partial updates installed on the device are listed. This information is available from *IGEL Universal Desktop* W7 *Version 3.12.100* and *IGEL Universal Management Suite Version 5.03.100*.

The following information regarding partial updates is shown.

- **Name**
- **Version**
- **Date**
- **Description**

File Transfer Status

As of UMS version 5.09.100 and device Firmware IGEL OS 10.05.100, the transfer status of assigned files is displayed here, regardless of whether they have been assigned directly or indirectly (via Profiles or FWC).

You will receive the following information:

- **Filename**
- **File ID**
- **Classification**: The classification assigned when the file is uploaded, or the use case of the firmware customization or the description of the profile.
- **Status** - possible values:
  - OK
  - Error
  - unknown
- **Status Message**
- **Assigned via**: For directly assigned files, the file name is displayed here, otherwise the name of the profile or of the firmware customization will be displayed.

User Login History

Specific types of user login can be logged in the UMS.

The user logins are logged if the following options are enabled:

- device or profile: **System > Remote management > Options > Log login and logoff events** checkbox
- *UMS*: **UMS Administration > Misc Settings > Enable user logon history** checkbox

If logging is enabled, the following information is saved:

- **User name**
- **Login time**
- **Logout time**
- **Login type**
  The following login types can be logged in the *UMS*:
  - **Shared Workplace**
  - **AD/Kerberos**
  - **Citrix**

Managing Devices

In the IGEL UMS, you can sort devices according to directories via a structure tree. You can use this facility to provide devices forming groups on the basis of their location or structure with the same profiles or to sort the devices in keeping with your company structure.

Actions performed at the directory level apply to all subdirectories and devices contained in this directory.

See also the video with an overview of how to search for devices, add directories, move devices to a directory and create profiles (see page 276) with settings for devices:

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=sXw9GW95dgw&list=PLwmmael4krnP_0oALne0k107MHvB9da3B&index=4

Creating a Directory in the IGEL UMS

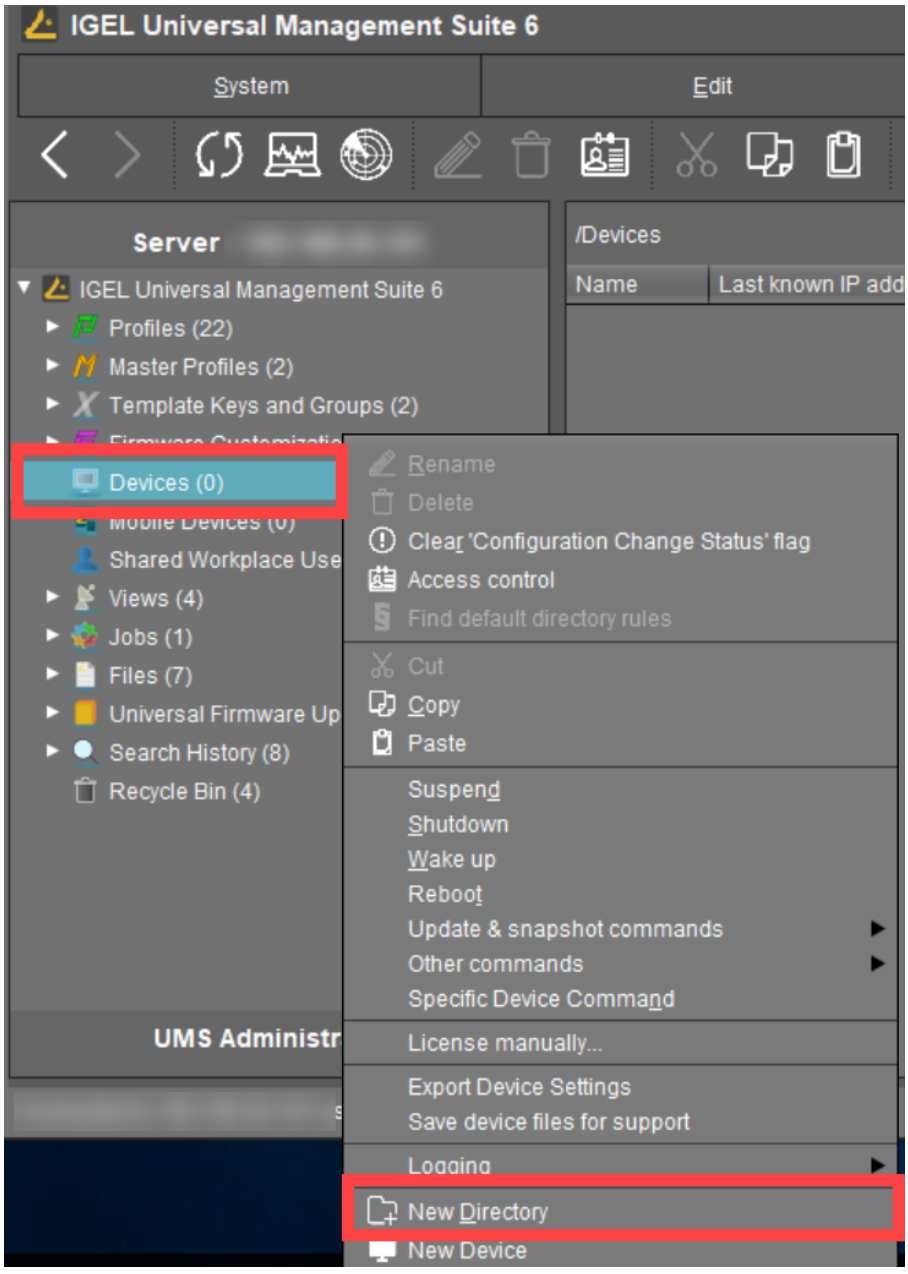
In the IGEL Universal Management Suite (UMS), you can create as many directories and sub-directories as you want in order to group the devices together. When you create sub-directories, the devices organized in it form sub-groups of a group.

> A device that is unequivocally identified by its MAC address can only be stored in a single directory, i.e. only as a member of a single group.

Alternatively, you can import a directory structure, see Importing a Directory (see page 360).

To create a directory or sub-directory, proceed as follows:

1. Select a directory, e.g. **Devices**.
2. Select the option **New Directory** from the context menu of the selected directory
   OR
   Click **System > New > New Directory** in the main menu bar.



3. Enter a name for the new directory. (Max. 100 characters)

4. Click **OK**.
   The new directory will be displayed directly below the selected directory in the structure tree.

You can now move devices to this new directory.

Copying a Device Directory

Menu path: Structure Tree **> Devices >** [Name of the device directory] > Context Menu **> Copy**

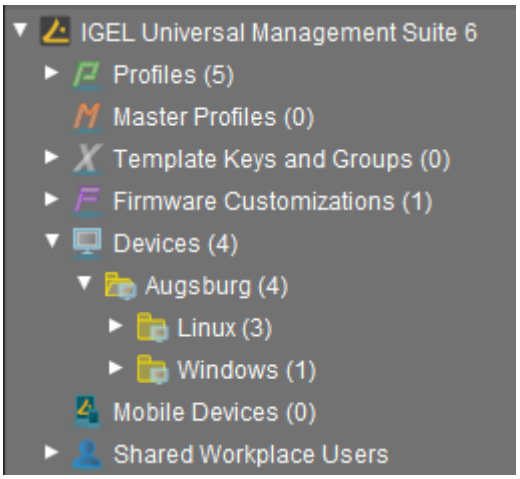
You can copy a device directory and paste it into any directory. Only an empty directory as well as the subdirectories contained in it will be copied; devices cannot be copied.

To copy a device directory, proceed as follows:

1. Click on the directory that you want to copy.
2. Open the context menu for the directory and select **Copy**.
3. Click on the directory in which you would like to paste the copy of the directory. This can also be the directory in which the original directory is located.
4. Open the context menu for the directory and select **Paste**.
   A new device directory which has the same name as the original directory will be created. The new directory will contain newly created copies of the subdirectories contained in the original directory.

Importing a Directory

If you are planning a complex directory structure, you do not need to set it up in a step-by-step manner in the *UMS* Console. Instead, you can create a `csv-` file (e.g. with a spreadsheet program) in which you determine the directory structure and then import the structure from this list.

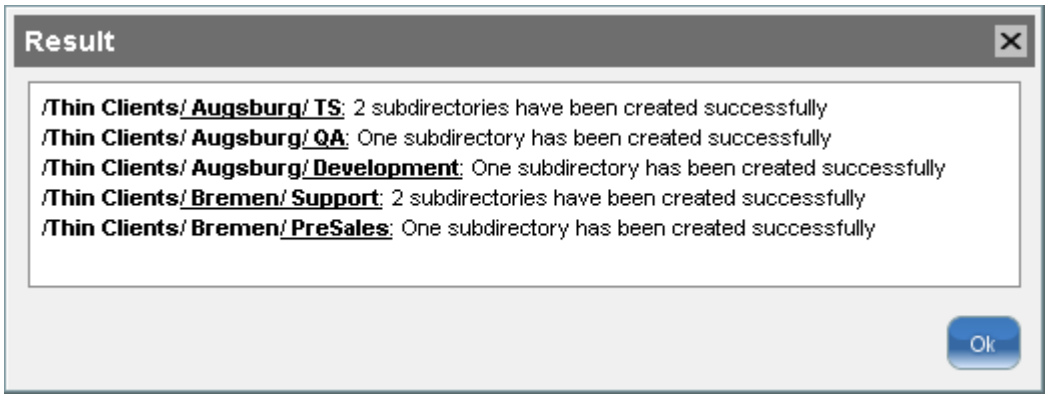


The tree structure shown above is based on the following file:

```
Devices; Augsburg; Linux
Devices; Augsburg; Windows
```

To import a directory structure from a `csv` file, proceed as follows:

1. Select **System > Import > Import Directories** from the main menu.
   The **Import Directories** window will appear.
2. Click **Open File** in order to load a `csv` file.In the first column, you must specify one of the default master directories. In this way, you can also import directory structures for profiles, tasks, views or files.
3. Click **Import Directories** in order to create the directory structure.
   A window showing the result of the import will appear. Any newly created directories will be underlined.


Result
/Thin Clients/ Augsburg/ TS: 2 subdirectories have been created successfully
/Thin Clients/ Augsburg/ QA: One subdirectory has been created successfully
/Thin Clients/ Augsburg/ Development: One subdirectory has been created successfully
/Thin Clients/ Bremen/ Support: 2 subdirectories have been created successfully
/Thin Clients/ Bremen/ PreSales: One subdirectory has been created successfully
Ok

Deleting a Directory

To delete a directory, proceed as follows:

1. Select the directory that is to be deleted.

   > Be sure to delete the directory in the structure tree rather than in the content panel of the console window, otherwise the entire directory path will be deleted at the same time.

2. Click **Delete** in the context menu of the directory
   or click **Delete** in the tool bar
   or press the [Del] button.

   A list of all objects that are to be deleted will appear.

   > If a directory is deleted, all sub-directories and objects such as devices, profiles or views contained in it will be deleted too.

3. Confirm that you wish to delete the relevant objects by clicking **OK**.

Moving Devices

Drag-and-drop is the easiest way of moving devices from one directory to another:

1. Press and hold down the [Ctrl] key if you would like to select a number of devices.
2. Use the [Shift] key to select a row of devices.
3. Confirm that you wish to move the relevant objects by clicking on **Yes**.
   The **Time Changed** window will appear. If profiles are indirectly assigned to a device or revoked as a result of the device being moved to a different directory, its configuration too will change. The new configuration can take effect either immediately or when the device is next rebooted.
4. Select when you want the changes to take effect and confirm this by clicking on **OK**.

You can disable these confirmation dialogs in the relevant window. You can then undo this change again under **Misc > Settings > General.**

Assigning Updates

There are various options for assigning a registered firmware update to a device:

- Directly:
  - using drag & drop
  - using **Assigned Objects** in the device view
- Indirectly:
  - via a directory

> Assigning a firmware update will not trigger the update process. Only the information required for the update will be transferred to the device.

> If you are using a Windows-based device, refer to the chapters Snapshots and Partial Update in the Windows 10 IoT manual.

The update process can be launched in two ways:

- Manually:
  a. Right-click on the device in the UMS structure tree.
  b. From the context menu, select **Update & snapshot commands > Update** or **Update when shutting down**.
- As a job:
  a. Right-click on **Jobs** in the UMS structure tree.
  b. Select **New Scheduled Job** from the context menu.
  c. Enter a **Name**.
  d. As **Command**, select **Update**, or **Update on Boot**, or **Update when shutting down**.
  e. Complete the setup procedure for the job, see Details (see page 404) and Schedule (see page 406).
  f. Assign the job to devices or directories, see Assignment (see page 407).

Default Directories

From *UMS version 5.03.100*, the rules for default directories can be found under **UMS Administration >** Default Directory Rules (see page 484). Information is available for *UMS version 5.03.100* and for the previous versions in the associated chapters in the manual.

Configuring Devices

You can configure a device via the UMS in the following ways:

1. Via **Structure tree > [Device Context Menu] > Edit Configuration**: Here, you can edit the device setup as you would if you were working at the device itself.
2. Via a profile: You assign part-configurations to the device via a profile.
3. Via shadowing with VNC: By shadowing the client, you can work in the setup on the device itself.

You can edit the device configuration locally in the client setup or directly for this client in the IGEL UMS:

▶ Double-click on the device in the structure tree
or select **Edit configuration** from the menu / context menu
or select the corresponding symbol from the symbol bar.

The configuration dialog for a device in the UMS and the profile configuration procedure are structured in the same way as the local setup for a device. Details of this are set out in the relevant manual.

	With a click on this symbol you can reset settings to the default value from UMS version *5.09.100* on.

From UMS Version *5.05.100*, the start page of the configuration dialog contains a link to the page last opened. The  symbol for the link is at the very top of the list of links. A link will also be created if the last page opened belongs to another device or to another profile. If the page last opened is not available in the configuration dialog that is currently open, a link to the next page up in the structure tree will be created. Example: In the configuration dialog for device 1, a setting for the RDP session **My RDP Session** was changed (menu path: **Sessions > RDP > RDP Sessions > My RDP Session**). The configuration dialog for device 2 is then opened but device 2 does not have a session with the session name **My RDP Session**. A link to the higher-level page **RDP Sessions** will therefore be shown (menu path: **Sessions > RDP > RDP Sessions**).

To determine when changes to the configuration are to take effect, proceed as follows.

1. Change the configuration.
2. Click on **Save**.
3. Select when the settings are to take effect.
   - **Next Reboot**: The device will automatically retrieve its settings each time it boots.
   - **Now**: The settings will be transferred to the device immediately.

   If the device is not switched on, this operation cannot be performed and the device will be given its settings the next time it reboots. In both cases, the settings will initially be saved in the database.

   If you have selected **Immediately**, a pop-up dialog will ask the user whether the new settings should take effect immediately. You can change the user message using the following two registry parameters:

`userinterface.rmagent.enable_usermessage` and `userinterface.rmagent.message_timeout`.

Copying a Session

You can copy a session in the configuration dialog of a device. This creates a duplicate with all properties of the original session.

To copy a session, proceed as follows:

1. Open the configuration dialog via **Structure tree > Devices > [Directory]** by double-clicking on the device.
2. In the configuration dialog, select **Sessions > [Session Type] > [Sessions of the Session Type]**.
   Example: **RDP sessions**
   The sessions already set up are shown.
3. Highlight the session that you want to copy.
4. Click  .
   A duplicate of the original session will be created and pasted below.

> From *UMS Version 5.03.100*, you can also copy a session via the context menu in the structure tree of the device configuration.

Exporting and Importing Data

You can export and import data for devices. The settings and parameters are saved in an XML format.

Export Firmwares

Menu path: **System > Export > Export Firmwares**

You can export the data for specific firmware versions. The exported data contain all settings parameters which are available in the UMS and in the local setup.

To export firmware data, proceed as follows:

1. Go to **System** > **Export** > **Export Firmwares**.
   In the **Export firmwares** window, all available firmware data will be shown.
2. In the **Include** column, select the firmware data that you want to export.
3. With **Create archive**, specify how the firmware data are to be saved:
   - ☑ The firmware data will be saved as a ZIP archive.
   - ☐ Each firmware data set will be saved in a file of its own.
4. Click on **OK** and select a save location.
5. Click on **Save**.
   The firmware data will be saved.

Import Firmwares

Menu path: **System > Import > Import Firmwares**

You can import the configuration data for specific firmware versions. The firmware configuration data contain all settings parameters that are available in the UMS and in the local setup of the device. These firmware data are needed to create profiles and when importing devices.

To import firmware data, proceed as follows:

1. Go to **System** > **Import** > **Import Firmwares**.
2. Select the file with the firmware data and click on **Open**.
   If you have selected an individual file, the firmware data will be imported immediately.
3. If you have selected a ZIP archive, select the firmware data to be imported and click on **OK**.
   The imported firmware data will be shown in the **Results** window.

Export Device Settings

Menu path: **System > Export > Export Device Settings**

You can export device settings. All changed settings are saved in the exported file, i.e. all settings which deviate from the default values.

To export device settings, proceed as follows:

1. If you would like to preselect device settings, highlight the desired devices or directories in the structure tree.
2. Go to **System** > **Export** > **Export Device Settings**.
   In the **Export Device Settings** window, the previously selected devices or all available devices will be displayed.
3. In the **Include** column, select the devices whose settings you want to export.
4. With **Create archive**, specify how the settings are to be saved:
   ☑ A dedicated XML file will be created for each device. The XML files will be combined in a ZIP archive.
   ☐ The settings for all devices will be saved in a single XML file.
5. Click on **OK** and select a save location.
6. Click on **Save**.

Import Devices as Profiles

Menu path: **System > Import > Import Devices as Profiles**

You can import device settings as profiles. In order for this to be possible, the settings must have been exported with **System** > **Export** > **Export Device Settings**; see Export Device Settings (see page 372).

To import device settings as profiles, proceed as follows:

1. Go to **System** > **Import** > **Import Devices as Profiles**.
2. Select the file with the settings and click on **Open**.
   The **Import Devices as Profiles** window will open.
3. In the **Import** column, select the settings that are to be imported.
4. In the **Firmware (selectable)** column, select the firmware on which the profile will be based. (default: the firmware installed on the device when the export takes place)
   The profiles are set up in the **Profiles** directory. The name of each profile is identical to the name of the device from which the settings originate.
   The profiles created from the import are shown in the **Results** window.

Send Immediate Messages

Menu path: **Structure tree > Devices > [Directories] > [Name of the device] > Other Commands > Send Message**

From UMS Version 5.07.100, an editor which helps you to write immediate messages in HTML or rich text format is available. You can use this service to send device users messages via remote access. This is possible via the UMS or via ICG.

You can launch the editor via the context menu in the **Device** node or via the main menu: **Devices > Other Commands > Send Message**.

> Devices with firmware from IGEL OS 10.03.100 can display these formatted messages. With older firmware versions, the message will be without formatting.

Under **Select Template**, you can choose from various format templates. These include 5 preset templates and those that you created under **UMS Administration > Global Configuration >** Rich Message Templates (see page 507):

- {01 template: Info}: For informative texts, with information symbol
- {02 template: Warning}: For warning texts, with attention symbol
- {03 template: Error}: For error messages, with error symbol
- {04 template: Custom Icon}: Freely configurable message with its own symbol (see below)
- {05 template: Alert}: Red alarm message, with information symbol and a table with a moving bell symbol
- {06 template: Blue}: Blue message window, with IGEL symbol
- ... own templates ...

Own Icon

In order to distribute your own icon from the UMS, select a PNG file which should not be bigger than 4 kB.

Users who have the right to send messages can view all saved templates and change them for an immediate message. However, these changes will not be saved.

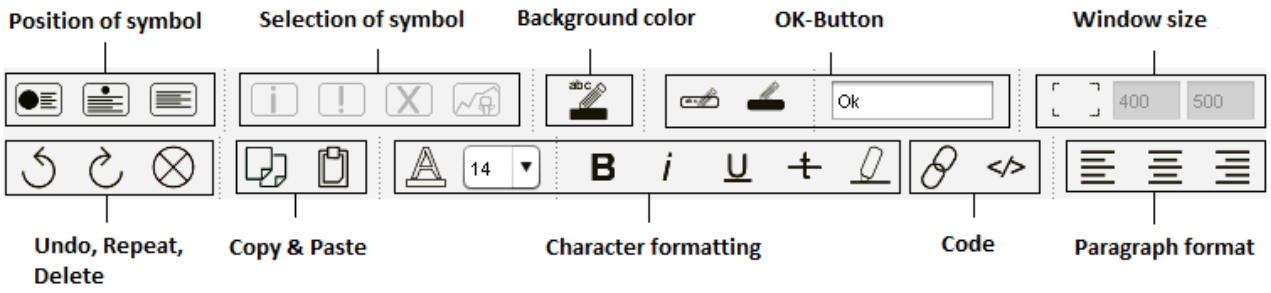
> In order to save templates, the user will need to write rights on the Rich Message Templates (see page 507) node.

In order to format the text, you can either use the integrated toolbar or you can create HTML snippets using an expert tool and insert them using copy and paste.

> A message may have up to 7,000 characters including the formatting elements.

Message Editor

Menu path: **Structure tree > Devices > [Directories] > [Name of the device] > Other Commands > Send Message**



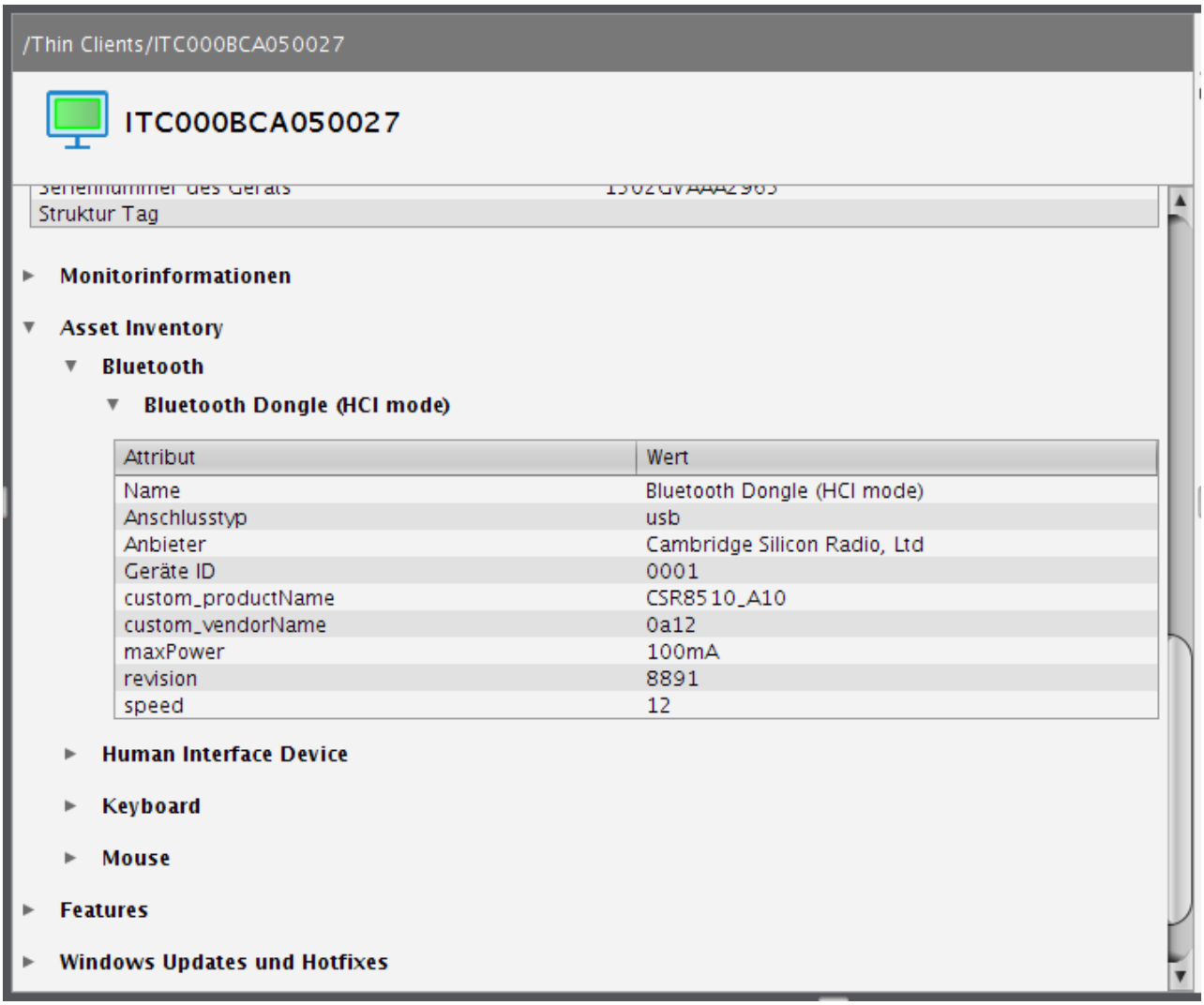
View Asset Information

License Required

For IGEL OS 11 devices:
The Asset Inventory Tracker requires a valid license from the IGEL Enterprise Management Pack (EMP). When the license expires, the feature is no longer available; devices whose license have expired will no longer send updated asset information to the UMS. For information on license deployment, see Setting up Automatic License Deployment.
For IGEL OS 10 devices:
The Asset Inventory Tracker requires a separate license; when the license has expired, the UMS will no longer update the asset information. For information on license deployment, see Licensing AIT.

With this function, you find information about peripherals connected to an endpoint device. The peripherals are sorted according to categories. A device can belong to more than one category and, accordingly, may be shown a number of times.

- Click on the triangle symbols to expand or collapse hierarchy levels.


/Thin Clients/ITC000BCA050027
ITC000BCA050027
Seriennummer des Geräts
1502GVAAA2963
Struktur Tag
Monitorinformationen
Asset Inventory
Bluetooth
Bluetooth Dongle (HCI mode)
Attribut
Wert
Name
Bluetooth Dongle (HCI mode)
Anschlusstyp
usb
Anbieter
Cambridge Silicon Radio, Ltd
Geräte ID
0001
custom_productName
CSR8510_A10
custom_vendorName
0a12
maxPower
100mA
revision
8891
speed
12
Human Interface Device
Keyboard
Mouse
Features
Windows Updates und Hotfixes

Read out Asset Data via API

If you have a license for Asset Inventory Tracker (AIT), you can read out asset information as well as the asset history via a REST interface. For details, see Asset Information in the IMI API V3 Reference.

Secure Terminal (Secure Shell)

You can establish a secure terminal connection to a device.

The device must meet the following requirements:

- The firmware of the devices is IGEL Linux v5.11.100 or higher or IGEL OS 10.01.100 or higher.

> You can allow access via the secure terminal for all registered devices. To do this, enable the **UMS Administration > Global Configuration > Remote Access > Enable secure terminal globally**.

For IGEL OS 10.01.100 or newer

1. In IGEL Setup, go to **System > Remote Access > Secure Terminal**.
2. Enable **Secure Terminal**.

For IGEL Linux v5

▶ In IGEL Setup, enable the following options under **System > Registry**:

- **network > telnetd > enabled > allow telnet access**
- **network > telnetd > secure_mode > secure telnet**

Configuring the Secure Terminal

With the following settings, you can configure and manage access to devices via a secure terminal.

- **Misc > Settings > Remote Access > External terminal client**: Command line for the external terminal client, made up of the path to the executable (e.g. `putty.exe`) and the appropriate parameters. IGEL recommends PuTTY[14].
  For PuTTy under MS Windows, the minimal command line without further configuration is:
  `[Path and file name for putty.exe] -telnet <hostname> -P <port>`
  For PuTTy under Linux, the minimal command line without further configuration is:
  `[Path and file name for the PuTTy executable] -telnet <hostname> -P <port>`

  > `<port>` and `<hostname>` are placeholders that are automatically replaced by the port number and the IP address of the device during execution. Background: The actual connection to the device is provided by the UMS and is available to the external terminal client as a tunnel.

  Examples:
  PuTTy under MS Windows: `C:\Program Files\PuTTY\putty.exe -telnet <hostname> -P <port>`
  PuTTy under Linux: `/bin/putty -telnet <hostname> -P <port>`
  If the **External terminal client** field is empty, the internal terminal client of the *UMS* will be used.
- **Misc > Settings > Remote Access > Show end dialog if two or more sessions are open**
  ☑ If two or more sessions are open, a closing dialog will be shown if you attempt to close a window of the external terminal client.
  ☐ No closing dialog will be shown when you close the window of the external terminal client.
- **Misc > Settings > Remote Access > Show warning for sessions that end unexpectedly**
  ☑ A warning will be shown if a session with an external terminal client was terminated without any user input.
  ☐ No warning will be shown.
- **UMS Administration > Global Configuration > Remote Access > Enable secure terminal globally**
  ☑ Access via the secure terminal is enabled for all registered devices. The firmware must be *IGEL* Linux *version 5.11.100* or higher.
  ☐ Access via the secure terminal is not enabled for all registered devices. However, it can be enabled for individual devices.

14 http://www.chiark.greenend.org.uk/~sgtatham/putty/

- **UMS Administration > Global Configuration > Remote Access > Log user for secure terminals**: Specifies whether the user name of the *UMS* user who established the connection to the device is logged. The log is shown under **System > Logging > Remote Access**.
  - ☑ The user name is contained in the log.
  - ☐ The user name is not contained in the log.
- **System > Logging > Remote Access**: Shows the log of all secure access to devices.
  The following data are logged:
  - **Device Name**
  - **MAC Address**
  - **Unit ID**
  - **Device IP**
  - **User**: The user name of the *UMS* user who established the connection to the device is logged. This is only logged if **Log user name for SSH remote access** is enabled.
  - **VNC Start time**: Point in time at which the connection was established
  - **Duration in seconds**
  - **Comment**
  - **Protocol**: Connection protocol

Using the Secure Terminal

To establish a secure terminal connection to a device, proceed as follows:

1. In the navigation tree, right-click the device that you would like to connect to.
2. Select **Secure Terminal** from the context menu.
   The terminal window opens. The **Security Certificate** dialog shows the device's certificate.
3. Click on **Accept** to accept the device certificate.
4. Log in with `user`.

   The secure terminal connection to the device is established. You can become `root` by entering `su`.

Shadowing (VNC)

The IGEL UMS Console allows you to observe the desktop of a device on your local PC via shadowing with VNC. In order to enable shadowing, you must allow remote access for the device: in the Setup or the configuration dialog in the UMS, select **System > Remote Access > Shadow > Allow remote shadowing**. If you want to enable secure VNC globally for all devices, see Remote Access (see page 501).

Limitations for Special Characters

Some special characters might not be transmitted through the VNC connection. The processing of special characters depends on the following factors:

- Keyboard layout configured on the VNC client and on the VNC server
- VNC viewer in use: An external viewer and the internal viewer behave differently.
- Firmware version of the endpoint device

See also the how-to document Secure Shadowing.

TechChannel

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=dqH6fBUBHXw

Launching a VNC Session

> **Limitations for Special Characters**
>
> Some special characters might not be transmitted through the VNC connection. The processing of special characters depends on the following factors:
> - Keyboard layout configured on the VNC client and on the VNC server
> - VNC viewer in use: An external viewer and the internal viewer behave differently.
> - Firmware version of the endpoint device

To launch a VNC session, proceed as follows:

1. In the context menu, click **Shadowing.**
   A connection dialog will appear.
2. Enter the password if you have set one in the security options.

If you have a user account, you can connect to the *UMS* Server and launch the *IGEL* VNC Viewer separately. The *IGEL* applications folder in the *Windows* Start Menu contains a link to it.

1. Enter a **host name** or the **IP address** manually on the first tab.
2. On the second tab, select a **device** from the structure tree.

IGEL VNC Viewer

If you have launched a VNC session, the shadowed desktop will be shown in the *IGEL* VNC Viewer window. This window has its own menu with the following items:

File	**Overview**	Shows an overview of all VNC sessions currently connected. Double-click of the displayed desktops for a full-screen view of it.
	Terminate	Terminates all VNC sessions and closes the window.
Tab	**New**	Opens the connection dialog so that you can launch another VNC session.
	Adjust	With this option, you can adjust the size of the window in which the desktop currently selected is displayed.
	Send Ctrl-Alt-Del	Sends the key combination [Ctrl]+[Alt]+[Del] to the remote host currently displayed.
	Refresh	Refreshes the window content.
	Screenshot	Saves a screenshot of the window contents on the local hard drive.
	Options	Opens a dialog window in which you can specify further options such as coding, color depth, update interval etc.
	Close	Closes the currently selected tab.
Help / Info		Shows the software version of the *IGEL* VNC Viewer.

You can specify the following parameters as options:

Preferred Coding	The coding used when sending image data from the device to your PC. The coding option **Tight** is particularly useful in a network with a low bandwidth. It contains two additional parameters: • **Compression level**: The higher the compression, the longer the computing operation takes! • **JPEG quality**: If you select **Off**, no JPEG data will be sent.
Use Draw Rectangle Method	This option improves performance. However, artifacts may be encountered.
Color Depth	8 or 24 bits per pixel

Update Period	Time period between two updates. A longer time period reduces network traffic, but the update may not be seamless. Please note: An update query will be sent as soon as you move the mouse or enter a key in the VNC Viewer. This event will be passed on to the remote host.
Save Properties as Standard Values	Saves the current settings as standard values for future VNC sessions.

External VNC Viewer

> **Limitations for Special Characters**
>
> Some special characters might not be transmitted through the VNC connection. The processing of special characters depends on the following factors:
> - Keyboard layout configured on the VNC client and on the VNC server
> - VNC viewer in use: An external viewer and the internal viewer behave differently.
> - Firmware version of the endpoint device

You can specify an external VNC Viewer program from another provider in the UMS Console:

▶ Click on **Misc > Settings > Remote Access**.

To pass on the IP address of the device to an external application, add the parameters and in **External VNC Viewer**.

Examples:

- TightVNC: `"C:\Program Files\TightVNC\tvnviewer.exe" <hostname>:<port>`
- UltraVNC: `"C:\Program Files\uvnc\UltraVNC\vncviewer.exe" -connect <hostname>:<port>`
- RealVNC: `"C:\Program Files\RealVNC\VNC Viewer\vncviewer.exe" <hostname>:<port>`
- TigerVNC: `"C:\Program Files\TigerVNC\vncviewer.exe" <hostname>:<port>`

  > Place the program path in double quotation marks as shown above to ensure that the call-up works even if there are spaces in the path.

Secure Shadowing (VNC with SSL/TLS)

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

> **Limitations for Special Characters**
>
> Some special characters might not be transmitted through the VNC connection. The processing of special characters depends on the following factors:
> - Keyboard layout configured on the VNC client and on the VNC server
> - VNC viewer in use: An external viewer and the internal viewer behave differently.
> - Firmware version of the endpoint device

The **Secure Shadowing** function is only relevant to clients which meet the requirements for secure shadowing and have enabled the corresponding option. Secure shadowing improves security when remote maintaining a client via VNC at a number of locations:

- **Encryption**: The connection between the shadowing computer and the shadowed client is encrypted.
  This is independent of the VNC Viewer used.
- **Integrity**: Only clients in the UMS database can be shadowed.
- **Authorization**: Only authorized persons (UMS administrators with adequate permissions) can shadow clients.
  Direct shadowing without logging in to the UMS is not possible.
- **Limiting**: Only the VNC Viewer program configured in the UMS (internal or external VNC viewer) can be used for shadowing.
  Direct shadowing of a client by another computer is likewise not permitted.
- **Logging**: Connections established via secure shadowing are recorded in the UMS server log.
  In addition to the connection data, the associated user data (shadowing UMS administrator, optional) can be recorded in the log too.

Shared Workplace

IGEL Shared Workplace is an optional, licensed feature of the IGEL OS firmware. It allows user-dependent configuration using profiles created in the IGEL Universal Management Suite and linked to the AD user accounts. In the process, user-specific profile settings are passed on to the device along with the device-dependent parameters.

You will find the complete documentation here: Shared Workplace (see page 594).

Views

Menu path: Structure tree **> Views**

A view is a selection of devices according to definable criteria which are logically linked one after another. You can generate views, edit or delete views and export results of a view in various formats (e.g. XML). This tree structure can also contain sub-directories for arranging views.

You can use a view to define a scheduled job for a specific selection of devices, e.g. a firmware update.

To specify which columns are shown in the view, proceed as follows:

1. Click on the selection button in the top right-hand corner of the window.

   The **Choose visible columns** dialog will open.

2. Select the columns that are to be displayed.

- Creating a New View (see page 391)
- Copying a View (see page 396)
- Copying a View Directory (see page 397)
- Saving the View Results List (see page 398)
- Sending a View as Mail (see page 399)
- Assigning Objects to a View (see page 400)

Creating a New View

Menu path: **Structure Tree > Views > Context Menu > New View**

To create a new view, proceed as follows:

1. Right-click on **Views** in the structure tree.
2. Select **New View** in the context menu
   or select **System > New > New View** in the menu.
   The **Create new view** window will open.
3. Give a **Name** and a **Description**.
4. Click on **Next**.
   The **Select criterion** window will open.
5. Select a parameter.
   You will find a list of all available search parameters under Possible Search Parameters (see page 393).
6. Click on **Next**.
7. In the entry field in the **Text search** window, enter a text with which the parameter value is to be compared and select one or more search options.
   Depending on the parameter, the following search options are available:
   - **Consider case**
     ☑ The case of the parameter value must match the case of the text entered.
     ☐ The case of the parameter value can differ from the case of the text entered.
   - **Compare whole text**
     ☑ The parameter value must match the text entered completely.
     ☐ The parameter value does not need to match the text entered completely; it is sufficient if the text entered is contained in the parameter value.
   - **Use regular expression**
     ☑ The **Consider case** and **Compare whole text** options are grayed out. You can enter a regular expression of your own in the entry field. Example: `RDD.*` selects all devices whose serial number contains the string `RDD`.

   You will find a list of the regular expressions supported by Java at Oracle under Class Pattern[15].
   ☐ You cannot enter a regular expression in the entry field. However, you can use regular expressions when subsequently editing the view.
   - **Not like**
     ☑ The parameter value must differ from the text entered.
     ☐ The parameter value must match the text entered.
   - **Exact**: The parameter value must match the value entered.
   - **Above**: The parameter value must be above the value entered.
   - **Below**: The parameter value must be below the value entered.
   - **Unequal**: The parameter value must differ from the value entered.

15 https://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html

8. Click on **Next**.
9. In the **Finish view criterion** window, click on one of the following options:
    - **Create view**: The view will be generated when you click on **Finish**.
    - **Narrow search criterion (AND)**: You can specify a further selection criterion that must likewise apply. This selection criterion and the previously defined selection criterion are linked with a logical AND.
    - **Create additional search criterion (OR)**: You can specify a further selection criterion that must apply as an alternative. This selection criterion and the previously defined selection criterion are linked with a logical OR.
10. Depending on the option selected, click on **Finish** or **Next**. You can add as many criteria with AND/OR links as you want.

Possible Search Criteria

The following parameters can be used as search parameters for a view:

Basic information

- **Comment**
- **Cost center**
- **Department**
- **Device License**
- **Device Serial Number**
- **Directory**
- **Expiration Date of Maintenance Subscription**
- **Igel Cloud Gateway**
- **In Service Date**
- **Keystore alias**
- **Last known IP Address**
- **MAC address**
- **Name**
- **Online**
- **Profile Assignment**
- **Serial Number**
- **Site**
- **Unit ID**

Asset Inventory

- **Asset ID**
- **BIOS Date**
- **BIOS Vendor**
- **BIOS Version**
- **CPU Speed**
- **CPU Type**
- **Device Type**
- **Duplex Mode**
- **Firmware Description**
- **Firmware Update (Relative)**
- **Firmware Version**
- **Flash Player**
- **Flash Player Version**
- **Flash Size**
- **Graphic Chipset 1**
- **Graphic Chipset 2**
- **Graphics Memory Size 1**
- **Graphics Memory Size 2**
- **Last Boot Time (Absolute)**

- **Last Boot Time (Relative)**
- **Memory Size**
- **Network Name**
- **Network Speed**
- **OS Type**
- **Partial Update (Name)**
- **Partial Update (Relative)**
- **Partial Update (Version)**
- **Product**
- **Product ID**
- **Total Operating Time**

Monitor Information

- **Monitor Date of Production**
- **Monitor Model**
- **Monitor Native Resolution**
- **Monitor Serial Number**
- **Monitor Size**
- **Monitor Vendor**

Monitor Information (legacy)

- **Monitor 1 Date of Production**
- **Monitor 1 Model**
- **Monitor 1 Native Resolution**
- **Monitor 1 Serial Number**
- **Monitor 1 Size**
- **Monitor 1 Vendor**
- **Monitor 2 Date of Production**
- **Monitor 2 Model**
- **Monitor 2 Native Resolution**
- **Monitor 2 Serial Number**
- **Monitor 2 Size**
- **Monitor 2 Vendor**

Example: Creating a View

Menu path: **Structure Tree > Views > Context Menu > New View**

In the following example, a view which covers all devices with IGEL OS whose firmware version is lower than 11.01.100 is created. With this view, you can determine which devices are to receive an upgrade.

1. Click on **Views** in the structure tree.
2. Select **New View** in the context menu.
3. Under **Name**, give a suitable name for the view, e.g. `UDLX Update`.
4. Click on **Next**.
5. In the **Select search parameter** window, select the parameter **Firmware Version**.
6. Click on **Next**.
7. In the **Version search** window, select the **below** option under **Version number** and enter `11.01.100` in the text box.
8. Click on **Next**.
9. In the **Finish view criterion** window, select the **Narrow search criterion (AND)** option.
10. Click on **Next**.
11. In the **Select criterion** window, select the parameter **Product ID**.
12. In the **Text search** window, enter the text `UD.*LX.*` and enable **Use regular expression**.
13. Click on **Next**.
14. Click on **Finish**.
    The result is shown in the content panel.

▶ If you want to change the view, e.g. in order to add further criteria, select **Edit view** in the context menu.

Copying a View

Menu path: **Structure Tree > Views > [Name of the View] > Context Menu > Copy**

You can copy a view and paste it in any view directory.

To copy a view, proceed as follows:

1. Click on the view that you want to copy.
2. Open the context menu for the view and select **Copy**.
3. Click on the view directory in which you would like to paste the copy of the view. This can also be the directory of the original view.
4. Open the context menu for the directory and select **Paste**.
   A new view which has the same name and properties as the original view will be created.

Copying a View Directory

Menu path: **Structure Tree > Views > [Name of the View Directory] > Context Menu > Copy**

You can copy a view directory and paste it in any directory.

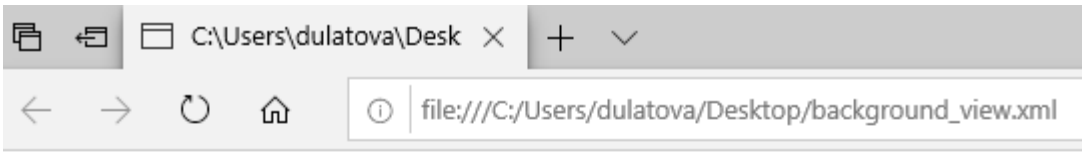
To copy a view directory, proceed as follows:

1. Click on the view directory that you want to copy.
2. Open the context menu for the directory and select **Copy**.
3. Click on the directory in which you would like to paste the copy of the view directory. This can also be the directory in which the original view directory is located.
4. Open the context menu for the directory and select **Paste**.
   A new view directory which has the same name as the original view directory will be created. The new view directory will contain newly created copies of the view contained in the original directory as well as copies of the sub-directories.

Saving the View Results List

▶ Select **Save as...** in the context menu of a view in order to save the current view results in file form. Four file formats are available for the export: XML, HTML, XSL-FO, and CSV.

Example of an XML file for a view:



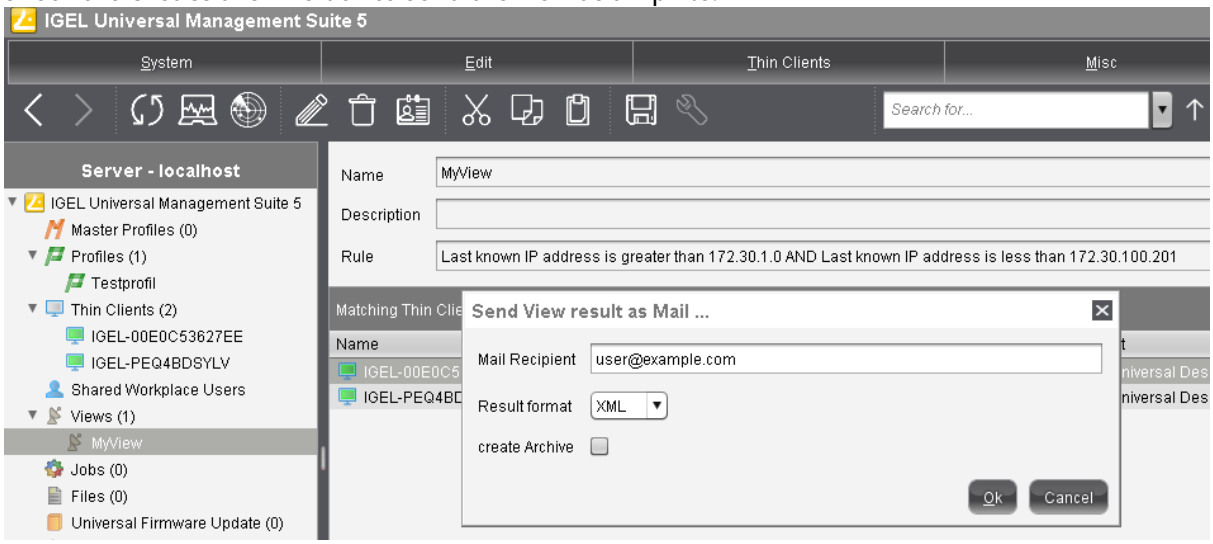

```
<?xml version="1.0" encoding="ISO-8859-1"?>
- <table>
    <creation-date>October 1, 2019</creation-date>
    <caption>background_profile_view</caption>
    <description/>
    <columnheader>Name</columnheader>
    <columnheader>Last Known IP Address</columnheader>
    <columnheader>MAC Address</columnheader>
    <columnheader>Product</columnheader>
    <columnheader>Version</columnheader>
  - <row>
      <cell>ITC00E0C520986A</cell>
      <cell>172.30.91.211</cell>
      <cell>00E0C520986A</cell>
      <cell>IGEL OS 11</cell>
      <cell>11.02.100.rc8</cell>
    </row>
</table>
```

Sending a View as Mail

To send a view as mail, proceed as follows:

> Mails can only be sent if you have configured appropriate mail settings (see page 506) under **UMS Administration > Global Configuration > Mail Settings**.

1. Right-click on a view.
2. Select **Send View Result as Mail...** in the context menu.
   The **Send View Result as Mail...** window opens.
3. Enter the recipient address in the **Mail recipient** field. A number of recipient addresses can be entered, separate them with a semicolon ";".
4. Under **Result format**, select the format in which the view is to be sent.
5. Check the **Create archive** box to send the view as a zip file.



> You can also send views automatically and regularly as an administrative task (see page 472).

Assigning Objects to a View

Via the context menu of a view, you can assign on a one-off basis objects to devices that you have filtered via the view. If you want to be certain that the object is assigned even to newly recorded devices that fulfill the view criterion, you can do this using an administrative task (see page 476).

> Using the same principle, you can assign objects to devices that you have filtered via a search (see page 419).

To assign an object to a view result, proceed as follows:

1. Create a corresponding view.
2. Right-click on the view to open the context menu.
3. Select **Assign objects to the devices of the view...** .
   The **Assign objects** window will open.
4. Select the desired object from the left-hand column and move it to **Selected objects** on the right by clicking on  .
5. Click **OK**.
   The **Update time** window will open.
6. Select **Next Reboot** or **Now**.
7. Click **OK**.

> Via **Detach objects from the devices of the view...**, you can undo the assignment of objects.

Jobs

Menu path: Structure tree **> Jobs**

You can define jobs for the UMS. A job consists in sending a command for specific devices automatically at a defined time. Jobs can be repeated at intervals or on specific days of the week.

You have the following options in the context menu for a job:

- **Edit Job**: Opens the **Edit Job** dialog with which you can change settings for the job.
- **Rename**: Opens the **Input** dialog in which you can give the job a new name.
- **Delete**: Removes the job.
- **Clear outdated results**: Removes outdated results.
- **Access control**: Opens the **Access control** dialog with which you can change the rights for the job. Further information can be found under Object-Related Access Rights (see page 521).
- **Cut**: Cuts the job from the current directory so that it can be pasted into another directory.
- **Paste**: Pastes the cut job into the current directory.
- **Logging: Messages**: Opens the **Messages** dialog. Further information can be found under User Logs (see page 528).
- **Execute Job**: Executes the job immediately.

Setting Up a New Job

Menu path: Structure tree **> Jobs >** [context menu] **> New Scheduled Job**

▶ To add a job, select **Jobs >** [context menu] **> New Scheduled Job** or **System > New > New Scheduled Job**.
The configuration window contains:

- Details (see page 404)
- Schedule (see page 406)
- Assignment (see page 407)

Commands for Jobs

Menu path: Structure tree **> Jobs >** [context menu] **> New Scheduled Job**

You can define one of the following commands for a job:

- **Update**: Executes the firmware update with the existing settings (IGEL OS).
- **Shutdown**: Shuts down the device.
- **Reboot**: Restarts the device.
- **Suspend**: Puts the device into suspend mode.
- **Wake up**: Starts the device via the network (Wake-on-LAN).
- **Update on Boot**: Executes the firmware update when the device is booting.
- **Update when shutting down**: Executes the firmware update when the device shuts down (IGEL OS).
- **Settings Device->UMS**: Reads the local device settings to the UMS.
- **Settings UMS->Device**: Sends the UMS local settings to the device.
- **Download Flashplayer**: Downloads the Flash Player plugin for Firefox (IGEL OS).
- **Remove Flashplayer**: Removes the Flash Player plugin for Firefox (IGEL OS).
- **Download Firmware Snapshot**: Executes the firmware update with the existing settings (WES).
- **Partial Update**: Executes the partial update with the existing settings (WES).
- **Update desktop customization**: Updates the desktop background and the boot logo (IGEL OS).
- **Deploy Jabra Xpress package**: Installs a Jabra Xpress package (IGEL OS).
- **OS 11 Upgrade**: Upgrades devices from IGEL OS 10 to IGEL OS 11. For details, see Mass Deployment Using a Scheduled Job.

Details

Menu path: Structure tree **> Jobs >** [context menu] **> New Scheduled Job**

Name: Name of the job.

Command: Command which is executed for all assigned devices. For more information, see Commands for Jobs (see page 403).

Execution time / Start date: Time of the first execution.

Enable

☑ Jobs can be enabled or skipped as necessary.

Comment: Further information regarding the job.

Options

Log results

☑ Loggable results are collected in the database. This is not possible with the `Wake-on LAN` command.

Retry next boot

☑ Parameter for the update command - devices that are switched off perform the update when they next boot.

Max. threads: Maximum number of processes executed simultaneously, these processes may thus be executed in block fashion.

Delay: The minimum waiting time before the UMS sends the command to the next device.

Timeout: The maximum waiting time before the UMS sends the command to the next device.

> The **Max. threads, Delay**, and **Timeout** options make sense for all commands which take a long time to execute or cause heavy network traffic, e.g. downloading a firmware update, codec or snapshot. To prevent a large number of devices downloading data from a file server at once, it is advisable to reduce the number of simultaneous threads (e.g. to 10) and to set up a delay (e.g. 1 minute).

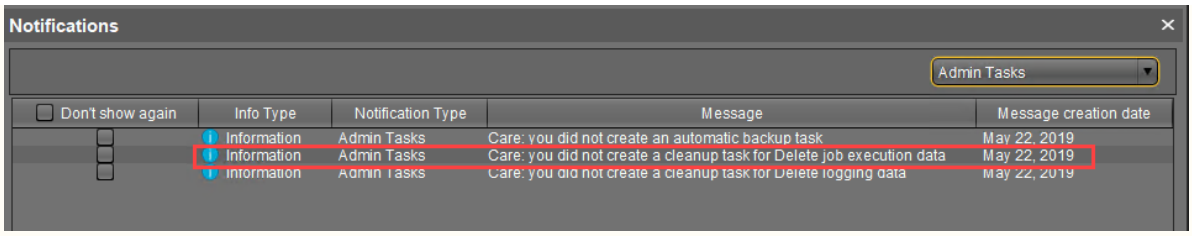
Job Info

Job ID: Internal job number which cannot be changed. This field is empty if a job is new.

Next execution: Date and time of the next execution.

User: Name of the UMS user executing the command.

> **Administrative Task Notification**
>
> If you have not set an administrative task "Delete Job Execution Data (see page 464)", after the start of the UMS Console, the following notification pop-up will be shown:



Only users with read permission for administrative tasks can see this notification. You can set the rights under **Edit** > **Access control**.
You can manage the display settings under **Misc > Settings > Notifications**.
You can find the notifications under **Help > Notifications**.

Schedule

Menu path: Structure tree **> Jobs >** [context menu] **> New Scheduled Job**

Execution time / Start date: Time of the first execution.

Expiration date / Time: After this point, no further commands will be executed.

Repeat job: A job can be repeated at fixed intervals or on specific days. Public holidays can be excluded separately. You can update the list of public holidays under **Misc > Scheduled Jobs > Manage Public Holidays**.

> ⚠ If **Update**, **Update when Starting** or **Update when Shutting Down** is selected as the command for the job, **Repeat job** should not be enabled.

Cancel job execution: Defines how long the system is allowed to wait for the completion of the job execution. Possible options:

- "Never": Jobs are never aborted.
- "Time": Point in time in hours and minutes when the job execution will be aborted.
  Example: If the **Execution time** and **Cancel job execution** are set to "19:00" and "20:00" respectively, the timeout for the job execution amounts to 1 hour. After 20:00, no further commands for the job execution will be sent to devices.

  > ⓘ If the **Time** configured under **Cancel job execution** precedes the **Execution time**, the job will not be aborted.

- "Max. duration": The maximum waiting time in hours and minutes for the completion of the job execution.
  Example: If **Max. duration** is set to "00:05", the timeout for the job execution amounts to 5 minutes. After 5 minutes starting from the **Execution time**, no further commands for the job execution will be sent to devices.

Assignment

By selecting **Add** (**+**), you can assign a job to specific devices.

You can also select a devices directory. The job will then be assigned to all devices located in this directory at the point of execution.

The most flexible assignment can be achieved by selecting devices dynamically with the help of a selected view. At the point of execution, the devices will first be ascertained on the basis of the selection conditions for the view. The jobs will then be assigned to them.

> Write authorization for the relevant objects is required in order to set up static devices assignment via the MAC address or dynamic assignment via the directory or view. At the point of execution, the user who has set up the job must have write authorization for the relevant devices. This must be taken into account, even if other users have write authorization for a job and especially if the database user has set up a job.

Execution Results

Menu path: Structure tree**> Jobs**

Execution Results appear in the view for a completed job. Here, you are given an overview of the status for the execution of a job. You can choose items from the overview using a selection list. This results view can be deleted and updated using two buttons. The following -**message**- job status reports are issued for the assigned devices:

Being executed	The job is currently being executed.
OK	The job is complete, all assigned devices have been dealt with.
Out of time	The job was aborted before all assigned devices could be dealt with because the abort time or the maximum duration has been reached.
Canceled	The job was stopped for an unknown reason (e.g. server failure).

The job execution status is also displayed for the devices:

Running	The command is currently being executed. The server is waiting for a reply.
Waiting	The job is running, the command will be executed when the next process is available.
Transferred	The command was successfully executed or transferred to the device.
Canceled	Aborted owing to an internal error or an unknown cause.
Failed	The command could not be executed, the reason is shown in the message column.
At next boot	The command will be executed when the device next boots.
Not done	The command was not executed because the time-out for the job was reached.

Files

Menu path: Structure tree **> Files**

Through a **file transfer**, you can save files in the device's local file system. A file must be registered on a UMS Server before it can be sent to the device. Examples include virus scanner signatures required locally on the device, browser certificates, license information, etc.

Registering a File on the UMS Server

A file must be registered on the UMS Server before it can be loaded onto a device.

To register a file on the UMS Server, proceed as follows:

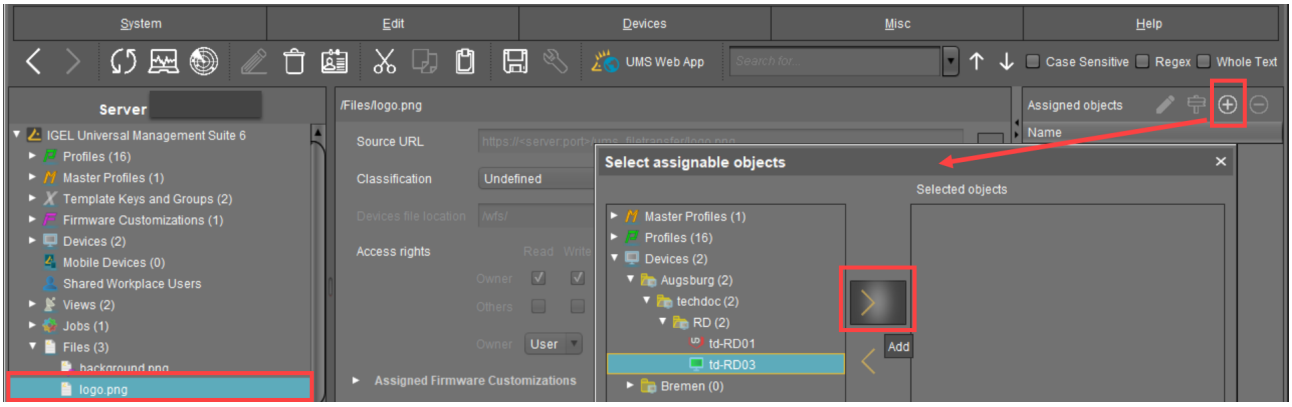
1. In the UMS Console, select **Files > [context menu] > New file** or **System > New > New File**.
2. Under **File source**, select a local file or one already on the server.
3. Select the upload location (URL). From UMS 5.01.100, you can only use the directory `ums_filetransfer` or sub-directories created in it.
4. Under **Classification**, select the type of file. This serves to automatically establish suitable storage locations and file authorizations. Choose between:
    - **Undefined**
    - **Web browser certificate**
    - **SSL certificate**
    - **Java certificate**
    - **IBM iAccess certificate**
    - **Common certificate**
5. For the **Undefined** classification, specify the path in the devices's local file system under **Device file location**.
6. For the **Undefined** classification, allocate **access rights** and the owner.
   These will be attached to the file when it is transferred to the device and will be used on the destination system.
7. Confirm the settings by clicking on **OK**.
   The file will now be copied to the web resource and will be registered on the UMS Server.

Transferring a File to a Device

In order to upload a file to a device, it must be assigned to the device either directly or indirectly via a device directory or profile.

▶ Via drag and drop, move the file to the device directory or integrate the file on the device itself in the **Assigned objects** window via the ⊕ symbol as you would when assigning profiles.

Example:



If a file has been assigned to a profile, it will be transferred to the assigned clients along with the profile settings.

When the UMS settings are transferred, a file assigned in this way will be copied to the device, e.g. while the device is booting. As long as the file is assigned to the device, it will be synchronized with the file registered on the UMS Server, for example, if the file `bookmarks.html` is replaced by a new version. The MD5 checksum for the file assigned to the device is compared to the registered file. If the checksums differ from each other, the file will be transferred again.

> ⓘ Up until UMS Version 5.02.100, the device must be able to contact the UMS Server with its fully qualified domain name (e.g. `mytcserver.mydomain.tld`). From UMS Version 5.02.100, the IP address of the UMS will be used when transferring the file. This ensures that the transfer works even in the event of DNS problems.

If a file was directly replaced in the file system in the `ums_filetransfer` directory, it must be updated in the UMS Console using the command **Update file version** from the file's context menu. The UMS Server will otherwise not recognize the change in the file version.

- Transferring a File Without Assignment (see page 412)

Transferring a File Without Assignment

A file registered on the UMS Server can also be transferred to the device without preparation:

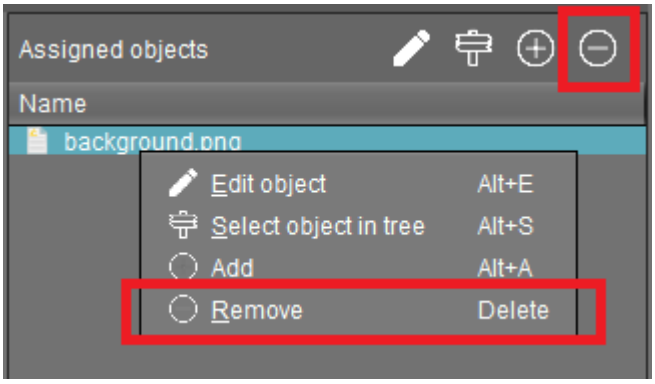
▶ Select **Other commands > File UMS->Device** from the device's context menu or under **Devices** in the menu bar. The file does not need to be assigned to the device.

This is a straightforward file copying operation. The file is not updated if the file version on the UMS Server changes.

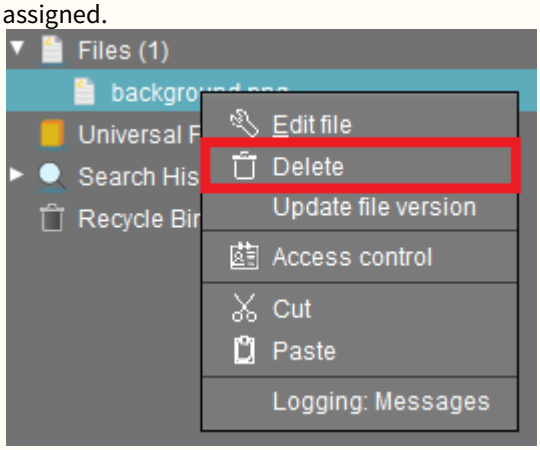
Removing a File from a Device

Permanent File Removal

▶ To permanently remove a file from a device, select the device in the structure tree and delete the file assignment in the **Assigned objects** (see page 271) area.



⚠ If you delete a file in the structure tree under **Files**, it will be removed from ALL devices to which it was assigned.



Temporary File Removal

▶ To temporarily remove a file from a device, select **Other commands > Delete file from device** in the device's context menu. The file assignment will remain in the Assigned Objects (see page 271) area, and the file will be present on the device again after the next reboot.

Transferring a File to the UMS Server

To download a file on a device to the web resources, proceed as follows:

▶ In the context menu of a device, select **Other commands > Device File->UMS**.

The UMS cannot search through the device's local file system. Therefore, you have to know the location and name of the file you would like to download to the web resource.

> A file transferred from a device to WebDAV is not automatically registered on the UMS Server. It can then be found in the UMS' http server area. However, you can register existing files later on via **New File**, see Registering a File on the UMS Server (see page 410).

Example

The **Device File->UMS** command can be used when you have to read out the current local configuration of the device and, thus, need to copy the two local files `setup.ini` and `group.ini` via the UMS.

1. Select **Other commands > Device File->UMS** from the device's context menu in the UMS Console.
2. Under **Device file location**, specify `/wfs/` as the source.
   Example: `/wfs/setup.ini`
3. Under **Target URL**, select the destination on the UMS Server and enter the name of the transferred file under **File Name**.
   Example: `https://umsserver.domain:8443/ums_filetransfer/setup.ini`
4. Begin the file transfer by selecting **Device File->UMS**.

See also Exporting the Local Device Configuration.

Universal Firmware Update

Menu path: Structure tree **> Universal Firmware Update**

In this area, you can search for new firmware updates for IGEL devices and devices converted by OSC and provide these for distribution.

The following options are available in the context menu:

- Check for New Firmware Updates (see page 416)
- Snapshot -> Universal Firmware Update (see page 417)
- Firmware Archive (Zip File) -> Universal Firmware Update (see page 418)

- **Access control**. See Access Rights (see page 516).

⚠ Once you have provided the update files, you must assign them to the devices and launch the update process. See Assigning Updates (see page 364).

ⓘ You can use an FTP server for distributing the firmware updates to the devices, as an alternative to the WebDAV capability of the UMS. An FTP server is required if your devices are connected via ICG. For further information, see Universal Firmware Update (see page 495).

Check for New Firmware Updates

Menu path: **Server - [UMS Server address] > Universal Firmware Update >** [context menu] **> Check for new firmware updates**

In this area, you can search the public IGEL server for firmware updates that can be downloaded and provided as Universal Firmware Updates by the UMS.

The icons at the top right of the window have the following meanings:

	Select a WebDAV directory as the target directory
	Specify an FTP target directory
	Undo changes

Universal Firmware Updates

Include

☑ The relevant firmware will be downloaded.

Model: Name of the firmware.

Version: The version number of the firmware for selection.

Target directory: Directory to which the firmware is downloaded.
This is the `ums_filetransfer` folder or, in the case of an FTP server, the directory specified under **UMS Administration > Global Configuration > Universal Firmware Update**.

Release notes: Show the release notes for the relevant firmware as an HTML page or in text format.

Show only latest firmware versions (hides already downloaded versions)

☑ Only the latest version of the relevant models is shown. If the latest version has already been downloaded to the UMS, it will no longer be shown.

☐ All available versions will be shown. (Default)

Download: The update will be added to the UMS structure tree and the current processing status will be shown.

Snapshot -> Universal Firmware Update

Menu path: **Universal Firmware Update >** [context menu] **> Snapshot -> Universal Firmware Update**

In this area, you can register as a Universal Firmware Update a snapshot of a Windows Embedded Standard device that was created earlier and stored in a WebDAV directory:

Snapshot file: Name of the snapshot file.

Select snapshot: Opens a dialog for the selection of the snapshot file.

Name: Name of the modified snapshot.

Firmware Archive (Zip File) -> Universal Firmware Update

Menu path: **Universal Firmware Update >** [context menu] **> Firmware Archive (Zip File) -> Universal Firmware Update**

In this area, you can load updates from a local source, e.g. from a USB stick.

> An item of firmware from a local source does not have the metainformation stored on the IGEL server.

Firmware file: Path and name of the zip file. Example: `c:\Updates\IGEL_LINUX_10.03.100.zip`, selectable by selecting a file.

Display name: Names for displaying the updates in the UMS.

WebDAV target directory: Directory in which the update is saved in order to distribute it to the devices.

Search History

Menu path: **Structure Tree > Search History**

Here, all search queries are saved as individual objects and can be edited further via the context menu.

Possible search types:

- Devices
- Profiles
- Views

- Context Menu of a Search Query (see page 420)

Context Menu of a Search Query

Menu path: **Structure Tree > Search History**

The following options are available to you in the context menu of a search query:

- **Delete**: Deletes the search result from the list.
- **Edit Search**: Allows you to change the search query.

The following options are only active if you have searched for devices:

- **Assign objects to the devices from the search...**: Assigns objects to the devices that you searched for.
  For details of the procedure, see Assigning Objects to a View (see page 400).
- **Detach objects from the devices from the search...**: Removes the assigned objects.

Recycle Bin

Menu path: Structure tree **> Recycle Bin**

In the IGEL Universal Management Suite, you can move objects to the **Recycle Bin** instead of permanently deleting them straight away. The Recycle Bin is enabled or disabled globally for all UMS users.

▶ Enable the Recycle Bin in the administration area under **Misc Settings > Enable Recycle Bin**.

If an object in the structure tree is deleted (**Delete** function in the symbol bar, in the context menu or the [Del] key), it will be moved to the Recycle Bin following confirmation.

> If the Recycle Bin is active, objects can also be deleted directly and permanently by pressing [Shift-Del].

Directories are moved to the Recycle Bin along with their sub-folders and all elements and can therefore be restored again as a complete structure. You will find the UMS Recycle Bin as the lowest node in the UMS Console structure tree. Elements in the Recycle Bin can be permanently deleted there or restored. To do this, bring up the context menu for an element in the Recycle Bin.

> If you cannot bring up the context menu for elements in the Recycle Bin, the Recycle Bin is probably inactive. Check the status of the Recycle Bin as described above.

Virtually all elements from the UMS structure tree can be moved to the Recycle Bin: devices, profiles, views, tasks, files, and their directories. Shared Workplace users cannot be deleted, while administrator accounts (in account management) and search history elements can only be deleted permanently (with [Shift-Del]). The highest nodes in the structure tree cannot be deleted either. However, this procedure will affect all deletable elements beneath this node!

- Objects in the Recycle Bin cannot be found via the search function or views and cannot be addressed by scheduled tasks.
- Devices in the Recycle Bin will not receive any new settings from the UMS but will remain registered in the UMS and can be restored again from the Recycle Bin along with all assigned profiles.
- The fact that profiles in the Recycle Bin are no longer effective means that the settings for devices may change. Profiles previously assigned to devices will be reactivated if they are restored again.
- Planned tasks, views and search queries in the Recycle Bin will not be executed.
- At the same time, assigned profiles, files, views, and firmware updates in the Recycle Bin are not active.

UMS Administration

UMS Network

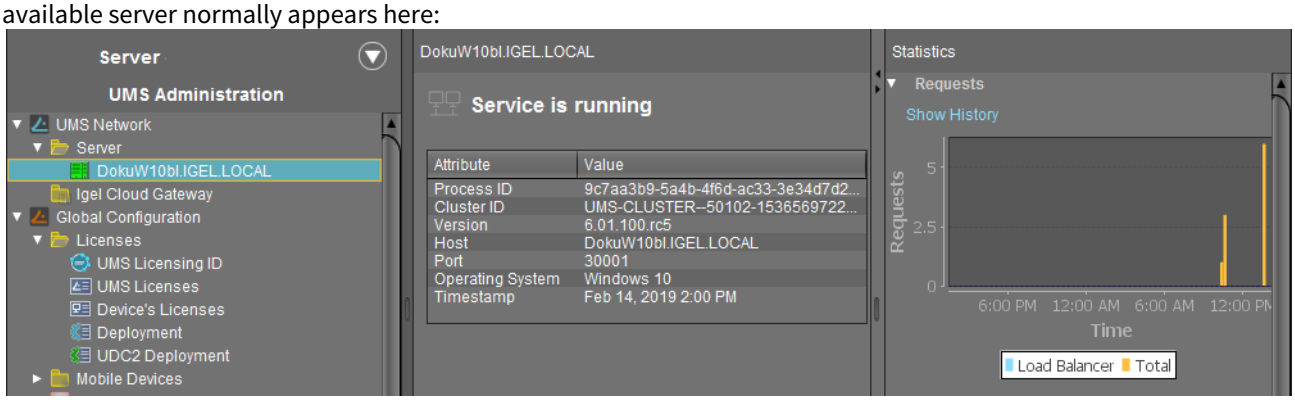
Menu path: **UMS Administration > UMS Network**

Here you can view and manage UMS Servers, UMS Load Balancers, and IGEL Cloud Gateways (ICG).

Server

Menu path: **UMS Administration > UMS Network > Server**

The **Server** subnode lists all servers belonging to the UMS installation. With a standard installation, only one available server normally appears here:



In an HA network (see page 560), all installed servers are shown.

The status of the servers is shown by the following icons:

	The server is online.
	The server is offline.
	The server status is unknown (when a new server is being propagated in the network).

Statistics

An overview of **requests** as well as **requests that are waiting or have been rejected** by devices makes it possible to estimate the server load across the relevant time period.

▶ Click on **Show History** to bring up a scalable view. You can use the mouse to zoom in on sections or restore the view by pressing the mouse button and moving the mouse to the left.

Load Balancer

Menu path: **UMS Administration > UMS Network > Load Balancer**

The **Load Balancer** subnode is visible in the UMS structure tree and active only if you have installed a UMS High Availability network with **UMS Load Balancer** activated. See High Availability (HA) (see page 560).

The **Load Balancer** lists all load balancers belonging to the UMS installation.

The status of the load balancers is shown by the following icons:

	The load balancer is online.
	The load balancer is offline.
	The load balancer status is unknown (when a new load balancer is being propagated in the network).

IGEL Cloud Gateway

Menu path: **UMS Administration > UMS Network > IGEL Cloud Gateway**

You can connect the UMS to one or more IGEL Cloud Gateways (ICG).

	Install a new IGEL Cloud Gateway with the ICG Remote Installer See Installing the IGEL Cloud Gateway.
	Uninstall the selected IGEL Cloud Gateway with the ICG Remote Installer. If the IGEL Cloud Gateway has been uninstalled with this function, it can be reinstalled using the ICG Remote Installer.
	Update the selected IGEL Cloud Gateway with the ICG Update Wizard See Updating the IGEL Cloud Gateway (ICG).
	Update the keystore of the selected IGEL Cloud Gateway with the Update Keystore Wizard See Certificate Management.
	Add an existing IGEL Cloud Gateway to the UMS database. This IGEL Cloud Gateway must be reachable.
	Remove the selected IGEL Cloud Gateway from the UMS database permanently. If you remove an IGEL Cloud Gateway from the UMS database, you can not add it to the UMS database again. In most cases, it is preferable to uninstall the IGEL Cloud Gateway and then reinstall it using the ICG Remote Installer.
	Edit the settings of the selected IGEL Cloud Gateway
	Navigate to the ICG instance view

Add an IGEL Cloud Gateway to the UMS Database

- **Displayname**: Display name of the gateway
- **Host**: DNS name or IP address of the gateway
- **Port**: TCP port on which the gateway is listening (default: 8443)
- **Host (external)**: External DNS name/IP address of the gateway
- **Port (external)**: TCP port on which the gateway is listening for external connections
- **Proxy Server Settings**:
  - **No Proxy Server**: Direct connection to ICG
  - **Use Default Proxy Server**: Use the proxy server which is configured as default in Proxy Server (see page 482)

- **Use selected Proxy Server**: Select a proxy server from the list

For details of how to set up all components for a connection to ICG, read Installation and Setup.

IGEL Cloud Gateway (Instance)

Menu path: **UMS Administration > UMS Network > IGEL Cloud Gateway > [Display Name]**

Here, you will find information regarding a configured gateway and can establish or disconnect the connection.

	Connect Cloud Gateway
	Disconnect Cloud Gateway
	Reload information about Cloud Gateway

Statistics

An overview of **Requests** by devices makes it possible to estimate the server load across the relevant time period.

▶ Click on **Show History** to bring up a scalable view. You can use the mouse to zoom in on sections or restore the view by pressing the mouse button and moving the mouse to the left.

Global Configuration

Menu path: **UMS Administration > Global Configuration**

Under **Global Configuration**, you can regulate administrative tasks (see page 452), integrate user data from the Active Directory (see page 499), set up Universal Firmware Updates (see page 495) and manage licenses (see page 430).

_____

Licenses

Menu path: **UMS Administration > Global Configuration > Licenses**

In this area, you can manage licenses for the UMS as well as licenses for devices which are managed by the UMS.

UMS Licensing ID

Menu path: **UMS Administration > Global Configuration > Licenses > UMS Licensing ID**

The UMS Licensing ID enables the communication between the UMS and the IGEL License Portal (ILP).

The UMS Licensing ID allows for using fully Automatic License Deployment (ALD), that is, Automatic License Deployment without the need to handle an ALD Token with each purchase. For this purpose, the UMS Licensing ID must be registered with the IGEL License Portal. For further information, see Setting up Automatic License Deployment (ALD).

The UMS Licensing ID consists of a public/private key pair. The public key is a certificate and can be exported as a `.cert` file. The registration of the UMS Licensing ID is done by uploading the certificate file to the IGEL License Portal.

A UMS Licensing ID is not affected or changed when the UMS database is restored from a backup. The UMS Licensing ID does not change if any parameters of the UMS installation are changed, for instance, the host name / IP address. Thus, it can be transferred to any other server. Also, multiple UMS installations can share one UMS Licensing ID, which allows for sharing Product Packs between them.

For the backup options of the UMS Licensing ID, see UMS Licensing ID Backup (see page 543) and UMS Licensing ID Backup on the Command Line (see page 544).

UMS Licensing ID

> The UMS Licensing ID is generated upon each UMS Server installation. Therefore, if you have a High Availability (see page 560) environment, each of the servers has its own UMS Licensing ID, i.e. **Local UMS Licensing ID**. For the communication of all HA servers with the ILP, a **Main UMS Licensing ID** is used. Therefore, the **Main UMS Licensing ID** must be synchronized between all servers in the HA network, see UMS Licensing ID status (see page 431) below.

Main UMS Licensing ID: The UMS Licensing ID used for communication with the ILP. The first and last 10 characters are displayed.

Export UMS Licensing ID: Export the UMS Licensing ID as a `.cert` file.

UMS Licensing ID Status

If you are operating a single server, this area shows the status of the UMS Licensing ID for your server.

If you are operating a UMS HA environment, this area lists the UMS Licensing ID status for each server of the HA network. Each server gets the UMS Licensing ID on startup or restart.

Host name: Name of the host server as shown under **UMS Administration > UMS Network > Server**.

UMS Licensing ID status: Indicates whether the server has the current main UMS Licensing ID or not. If it has the main UMS Licensing ID, the field reads "Main UMS Licensing ID" or "in sync". If not, the server must be restarted to get synchronized.
Possible values:

- 'Main UMS Licensing ID'
- 'In sync'
- 'Not in sync, please restart server'

> If the restart was unhelpful, the UMS Licensing ID has to be synchronized manually, see Manual Synchronization of the UMS Licensing ID (see page 127).

UMS Licensing ID: The UMS Licensing ID currently used on the server. The first and last 10 characters are displayed.

Server status: Status of the server, e.g. "Running"
Possible values:

- 'Running'
- 'Not running'

UMS Licenses

Menu path: **UMS Administration > Global Configuration > Licenses > UMS Licenses**

In this area, you are given an overview of the availability and status of all licenses for UMS extensions.

License Summary

- **License Type**: Name of the licensed UMS extension
- **Available Licenses**: Total number of units in the license file
- **Used Licenses**: License units which are currently used by the system
- **License Status**: Validity of the license

Registered Licenses

	Add license file
	Delete license
	Show content of the license file

- **License ID**: Identification number of the license
- **License registered on**: Point in time when the license file was generated on the activation portal
- **Quantity**: Total number of units in the license file
- **Customer**: Customer name (optional)
- **Services**: Licensed service, e.g. IGEL Cloud Gateway
- **Maintenance Subscription**: Authorization to install updates for the licensed extension
- **Activation Key**: Key used to generate the license in the activation portal
- **Test License**: Shows whether a license is a test license
- **Expiration Date**: End of the license period

Device Licenses

Menu path: **UMS Administration > Global Configuration > Licenses > Device Licenses**

IGEL Licenses

Here, you can manage licenses for devices, e.g. for devices converted with UDC3.

	Add license file
	Delete license
	Show content of the license file

- **Filter**: Restricts the list view to specific licenses:
  - Show all licenses
  - Show valid Maintenance Subscriptions
  - Show expired Maintenance Subscriptions
  - Show Maintenance Subscriptions which will expire in the next
    - months
    - days
  - Show all licenses of device
    - Unit ID
    -  (Browse device tree)
  - Show test licenses

List columns:

- **Order number**: Order number under which the license was ordered
- **Hardware type**: Hardware property, z.B. **MAC address**
- **Maintenance Subscription**: Shows whether a subscription exists
- **Activation key**: Activation key with which the license was generated
- **Test license**: Shows whether a license is a test license
- **Expiration date**: End of the license period

Hardware

Here, you can show device lists or export them for the activation portal. You can also create UDC2 licenses from a smartcard.

- **Export unit ID list**: Opens the export wizard
- **Device lists**: Opens the end device list with a filter option

Deployment

Menu path: **UMS Administration > Global Configuration > Licenses > Deployment**

You can enable and configure the automatic deployment of licenses by the UMS. Automatic license deployment includes licenses for UDC3/OSC, UMA and UD Pocket.

> Demo licenses are not supported by Automatic License Deployment. To deploy a demo license, see Activate Your IGEL OS (see page 435).

Automatic license deployment requires a connection between the UMS and the IGEL license server as well as the IGEL update server. This connection can be established via a proxy.

For details about the process of automatic license deployment, see Intervals for Automatic License Deployment.

> If a number of Product Packs for which suitable and non-allocated licenses are available, a selection will be made in accordance with the following criteria:
> - The Product Pack with the most allocated licenses will be used first.
> - Product Packs with an earlier registration date will be used before Product Packs with a later registration date.

As soon as a license is registered in the UMS, the UMS stores the license and adds a license download link to the device settings. After that, the UMS sends the settings to the devices. When the devices have received their settings, they download the licenses and reboot. After the reboot, all licensed features are available on the devices.

For further information about setting up and using automatic license deployment, see Setting up Automatic License Deployment (ALD).

- **Enable automatic deployment**
  - ☑ Automatic license deployment is enabled.
  - ☐ No automatic license deployment will take place.
- **Used proxy server**: Description of the proxy currently used
- **Edit proxy configuration**: Opens a dialog allowing you to select a proxy for communication with the license server. Under **UMS Administration > Global Configuration > Proxy Server**, one or more proxies must be configured; see Proxy Server.
  Possible options:
  - **No proxy server**: No proxy server will be used.
  - **Use default proxy server**: The default proxy server defined under Proxy Server will be used.
  - **Use selected Proxy Server**: A server from the **Configured Proxy Servers** list can be selected.
- **Connection test**: Shows the result of the connection test.
- **Test connection**: Tests the connection between UMS or the proxy and the IGEL license server as well as the IGEL update server (http://fwu.igel.com/).

Registered packs

This table shows all Product Packs currently registered in the UMS. You can add, delete, enable or disable Product Packs.

Search for:	Search in all columns of the table
	Add Product Pack
	Delete Product Pack
	Enable Product Pack
	Disable Product Pack. A disabled Product Pack will not be used for deploying licenses.
	Update information regarding all registered Product Pack. The current information will be obtained from the license server
	Show Product Pack details: • **Attribute**: Shows the attributes of a Product Pack. • **Licensed hardware**: Shows all devices licensed with the Product Pack belonging to the entry.

The following information is shown:

- **Pack ID**: ID of the Product Pack
- **Product**: Product pack type
- **Used licenses**: Licenses currently in use
- **Subscription status (expiration date/validity persion)**: For new Product Packs, the validity period is shown; for activated Product Packs, the expiration date is shown.
- **Status**
  Possible statuses:
  - "Active"
  - "Inactive"
- **Manual Distribution**
  Possible statuses:
  - "Enabled"
  - "Disabled"
- **Automatic Distribution**
  Possible statuses:
  - "Enabled"
  - "Enabled (with conditions)"
  - "Disabled"
- **Registration Error**: If the registration of e Product Pack has failed, the error message is shown here.

Executed actions

The actions last performed are shown in this area.

	Delete entries older than a specific date
	Delete selected entries
	Update display
	Show details regarding the selected action

The following information is shown:

- **Time**: Time at which the action was performed
- **Action**: Description of the action
- **Used Pack ID**: ID of the Product Pack
- **Number of affected devices**: Number of devices for which a license was deployed
- **Result**: Result of the action
  Possible results:
  - "Successful"
  - Error message

UDC2 Deployment

Menu path: **UMS Administration > Global Configuration > Licenses > UDC2 Distribution**

From Version 5.02.100, the UMS offers the option of using an IGEL device as a license server in order to automatically allocate licenses to devices converted using UDC2.

> This method for automatic license deployment only works for UDC2, not for UDC3. From UMS Version 5.08, there is a method for automatic license deployment with UDC3 which uses the license server; see Distribution.

The How-To Setting up Automatic UDC2 License Deployment describes the complete procedure.

- **Enable automatic UDC deployment**:
  - ☑ *UDC2* devices newly registered on the *UMS* will automatically receive a license.
  - ☐ Automatic license distribution is disabled.
- **License server**: Select one of the license servers shown.
- **Connection state:** Indicates whether a network connection to the license server exists.
- **License type:** The licenses available on the license server
- **License OS:** Operating system for which licenses are available
- **Number of licenses**: Number of licenses still available
- **Check license server again**: Checks the network connection to the license server again, for example if you have switched on the server in the meantime.
- **Deployed licenses**: List of licenses deployed by the selected license server since it was last restarted.
  - **License deployed at**: Date and time when the license was deployed
  - **Unit ID**: Unique ID of the device

Mobile Devices

Menu path: **UMS Administration > Global Configuration > Mobile Devices**

In this area, you can manage mobile devices that are connected to the UMS. Scan the QR code with the IGEL MDM App for iOS to enroll your device. For more information, see Connecting Mobile Devices to the UMS (see page 643).

- **Displayname**: The display name
- **Host**: The host
- **Port**: The port
- **Apns Status**: Status of the connection to the Apple Push Notification service
- **Firmware available**: Shows if the firmware required for MDM is available
- **Enrollment URL**: The enrollment URL

Possible actions related to the QR code:

- **show**: Show the QR code in a separate window
- **send via email**: Send the QR code via email
- **save as jpg**: Save the QR code as JPG file
- **send as png**: Save the QR code

- Apple iOS Devices (see page 440)

Apple iOS Devices

Menu path: **UMS Console > UMS Administration > Global Configuration > Mobile Devices > Apple iOS devices**

In this section, you can set up the required certificate for connecting the UMS to the Apple Push Notification Service. How you set up the certificate to connect the UMS with the Apple Push Notification Service is described in the MDM Setup Guide (see page 641).

You can perform the following actions:

Icon	Description
	Create a new certificate-signing request and save it as a *.csr file
	Open the Apple Push Certificate Portal at https://identity.apple.com in the system browser
	Import the Apple MDM Push Certificate (*.pem file)
	Create and save certificate-signing request for renewal
	Show the certificate details of the Apple MDM Push Certificate
	Cut the certificate
	Delete the certificate

Status information:

Icon	Description
	Certificate successfully set up
	Waiting for certificate upload
	Incomplete / certificate error

You may further specify:

- **Enrollment profile displayname**: Displayname for the enrollment profile
- **Enrollment profile description**: Description of the enrollment profile
- **Adjust UMS-internal name with name on device**

For further instructions, see:

- MDM Manual (see page 621)
- MDM How-Tos (see page 640)
- MDM Troubleshooting (see page 647)

Certificate Management

Menu path: **UMS Administration > Global Configuration > Certificate Management**

In this section, you can manage certificates for the communication between the UMS and the devices. The preconfigured certificate, which has the **Keystore alias** "tckey", is used by default if no changes are made.

You can set a different certificate as default; if you do so, all newly registered devices will use this certificate, and already registered devices will replace their previously used certificate with the new default certificate.

At an interval of 5 minutes, the UMS checks whether the certificate on the device and the default certificate are still identical.

If a device does not support the default certificate, the UMS checks for each certificate whether it is supported, starting from the top of the list. The first one that matches the requirements will be used. If no certificate matches, the device is not registered.

If you select a certificate in the area **Certificate management**, all devices which use this certificate are shown in the area **Devices which use the selected certificate (**<number>**)**.

High Availability

If you are running the UMS in a High Availability (HA) network, be aware that if you make changes to certificates (import a new keypair, generate a new keypair, delete a certificate or change the default certificate), a new network token is automatically generated and you will have to:

1. Define a location in which the new network token should be stored.
2. Deinstall all load balancers of the HA network.
3. Reinstall the load balancers using the new network token.
4. Restart all IGEL RMGUIServer/igelRMserver services in the HA network.

Restoring from a Backup

When restoring from a backup, check if certificates included in the backup differ from the certificates that are currently in use. If this is the case, all devices that have been registered before restoring will have to be registered again.

UMS Update

Certificates are not overwritten in the course of an update.

Possible Actions

 Import a certificate from a file. The file format must be PFX, and the private key must be included in the file. The file path is provided under **Keystore file** and the import password is entered under **Keystore password**. The certificate's signature algorithm is checked. If the signature algorithm is not supported by the UMS, the certificate is not imported.

Supported Signature Algorithms

The following signature algorithms are supported: SHA512withRSA, SHA384withRSA, SHA256withRSA, SHA1withRSA, SHA256withDSA, and SHA1withDSA.

Certificates which use the MD5 algorithm are not supported.

No Support for Certificate Chains

Do not import certificate chains. If you configure such a certificate, the communication between the UMS and the device will fail.

The import of expired certificates is not possible.

 Generate a new certificate.

 Delete the selected certificate.

Do not delete a certificate that is being used by a device; otherwise, the UMS will not be able to communicate with this device anymore.

 Move the selected certificate up in the list to increase its priority.

If you move the selected certificate to the top of the list, it will become the default certificate. In this case, you must restart the IGEL RMGUIServer/igelRMserver service.
The change of the default certificate is propagated to the devices in a background task of the UMS. This task replaces the certificate on all devices that are compatible with this certificate and runs every 5 minutes.

 Move the selected certificate down in the list to decrease its priority.

 Activate the selected certificate. When a certificate is activated, it can be used for communication between UMS and devices.

 Deactivate the selected certificate. A deactivated certificate will not be used when a new device is registered. If a certificate is deactivated while it is in use, communication between UMS and device is still possible. If only 1 certificate is active, this certificate can not be deactivated.

 Export the selected certificate.

 Export the key pair of the selected certificate.

 Show the content of the selected certificate.

Device Network Settings

Menu path: **UMS Administration > Global Configuration > Device Network Settings**

Configuration of the System Information Update

Update system information on selection of a device

☑ The system information of the device will be read in again as soon as the **device** is selected. (Default)

☐ The system Information from the last update will be shown.

Advanced Device's Status Updates

Devices send updates

☑ The devices report changes in their advanced status. (Default)

☐ The only thing that is displayed is whether a device is online or offline.

Automatic Registration

Enable automatic registration (without MAC address import): This option is provided for the following scenario: The MAC addresses were already imported before the devices were added to the UMS database. As a result, preparations such as creating profiles can be made before the devices are delivered. If the option is enabled, each device will automatically receive the intended settings after it has logged on for the first time.

Further information regarding the importing of devices can be found under Import Devices (see page 236).

☑ Each device that contacts the UMS will automatically be registered in the UMS database.

☐ A device that contacts the UMS will not be automatically registered. (Default)

Device Requests

Maximum number of concurrent threads for device requests: Defines the number of concurrent device requests that are accepted by the UMS. (Default: 50)

> ⓘ If you require higher performance and high availability, you can use IGEL UMS High Availability (HA) (see page 560).

Queue limit:

No limit: Additional request will have to wait until a thread is available. (Default)

Queue size: Defines the queue size. Additional threads that exceed the queue size will be rejected. (Default value: 0)

Adjust Names of Devices

Adjust UMS-internal names if network name has been changed

☑ If the network name of the device is changed, the UMS-internal name will be set to the new network name.

☐ The UMS-internal name will not be set to the network name of the device. (Default)

Adjust network name if UMS-internal name has been changed

☑ If the UMS-internal name of the device is changed, the network name of the device will be set to the new UMS-internal name.

☐ The network name of the device will not be set to the UMS-internal name. (Default)

> ⓘ From UMS *Version 5.07.100*, only DNS-compliant names can be entered if the network name is modified automatically.

Naming Convention

Enable naming convention

☑ The UMS-internal names of the devices will be formed from the **prefix** and a consecutive number.

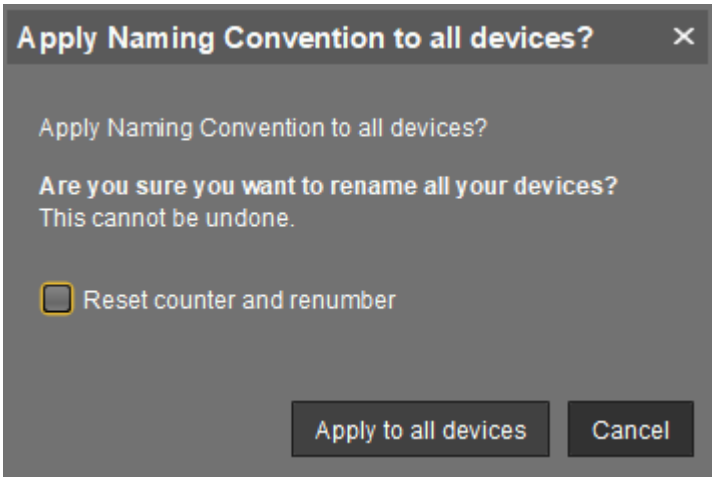
☐ The names of the devices will not be allocated in accordance with the naming convention. (Default)

Prefix: Prefix for automatically allocating names. In the neighboring field, the current naming convention comprising a prefix, a dash "`-`" and a consecutive number with the number of digits specified under **Min. digits** will be shown.

Minimum digits: Minimum number of digits for the consecutive number. The digits not allocated will be filled with zeros. Examples: If **2** is selected, the consecutive number of the first device will be **01**, if **3** is selected, the consecutive number will be **001** and so on.

> ⓘ If the number of devices exceeds the value defined here, the numbering will simply continue without an error occurring.

Apply to all devices: If you click on this button, a confirmation dialog **Apply Naming Convention to All Devices?** will apper. If you confirm it by clicking **Apply to all devices** button, all devices registered in the UMS will be renamed in accordance with the naming convention.



Reset counter and renumber

☑ When all devices are renamed (as a result of clicking on **Apply to all devices**), this will result in continuous, end-to-end numbering. All names will be reallocated, even for devices that were already renamed in accordance with the naming convention. If numbers have become free because devices were taken out of service, these numbers will be used for other devices.

☐ If all devices are renamed in accordance with the naming convention, numbers previously allocated will be retained. Only devices that do not yet conform to the naming convention will be renamed. (Default)

Server Network Settings

Menu path: **UMS Administration > Global Configuration > Server Network Settings**

Online Check Parameters

Disable online check

☑ The online check is disabled on the UMS Console.

Timeout (ms): Specifies how long the system will wait for a response to an online status query message. The UMS Console attempts to contact all devices that are currently visible in the UMS Console. Each device in this area must respond to the status query in the specified time or will otherwise be flagged as “offline”. (Default: 100)

Scheduled Jobs

Scheduled jobs never expire

☑ No time limit for scheduled jobs

Expiration time for scheduled jobs: Time in minutes after which a scheduled job will expire. (Default: 40)

Scan Parameters

Timeout (ms): Specifies how long in milliseconds the UMS will wait for a response to scan packages. (Default: 6000)

Broadcast IP: Broadcast address that is used for scan packages. It is only used for scanning the local network. If IP ranges are used, the UDP packets will be sent to each client within the IP range. (Default: 255.255.255.255)

Specify scan reply port (UDP): Allows you to specify a set port via which the devices respond if the UMS scans via UDP. If TCP is used, this port is not needed because the response is given via a configured socket. If you leave the default setting and do not specify a port, the application will select any free port.

Cloud Gateway Options

Menu path: **UMS Administration > Global Configuration > IGEL Cloud Gateway**

Here you can create and manage ICG certificates and first-authentication keys for connecting devices via IGEL Cloud Gateway (ICG).

For details of how to set up all components for a connection to the ICG, read Installation and Setup.

Certificates

	Generate root certificate
	Import root certificate
	Generate signed certificate
	Delete certificate
	Export certificate chain in the IGEL Cloud Gateway Keystore format
	Show content of the certificate
	Navigate to ICG instance view

Generate root certificate

- **Displayname**: Name in the root certificate (common name, CN).
- **Your organization**: Organization, company, government agency.
- **Your city or district**: The location of the organization.
- **Your two-letter country code**: ISO 3166 country code, e.g. DE for Germany.
- **Valid until**: Local date on which the certificate expires. (Default: in 10 years)

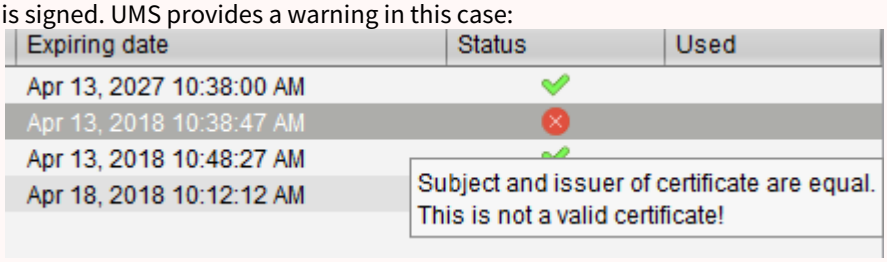
Import root certificate

- The file selection window opens, allowing you to select the certificate file which must be in the PEM format.

Generate a signed certificate

- **Name**: Name in the certificate (common name, CN).
- **Your first name and surname**: Name of the certificate holder.
- **Your organization**: Organization, company, government agency.
- **Your city or district**: The location of the organization.

The name in a signed certificate must be different from the one in the root certificate with which it is signed. UMS provides a warning in this case:



- **Your country code (two letters)**: ISO 3166 country code, e.g. DE for Germany.
- **Host name and/or IP of the target server for the certificate**: Host name(s) and IP address(es) for which the certificate is valid. Multiple entries should be separated by a semicolon. To generate a wildcard certificate, use the asterisk, e.g. *.example.com.
- **Valid until**: Local date on which the certificate expires. (Default: in a year)
- **Certificate type**
  Possible options:
  - **CA Certificate**: The certificate can be used to sign other certificates, but it can not be used by the ICG.
  - **End Entity**: The certificate can be used by the ICG, but it can not be used to sign other certificates.

Context menu (root certificate)

- **Generate signed certificate**: Collects certificate data and signs them with the selected root certificate.
- **Import signed certificate**: Imports a certificate in PEM format that was already signed outside the UMS by the imported CA.
- **Import decrypted private key**: Imports a private key file.

  If the private key is protected with a passphrase, you must decrypt it on the command line with OpenSSL before importing it: `openssl rsa -in encrypted.key -out decrypted.key`

- **Delete certificate**: Deletes the certificate from the UMS.
- **Export certificate chain in the IGEL Cloud Gateway Keystore format**: Produces a file for ICG installation program.
- **Export certificate**: Exports certificate file in the PEM format.
- **Show content of the certificate**: Shows the content of the certificate in a text window.

First-authentication Keys

	Create new one-time passwords
	Delete logon data

	Disable logon data
	Enable logon data
	Send one-time passwords via mail
	Export one-time passwords (in XML, HTML or CSV format)
	Allows you to copy one-time passwords to the clipboard

If you send one-time passwords via mail, anyone who can read the mail can log in to the IGEL Cloud Gateway. It is advisable to combine sending via mail with a link to unit IDs.

Create new first-authentication keys

You have the following options here:

- **Create new one-time keys**
  - **Quantity**: Desired number of passwords to be created
- **Create new one-time passwords associated with a device**
  - **Unit ID**
    - **Add**: Adds unit ID entered in the text field to the list.
    - **Select**: Selects from the devices in the UMS structure tree.
    - **Import**: Reads in a CSV file with unit IDs.
- **Create new mass-deployment key**
  - **Generate random mass-deployment key**:
    ☑ A random multiple-time password will be generated. (Default)
    ☐ You can enter the desired password yourself.

Device Attributes

Menu path: **UMS Administration > Global Configuration > Device Attributes**

In this area, you can set up additional attributes for devices.

> The additional device attributes are used when displaying device system information, in views, and in searches.

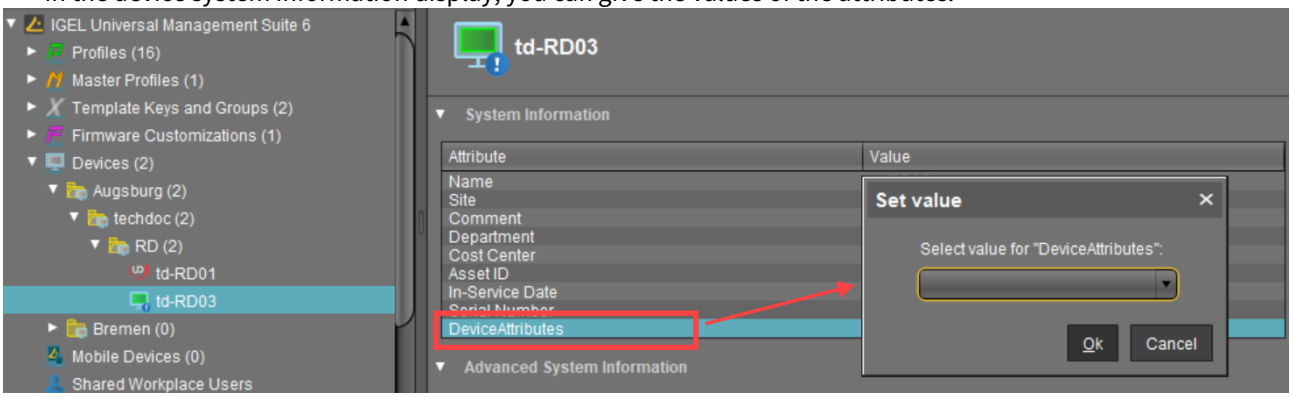
> From UMS *Version 5.07.100*, attributes with set values can be defined, e.g. to avoid typing errors when entering the values. To do this, select the “List” **attribute type** and give the values together with any descriptions under **List entries**.

▶ Click on ⊕ to set up a new device attribute.

- **Name**: Name of the attribute
- **Type**: Data type of the attribute
  Possible values:
  String: A sequence of letters, numbers, and special characters is expected.
  List: A list of values is provided for selection. These values are specified as shown below:
  List entries
  - **Value**: Name of the predefined value
  - **Description**: Optional description of the value
  Number: A numerical value is expected.
  Date: A date is expected.
- **Description**: Optional description of the attribute

▶ Using the **up** and **down arrows**, you can change the order of the additional attributes.

▶ In the device system information display, you can give the values of the attributes.

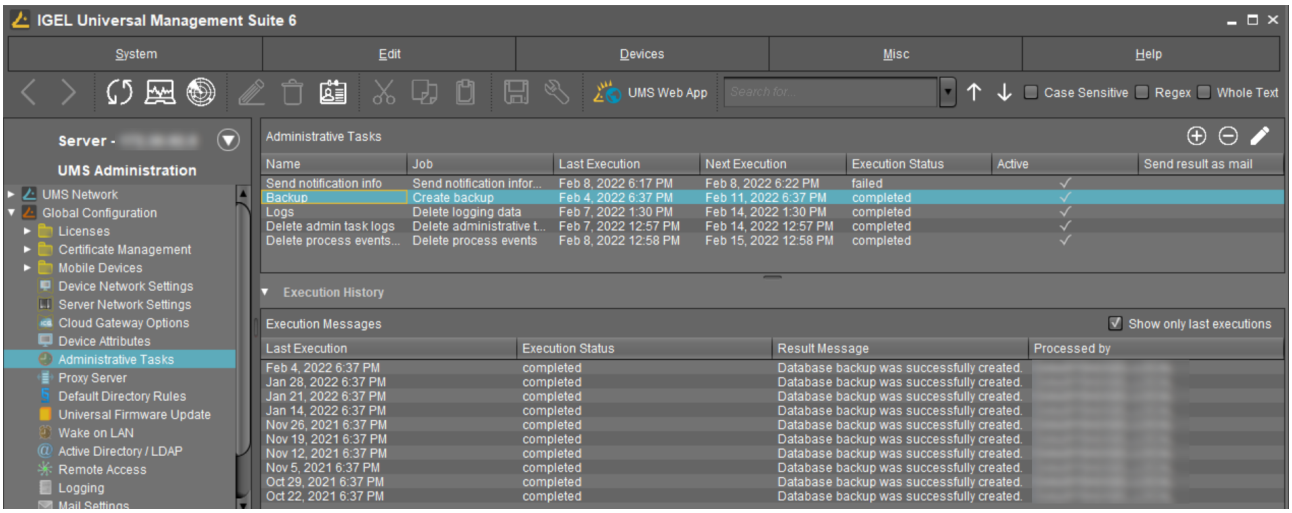


Administrative Tasks - Configure Scheduled Actions for the IGEL UMS

You can define administrative tasks for the IGEL Universal Management Suite (UMS). A task consists in sending an action automatically at a defined time. Examples of such actions include creating a database backup (for embedded databases only) or removing unused firmware files. Tasks can be repeated at intervals or on specific days of the week.

To avoid problems with UMS performance and with backup restoring (see Restoring a Backup (see page 550)), it is highly recommended to use administrative tasks to automatically clean up logs – logging data, job execution data, execution data of administrative tasks, process events, asset information history.

Menu path: **UMS Administration > Global Configuration > Administrative Tasks**



How to Create an Administrative Task

To create an administrative task, proceed as follows:

1. Click on .
2. In the **Create Administrative Task** dialog, configure the necessary settings. What settings are available depends on the chosen **action**. The settings are spread over a number of pages. You can switch between these by clicking on **Next** and **Back**.
   The following actions are available:
   - Create Data Backup (see page 454)
   - Remove Unused Firmwares (see page 457)
   - Refresh Caches (see page 459)
   - Delete Logging Data (see page 461)
   - Delete Job Execution Data (see page 464)

- Delete Administrative Job Execution Data (see page 466)
- Delete Process Events (see page 468)
- Delete Devices (see page 470)
- Export View Result via Mail (see page 472)
- Save View Results in the File System (see page 474)
- Assign Objects to the Devices of Views (see page 476)
- Delete Asset Information History (see page 478)
- Send Notification Information via Email (see page 480)

3. Click on **Finish**.
   The task is defined and will be shown in the content panel. The **Execution Status** will show if the administrative task was executed successfully or failed.

Create Data Backup

Menu path: **UMS Administration > Administrative Tasks >** Dialog "**Create Administrative Task**" **> Action** "**Create backup**"

You can define a scheduled backup of the database as an administrative task.

General

Name: Name for the task.

Action: "**Create backup**".

Description: Optional description of the task.

Send result as mail

☑ The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

☑ The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under Mail Settings (see page 506).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

☑ The task will be executed at the set time. (Default)

☐ The task will not be executed.

Configuration

Maximum amount of backups: If the number of backup files defined in **Target directory** of the data backup package is reached, the oldest backup file will be deleted when a new backup is created. The value "0" means that the number of backup files is unlimited.

Target directory: Local directory path on the UMS Server in which the backup files are saved.

> ⓘ Ensure that the target directory is a valid local directory path on the UMS Server. The UMS Server can be on a different computer, i.e. not on the one where the UMS Console is located.

Backup components: Select at least one of the following components:

- "Database (embedded DB only)"
- "Licenses (embedded DB only)"
- "Configurations"
- "Transfer files (embedded DB only)"

Server Assignment

> The **Server Assignment** settings page is displayed only if you deploy High Availability (see page 560) environment.

Assignment type

Possible options:

- "One server (random)": The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- "One server (select one)": You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- "All servers": The task will be executed by all servers.

Assigned servers: List of servers that are available for this task.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

☑ The task will be repeated at the set time interval.

☐ The task will not be repeated at the set time interval.

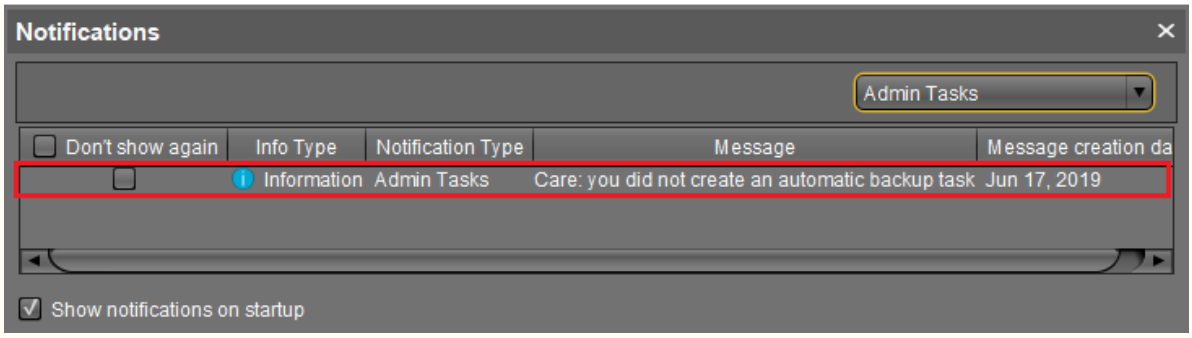
Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via ... . Further information on the public holiday lists can be found under Misc (see page 253).

Expiration: Point in time as of which the task will no longer be repeated.

> **Administrative Tasks Notification**
>
> If you have not set an administrative task "Create Data Backup (see page 454)", after the start of the UMS Console, the following notification pop-up will be shown:



Only users with read permission for administrative tasks can see this notification. You can set the rights under **Edit** > **Access control**.
You can manage the display settings under **Misc > Settings > Notifications**.
You can find the notifications under **Help > Notifications**.

Remove Unused Firmwares

Menu path: **UMS Administration > Administrative Tasks >** Dialog **Create Administrative Task >** Action "**Remove unused firmwares**"

You can define the removal of unused firmware as an administrative task.

> The first firmware that was registered in your UMS installation can not be removed.

General

Name: Name for the task.

Action: "**Remove unused firmwares**".

Description: Optional description of the task.

Send result as mail

☑ The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

☑ The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under Mail Settings (see page 506).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

☑ The task will be executed at the set time. (Default)

☐ The task will not be executed.

Server Assignment

> The **Server Assignment** settings page is displayed only if you deploy High Availability (see page 560) environment.

Assignment type

Possible options:

- "One server (random)": The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- "One server (select one)": You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- "All servers": The task will be executed by all servers.

Assigned servers: List of servers that are available for this task.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

☑ The task will be repeated at the set time interval.

☐ The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via ... . Further information on the public holiday lists can be found under Misc (see page 253).

Expiration: Point in time as of which the task will no longer be repeated.

Refresh Caches

Menu path: **UMS Administration > Administrative Tasks >** Dialog **Create Administrative Task > Action** "**Refresh Caches**"

You can define an administrative task as a result of which the cache of the UMS Server will be refreshed.

Information regarding configuration of the cache can be found under Cache (see page 505).

General

Name: Name for the task.

Action: "**Refresh caches**".

Description: Optional description of the task.

Send result as mail

☑ The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

☑ The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under Mail Settings (see page 506).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

☑ The task will be executed at the set time. (Default)

☐ The task will not be executed.

Server Assignment

> ⓘ The **Server Assignment** settings page is displayed only if you deploy High Availability (see page 560) environment.

Assignment type

Possible options:

- "One server (random)": The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- "One server (select one)": You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- "All servers": The task will be executed by all servers.

Assigned servers: List of servers that are available for this task.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

☑ The task will be repeated at the set time interval.

☐ The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via ... . Further information on the public holiday lists can be found under Misc (see page 253).

Expiration: Point in time as of which the task will no longer be repeated.

Delete Logging Data

Menu path: **UMS Administration > Administrative Tasks >** Dialog "**Create Administrative Task**" **> Action** "**Delete logging data**"

You can define the deletion of UMS message and event logs as an administrative task.

> The logs for Secure Shadowing (see page 388) will not be deleted as a result of this administrative task.

General

Name: Name for the task.

Action: "**Delete logging data**".

Description: Optional description of the task.

Send result as mail

☑ The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

☑ The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under Mail Settings (see page 506).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

☑ The task will be executed at the set time. (Default)

☐ The task will not be executed.

Configuration

Target directory for export files: Local directory path on the UMS Server in which the backup files are saved. If you leave the field empty, the directory `\rmguiserver\temp` will be used. The file names will be formed as follows: `Igel_log_events_.xml`, `Igel_log_messages_.xml.`

> Ensure that the target directory is a valid local directory path on the UMS Server. The UMS Server can be on a different computer from the one on which the UMS Console is located. If you do not specify a directory, the data will automatically be exported to the following directory: `C:\Program Files\IGEL\RemoteManager\rmguiserver\temp`

The following deletion settings specify which data from the **Delete logging data** administrative task are deleted. The deletion settings only take effect if this administrative task is executed.

Log message deletion settings

- **Keep no more than [number] messages**: When this administrative task is executed, the oldest log entries will be deleted so that the number of log entries set here is retained. (Default: 10,000)
  Example: In the UMS, 100 log entries are saved. In the administrative task, **Keep no more than 10 messages** is set. When the administrative task is executed, the 90 oldest log entries will be deleted while the 10 newest log entries will be retained.
- **Delete messages older than [number] days**: Message log entries that are older than the number of days specified here will be deleted. (Default: 5)

Log event deletion settings

- **Keep no more than [number] events**: The oldest event log entries will be deleted so that the number of event log entries set here is retained. (Default: 10,000)
  Example: In the UMS, 100 event log entries are saved. In the administrative task, **Keep no more than 10 events** is set. When the administrative task is executed, the 90 oldest event log entries will be deleted while the 10 newest event log entries will be retained.
- **Delete events older than [number] days**: Event log entries that are older than the number of days specified here will be deleted. (Default: 5)

Server Assignment

> The **Server Assignment** settings page is displayed only if you deploy High Availability (see page 560) environment.

Assignment type

Possible options:

- "One server (random)": The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- "One server (select one)": You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- "All servers": The task will be executed by all servers.

Assigned servers: List of servers that are available for this task.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

☑ The task will be repeated at the set time interval.

☐ The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

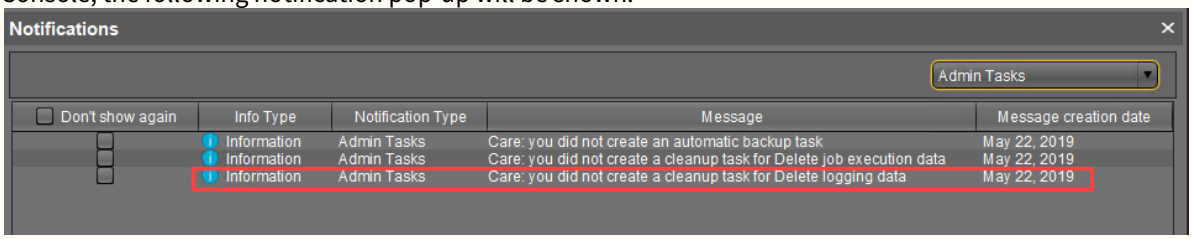
Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via ... .
Further information on the public holiday lists can be found under Misc (see page 253).

Expiration: Point in time as of which the task will no longer be repeated.

Administrative Task Notification

If you have not set an administrative task "Delete Logging Data (see page 461)", after the start of the UMS Console, the following notification pop-up will be shown:



Only users with read permission for administrative tasks can see this notification. You can set the rights under **Edit** > **Access control**.
You can manage the display settings under **Misc > Settings > Notifications**.
You can find the notifications under **Help > Notifications**.

Delete Job Execution Data

Menu path: **UMS Administration > Administrative Tasks >** Dialog "**Create Administrative Task**" **> Action** "**Delete job execution data**"

You can define the deletion of the results of **Jobs** (see page 401) as an administrative task.

General

Name: Name for the task.

Action: "**Delete job execution data**".

Description: Optional description of the task.

Send result as mail

☑ The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

☑ The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under Mail Settings (see page 506).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

☑ The task will be executed at the set time. (Default)

☐ The task will not be executed.

Configuration

Target directory for export files: Directory on the UMS Server in which the logging data are to be backed up before they are deleted from the UMS database. The data will only be deleted from the database if the backup was successful. If you leave the field empty, the directory `\rmguiserver\temp` will be used. The file name for the logging data is structured as follows: `Igel_deleted_job_exec_.csv`.

Deletion settings: You can specify here the criteria according to which task protocols are deleted.

- **Keep no more than [number] executions per job**: Each job has executions. Each execution can have thousands of results. This task deletes all executions and their results except for the specified number of the newest executions. (Default: 10)
- **Delete events older than [number] days**: Protocols that are older than the number of days specified here will be deleted. (Default: 5)

Server Assignment

> The **Server Assignment** settings page is displayed only if you deploy High Availability (see page 560) environment.

Assignment type

Possible options:

- "One server (random)": The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- "One server (select one)": You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- "All servers": The task will be executed by all servers.

Assigned servers: List of servers that are available for this task.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

☑ The task will be repeated at the set time interval.

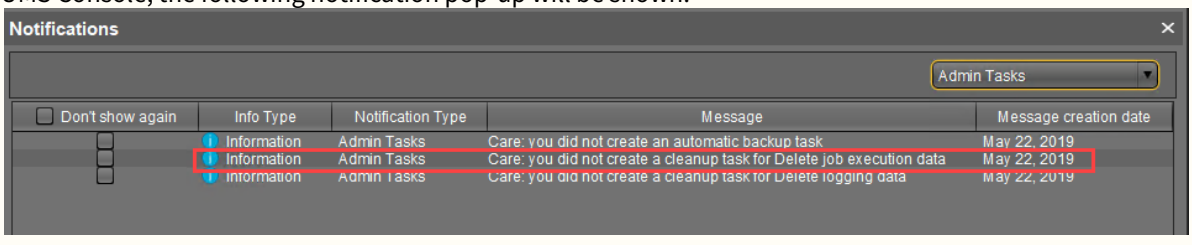
☐ The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via ... . Further information on the public holiday lists can be found under Misc (see page 253).

Expiration: Point in time as of which the task will no longer be repeated.

> **Administrative Task Notification**
>
> If you have not set an administrative task "Delete Job Execution Data (see page 464)", after the start of the UMS Console, the following notification pop-up will be shown:
>
> 
>
>
> Only users with read permission for administrative tasks can see this notification. You can set the rights under **Edit** > **Access control**.
> You can manage the display settings under **Misc > Settings > Notifications**.
> You can find the notifications under **Help > Notifications**.

Delete Administrative Job Execution Data

Menu path: **UMS Administration > Administrative Tasks >** Dialog **Create Administrative Task > Action "Delete administrative job execution data"**

You can define the deletion of the results of **Administrative Tasks** (see page 452) as an administrative task.

General

Name: Name for the task.

Action: "**Delete administrative job execution data**".

Description: Optional description of the task.

Send result as mail

☑ The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

☑ The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under Mail Settings (see page 506).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

☑ The task will be executed at the set time. (Default)

☐ The task will not be executed.

Configuration

Directory for export files: Directory on the UMS Server in which the logging data are to be backed up. The data will only be deleted from the database if the backup was successful. If you leave the field empty, the directory `\rmguiserver\temp` will be used. The file name for the logging data is structured as follows: `Igel_deleted_job_exec_.csv` .

Keep no more than [number] executions per administrative task: Each administrative task has executions. Each execution can have thousands of results. This task deletes all executions and their results except for the specified number of the newest executions. (Default: 10)

Delete events older than [number] days: Event log entries that are older than the number of days specified here will be deleted. (Default: 5)

Server Assignment

> The **Server Assignment** settings page is displayed only if you deploy High Availability (see page 560) environment.

Assignment type

Possible options:

- "One server (random)": The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- "One server (select one)": You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- "All servers": The task will be executed by all servers.

Assigned servers: List of servers that are available for this task.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

☑ The task will be repeated at the set time interval.

☐ The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via ... . Further information on the public holiday lists can be found under Misc (see page 253).

Expiration: Point in time as of which the task will no longer be repeated.

Delete Process Events

Menu path: **UMS Administration > Administrative Tasks >** Dialog **Create Administrative Task > Action "Delete process events"**

You can define the deletion of process events as an administrative task.

General

Name: Name for the task.

Action: "**Delete process events**".

Description: Optional description of the task.

Send result as mail

☑ The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

☑ The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under Mail Settings (see page 506).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

☑ The task will be executed at the set time. (Default)

☐ The task will not be executed.

Configuration

Directory for exported files: Directory on the UMS Server in which the logging data are to be backed up before they are deleted from the UMS database. The data will only be deleted from the database if the backup was successful. If you leave the field empty, the directory `\rmguiserver\temp` will be used. The file name for the logging data is structured as follows: `Igel_deleted_job_exec_.csv`.

Keep no more than [number] process events: When this administrative task is executed, the oldest log entries will be deleted so that the number of log entries set here is retained. (Default: 1,000)
Example: In the UMS, 100 log entries are saved. In the administrative task, **Keep no more than 10 process events** is set. When the administrative task is executed, the 90 oldest log entries will be deleted while the 10 newest log entries will be retained.

Delete events older than [number] days: Event log entries that are older than the number of days specified here will be deleted. (Default: 5)

Server Assignment

> The **Server Assignment** settings page is displayed only if you deploy High Availability (see page 560) environment.

Assignment type

Possible options:

- "One server (random)": The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- "One server (select one)": You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- "All servers": The task will be executed by all servers.

Assigned servers: List of servers that are available for this task.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

☑ The task will be repeated at the set time interval.

☐ The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via ... . Further information on the public holiday lists can be found under Misc (see page 253).

Expiration: Point in time as of which the task will no longer be repeated.

Delete Devices

Menu path: **UMS Administration > Administrative Tasks >** Dialog **Create Administrative Task > Action "Delete devices"**

You can define an administrative task as a result of which specific devices will be deleted from the UMS database. Which devices are to be deleted is defined through the criteria of a view. Example: All devices that have not been booted for more than a year.

General

Name: Name for the task.

Action: "**Delete devices**".

Description: Optional description of the task.

Send result as mail

☑ The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

☑ The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under Mail Settings (see page 506).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

☑ The task will be executed at the set time. (Default)

☐ The task will not be executed.

Configuration

Attach to view: View which specifies the criteria for deleting devices. The view is selected via the ... button.

View ID: ID of the selected view.

Server Assignment

> ⓘ The **Server Assignment** settings page is displayed only if you deploy High Availability (see page 560) environment.

Assignment type

Possible options:

- "One server (random)": The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- "One server (select one)": You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- "All servers": The task will be executed by all servers.

Assigned servers: List of servers that are available for this task.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

☑ The task will be repeated at the set time interval.

☐ The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via ... . Further information on the public holiday lists can be found under Misc (see page 253).

Expiration: Point in time as of which the task will no longer be repeated.

Export View Result via Mail

Menu path: **UMS Administration > Administrative Tasks >** Dialog **Create Administrative Task >** Action "**Export view result via mail**"

You can define an administrative task as a result of which the results of a view will be exported as a mail attachment.

> In order for emails to be sent, the UMS mail settings must be correct. Further information can be found under Mail Settings (see page 506).

General

Name: Name for the task.

Action: "**Export view result via mail**".

Description: Optional description of the task.

Send result as mail

☑ The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

☑ The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under Mail Settings (see page 506).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

☑ The task will be executed at the set time. (Default)

☐ The task will not be executed.

Configuration

View ID: ID of the selected view. The view is selected via the  button.

Visible columns configuration: Data fields which the email will contain.

Mail recipients: Email addresses of the recipients. If you enter a number of addresses, you must separate them using a semicolon ";".

Result format: Data format in which the results are sent as a mail attachment.
Possible options:

- "XML"
- "HTML"
- "CSV"

Create archive

☑ The mail attachment will be compressed as a ZIP archive.

☐ The mail attachment will retain its data format (XML, HTML, or CSV). (Default)

Server Assignment

> The **Server Assignment** settings page is displayed only if you deploy High Availability (see page 560) environment.

Assignment type

Possible options:

- "One server (random)": The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- "One server (select one)": You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- "All servers": The task will be executed by all servers.

Assigned servers: List of servers that are available for this task.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

☑ The task will be repeated at the set time interval.

☐ The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via  . Further information on the public holiday lists can be found under Misc (see page 253).

Expiration: Point in time as of which the task will no longer be repeated.

Save View Results in the File System

Menu path: **UMS Administration > Administrative Tasks >** Dialog **Create Administrative Task >** Action"**Save view results in the file system**"

You can define an administrative task as a result of which the results of a view will be saved in the file system of the UMS Server.

General

Name: Name for the task.

Action: "**Save view results in the file system**".

Description: Optional description of the task.

Send result as mail

☑ The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

☑ The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under Mail Settings (see page 506).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

☑ The task will be executed at the set time. (Default)

☐ The task will not be executed.

Configuration

View ID: ID of the selected view. The view is selected via the ... button.

Visible columns configuration: Data fields which the email will contain. The data fields are selected via the ... button. With the checkbox next to **Column name**, you can select all data fields at once.

Target directory for export files: Directory on the UMS Server in which the view results are saved. If no directory is specified, the default directory will be used. The target directory is shown under the entry field.

Result format: Data format in which the results are saved:
Possible options:

- "XML"
- "HTML"
- "CSV"

Create archive

☑ The file is compressed as a ZIP archive.

☐ The file retains its data format (XML, HTML, or CSV). (Default)

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

☑ The task will be repeated at the set time interval.

☐ The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via ... . Further information on the public holiday lists can be found under Misc (see page 253).

Expiration: Point in time as of which the task will no longer be repeated.

Assign Objects to the Devices of Views

Menu path: **UMS Administration > Administrative Tasks >** Dialog **Create Administrative Task > Action** "**Assign objects to the devices of views**"

You can assign objects to devices that you have filtered via a view or search and update this assignment regularly using a schedule.

See also the instructions in Assigning Objects to a View (see page 400).

General

Name: Name for the task.

Action: "**Assign objects to the devices of views**".

Description: Optional description of the task.

Send result as mail

☑ The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

☑ The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under Mail Settings (see page 506).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

☑ The task will be executed at the set time. (Default)

☐ The task will not be executed.

Select Views / Device Searches

▶ Click on  to select views or device searches that will be assigned to one or more objects.

Select Objects

▶ Click on  to select one or more objects to which you would like to assign the views or device searches.

Objects can be

- profiles
- firmware customizations
- files
- firmware updates.

Server Assignment

> The **Server Assignment** settings page is displayed only if you deploy High Availability (see page 560) environment.

Assignment type

Possible options:

- "One server (random)": The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- "One server (select one)": You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- "All servers": The task will be executed by all servers.

Assigned servers: List of servers that are available for this task.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

☑ The task will be repeated at the set time interval.

☐ The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via ... . Further information on the public holiday lists can be found under Misc (see page 253).

Expiration: Point in time as of which the task will no longer be repeated.

Delete Asset Information History

Menu path: **UMS Administration > Administrative Tasks >** Dialog **Create Administrative Task > Action** "**Delete asset information history**"

You can define the deletion of the history of asset information (see page 606) as an administrative task.

General

Name: Name for the task.

Action: "**Delete asset information history**".

Description: Optional description of the task.

Send result as mail

☑ The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

☑ The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under Mail Settings (see page 506).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

☑ The task will be executed at the set time. (Default)

☐ The task will not be executed.

Configuration

Target directory for export files: Directory on the UMS Server in which the asset data are to be backed up. If you leave the field empty, the directory `C:/Program Files/IGEL/RemoteManager/rmguiserver/temp` wil l be used.

History deletion settings

Delete asset info history older than: Indication in days how old the information to be deleted should be. (Default: 5)

Delete only unused assets:

☑ Only unused assets are deleted in the specified time period. (Default)

☐ All assets are deleted in the specified time period.

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

☑ The task will be repeated at the set time interval.

☐ The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via ... . Further information on the public holiday lists can be found under Misc (see page 253).

Expiration: Point in time as of which the task will no longer be repeated.

Send Notification Information via Email

Menu path: **UMS Administration > Global Configuration > Administrative Tasks >** Dialog **Create Administrative Task > Action** "**Send notification information via email**"

You can send a notification (see page 177) information via email scheduled with an administrative task.

General

Name: Name for the task.

Action: "**Send notification information via email**".

Description: Optional description of the task.

Send result as mail

☑ The result of the task will be sent to the specified recipients via email.

The following two options are active if **Send result as mail** is enabled:

Send to default recipient (not defined)

☑ The email will be sent to the email address defined under **Mail Settings > Mail Recipient**. Further information can be found under Mail Settings (see page 506).

Additional recipients: Other email addresses to which the email will be sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Active

☑ The task will be executed at the set time. (Default)

☐ The task will not be executed.

Configuration

Mail recipients: Email address(es) of the recipients.

Result format: Data format in which the results of the task are sent as a mail attachment.
Possible options:

- "XML" (Default)
- "HTML"
- "CSV"

Create archive

☑ An archive is created.

☐ No archive is created. (Default)

Export: Defines whether all notifications or only new ones have to be exported.
Possible options:

- **All notifications** (Default)
- **Only new notifications**

Export notifications about: Defines the type of notifications (see page 262) that will be exported.
Possible options:

- **Universal Firmware Updates**
- **Universal Management Licenses**
- **Device Licenses**
- **Disk Usage**
- **Global Notifications**

Schedule

Start: Point in time at which the task is executed.

Task starts every [number of time units]

☑ The task will be repeated at the set time interval.

☐ The task will not be repeated at the set time interval.

Weekdays: The task will be executed on the activated weekdays at the point in time specified under **Start**.

Monthly: The task will be executed monthly at the point in time specified under **Start**.

Exclude public holidays: The task will not be executed on the days listed in the public holiday lists selected via ... .
Further information on the public holiday lists can be found under Misc (see page 253).

Expiration: Point in time as of which the task will no longer be repeated.

Proxy Server

Menu path: **UMS Administration > Global Configuration > Proxy Server**

In this area, you can add and configure proxy servers in order to use them in the following scenarios:

- IGEL Cloud Gateway
- Automatic license distribution
- Universal Firmware Update
- UMS update check

> After an update to UMS *Version 5.08.100*, the proxy server that was previously used for the Universal Firmware Update will be adopted as the default proxy server.

The automatic license distribution, Universal Firmware Update and UMS update check scenarios are automatically linked to the default proxy server.

> The settings for the IGEL Cloud Gateway are not changed; the proxy server must be added manually here.

Proxy Server

All configured proxy servers are shown in this list.

- **Show passwords**
  - ☑ Passwords are made visible in the list.
  - ☐ Passwords are not shown. (Default)

	Add proxy server
	Delete proxy server
	Edit proxy server
	Define selected proxy server as default server

> Only servers that are not used can be deleted. The proxy server added first will automatically be the default proxy server.

Proxy Server Uses

All uses for the selected proxy servers are shown in this list.

The entries in this list appear automatically as soon as an application was linked to a selected proxy server.

Default Directory Rules

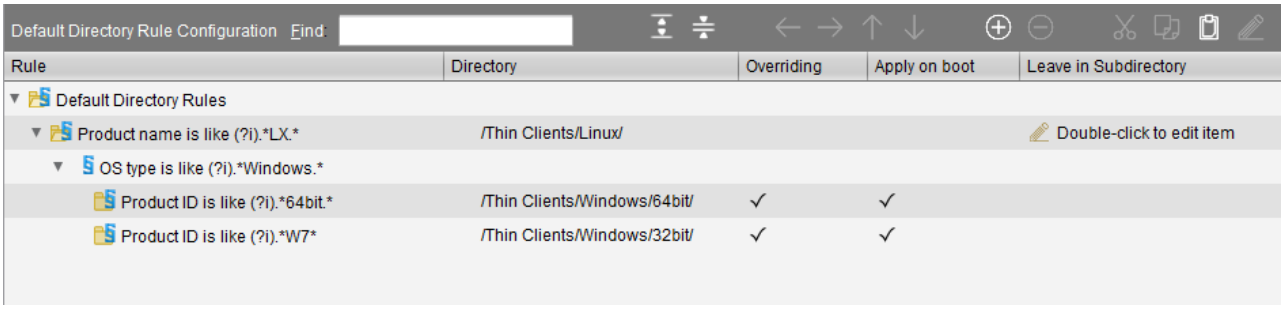
Menu path: **UMS Administration > Global Configuration > Default Directory Rules**

Rules for default directories are used to automatically classify devices into specific directories during registration. These directories can be linked to profiles which are then assigned to the devices contained. As a result, you can automatically configure the devices during registration (zero touch deployment).

See also the following how-tos for further information:

- Creating a Default Directory Rule (see page 486)
- Using Structure Tags (see page 68)

▶ Go to **UMS Administration > Global Configuration > Default Directory Rules**.
The user interface looks like this:



When you open a UMS database from an older version with UMS *Version 5.03.100* or newer for the first time, the default directory rules will automatically be converted into the new structure. Rules for the IP range will be split into two rules (IP greater than and IP less than).

- Symbol Bar (see page 485)
- Creating a Default Directory Rule (see page 486)
- Finding Default Directory Rules (see page 489)
- Applying Rules (see page 490)
- Editing a Rule (see page 491)
- Combining Conditions (see page 492)
- Using the Netmask (see page 494)

Symbol Bar

Menu path: **UMS Administration > Global Configuration > Default Directory Rules**

In the symbol bar for default directory rules, you will find buttons for frequently used commands:

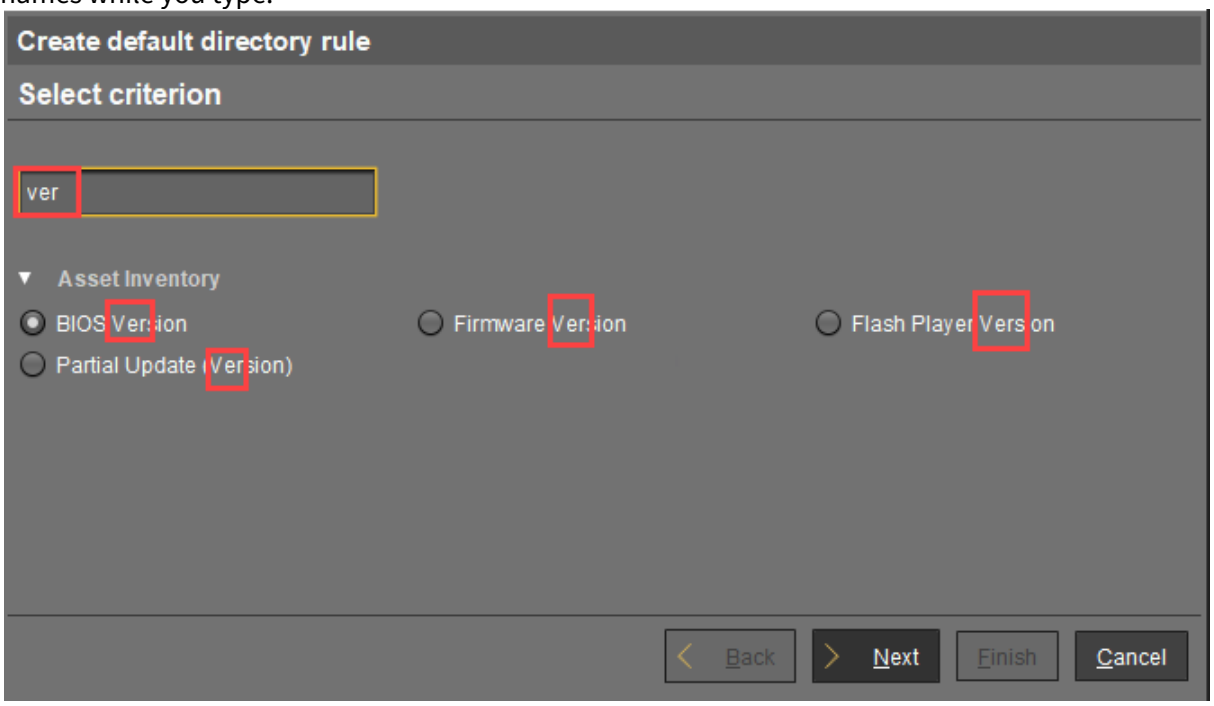
The symbols are as follows (in the correct order):

	Find (in all columns)
	Expand all rules
	Collapse all rules
	Move rule a level up
	Move rule a level down
	Move rule up in the sequence
	Move rule down in the sequence
	Add rule (as last child of the currently selected rule)
	Delete rule (including subordinate rules)
	Cut objects
	Copy objects
	Paste objects
	Edit

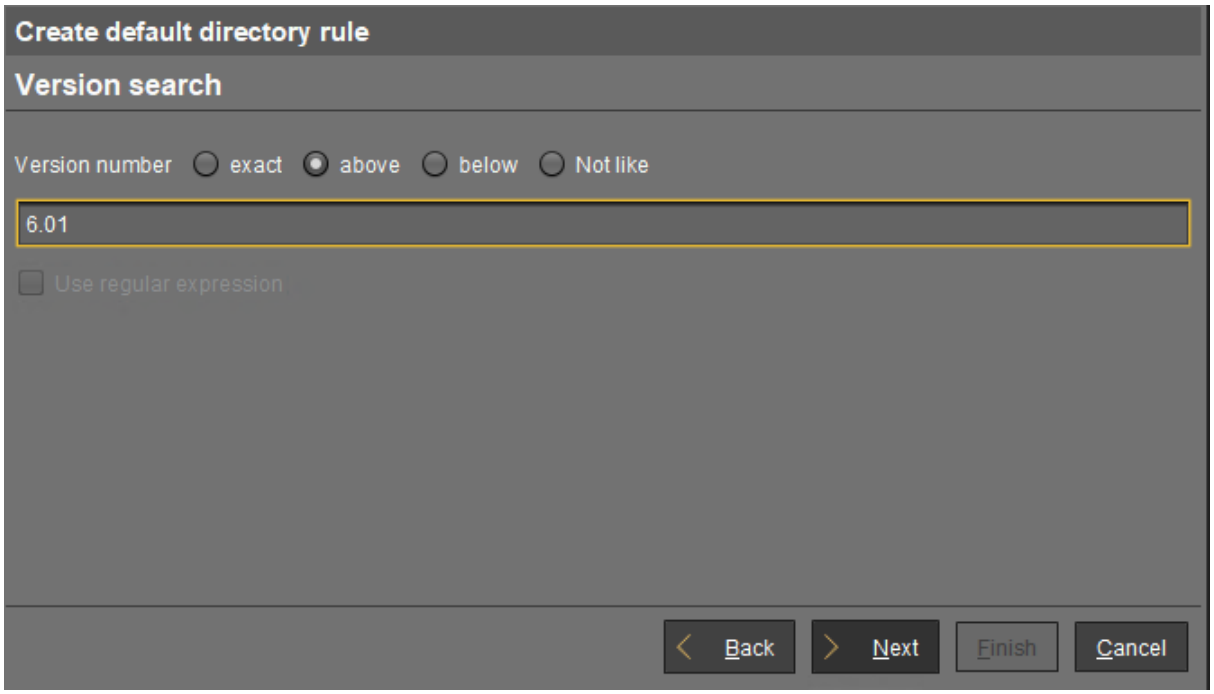
Creating a Default Directory Rule

Menu path: **UMS Administration > Global Configuration > Default Directory Rules**

1. Click on the ⊕ symbol.
2. The **Create Default Directory Rule** dialog will open.
3. Select a **criterion**. To help you, a search field narrows down the selection to matching parameter names while you type.

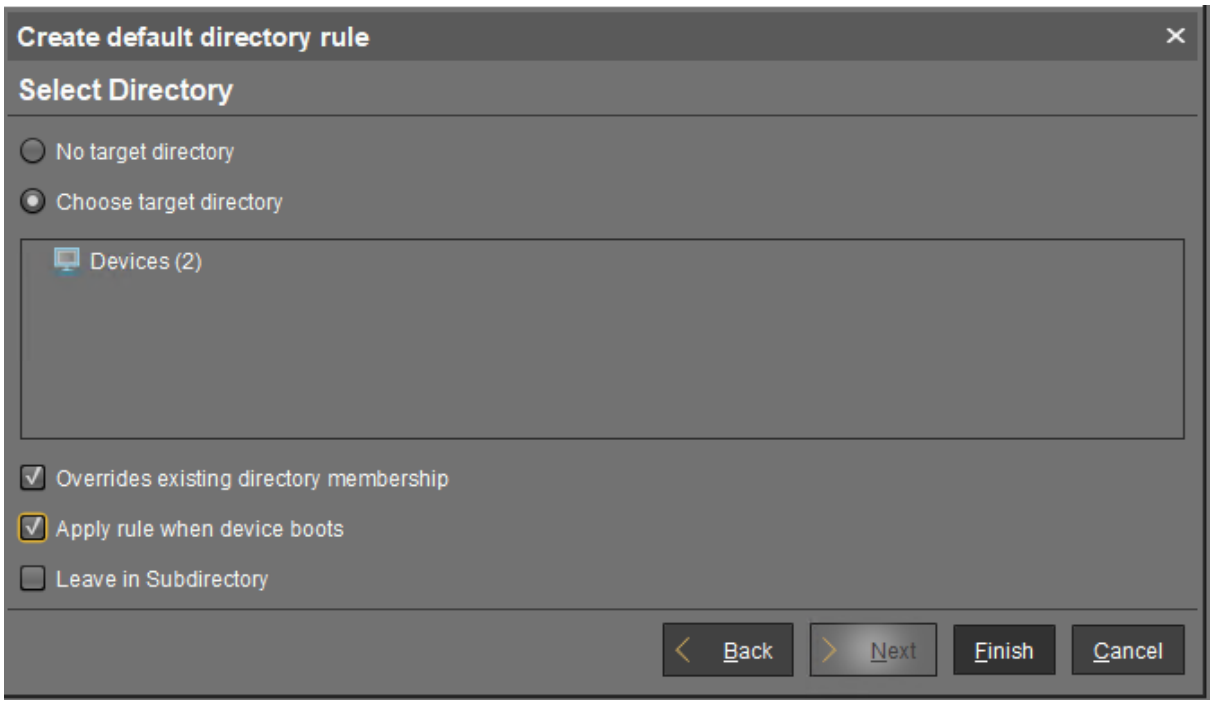


4. Specify the comparative value and comparative operator for the criterion.



If you create a rule which contains a range (from - to), this will automatically be converted into a pair of rules linked with AND (from AND to). This applies for example to date or IP ranges.

5. Select a target directory (must already exist) or select the **No target directory** option.
   With the **Choose target directory** option, you have the following further options:
   - **Overides existing directory membership**
     ☑ A previously registered device is re-registered in the target directory.
   - **Apply rule when device is booting**
     ☑ The rule is applied not only when registering but also each time the devices boot.
   - **Leave in Subdirectory**
     ☑ A device will not be moved if it is already in a subdirectory of the target directory.



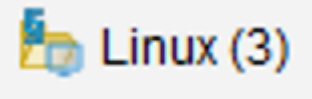
6. Finish creating the rule by clicking on **Finish**.

> The order of the rules is important. Generally speaking, the default directory rules tree is worked through from top to bottom for each device. If the criterion of a rule applies and it has a target directory, its children rules will be scrutinized. If none of the children rules apply, the device will be moved to the target directory of the rule above. If however one of the children rules applies and it has a target directory, this child rule will be taken as a new starting rule and the search will begin again. If an applicable rule does not have a target directory, its children rules will be scrutinized.

Finding Default Directory Rules

From UMS Version 5.03.100 only:

In the structure tree, you can see which directories are the target of a default directory rule. The folder symbol then has a small § symbol.



> A directory which is the target of a default directory rule cannot be deleted. In order to delete it, you must change or delete the directory rule first.

To jump from the directory straight to linked rules, proceed as follows:

1. Right-click on the folder symbol.
2. Select **Find default directory rules** in the context menu.
   The view will switch to the overview of the default directory rules. The first linked rule is highlighted.
3. Press the enter key to jump to further found rules.

Applying Rules

The rules can be applied regardless of new clients being imported or existing clients booting:

From UMS Version 5.03.100:

1. Right-click on **Default Directory Rules** under **UMS Administration > Global Configuration**.
2. Select **Apply rules now...**
   A dialog with further options will open.
3. Select from the following options:
   - **Overrides all existing directory memberships**
     ☑ A previously registered device is re-registered in the target directory.
   - **Default directory for devices:**
     - Leave in current directory
     - Device root directory
     - Other directory (select)
4. Click **Apply** to apply the rules.

Prior to UMS Version 5.03.100:

1. Click on the **Apply rules now...** button in the overview of directory rules.
   A dialog with further options will open.
2. Select from the following options:
   - **Overwrite all existing directory allocations**
     ☑ A previously registered device is re-registered in the target directory.
   - **Default directory for devices:**
     - Leave in current directory
     - Basic directory for devices
     - Other directory (select)
3. Click **Apply** to apply the rules.

Editing a Rule

From UMS Version 5.03.100:

▶ In the rule overview, double-click on a row...

- in the **Rule** column in order to edit the **Criterion**, **Operator** and **Value**.
- in the **Directory** column in order to change or remove the target directory.
- in the **Overiding**, **Apply on boot** or **Leave in subdirectory** column in order to change these options.

Prior to UMS Version 5.03.100:

1. Highlight the desired rule in the overview by clicking on it once.
2. Click the symbol 
   The **Modify Default Directory Rule** window will open.
3. Change the **Directory**, **Criterion**, **Operator**, **Value** and options as required.
   You can also add further conditions with AND or OR links here, see Combining conditions.

Combining Conditions

In the *UMS*, you can combine the conditions of directory rules using AND and OR links.

From UMS Version 5.03.100:

▶ Indent a rule using  in order to create an AND link with the condition of the superordinate rule:

Rule	Directory	Overriding
Default Directory Rules		
Product name is like (?i).*LX.*	/Thin Clients/Linux/	
OS type is like (?i).*Windows.*		
AND Product ID is like (?i).*64bit.*	/Thin Clients/Windows/64bit/	✓
Product ID is like (?i).*W7*	/Thin Clients/Windows/32bit/	✓

Example: In the illustration, devices whose **product ID** contains `Windows` AND `64bit` are moved to the `/devices/Windows/64bit/` directory.

> ⓘ You can use rules which do not have a target directory (linking rules) to combine conditions.

▶ Leave rules equally indented and assign to them the same target directory in order to create an OR link for the conditions.

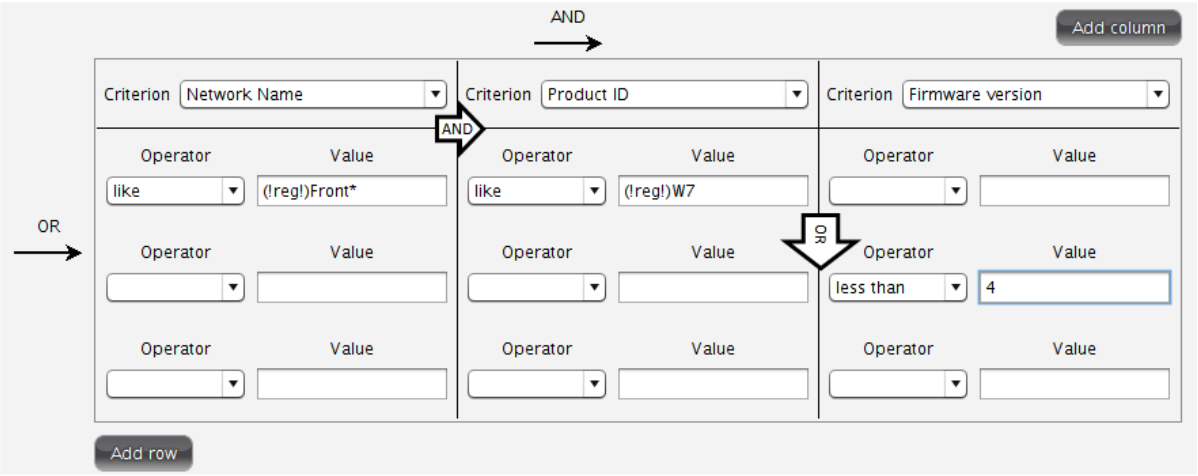
Rule	Directory	Overriding
Default Directory Rules		
Product name is like (?i).*LX.*	/Thin Clients/Linux/	
OS type is like (?i).*Windows.*		
OR Product ID is like (?i).*64bit.*	/Thin Clients/Windows/64bit/	✓
Product ID is like (?i).*W10*	/Thin Clients/Windows/64bit/	✓
Product ID is like (?i).*W7*	/Thin Clients/Windows/32bit/	✓

Example: In the illustration, devices whose **product ID** contains `64bit` OR `W10` are moved to the `/devices/Windows/64bit/` directory.

You can move rules and groups of rules using drag and drop or by copying and pasting with the help of the symbol bar.

Prior to UMS Version 5.03.100:

- When adding a new rule:
  - Select **Narrow search criterion** in the wizard to add an AND-linked condition.
  - Select **Create additional search criterion** to add an OR-linked condition.
- When editing an existing rule:
  - Add a further condition on the right-hand side to create an AND link.
  - Add a further condition below to create an OR link.



Using the Netmask

When creating a directory rule, select the criterion **Net mask**. The thin clients will then be sorted into automatically created directories according to IP address ranges. The name of the folder is determined through this bitwise operation:

```
Folder = IP address of the thin client AND net mask
```

Examples:

IP address	Net mask	Resulting directory
`130.094.122.195`	`255.255.255.224`	`130.094.122.192`
`172.16.232.15`	`255.255.0.0`	`172.16.0.0`
`192.168.1.1`	`255.255.255.0`	`192.168.1.0`

As the **target directory**, select the device directory under which the subfolders for the IP address ranges are to be created.

Because this rule always applies, it is not a good idea to define a further rule. If the net mask rule sorts all devices into directories, no further rule is active.

Universal Firmware Update

Menu path: **UMS Administration > Global Configuration > Universal Firmware Update**

IGEL's public update server is pre-configured. If you would like to use your own FTP server for distributing updates, you can change the server settings accordingly here:

Edit...: Changes the FTP server settings.

- '**Proxy Server**': Host name of the server
- '**Host**': Host name of the server
- '**Port**': Port number. (Default: 21)
- '**User Name**': Name of the user
- '**Password**': User password
- '**Directory**': FTP server path

> Note that **UMS Administration > Global Configuration > Universal Firmware Update** uses active FTP only.

Edit Proxy Configuration:
Possible options:

- '**No Proxy Server**': Direct connection to ICG
- '**Use Default Proxy Server**': Use the proxy server which is configured as default in Proxy Server. (see page 482)
- '**Use Selected Proxy Server**': Select a proxy server from the list.

Test Server Connection: Tests communication between the IGEL server and your own FTP server.

For further information regarding Universal Firmware Update, see Universal Firmware Update (see page 415).

Wake-on-LAN

Menu path: **UMS Administration > Global Configuration > Wake On LAN Configuration**

Devices can be wakened via the network using *magic packets*. A *magic packet* contains the MAC addresses of the devices that are to be wakened. In order for a device to be wakened, it must be in either S3 (suspend to RAM – STR), S4 (suspend-to-disk – STD) or S5 (soft-off) mode. In the *UMS* administration, you can specify the network addresses to which the *magic packets* are sent.

For scenarios where the *UMS* is outside the devices' network and broadcast packets from the WAN are not allowed, you can define one or more Linux devices as a Wake-On-LAN proxy.

> The Wake-On-LAN proxy function is supported by Linux devices from *Version 5.09.100*.

- **Broadcast address**
  ☑ The *magic packet* will be sent to the broadcast address of the network.
- **Last known IP address of the Device**
  ☑ The *magic packet* will be sent to the last known IP address of the device.

- **Automatic Wake On LAN Proxy Detection**
  ☐ If any other client in the subnet is online, this client is automatically used as WoL proxy.

- **All defined subnets**
  ☑ The *magic packet* will be sent to the network addresses of all subnets that are defined for the *UMS*.

  To add a subnet, proceed as follows:
  a. Click on ⊕ in the area below **All defined subnets**.
     The **Define subnets** dialog will open.
  b. In the **Subnet** field, enter the network address of the subnet.
  c. Under **CIDR** (Classless Inter-Domain Routing), select the suitable suffix for the network mask.

  > Values between 8 and 28 are appropriate. Example 1: The network address `10.43.8.0` with the suffix 24 corresponds to the CIDR notation `10.43.8.0/24` with the network mask `255.255.255.0`. This network corresponds to a Class C network. The addresses that can be used by hosts lie between `10.43.8.1` and `10.43.8.254`. Example 2: The network address `10.43.8.64` with the suffix 28 corresponds to the CIDR notation `10.43.8.64/28` with the network mask `255.255.255.240`. The addresses that can be used by hosts lie between `10.43.8.65` and `10.43.8.78`.

  a. If you wish, add a **Comment**.
  b. Click on **OK**.

- **Network address of the last known IP address**
  ☑ The *magic packet* is sent to the network address of the network in which the last known IP address of the device is located. In order for this network address to be determined, you will need to specify a network mask for each of the possible networks.

  To add a network mask, proceed as follows:
  a. Click on  in the area below **Network address of the last known IP address**.
     The **Define network mask** dialog will open.
  b. Enter the **Network Mask**.
  c. If you wish, add a **Comment**.
  d. Click on **OK**.
- **Wake On LAN Proxies**
  ☑ The *magic packet* will be sent to the devices defined as Wake-On-LAN proxies. Each Wake-On-LAN proxy will send the *magic packets* as a broadcast within the network in which it is located.

  > The **Broadcast address**, **Last known IP address of the device**, **All defined subnets** and **Network address of the last known IP** settings have no effect on the Wake-on-LAN proxy.

  ☐ The *magic packet* will not be sent to the devices defined as Wake-On-LAN proxies.

  > Devices configured as a Wake-on-LAN proxy will retain their role, even if **Wake-On-LAN proxies** is disabled.

  To define one or more devices as a Wake-On-LAN proxy, proceed as follows:

  a. Click on  in the area below **Wake On LAN Proxies**.
     The **Edit Wake On LAN Proxies** dialog will open.
  b. Highlight the desired device in the left-hand column.
  c. Click on  to select the device.
  d. Click on **OK**.
     The device will now function as a Wake-On-LAN proxy.

  > A device that is configured as a Wake-On-LAN proxy can no longer be put on standby or shut down. This restriction applies as soon as the device receives the settings from the *UMS*.

  To undo the configuration as a Wake-On-LAN proxy, proceed as follows:

  a. Click on  in the area below **Wake On LAN Proxies**.
     The **Edit Wake On LAN proxies** dialog will open.
  b. Highlight the desired device in the right-hand column.
  c. Click on  to deselect the device.

d. Click on **OK**.
The device will no longer be configured as a Wake-On-LAN proxy as soon as the setting is sent to the device.

Active Directory / LDAP

Menu path: **UMS Administration > Global Configuration > Active Directory / LDAP**

It can make sense to link the UMS Server to an existing Active Directory for two reasons:

- You would like to import users from the AD as UMS administrator accounts.
- You would like to use user profiles via IGEL Shared Workplace.

For both purposes, you first need to link the relevant Active Directories in the **UMS Administration** area under **Global Configuration > Active Directory / LDAP**. See also the how-to Configuring an AD Connection (see page 150).

1. Add a new entry to the list of linked Active Directories by selecting **Add (+)**.
2. Specify the **Domain Name**.
3. Enter the **Domain Controller(s)**.

   If the option **Use LDAPS connection** (see below) is activated, a fully qualified name of the domain controller must be entered, e.g. `dc01.your.domain`

   To separate several domain controllers, a semicolon must be used.
4. Specify the **Page Size**.
   The page size limits the number of hits (i.e. objects) in the Active Directory on the server side. The default value is "1000". Change this value according to your server configuration.
5. Activate **Use LDAPS connection** to secure the connection with the provided certificate.
   The **Port** changes automatically to the default value "636".
6. Click **Import SSL Certificate** to configure the certificate and to verify the **Certificate DN**.

   The **Domain Controller** name and the certificate must correspond, otherwise the connection to the LDAP server will fail. See Problems When Configuring an Active Directory with LDAP over SSL (see page 161).

   If more than one domain controller is used, the root certificate of the domain must be configured.

   The supported certificate formats are `.cer`, `.pem` and `.der`
7. Enter valid user data under **User name** and **Password**.

   For the user, the read permission is sufficient since no changes will be made to the AD data.
8. Specify aliases under **UPN Suffix** if they have been configured (semicolon separated list). Example: `domain.local;test.local`
9. Click **Test connection** to check the connection.

> Several Active Directories can be linked. Therefore, you should ensure that you provide the correct domain when logging in (e.g. to the UMS Console).

> In this document, the terms "Active Directory" and "LDAP" are, to an extent, used interchangeably:
> - Administrative users / UMS administrators can be imported both from an AD and from LDAP.
> - Shared Workplace users can only authenticate against an Active Directory. An LDAP service cannot be used for this purpose.

10. Click **Ok** to save the changes.

Remote Access

Menu path: **UMS Administration > Global Configuration > Remote Access**

You can enable a secure terminal session and a secure VNC connection globally.

Secure terminal

- **Enable secure terminal globally**:
  ☑ Access via the secure terminal is enabled for all registered devices. The firmware must be *IGEL* Linux *Version 5.11.100* or higher.
  ☐ Access via the secure terminal cannot be enabled for all registered devices. However, it can be enabled for individual devices.
- **Log user for secure terminal**: Specifies whether the user name of the *UMS* user who established the connection to the device is logged. The log is shown under **System > Logging > Log secure access**.
  ☑ The user name is contained in the log.
  ☐ The user name is not contained in the log.

Secure VNC

- **Enable secure VNC globally**:
  ☑ Access via secure VNC is enabled for all registered devices.
  ☐ Access via secure VNC is not enabled for all registered devices. However, it can be enabled for individual devices.
- **Log user for secure VNC**: Specifies whether the user name of the *UMS* user who established the connection to the device is logged. The log is shown under **System > Logging > Remote Access**.
  ☑ The user name is contained in the log.
  ☐ The user name is not contained in the log.
- **Preferred encoding**
  Possible options:
  - **Tight**
  - **Raw**
  - **RRE**
  - **Hextile**
  - **Zlib**
- **Color depth**
  Possible values:
  - **24 bit**
  - **8 bit**
- **Refresh Period**: Time in milliseconds within which the display in the VNC Viewer is refreshed.
- **Compression Level**: Specifies the extent to which the transferred data are compressed.
- **JPEG Quality**: Specifies the image quality.
- **Use "Draw Rectangle" mode**
  ☑ The "draw rectangle" mode will be used.

Override VNC viewer settings:

☑ The settings for the VNC Viewer will be overwritten by the settings here.

☐ The VNC Viewer can overwrite the settings here.

Logging

Menu path: **UMS Administration > Global Configuration > Logging**

In this area, you can specify the logging behavior of the UMS for messages and events.

Log Message Settings

Enable logging

☑ UMS user actions will be logged.

☐ UMS user actions will not be logged.

> Logs can be viewed via:
> 1) Menu Bar **> System > Logging > Log Messages**
> 2) Context menu of an object in the structure tree **>** (**Logging**) **> Logging: Messages**

The following options are available if **Enable logging** is activated:

Log administrator data

☑ The name of the administrator who started the action will be logged.

☐ The name will not be logged.

Log level

- Message body and details: The log tells you what action was performed on which object. Further information regarding the object is also saved.
- Message body only: The log tells you what action was performed on which object.

Log level configuration: Enables or disables logging for individual start commands. Examples: **Create profile**, **Delete view**.

Log Event Settings

Activate event logging

☑ Actions initiated by a device will be logged.

☐ Actions initiated by a device will not be logged.

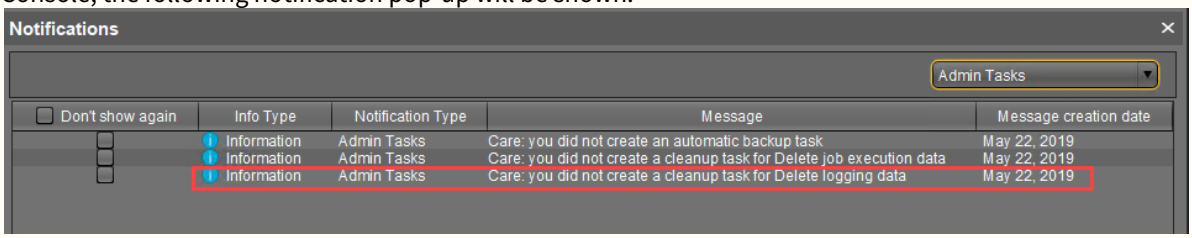
> Logs can be viewed via:
> 1) Menu Bar **> System > Logging > Event Messages**
> 2) Context menu of an object in the structure tree **>** (**Logging**) **> Logging: Event Messages**

The following option is available if **Activate event logging** is enabled:

Log level configuration: Enables or disables logging for individual start commands. Examples: **Authenticate user**, **Shut down device**.

Administrative Task Notification

If you have not set an administrative task "Delete Logging Data (see page 461)", after the start of the UMS Console, the following notification pop-up will be shown:



Only users with read permission for administrative tasks can see this notification. You can set the rights under **Edit** > **Access control**.
You can manage the display settings under **Misc > Settings > Notifications**.
You can find the notifications under **Help > Notifications**.

Cache

Menu path: **UMS Administration > Global Configuration > Cache**

The cache or clipboard is integrated into the UMS GUI server. It is designed to improve overall performance when the device retrieves its settings. Furthermore, the UMS can provide the device settings even if the UMS database is not running. Please bear in mind, however, that you cannot change device settings if the database is not enabled.

Activate cache	Enable or disable cache
Delete orphaned objects	Deletes entries in the cache that cannot be found in the database.
Refresh all	When the cache is updated, you can add to it the settings for all devices which are known to the UMS. Otherwise, only the settings of the devices which have connected at least once to the UMS of the current host will be added.
Refresh on serverstart	The cache is updated when the server is launched. To make detailed changes to the update settings, go into the **UMS Console** and click on **Administrative Tasks** in the **UMS Administration**.

▶ Select **Extras > Manage Cache** in the UMS Console menu.
Various details about the cache are shown in the dialog window. These include which entries can be found in the cache, when the next update will take place etc.

A number of cache actions can also be performed here:

Refresh panel	Provides an updated view of the cache information.
Refresh cache	Updates all cache contents immediately.
Empty cache	Removes all cache entries immediately.

ⓘ The Administration area of the UMS Console also allows you to set up an **administrative task** in order to update the cache automatically on a regular basis.

Mail Settings

Menu path: **UMS Administration > Global Configuration > Mail Settings**

The mail settings described here are required for the following functions:

- Sending a View as Mail (see page 399)
- Export view result as mail (see page 472)
- Export results of the following administrative tasks as mail:
  - Database backup (only for embedded DB) (see page 454)
  - Remove unused firmwares (see page 457)
  - Refresh caches (see page 459)
  - Delete logging data (see page 461)
  - Delete job execution data (see page 464)
  - Delete Devices (see page 470)
  - Assign Objects to the Devices of Views (see page 476)
- Mailing of one-off passwords for IGEL Cloud Gateway (ICG)
  If you would like to use Gmail for sending mails, read the E-Mail Settings for Gmail Accounts (see page 186) How-To.

Mail Settings

- **SMTP host**: Host name or IP address of the SMTP server (outbox)
- **Sender address**: Sender address which is to appear in UMS mails.
- **Enable SMTP authentication**
  ☑ The UMS will log on to the SMTP server in order to send mails. The login data must be defined under **SMTP user name** and **SMTP password**.
- **SMTP user name**: User name when logging on to the SMTP server
- **SMTP password**: Password when logging on to the SMTP server
- **SMTP port**: Port for the connection between the UMS and the SMTP server. For unencrypted SMTP, port 25 is used by default. For SMTP SSL, the default is port 465 and for STARTTLS it is port 587.
- **Enable SMTP-SSL**
  ☑ The mails will be sent with SMTPS encryption.
- **Enable SMTP-STARTTLS**
  ☑ TLS encryption for transporting mails will be enabled in accordance with the STARTTLS procedure.
- **Send Test Mail**: If you click on this button, the UMS will send a test mail.
  You have two options:
  - Test mail will be sent to the sender address (no sender address configured) (Default)
  - Send test mail to the following address
- **Result**: Indicates whether the test mail was sent successfully. If the mail was sent successfully, the text will be highlighted in green. If not, it will be highlighted in red.
- **Mail recipients**: Mail addresses to which the result mails for administrative tasks and the service mails are sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Rich Message Templates

Menu path: **UMS Administration > Global Configuration > Rich Message Templates**

This is the place where to define templates for your rich messages.

To write a message, go to **Devices > Other Device Commands > Send Messages** either in the context menu of a device or in the main menu under **Devices**.

Misc Settings

Menu path: **UMS Administration > Global Configuration > Misc Settings**

The following global parameters can be found here.

Recycle Bin

Enable recycle bin

☑ The recycle bin is enabled. If an object is deleted in the structure tree, it will be moved to the recycle bin. (Default)

See also Deleting Objects in UMS / Recycle Bin (see page 275).

Template Profiles

Enable template profiles

☑ Template profiles (see page 321) are enabled.

Master Profiles

Enable master profiles

☑ Master profiles (see page 319) are enabled.

User Login History

Enable user login history

☑ Recording of the user login activity is enabled. (Default)

Add last device users to quick search

☑ The user who logged in last will be added.

Add only still logged-in users

☑ Only users who are currently logged in will be added. (Default)

ⓘ In the event of configuration changes, the page will need to be reloaded by clicking on  in order for the settings to be applied.

ⓘ In order to view the user login history for a device, click on the relevant device in the structure tree under **Devices**. All information regarding the device will now be shown in the content panel. Scroll right to the bottom to open **User Login History**. The following information is recorded here:

- **User name**: Name of the user who logged in to the device
- **Login time**: Time at which the user logged in
- **Logoff time**: Time at which the user logged off
- **Logon type**: At the moment, this can be Shared Workplace or Kerberos/Active Directory.

Notifications

Enable notifications

☑ Notifications are enabled and will be shown on each connection to the UMS Console, see also Notifications (see page 262). (Default)

☐ The notification function is disabled for all users.

Create warnings [...] days before license expiration: Sets a time limit for a warning to remind you about the expiration of your license. (Default: 30)

Create warnings when free drive space is below [...] MB: When the free drive space is below this value, a warning will be created. (Default: 2048)

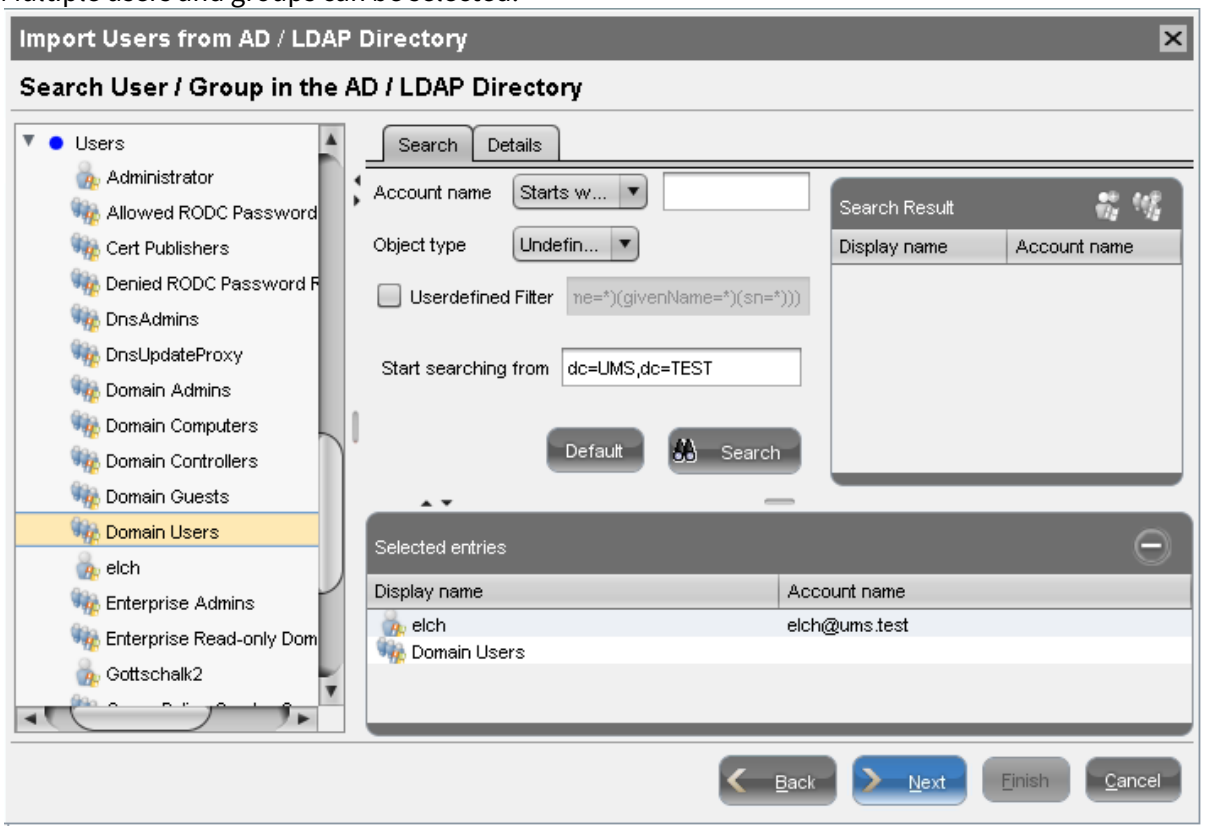
Importing Active Directory Users

Users can be imported from the Active Directory to the UMS console in three steps:

- Logging in to the Active Directory
- Selecting the users to be imported and starting the import
- Logging the import process

To import users from the Active Directory to the UMS console, proceed as follows:

1. Launch the UMS console's import dialog via **System > Administrator Accounts > Import**.
2. Log in to the AD/LDAP service.
   The connection process is described under Linking Active Directory / LDAP (see page 499). When importing user accounts, only connected ADs are available for selection.
3. Click on **Continue**.
   The Active Directory browser will open.
4. Select individual users or groups from the navigation tree of your AD.
   The highlighted users/groups can be added to or removed from the selection to be imported via the context menu or using drag and drop. The users/groups found in the **Found AD Accounts** hit list can be transferred to the **Selected Accounts** list using the symbols.
   Multiple users and groups can be selected.



As an alternative to navigating in the navigation tree, you can also highlight and add users or groups to the selection via the **Search** function.

5. Click on **Continue** to start the import.
   A confirmation window will appear.

Once a user has been successfully imported, this action cannot be undone. A UMS administrator set up by mistake must be deleted manually via the administrator account management system. The *IGEL* UMS uses the **account** as the name of the AD user imported.

Searching in the Active Directory

The options in the AD navigation tree have the following meanings:

Account name: Allows you to search on the basis of account names of parts thereof

Object type: Allows you to restrict a search to users or groups

User-defined filter: Filter criteria in accordance with the RFC-2254 standard

Start searching from	Element within the tree where the search begins
Default	Resets all search options to the standard values
Search	Starts the specified search

The context menu allows the following actions to be performed on items in the list of hits:

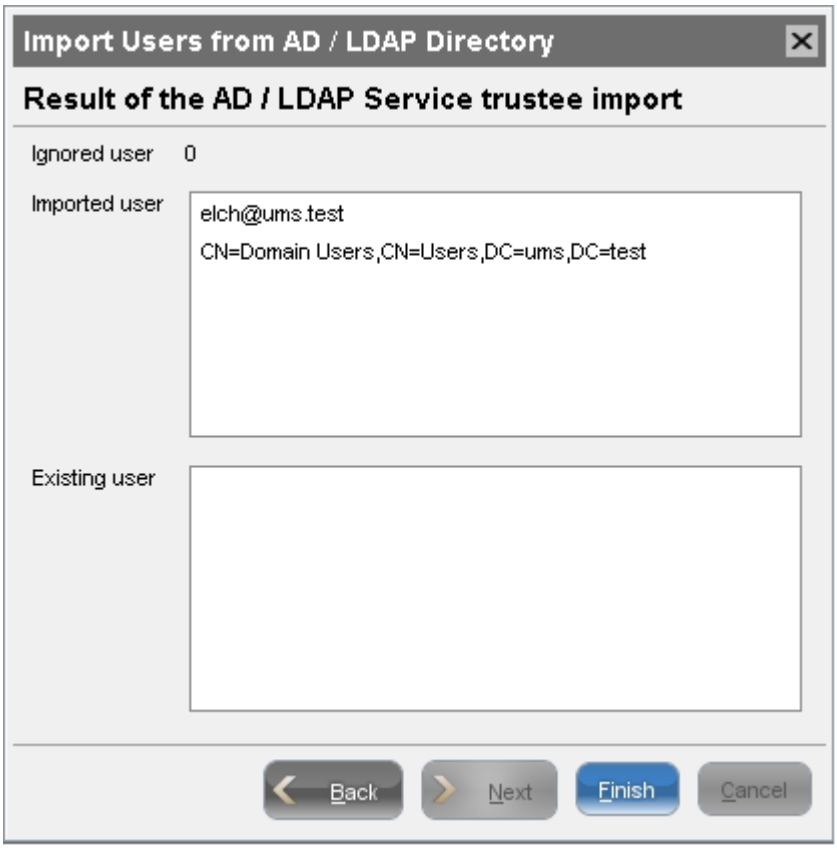
- **Add user**
- **Add group**
- **Start searching from**
- **Details...**

Under **Details**, you can once again bring up the properties of the objects selected for import and remove objects prior to the import if necessary.

Import Results List

Once the import is complete, a results window will appear.

This shows how many accounts were ignored during the import and which ones were imported successfully. If a user account already exists in the UMS, this AD account will be skipped during the import.



Create Administrator Accounts

Menu path: Menu bar **> System > Administrator accounts**

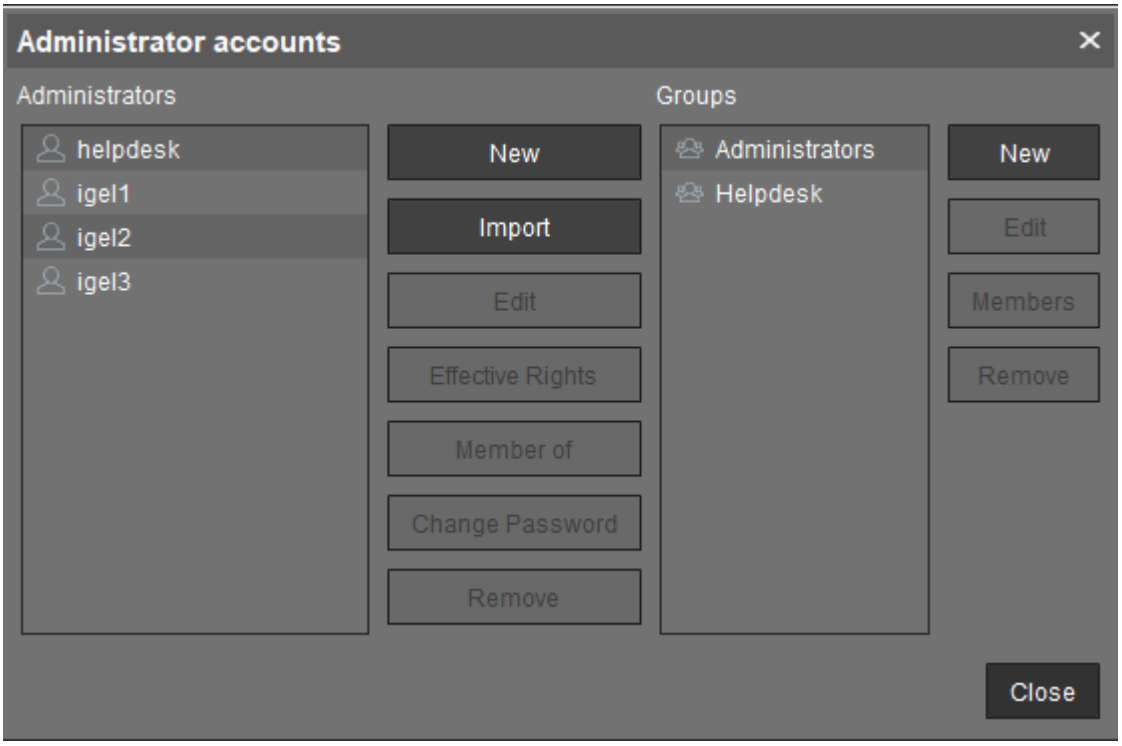
For the purpose of logging in to the UMS Console, you can either import UMS administrator accounts from a linked Active Directory or create, organize, and remove accounts manually.

Access rights to objects or actions within the IGEL UMS are attached to these administrator accounts and groups. The rights of database users who were created during the installation or when setting up the data source cannot be restricted. They always have full access rights in the UMS.

Administrators and Groups

Menu path: Menu bar **> System > Administrator accounts**

▶ In the menu bar, click **System > Administrator accounts** to manage the IGEL UMS administrator accounts.



All available accounts are listed in the left-hand column, while the available groups are listed in the right-hand column. To the right of each column, you will find the associated buttons such as **New**, **Edit**, and **Remove**. For administrator accounts, you can also change the password (**Change Password**) and show group memberships (**Member of**). The **Members** button provides details on the members who make up a selected group. The **Effective Rights** button provides an insight into the rights that were directly or indirectly granted to users or taken away from them.

Access Rights

Access rights in the IGEL UMS include:

- General rights which can be granted to an administrator or denied either directly via the account or indirectly on the basis of the group membership
- Access rights to objects in the structure tree
- Actions within the UMS Console

The indirect rights given to an administrator on the basis of their group membership can be changed further for each administrator in the group. In this case, rights that were granted directly have precedence over those granted indirectly.

An administrator can be a member of several groups and receive the corresponding rights. If permission settings contradict each other, the withdrawal of permissions takes precedence over the granting. If a prohibition regarding an action or object from a group is issued, it will overrule all rights from other groups.

Generally speaking, the same permission settings are used for groups and administrators. The following description of individual configuration options for administrators therefore applies equally to groups too.

- Basic Access Rights (see page 517)
- General Administrator Rights (see page 518)
- Object-Related Access Rights (see page 521)
- Access Rights in the Administration Area (see page 527)

Basic Access Rights

The following table lists the basic access rights needed to set up, edit, or delete objects. An object can be a directory, an element in a tree structure (devices, profiles...) or nodes in the administration area of the UMS Console, e.g. administrative tasks or the AD connection.

Action	Objects affected	Browse	Read	Move	Edit Configuration	Write	Access control
General							
View Object	Tree Element (Profile, TC...)		X				
	Directory	X					
Create Object	Target Directory					X	
Delete Object	Object					X	
	Source Directory					X	
Edit Object	Object					X	
Rename Object	Object					X	
Show Configuration	Thin Client, Profile		X				
Edit Configuration	Thin Client				X		
	Profile					X	
Show Effective Rights	Object		X				
	Directory	X					
Edit Object Permissions	Object, Directory						X
Import	Target Directory					X	

General Administrator Rights

Menu path: Menu bar **> System > Administrator accounts**

Permissions are managed via **System > Administrator accounts**. An administrator can grant himself and others rights, take away those rights and set up new accounts.

The following options are available here, split according to administrators or groups:

New: A new administrator or a new group will be created.

Import: A user will be imported from the AD/LDAP directory.

> This procedure requires an AD/LDAP connection. For further details, see Importing Active Directory users (see page 510).

- **Domain**: Domain in which the AD/LDAP service runs
- **User**: Name of the user
- **Password**: Password of the user

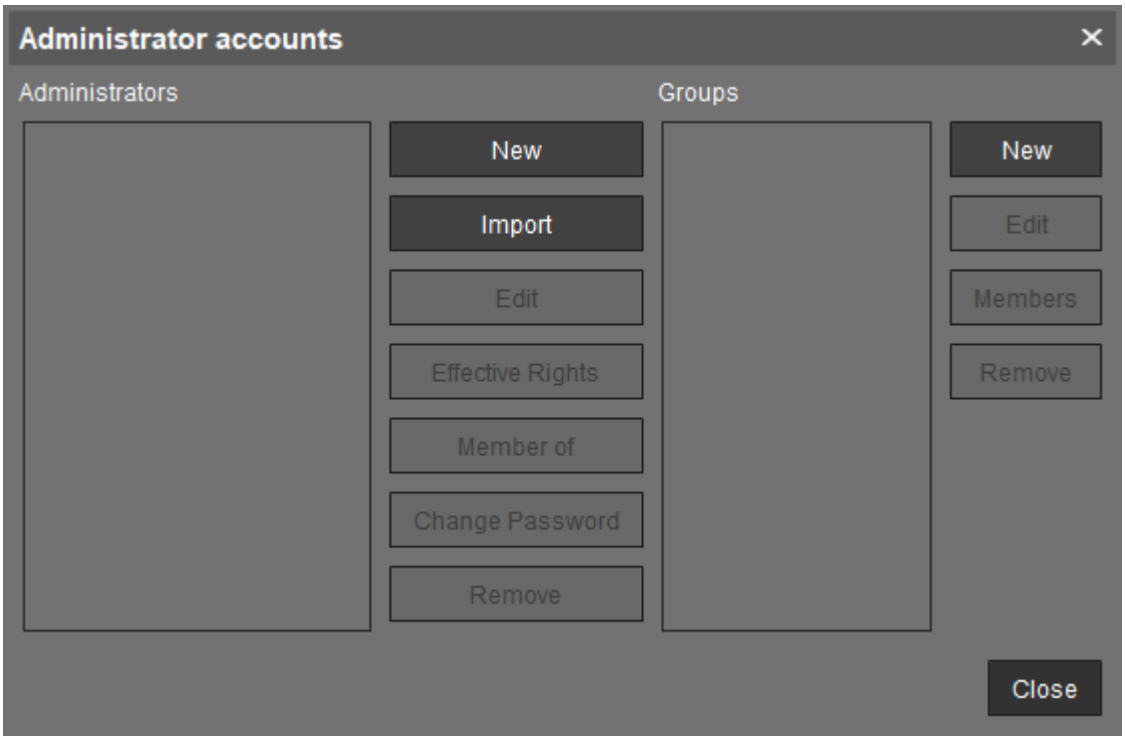
Edit: Existing administrator or group settings can be edited.

Effective Rights: A list of all assigned rights for a specific administrator is shown.

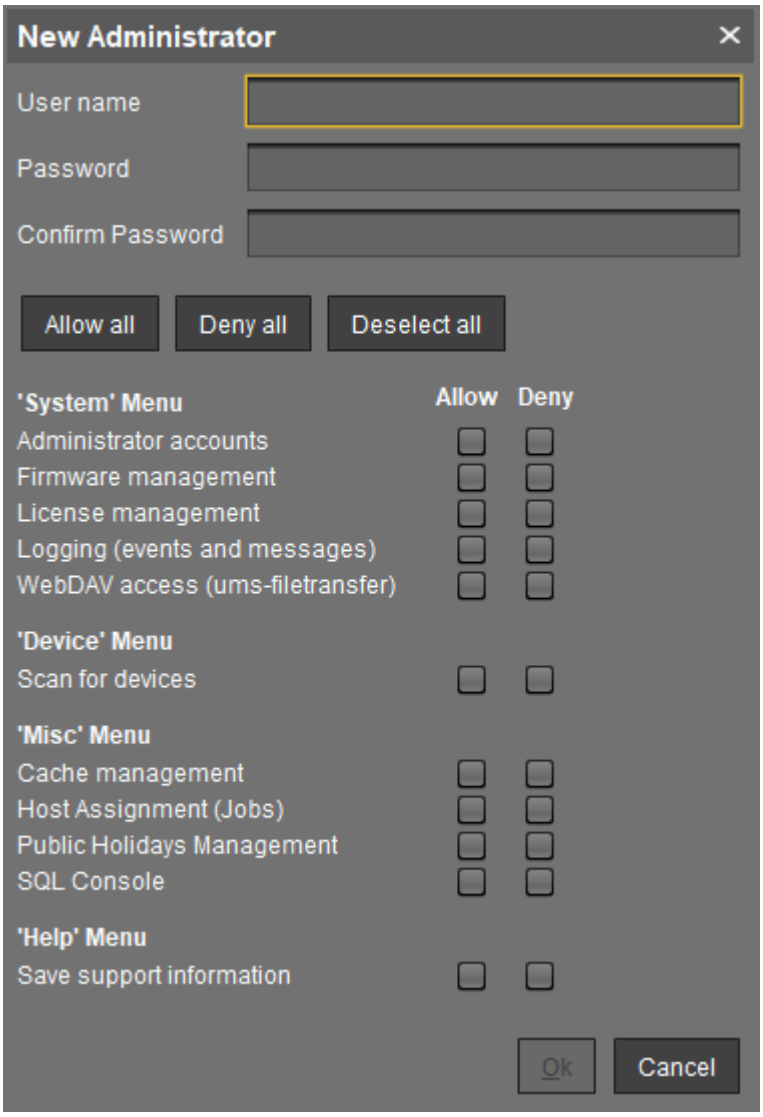
Member of / Members: The assignment of memberships and groups is shown.

Change Password: Changes an administrator password.

Remove: Removes a highlighted administrator or a group.



Below, you will find a list of permissions that can be given to individual administrators or groups under **System > Administrator accounts > New** or **Edit**. Each permission has three possible states: not set, **Allow** or **Deny**.



'System' Menu

Administrator accounts

☑ The management of permissions can be performed: administrators and groups, as well as their rights, can be added and edited.

Administrator accounts permission should only be granted to users who are to have full access to all objects and actions in the UMS!

Firmware management

☑ Firmware versions can be imported, exported, and removed from the database.

License management

☑ IGEL firmware licenses can be allocated to devices.

Logging (events and messages)

☑ The event and message log may be viewed if **Logging** is enabled.

WebDAV access (ums-filetransfer)

☑ The user is authorized to add, modify, and delete files in the directory `/ums_filetransfer/`.

'Devices' Menu

Scan for devices

☑ The network can be scanned for devices, for example if they are to be registered on the UMS Server.

'Misc' Menu

Cache management

☑ The UMS Server cache can be viewed, updated, and deleted.

Host Assignment (Jobs)

☑ Scheduled jobs can be assigned to various hosts.

Public Holidays Management

☑ Public holidays can be defined in order to plan jobs.

SQL Console

☑ The SQL Console may be run. **Warning:** The SQL Console can cause considerable damage to the database.

'Help' Menu

Save support information

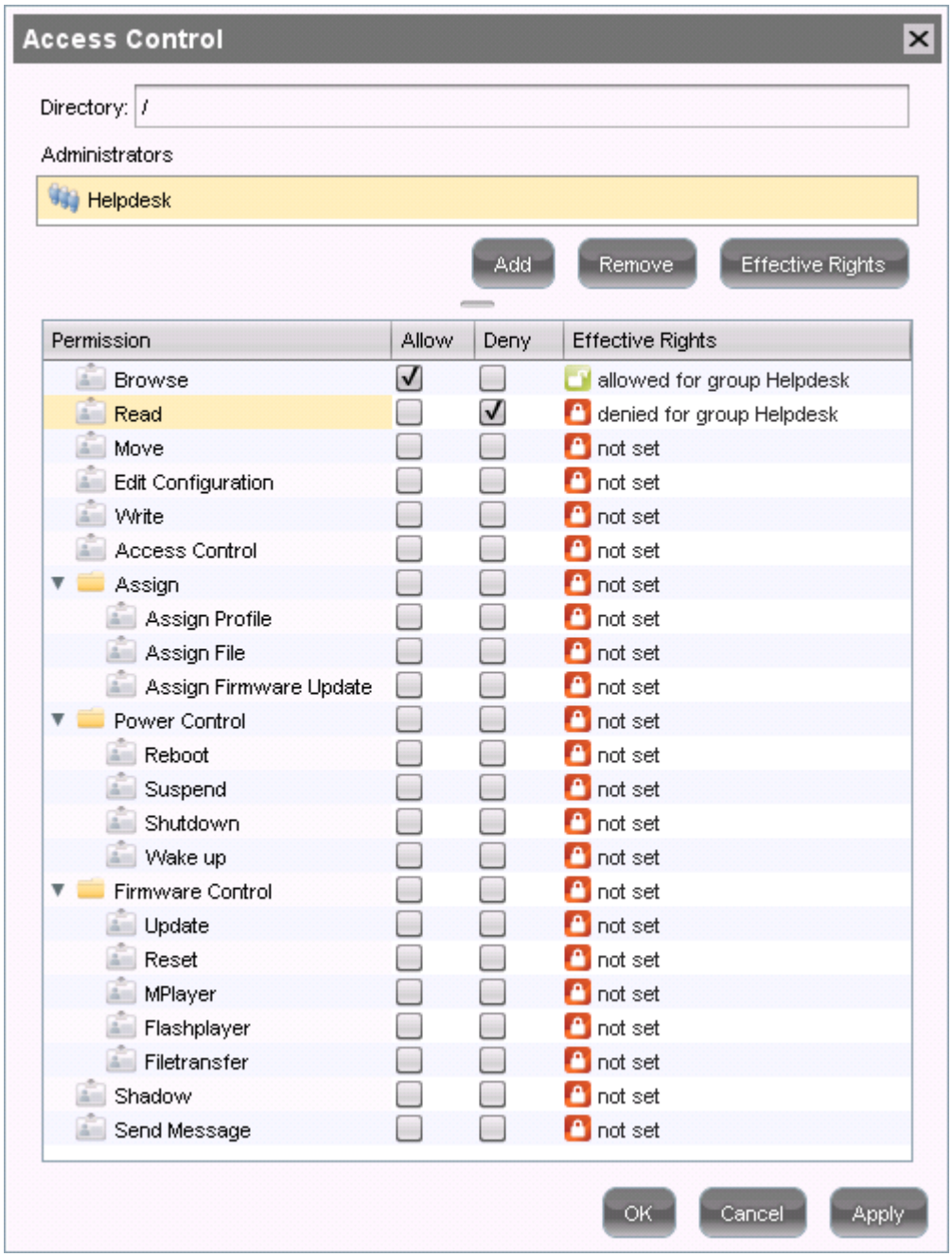
☑ Database and server log files can be exported for support purposes.

Object-Related Access Rights

Administrators and administrator groups can be granted specific rights with regard to objects in the structure tree. These permissions are inherited "downwards", e.g. from a folder to the devices within this folder.

You can change the permission settings after selecting an object in the following ways:

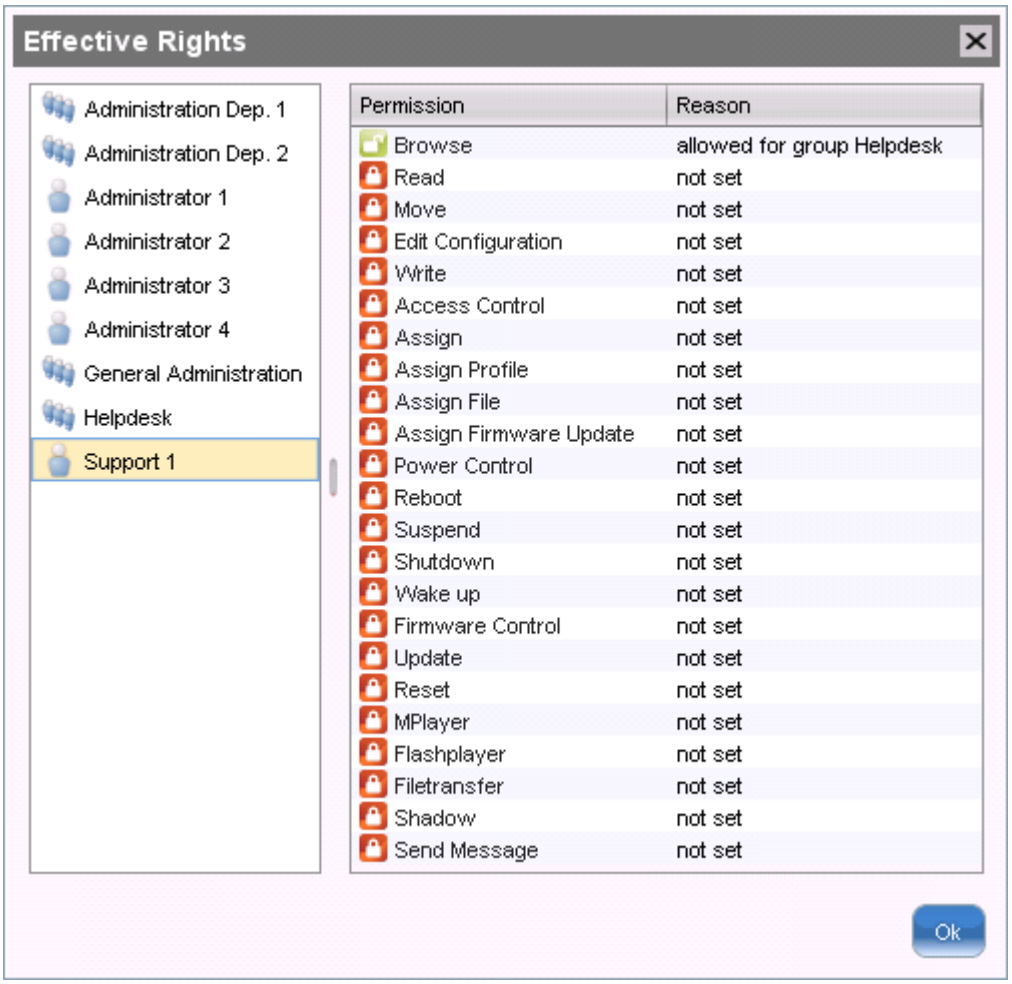
- via **Access control** in the context menu of the object
- via the **Access control** symbol  in the toolbar
- via the menu item **Edit > Access control**



The above list contains all object-related permissions available in the UMS structure tree. Only one selection is available for each selected object. For example, a view cannot be assigned updates and cannot be shut down.

Associated permissions are automatically set together but can be changed manually later on. Enabled permissions or denials relating to nodes affect all objects within the node.

The overview shows selected administrator rights to an object. Details can be found under **Effective Rights**. The rules for determining rights are also shown here, e.g. whether the permission was granted directly or whether it is granted via a group or an inheritance within the tree structure.


Effective Rights
Administration Dep. 1
Administration Dep. 2
Administrator 1
Administrator 2
Administrator 3
Administrator 4
General Administration
Helpdesk
Support 1
Permission
Reason
Browse
allowed for group Helpdesk
Read
not set
Move
not set
Edit Configuration
not set
Write
not set
Access Control
not set
Assign
not set
Assign Profile
not set
Assign File
not set
Assign Firmware Update
not set
Power Control
not set
Reboot
not set
Suspend
not set
Shutdown
not set
Wake up
not set
Firmware Control
not set
Update
not set
Reset
not set
MPlayer
not set
Flashplayer
not set
Filetransfer
not set
Shadow
not set
Send Message
not set
Ok

Available Rights

General	**Browse**	Visibility of the object in the structure tree (path as far as the object must also be allowed!)
	Read	Read permission in respect of folder contents and object attributes
	Move	Devices can be moved without write permission.
	Edit configuration	Write permission for the configuration of a device (TC Setup)
	Write	Write permission in respect of folders and object attributes (not TC Setup)
	Access Control	The permission settings for the object can be changed.
	Shadowing	VNC access to the device
	Send message	The device's message function
Assignment	**Assign profile**	A profile may be assigned to the object.
	Assign file	A file may be assigned to the object.
	Assign update	A firmware update may be assigned to the object.
Energy	**Reboot**	Rebooting the device.
	Idle state	Putting the device into the idle state.
	Shut down	Shutting down the device
	Wake up	Waking up the device using wake-on-LAN.
Firmware	**Update**	The firmware update may be carried out.
	Reset	Resetting the firmware to the factory defaults.
	Media Player	Downloading Media Player codec licenses.
	Flash Player	Downloading an Adobe Flash Player license.
	File transfer	An assigned file may be transferred to the device.

Assignment of Objects

The assignment of objects requires the following permissions:

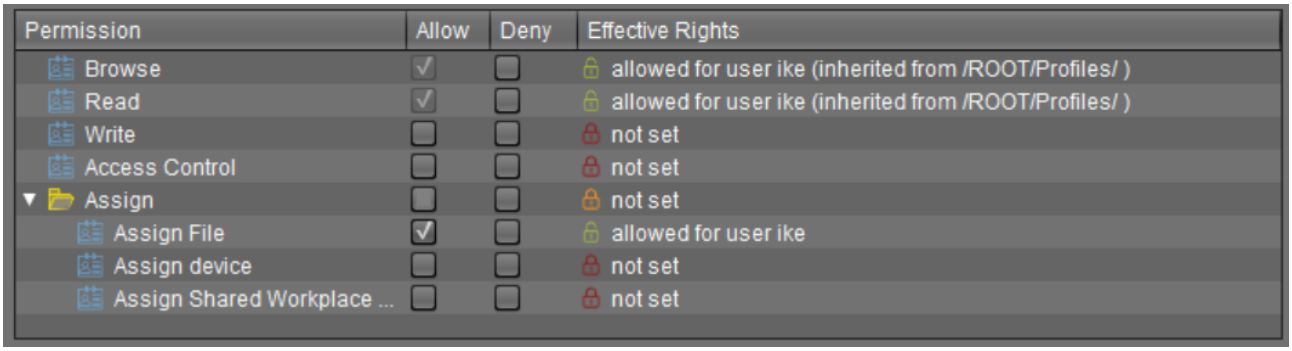
- **Browse**
- **Read**
- **Assign** on both sides

> **Write** permission is not required directly for the assignment of objects.

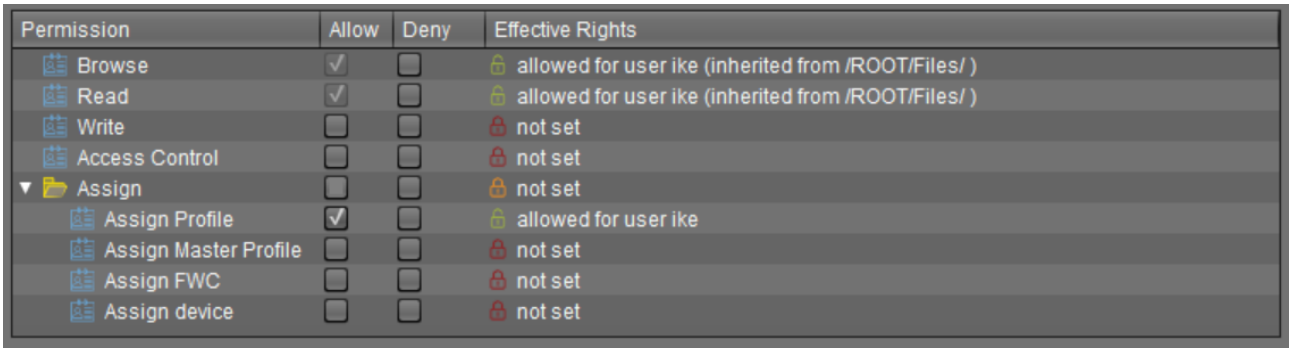
Example 1: Assigning a File to a Profile

A user can only assign a file to a profile or delete this assignment. He cannot make any changes to the file or profile, i.e. he cannot edit, rename, or delete them.

Permissions on the Profile



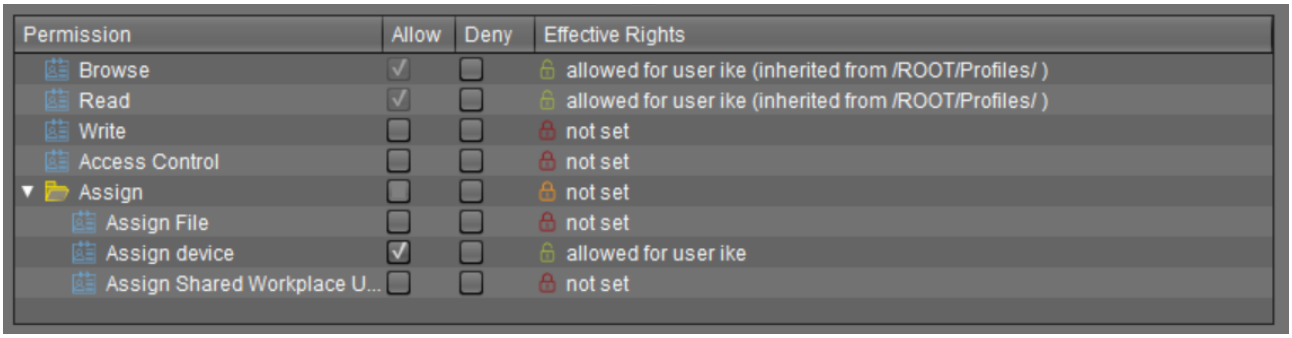
Permissions on the File



Example 2: Assigning a Device to a Profile

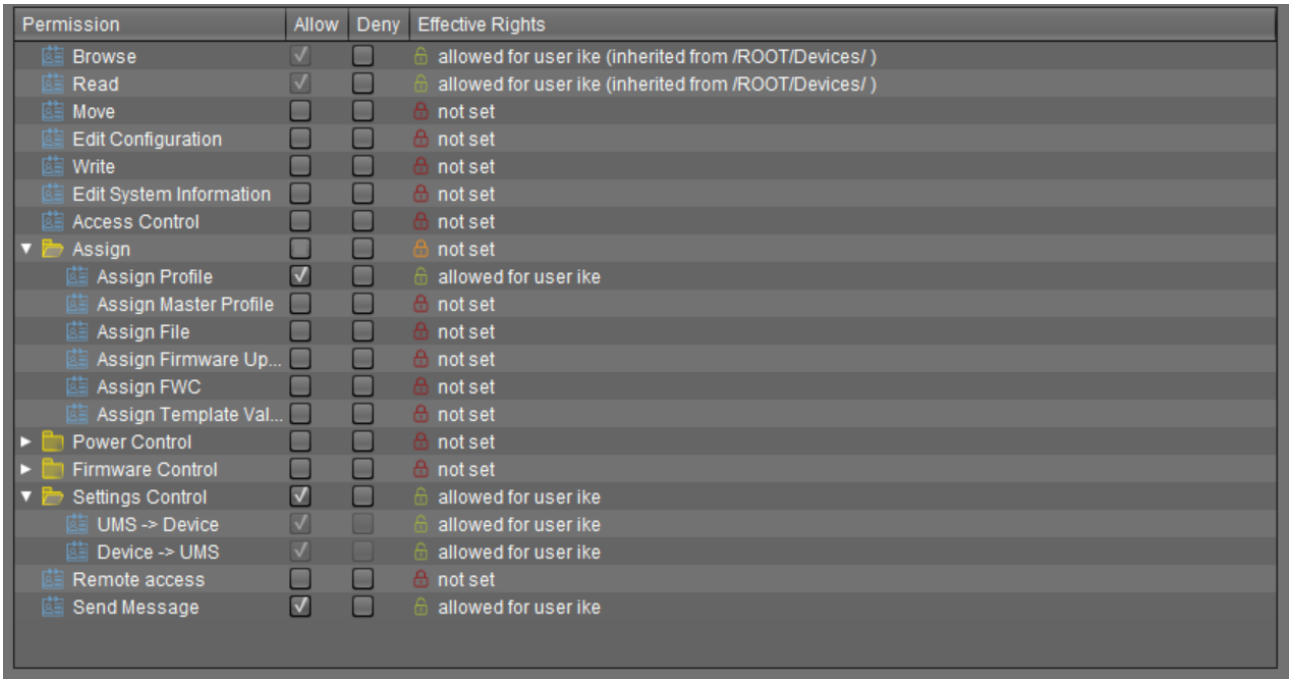
A user can only assign a device to a profile or delete this assignment. He cannot make any changes to the device or profile, i.e. he cannot rename, delete the device or profile, or edit their configuration.

Permissions on the Profile



Permission	Allow	Deny	Effective Rights
Browse	☑	☐	allowed for user ike (inherited from /ROOT/Profiles/)
Read	☑	☐	allowed for user ike (inherited from /ROOT/Profiles/)
Write	☐	☐	not set
Access Control	☐	☐	not set
▼ Assign	☐	☐	not set
Assign File	☐	☐	not set
Assign device	☑	☐	allowed for user ike
Assign Shared Workplace U...	☐	☐	not set

Permissions on the Device



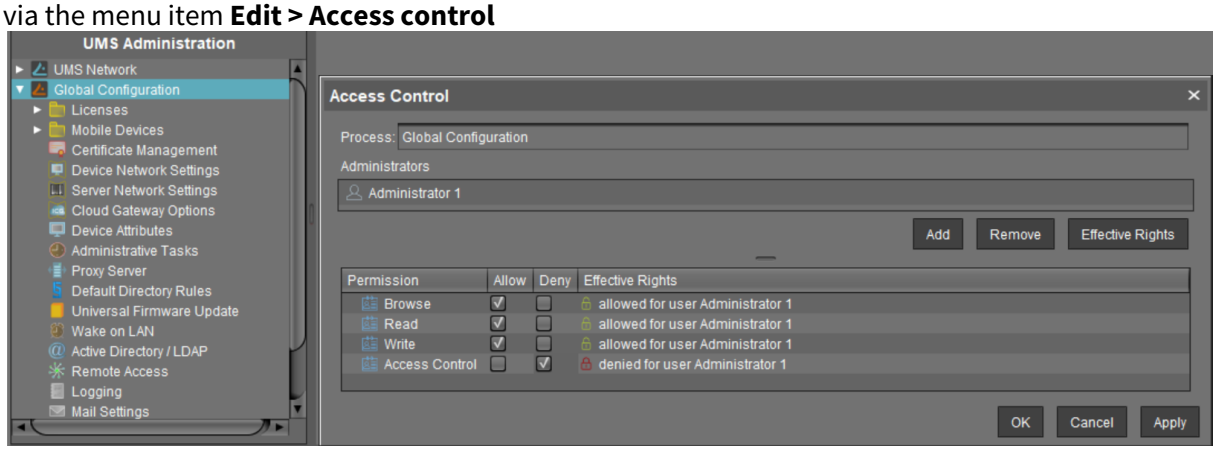
Permission	Allow	Deny	Effective Rights
Browse	☑	☐	allowed for user ike (inherited from /ROOT/Devices/)
Read	☑	☐	allowed for user ike (inherited from /ROOT/Devices/)
Move	☐	☐	not set
Edit Configuration	☐	☐	not set
Write	☐	☐	not set
Edit System Information	☐	☐	not set
Access Control	☐	☐	not set
▼ Assign	☐	☐	not set
Assign Profile	☑	☐	allowed for user ike
Assign Master Profile	☐	☐	not set
Assign File	☐	☐	not set
Assign Firmware Up...	☐	☐	not set
Assign FWC	☐	☐	not set
Assign Template Val...	☐	☐	not set
▶ Power Control	☐	☐	not set
▶ Firmware Control	☐	☐	not set
▼ Settings Control	☑	☐	allowed for user ike
UMS -> Device	☑	☐	allowed for user ike
Device -> UMS	☑	☐	allowed for user ike
Remote access	☐	☐	not set
Send Message	☑	☐	allowed for user ike

Access Rights in the Administration Area

In the **UMS Administration** area of the UMS Console, you can grant or deny general rights **Browse**, **Read**, and **Write**, as well as **Access Control** for administrator accounts. Permissions should only be granted to users who will actually perform administrative tasks on the UMS.

You can change the permission settings after selecting a tree node in the following ways:

- via **Access control** in the context menu
- via the **Access control** symbol  in the symbol bar
- via the menu item **Edit > Access control**



User Logs

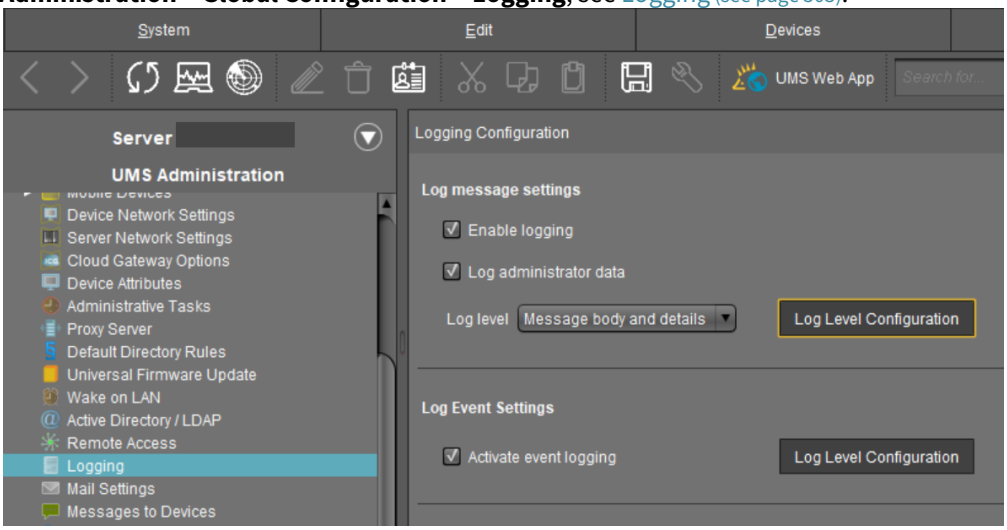
The logging system is used by the UMS and the registered devices in order to record all changes to the database. Only successful actions are logged. You will not find details of any errors in the log file of the UMS GUI Server.

The logging system is subdivided into two areas:

Messages:	Actions initiated by a user
Events:	Actions initiated by a device

Administration

The administration settings for the logging procedure are configured in the IGEL UMS Console under **UMS Administration > Global Configuration > Logging**, see Logging (see page 503).



- **Messages** can be logged either with or without details.
  There are no details for **events**.
- With the **Log Level Configuration** buttons, you can enable logging for selected commands.
  Logging for all possible commands is selected as standard.
- The deletion and export of log messages are configured under **UMS Administration > Global Configuration > Administrative Tasks**.

Displaying Logs

Information regarding **messages** and **events** can be displayed in the UMS Console in the following ways:

- via the **System > Logging** menu
- via **Logging** in the context menu of the directories and objects in the tree structure

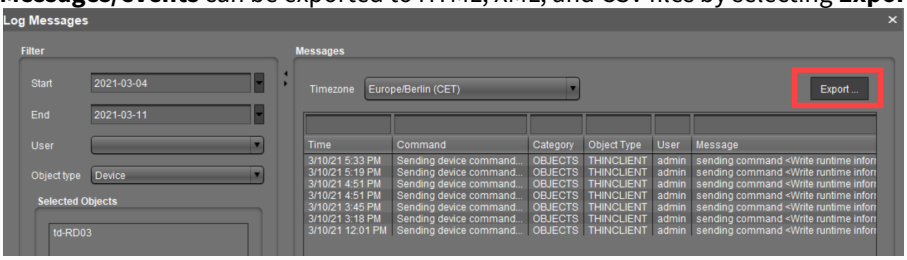
- Logging Dialog Window: Setting a Filter (see page 530)

Logging Dialog Window: Setting a Filter

To set a filter, proceed as follows:

1. In the **Filter** window area, specify criteria in order to load a specific selection of messages from the database.
   All filter fields are combined with the operator **AND**.
   These values can be connected with the operator **OR** only if a filter field allows multiple selections, e.g. if several devices can be selected.
2. Click on **Apply Filter** to enable the new settings.
   The log messages or events will be reloaded from the database on the basis of the filter settings.

Messages/events can be exported to HTML, XML, and CSV files by selecting **Export**.

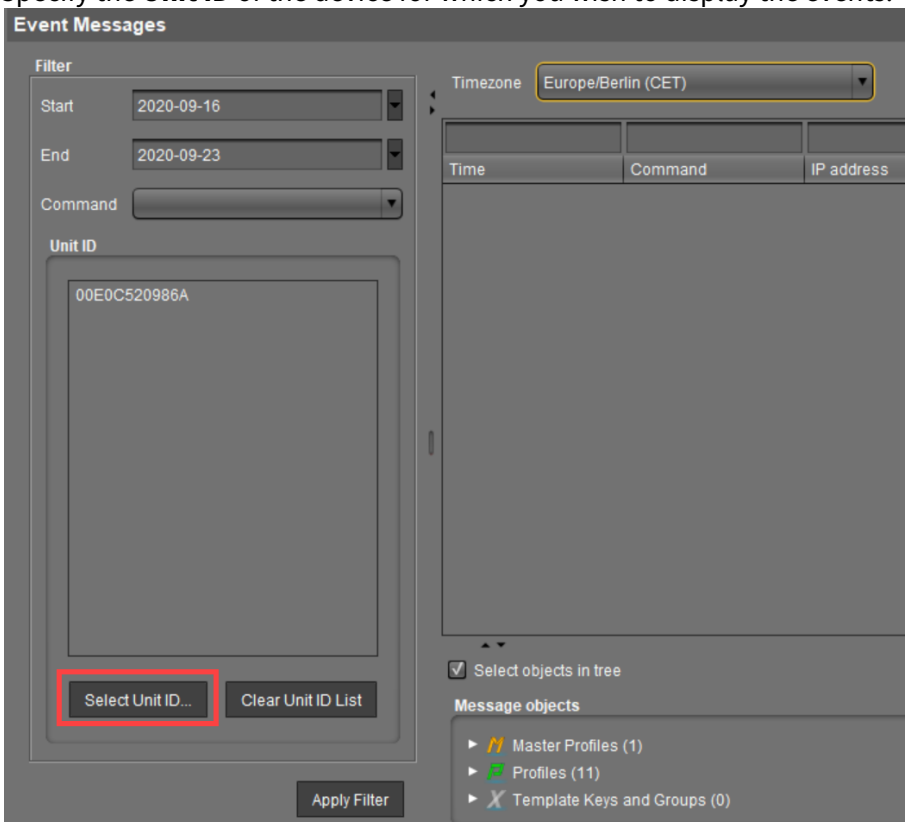


- Setting a Filter for Events (see page 531)
- Filter for Messages (see page 532)
- Setting a Filter for Categories (see page 533)
- Notes (see page 534)

Setting a Filter for Events

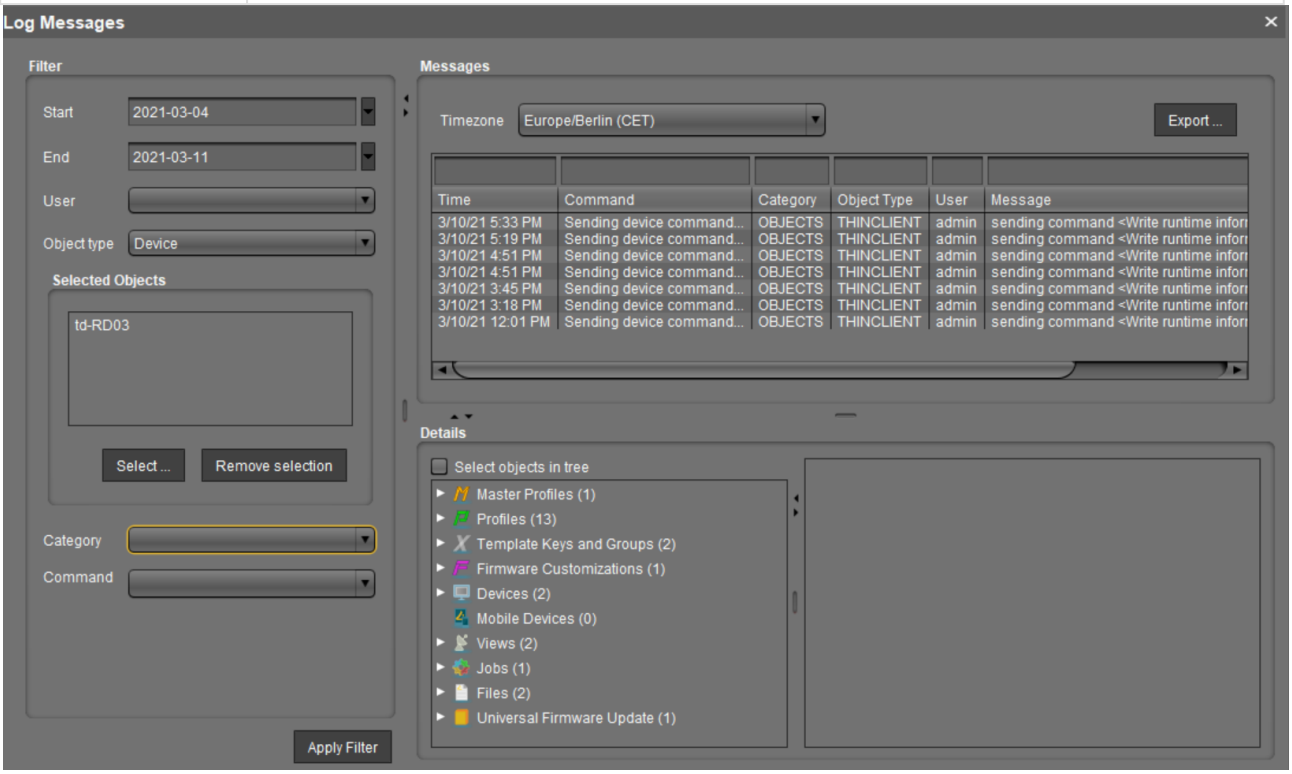
To set a filter for events, proceed as follows:

1. Specify the **Command** if you know which one you need.
2. Specify the **Unit ID** of the device for which you wish to display the events.



Filter for Messages

User	Select the name of the UMS administrator who is responsible for the message.
Object type	Specify an object for which you would like to display the messages.
Category	Each command belongs to a category, e.g. security, settings and objects.
Command	If a command is known, you can specify it yourself.
Time zone	You can specify the time zone with which the logging time for messages is shown.



Setting a Filter for Categories

▶ To adjust the filter, select the option **Category** if you would like to select all messages for a specific category (e.g. those relating to firmware updates).
All commands within this category such as **Delete firmware update** or **Assign firmware update** will then be evaluated in order to identify the messages or events.

Notes

The quick filter does not apply to the export action.

One of the most important commands is the command `GET_SETTINGS_ON_REBOOT`. The time stamp for this command provides details of the time when the device last booted. This can be used to define a new **BOOT TIME** view criterion. With the help of this criterion, you can easily determine which devices have not been booted after a certain date.

> The administration settings for the number of messages and – more importantly – for the events should be handled with great care. The higher these values are, the more space will be required for the tablespace in the database. If you enable logging, you should monitor your database closely until you are sure that sufficient space is available for the messages and/or events.

Save Support Information / Send Log Files to Support

If you have problems with the UMS and contact your service provider, you can send various UMS log files to Support. The Support Wizard (see page 536) will help you here.

If you have any questions regarding an IGEL product and are already an IGEL customer, please contact your dedicated sales partner first.

If you are currently testing IGEL products or your sales partner is unable to provide the help you need, please fill in the support form after logging on to the IGEL Customer Portal[16].

We will then contact you as soon as possible. It will make things easier for our support staff if you provide us with all the information that is available. Please see our notes regarding support and service information[17] too.

16 https://support.igel.com
17 https://www.igel.com/wp-content/uploads/2019/11/F-501-EN.pdf

Support Wizard

Menu path: **Menu Bar > Help > Save support information**

With the Support Wizard, you can collect the log files which are important for your support case and send them as a mail to IGEL Support.

The Support Wizard saves log files from the UMS Server and UMS Console as well as profiles and associated firmware information for the selected devices in a ZIP file. If IGEL Cloud Gateway (ICG) is being used, log files from the connected ICGs will also be saved. If the IGEL Management Interface (IMI) extension is being used, its API log file will be saved too.

> In order to send log files using the Support Wizard, the mail settings must be correct; further information can be found under Mail settings (see page 506). The support ID must also be valid.

To send log files using the Support Wizard, proceed as follows:

1. Click on **Help > Save Support Information** in the menu bar.
2. Optionally, enter the **support ID** for your support case.
3. Click on **Next**.
4. If the support case concerns devices (otherwise click on **Next**): Highlight the devices where the problem has occurred.
5. If the support case concerns devices (otherwise click on **Next**): Click on  to select the highlighted devices.
6. Click on **Next**.
7. Under **Number of days back**, specify the maximum age in days of the log entries to be sent.
8. Click on **Next**.
9. Using **Look In**, select the directory in your file system in which the zipped log files are to be saved.
10. Click on **Next**.

    > If the zipped log files have already been saved, you will be asked whether the existing ZIP file should be overwritten.

    If the mail settings are configured, entry fields for the mail will be shown.
    If the mail settings are not configured, a message about saved files will be shown.
11. If applicable, give the following information for the mail:
    - **Cc**: Mail address to which a copy is to be sent. If you enter a number of addresses, you must separate them using a semicolon ";".
    - **Reply address**: Mail address to which the reply from Support is to be sent. If you leave the field empty, the reply will be sent to the **mail sender address** defined under **UMS Administration > Mail Settings**.
    - **Subject**: Subject of the mail. When the mail is sent, the **support ID** will be shown before this text.
    - Text entry field: Mail text.
12. Check the information in the mail and click on **Send**.
13. Click on **Finish**.

Save Device Files for Support

Menu path: **Menu bar > Help > Save device files for support**

You can use the UMS for collecting log files from a device. These log files will be zipped, so you can easily send them to the IGEL support team. The exact behavior is dependent on the device's firmware version.

Saving the Log Files of a Device

1. Go to **Help > Save device files for support**.
   A wizard appears. In the screen **Select Devices**, the devices section of the structure tree is shown.
2. Select the device whose log files you want to save and click **Next**.
   The screen **Select a target directory for the zipped files** is shown.
3. Select a target directory and click **Next**.
   The log files are collected from the device and zipped. The file path is shown.
4. Click **Finish**.

For the detailed instruction with screenshots, see Sending Device Log Files to IGEL Support.

Log Files Collected with IGEL OS 10.04 or Higher

The UMS asks the device to send log files. The selection of log files is configurable on the device. The following log files are collected by default:

- `/config/Xserver/card0`
- `/config/Xserver/monitor-info`
- `/config/Xserver/xorg.conf-0`
- `/config/sound/card0`
- `/config/sound/default_card_name`
- `/var/log/Xorg.0.log`
- `/wfs/group.ini`
- `/wfs/setup.ini`
- dhclient lease files

You can add more log files via the IGEL Setup under **Accessories > System Log Viewer > Options**. For further information, see Options.

Log Files Collected with Other IGEL OS Versions

The UMS requests the following log files:

- `setup.ini`
- `group.ini`

- `messages`
- `Xorg.0.log`
- `xorg.conf-0`
- `Xorg.0.log.old`
- `wpa_debug.all`
- `tcsetup.log`
- `tcsetup.log.1`

Log Files Collected with Windows IoT 4.03 or Higher

The UMS asks the device to send log files. The selection of log files is configurable on the device. The following log files are collected by default:

- `D:\data\setup.ini`
- `D:\data\group.ini`
- `D:\data\sysinfo.ini`
- `D:\data\uptime.ini`
- `D:\data\ftreg\ftreg.ini`
- `C:\Program Files (x86)\IGEL\upd\tcsetup.log`
- `C:\Program Files (x86)\IGEL\upd\xplog.txt`
- `C:\Program Files (x86)\IGEL\z_ramdrive`
- `C:\Program Files (x86)\IGEL\log`
- `C:\ProgramData\IGEL\DualbootQT_Inst_Log.txt`
- `C:\ProgramData\IGEL\DualbootQT_UnInst_Log.txt`
- `C:\ProgramData\IGEL\LogMisc.txt`
- `C:\Windows\System32\winevt\Logs\Application.evtx`
- `C:\Windows\System32\winevt\Logs\System.evtx`
- `C:\Windows\System32\Sysrep\Panther\setuperr.log`

You can add more log files via the IGEL Setup under **System > Registry > System > support_files% > Add Instance** (Registry key: `system.support_files%` resp. `system.support_files<number>`).

The IGEL UMS Administrator

The IGEL UMS Administrator application is only available on a UMS Server as this makes it possible to intervene directly in communications between the services. It allows basic data such as the ports used or data sources connected to be edited. These functions are not available in the administration area of the UMS Console.

If the UMS Administrator cannot be launched under Linux via a menu or desktop link, you can launch the application on the command line as `root` with the following command: `[IGEL installation directory]/RemoteManager/RMAdmin.sh` (when the default installation directory is used: `/opt/IGEL/RemoteManager/RMAdmin.sh`).

The default path to the UMS Administrator under Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`

You can change the language of the Administrator tool under **File > Settings > Language**.

The rights for changing the settings depend on whether the user is authorized to change IGEL UMS files on the server system. When using the IGEL UMS Administrator, you should therefore use the same user account as you did when you installed the UMS.

Settings

Menu path: **UMS Administrator > Settings**

> Default path to the UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> The IGEL UMS Administrator application can only be started on the UMS Server.

Using the UMS Administrator, you can change various server settings.

Ports

Server port: The devices connect to this port. (Default: 30001)

> Changes to this port can only be made if you ensure that devices will establish a connection on the new port.

GUI server port: Establishes the connection to the server. This port must be entered in the login window for the IGEL UMS Console. (Default: 8443)

JWS server port: This port allows the UMS Console to be started with Java Web Start (see page 169) via a non-encrypted connection. For this to be possible, this port must be specified in the connection URL, e.g. `http://hostname:9080/start_rm.html`. (Default: 9080)

Database port (embedded DB): Port for communication with the embedded DB. (Default: 1528)
For external databases, the port is defined under **Data Sources**.

Allow connection via SSL only

☑ A connection will only be allowed via SSL.

> Do not use the **Allow connection via SSL only** option if you use Windows Embedded 7 in Version 3.08.100 or older and would also like to use the Universal Firmware Update feature. These older Windows firmware versions do not support firmware updates via HTTPS.

Database Setup Configuration

Remote manager ID (read-only): Unique key for the UMS instance. This is read out automatically.

Cipher (Server-Side)

> The cipher configuration is server-specific and excluded from database backups.

If you are using UMS High Availability (HA), the ciphers have to be configured for each server separately.

Configure Ciphers: Use this button to open the **Cipher Selection** dialog, where you can define which ciphers can be used by the UMS Server.

In the **Cipher Selection** dialog, you can perform the following actions:

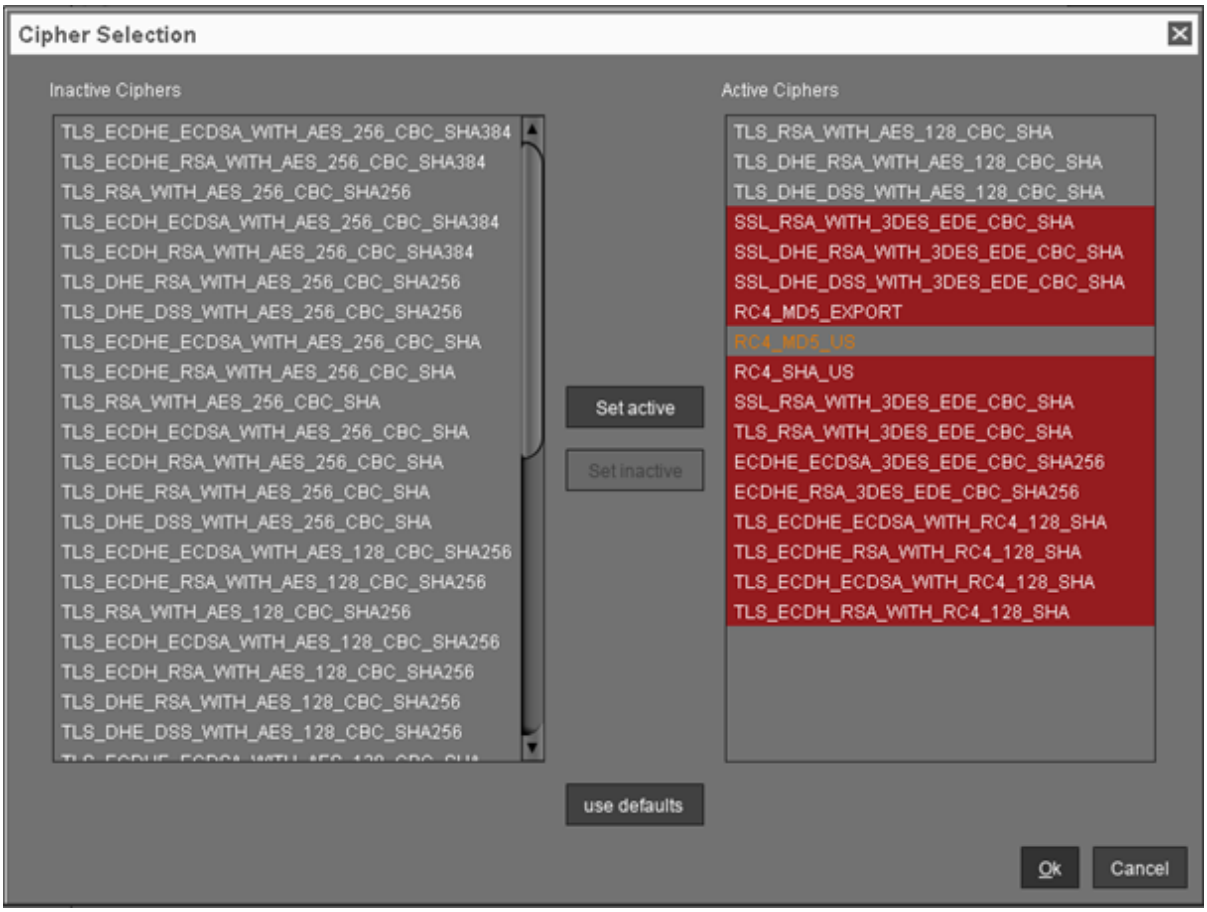
- **Set active**: Add the cipher selected in the **Inactive Ciphers** list to the list of active ciphers.
- **Set inactive**: Remove the cipher selected in the **Active Ciphers** list from the list of active ciphers.
- **Use defaults**: Restore the default cipher settings.
- **Ok**: Save the changes.
- **Cancel**: Discard all changes.

If your server has ciphers from previous installations, there is a possibility that some ciphers are not considered trustworthy any longer.

The levels of security are represented by colors:

- Normal display color (black or white, depending on the theme): The cipher is considered trustworthy and is used by Tomcat.
- Red color: The cipher is not considered trustworthy and is not used by Tomcat. This cipher cannot be used.
- Orange color: The cipher is used by Tomcat but is not considered trustworthy by IGEL or Tomcat or another institution. It is recommended not to use this cipher.

The following example includes ciphers with all 3 levels of security:


Cipher Selection
Inactive Ciphers
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
Active Ciphers
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
RC4_MD5_EXPORT
RC4_MD5_US
RC4_SHA_US
SSL_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
ECDHE_ECDSA_3DES_EDE_CBC_SHA256
ECDHE_RSA_3DES_EDE_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_ECDH_ECDSA_WITH_RC4_128_SHA
TLS_ECDH_RSA_WITH_RC4_128_SHA
Set active
Set inactive
use defaults
Ok
Cancel

UMS Licensing ID Backup

Menu path: **UMS Administrator > UMS Licensing ID Backup**

> Default path to the UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> The IGEL UMS Administrator application can only be started on the UMS Server.

> The UMS Licensing ID is generated upon each UMS Server installation. Therefore, if you have a High Availability (see page 560) environment, each of the servers has its own UMS Licensing ID, i.e. **Local UMS Licensing ID**. For the communication of all HA servers with the ILP, a **Main UMS Licensing ID** is used. Further information about the UMS Licensing ID can be found under UMS Licensing ID (see page 431).

Main UMS Licensing ID: The first and last 10 characters of the main UMS Licensing ID are displayed here.

Local UMS Licensing ID: The first and last 10 characters of the local UMS Licensing ID are displayed here.

> In an HA environment, the local UMS Licensing ID can differ from the main UMS Licensing ID. If this is the case, restart the server to get it synchronized. See also Manual Synchronization of the UMS Licensing ID (see page 127).

Create new Main UMS Licensing ID: If the installation does not have a UMS Licensing ID, then this was not created during the installation and the creation must be triggered manually.

UMS Licensing ID Backup

Directory: Path where to store the backup.

UMS Licensing ID backup name: The name of the backup which you have defined during the creation.

Date: Date of the backup.

Creating a Backup

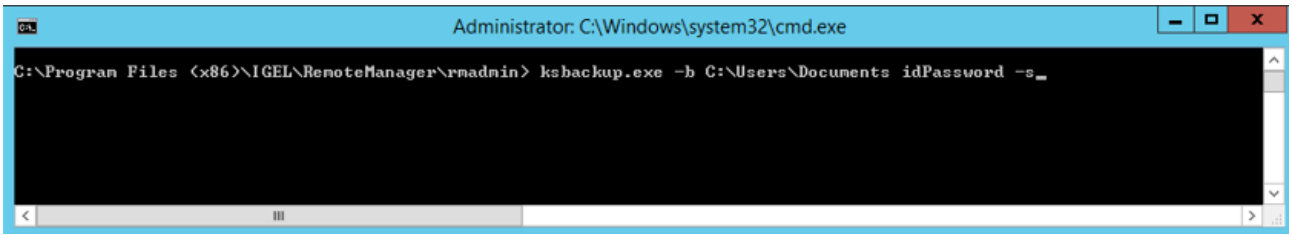
UMS Licensing ID backup name: Define the name of the backup.

Set UMS Licensing ID password: The backup of the UMS Licensing ID can only be restored if you enter the password specified here.

UMS Licensing ID Backup on the Command Line

You can create and restore backups of the UMS Licensing ID (see page 431) using the command line program `ksbackup.exe`. It can be found in the `rmadmin` sub-directory in the UMS installation directory.

Example:



Program Launch Options

`-b path/file_name password`	Creates a backup of the specified file secured by a given password.
`-r path/file_name password`	Restores the specified backup file with a given password.
`-s`	During processing, all program outputs (except error messages) will be suppressed.

- The part of the path after the last / or \ is always used as the file name. If a backup is created and the file path ends with a / or \, the backup will be saved as `umsLicensingIDBackup.ksbak`.
- If a new backup is given a file name of a backup which already exists in this directory, the existing backup will automatically be overwritten.
- If you are using an HA environment (see page 560), please note the following:
  It is always the UMS Licensing ID of the local server that is backed up. If this server is part of an HA environment, it is not guaranteed that this local UMS Licensing ID is the same as the main UMS Licensing ID. This has to be manually checked beforehand. If the local UMS Licensing ID does differ from the main UMS Licensing ID, restart the server to get it synchronized. See also Manual Synchronization of the UMS Licensing ID (see page 127).

Backups

Menu path: **UMS Administrator > Backups**

> Default path to the UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> The IGEL UMS Administrator application can only be started on the UMS Server.

The internal Embedded DB of the UMS Server can be backed up directly via the UMS Administrator. Backups created previously can also be loaded up again.

- Creating a Backup (see page 546)
- Restoring a Backup (see page 550)
- Deleting a Backup (see page 551)
- Backup on the Command Line (see page 552)
- Planned Backup (see page 553)

> For external database systems, please use the backup and recovery procedures recommended by the DBMS manufacturer. For more information, see Creating a Backup (see page 546).

Creating a Backup

Menu path: **UMS Administrator > Backups**

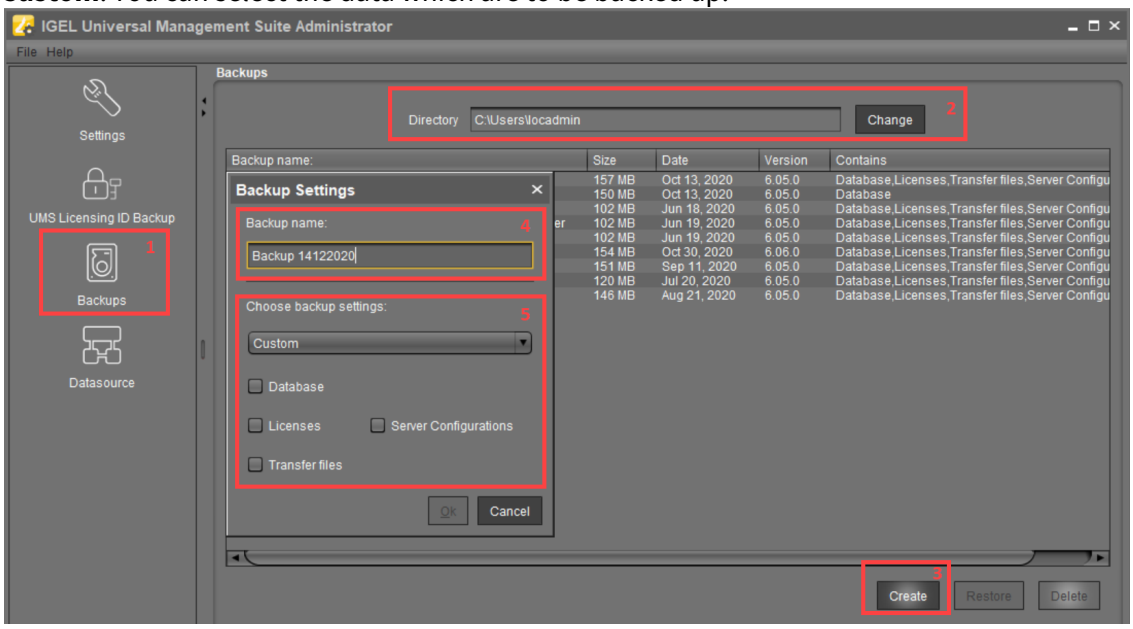
> Default path to the UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> The IGEL UMS Administrator application can only be started on the UMS Server.

Embedded Database

To create a backup of the UMS installation with the embedded database, proceed as follows:

1. In the left-hand column, select **Backups**.
2. Click on **Change** to change the storage location for your backups.
3. Click on **Create**.
4. Under **Backup name**, enter a name for the backup.
5. Select the backup settings under **Choose backup settings**:
   The following can be selected:
   - **Select all**: Database, licenses, server configurations (see page 547), and transfer files (normally, you'll use this option to ensure that no components are missing from the backup)
   - **Legacy**: Database
   - **All files**: Licenses and transfer files (e.g. images, session certificates, etc.)
     Note that licenses and files which have not been registered in the UMS, but are only stored in the system web resources (e.g. were manually placed in folders `e08ce61-d6df-4d2b-b44a-14c1ec722c44` and `ums_filetransfer`) are NOT backed up by the UMS Administrator.

- **Custom**: You can select the data which are to be backed up.



> As of UMS version 5.09, all certificates are included in the database backup.

> **Universal Firmware Updates**
>
> The files of firmware updates are not part of the UMS embedded DB backup. They are not included in the **Transfer files** backup, and, therefore, have to be copied manually from `[IGEL installation directory]/rmguiserver/webapps/ums_filetransfer`.

> The backup of **Server configurations** includes most configurations of the Settings (see page 540) area in the UMS Administrator application. Exceptions: **GUI server port**, **JWS server port**, and **ciphers** – they are host-specific, i.e. stored separately on each server and cannot be part of any backup. Therefore, you should note the values of these settings if they differ from the defaults and, in the case of recovery/migration procedure, they must be changed on each server manually.

6. Confirm your selection by clicking on **OK**.
   The data will be saved in the directory you have selected.

   Remember to back up also the UMS Licensing ID, see UMS Licensing ID Backup (see page 543) or UMS Licensing ID Backup on the Command Line (see page 544).

External Database

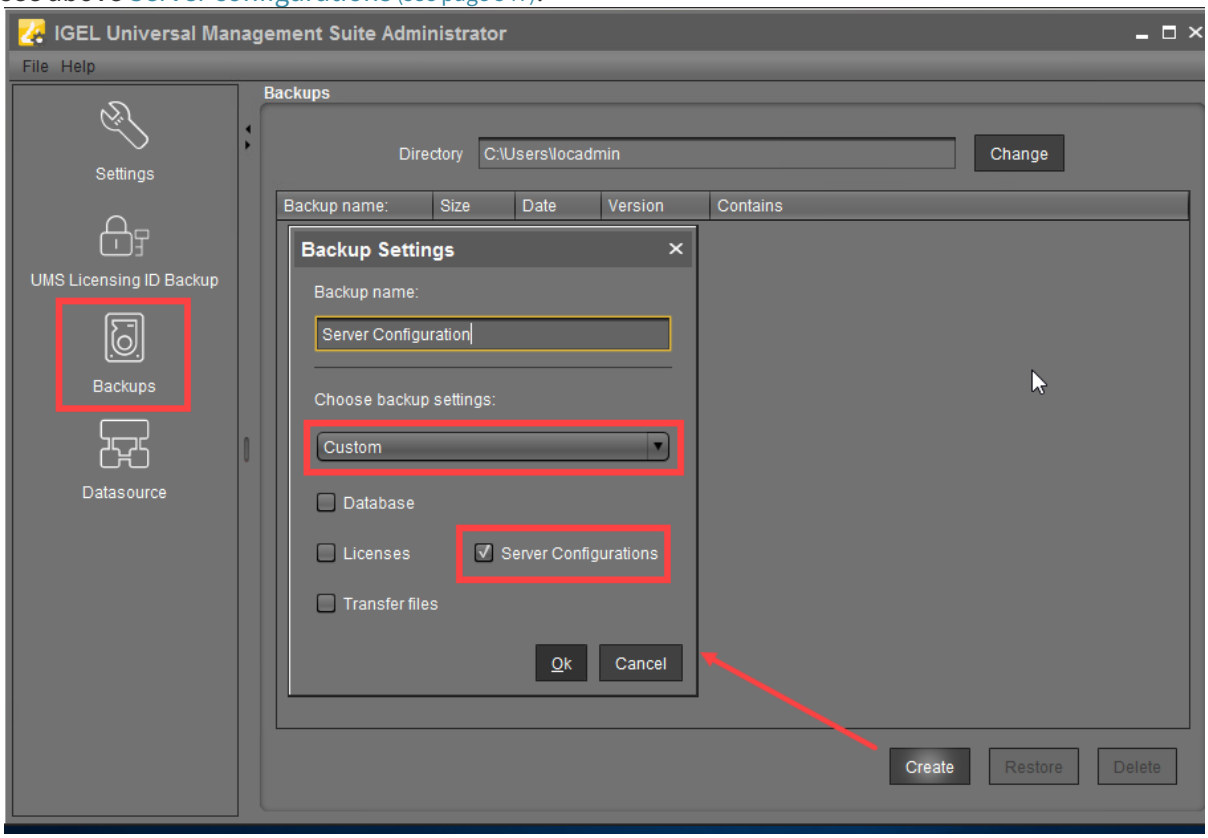
The full range of backup options in the UMS Administrator is only available if you use the embedded database for your UMS Server installation.

If you use an external database (see page 220), proceed as follows to make a complete backup of your system:

1. For the database itself, use the backup and recovery procedures recommended by the DBMS manufacturer.

   > As of UMS version 5.09, all certificates are included in the database backup.
   > If you need to back up the certificates manually, you can find them here:
   > - `[IGEL installation directory]/rmtcserver/*` (includes the `tc.keystore` file, which is necessary for the communication with the endpoint devices)
   > - `[IGEL installation directory]/rmclient/cacerts`
   > - `[IGEL installation directory]/rmguiserver/cacerts`
   > - `[IGEL installation directory]/rmguiserver/irm_keystore`

2. Back up server configurations with the **UMS Administrator > Backups > Create > Custom > Server configurations**. Note separately host-specific configurations that differ from the defaults, see above Server configurations (see page 547):



3. Licenses, files, and firmware updates must be backed up separately, i.e. manually copied to a secure storage medium. You can find them here:

Device licenses	• `[IGEL installation directory]/rmguiserver/webapps/e08ce61-d6df-4d2b-b44a-14c1ec722c44`
Files and firmware updates	• `[IGEL installation directory]/rmguiserver/webapps/ums_filetransfer`

4. Back up also the UMS Licensing ID, see UMS Licensing ID Backup (see page 543) or UMS Licensing ID Backup on the Command Line (see page 544).

   If you are using an HA environment, note the following:
   It is always the UMS Licensing ID of the local server that is backed up. Therefore, make sure at first that the **local UMS Licensing ID** is the same as the **main UMS Licensing ID**. If not, restart the UMS Server to synchronize the local UMS Licensing ID with the main UMS Licensing ID and then proceed with creating the backup. See also Manual Synchronization of the UMS Licensing ID (see page 127).

5. For HA installations (see page 560) only: Save the current IGEL network token (allows the integration of new servers into the same HA network). This is usually a token created during the installation, see Installing the First Server in an HA Network (see page 566). If a new IGEL network token has been generated in the meantime, e.g. if changes to certificates were made (see "High Availability" under Certificate Management (see page 442)), this is the token to be backed up.

Restoring a Backup

Menu path: **UMS Administrator > Backups**

> Default path to the UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> The IGEL UMS Administrator application can only be started on the UMS Server.

> When a backup is restored, your current database status will be overwritten. It is strongly recommended that you create a backup of the current data before another backup is restored.

To restore a saved backup, proceed as follows:

1. Check if the **Directory** is the one that contains your backup; if not, click **Change** to change to the right directory.
2. Select the desired backup from the backup list.
3. Click on **Restore**.
   Once your data have been restored, the login data for the database will be displayed.

Deleting a Backup

Menu path: **UMS Administrator > Backups**

> Default path to the UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> The IGEL UMS Administrator application can only be started on the UMS Server.

To delete a saved backup, proceed as follows:

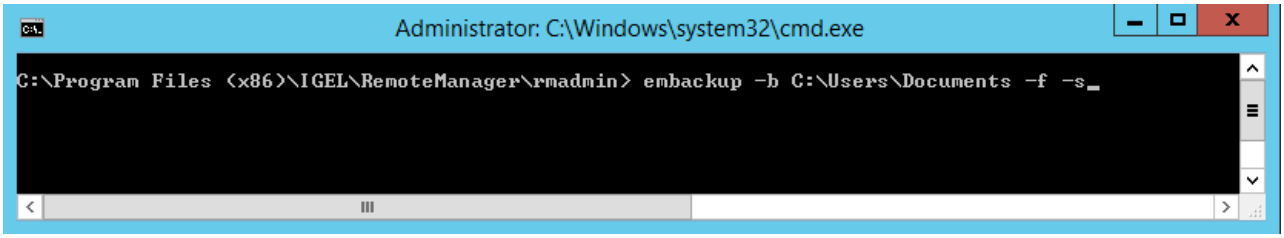
1. Select the desired backup from the backup list.
2. Click **Delete** to remove backups that you no longer need.

   > Both the entry in the UMS Administrator and the backup file on the hard disk will be deleted!

Backup on the Command Line

A command line program for creating a backup with batch file scripts is also available. With the `embackup.exe` command line program, you can create backups with the help of batch scripts. You will find `embackup.exe` in the `rmadmin` sub-directory in the UMS installation directory.

Example:



Program Launch Options

`-b path/file name`	Creates a backup of the database.
`-b path/file name -f`	Creates a backup with all four components.
`-r path/file name`	The backup file with the specified path will be restored in the database.
`-s`	During processing, all program outputs (except error messages) will be suppressed.

- The part of the path after the last `/` or `\` is always used as the file name. If for example when calling up `-b` the path of a directory is specified, a backup with the name of the directory will be created and saved in the higher-level directory.
- If a new backup is given a file name of a backup which already exists in this directory, the existing backup will automatically be overwritten.
- When a backup is created, the UMS server does not shut down.
- When a backup is restored, the UMS server briefly shuts down and automatically restarts afterwards.

Planned Backup

You can define a scheduled backup under **UMS Administration > Administrative Tasks**, see Create Data Backup (see page 454).

Data Source

Menu path: **UMS Administrator > Datasource**

The connection to a database system is provided via data sources which you can manage in the UMS Administrator.

> Default path to the UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> The IGEL UMS Administrator application can only be started on the UMS Server.

If you have chosen the standard installation, the embedded DB is already set up as the data source and enabled.

See also Connecting External Database Systems (see page 220).

Setting up a Data Source

Menu path: **UMS Administrator > Datasource**

> Default path to the UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> The IGEL UMS Administrator application can only be started on the UMS Server.

To set up a data source, proceed as follows:

1. Click on **Add...** to add a first data source or an additional one.
   A dialog window **New Datasource** will open.

2. Select the **DB type**, the **Host** and **Port** for establishing the connection and the user setup on the DBMS. For SQL Server Cluster and Oracle RAC, specify the **Instance**.
   More detailed information regarding the supported DBMS can be found in the "Supported Environment 6.02.100 (see page 776)" section of the release notes (see page 649).

   > Provided that a data source has not been enabled, these settings can still be changed by selecting **Edit**. The active data source is protected against changes to its configuration. By selecting **Change Password**, you can set a new password for the database user. This is also possible when a data source is active.

3. Click on **Test** to test the connection to the database.
   This is also possible when a data source is inactive.

Activating a Data Source

Menu path: **UMS Administrator > Datasource**

> Default path to the UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> The IGEL UMS Administrator application can only be started on the UMS Server.

You can set up a number of data sources. However, only one can be actively used by the server.

To activate this data source, proceed as follows:

1. Select a data source from the list of sources that have been set up.
2. Click **Activate**.
3. Enter the password for the data source that you have selected.
   While the data source is being activated, the application checks whether a valid database schema can be found. If no schema is found, a new schema will be created. An out-of-date schema will be updated, and, if the schema contains unfamiliar data, these will be overwritten.
4. Confirm each of these actions.

   > Overwriting existing data means that the entire database schema will be deleted and not just the out-of-date tables used by the IGEL UMS.

Copying a Data Source

Menu path: **UMS Administrator > Datasource**

> Default path to the UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> The IGEL UMS Administrator application can only be started on the UMS Server.

To switch from the standard installation with an Embedded DB to an external database system, e.g. an Oracle RAC cluster, proceed as follows:

1. Prepare the new database in accordance with the installation instructions for the UMS.
2. Set up a suitable new data source for this DBMS.
3. Select the Embedded DB data source which is still active.
4. Click **Copy**.
5. Select the destination data source.
6. Start the process after entering the destination login data.
7. Activate the new data source.

Optimizing the Active Embedded DB

Menu path: **UMS Administrator > Datasource**

> Default path to the UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> The IGEL UMS Administrator application can only be started on the UMS Server.

▶ Click **Optimize Database** to optimize an active embedded database.
The contents of the database will be restructured.
The database index will be renewed in order to speed up database operations.
A message window will appear once the procedure has been successfully completed.

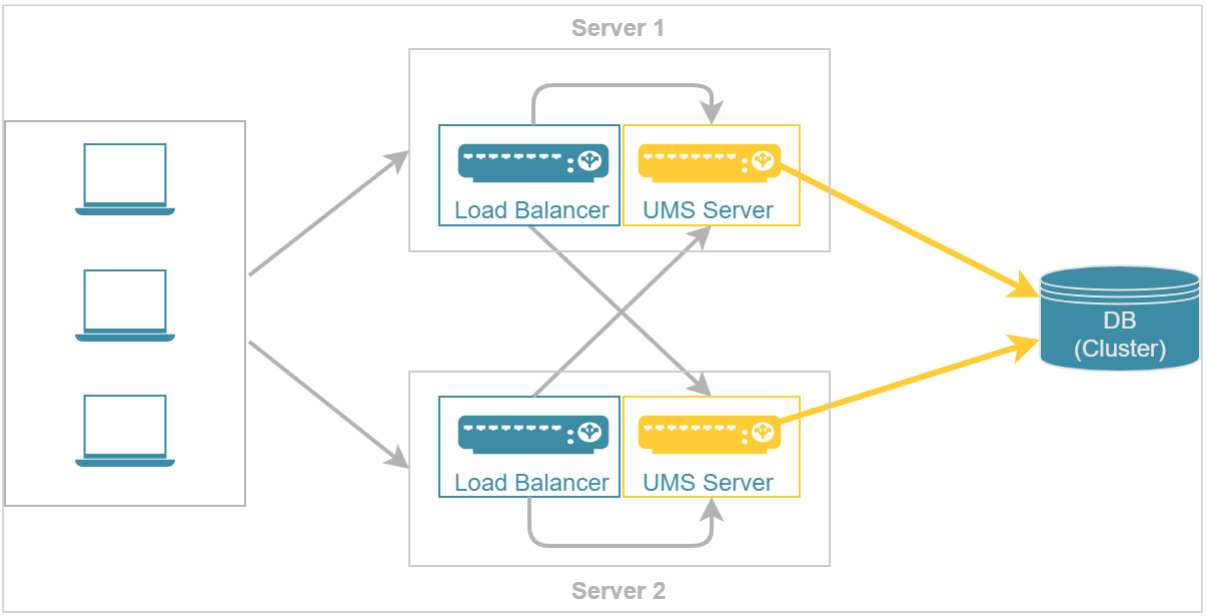
UMS Extensions

High Availability (HA)

The optional High Availability extension is part of the IGEL UMS. It is designed to address the needs of large environments in which new settings need to be rolled out at once, or in which the fail-safe rollout of new settings is mission-critical for the organization concerned. The technical implementation is based on a network of several UMS Servers.

An upstream UMS Load Balancer takes over the load distribution and thus ensures that each device can receive new settings at any time – even at the start of a working day when a large number of devices log in to the UMS Server simultaneously and request new configuration profiles or firmware updates. To ensure maximum process reliability and high availability, IGEL also recommends that the UMS Load Balancer and the database have a redundant design.

Example:



See also Configuration Options (see page 562).

Licensing with the IGEL OS 11 Licensing Model

The High Availability extension is included in the Workspace Edition, so that IGEL OS 11 devices can use a UMS High Availability network without an additional license.

- Configuration Options (see page 562)
- HA Installation (see page 564)
- Updating the Installation of an HA Network (see page 576)
- Switching from a Standard UMS Installation to an HA Installation (see page 581)
- Licensing the High Availability Extension (see page 591)
- HA Services and Processes (see page 592)

See also the collection of articles High Availability (see page 117).

Configuration Options

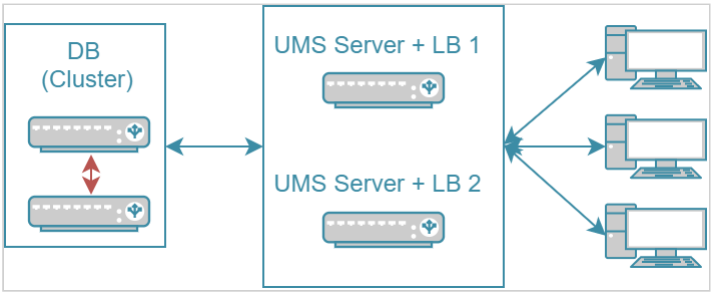
When planning the configuration of your High Availability (HA) network, you have to decide whether you want to install the UMS Server and UMS Load Balancer on the same host or on separate hosts. At the same time, there is a question how many UMS Servers and UMS Load Balancers are required. The following article describes the most common use cases and provides only general sizing recommendations. Your individual configuration may differ.

> When deciding how many UMS Servers and UMS Load Balancers you need, simply counting your endpoint devices is not enough. Most importantly, you have to analyze the entire network environment as well as the other circumstances within your workplace. Contact your IGEL reseller to get counsel.

UMS Server & UMS Load Balancer Are Installed on the Same Host Machine

The most common scenario when deploying UMS High Availability is to install the UMS Server and UMS Load Balancer on the same host machine. Both the UMS Server and the UMS Load Balancer offer redundancy and are installed on two servers. The database is ideally designed as a cluster.

Typical Use Cases	#UMS Server + UMS Load Balancer
The installation on the same host machine is suitable if • the number of devices < 50,000 • you use the Shared Workplace (see page 594) feature	2 UMS Servers 2 UMS Load Balancers

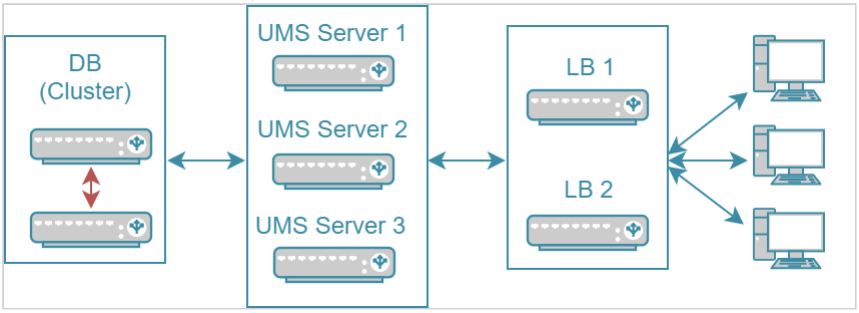


In this configuration, each of the two servers can also perform the tasks as a UMS Server alone. If both servers are active at the same time, this has a load-distributing effect. Note, however, that the load balancer generates extra load along with the actual UMS Server.

UMS Server & UMS Load Balancer are Installed on Separate Host Machines

If you need to manage a very large number of devices and/or do not want the server resources to be shared between the load balancer and the UMS Server, the installation on separate hosts should be considered.

Typical Use Cases	#UMS Server Standalone & Load Balancer Standalone
The installation of the load balancer on a separate host machine is • required if the number of devices > 50,000 • recommended if you do not want the load balancer to consume resources on the UMS Server host	Smallest typical configuration: 2-3 UMS Servers 2 UMS Load Balancers General sizing recommendations: • up to 6 UMS Servers • up to 3 UMS Load Balancers • 1 LB per max. 3 UMS Servers

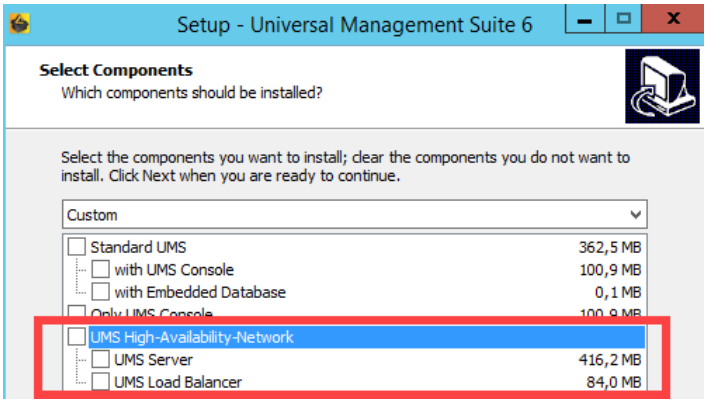


In the smallest typical configuration, queries from the devices are passed on to the UMS Servers by both load balancers. If one of the load balancers should fail, the other remains available and assumes responsibility for communications alone. A great number of UMS Servers could overload a single load balancer, which would then become itself a bottleneck. Therefore, there are provisions for no more than three UMS Servers in this configuration. For very large installations with more than three UMS Servers, the number of load balancers should be increased accordingly.

⚠ All UMS Servers and UMS Load Balancers must reside on the same VLAN. Network traffic must be allowed over UDP broadcast port 6155, and TCP traffic and UDP broadcast traffic over port 61616. For more information on UMS ports, see UMS Communication Ports (see page 26).
Note: IGEL UMS Server HA is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks.

HA Installation

To use the High Availability Extension, you have to select the option for installing the HA network components in the UMS installer.



When installing the High Availability Extension, it is important to differentiate between the installation of the first HA server and further HA servers.

During the installation of the first HA server (UMS Server obligatory), an IGEL network token is created. This network token allows the integration of new servers into the same HA network and, thus, must be used when installing all subsequent HA servers.

Follow these instructions to install the High Availability Extension:

- Installation Requirements (see page 565)
- Installing the First Server in an HA Network (see page 566)
- Adding Further Servers to the HA Network (see page 571)

For information on how to update the HA installation, see Updating the Installation of an HA Network (see page 576).

Installation Requirements

In order to install an IGEL UMS High Availability network, your hardware and software must meet the following minimum requirements.

Installing a UMS High Availability Network

UMS Server (includes UMS Server, UMS Administrator and UMS Console)

Operating system: Microsoft Windows Server 2008 R2 or newer

- At least 5 GB of RAM (UMS Server)
- At least 2 GB of free HDD space (UMS Server)

- At least 2 GB of RAM (UMS Console)
- At least 1 GB of free HDD space (UMS Console)

> The UMS Server must not be installed on a domain controller system.
> Manually modifying the Java Runtime Environment on the UMS Server is not recommended.
> Running additional Apache Tomcat web servers together with the UMS Server is not recommended either.

UMS Load Balancer

- At least 1 GB of RAM
- At least 1 GB of free HDD space

> All UMS Servers and UMS Load Balancers must reside on the same VLAN. Network traffic must be allowed over UDP broadcast port 6155, and TCP traffic and UDP broadcast traffic over port 61616. For more information on UMS ports, see UMS Communication Ports (see page 26).
> Note: IGEL UMS Server HA is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks.

Database Systems (DBMS)

> For details on the supported database systems, see the "Supported Environment" section of the release notes (see page 649). Details of the requirements when installing and operating the database can be found in the documentation for the particular DBMS.

> The embedded database **cannot** be used for an HA network. You can use the embedded database only for a dedicated test installation with only a single server for the UMS Server and UMS Load Balancer.

> The database system must be accessible to all UMS Servers.

Installing the First Server in an HA Network

Prerequisites

- A set of servers with the operating system supported by the UMS; see the "Supported Environment" section of the release notes (see page 649).
- A database system supported by the UMS; see the "Supported Environment" section of the release notes (see page 649).
- All installation requirements described under Installation Requirements (see page 565) are fulfilled.
- The current version of the UMS is downloaded from the IGEL Download Server[18].

For the first installation, it is advisable to use a server without an existing UMS installation.

Instructions

To install the UMS High Availability (HA) Extension on the first server, follow the instructions in the order given:

1. Preparing the Database (see page 566)
2. Preparing the Servers (see page 566)
3. Starting the Installation (see page 567)
4. Defining the Database Connection (see page 568)
5. Checking the Installation (see page 569)
6. Saving the IGEL Network Token (see page 570)

Preparing the Database

▶ Create a database schema and a user for the UMS. Use the relevant DBMS program and its documentation. See also Connecting External Database Systems (see page 220).

Preparing the Servers

1. Verify that each server can "see" the other servers via the network.

   All UMS Servers and UMS Load Balancers must reside on the same VLAN. Network traffic must be allowed over UDP broadcast port 6155, and TCP traffic and UDP broadcast traffic over port 61616. For more information on UMS ports, see UMS Communication Ports (see page 26).
   Note: IGEL UMS Server HA is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks.

2. Verify that the time on all servers is synchronized.

   To avoid problems with your HA installation, make sure that the time on the servers of the HA network does not differ by more than one minute. After each manual time reset, the HA services on the relevant server must be restarted.

18 https://www.igel.com/software-downloads/workspace-edition/

3. For Linux systems, make the directory `/root` writable for the user `root`.

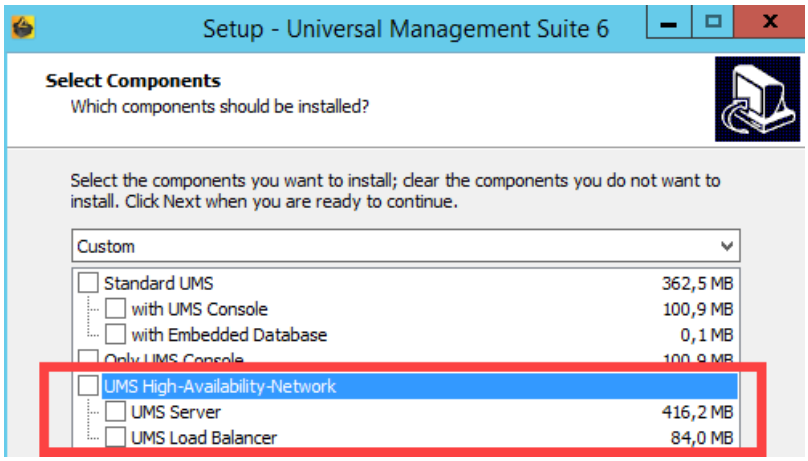
Starting the Installation

1. Launch the UMS installer.

   > You will need administration rights in order to install the IGEL UMS HA.

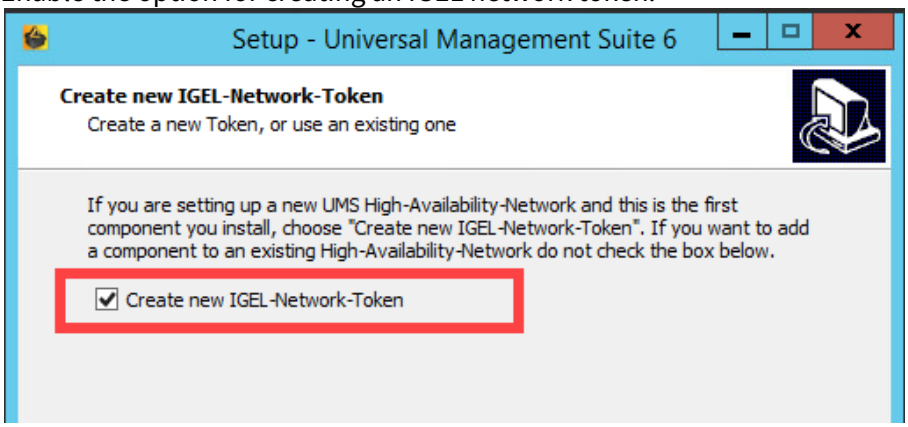
2. Read and confirm the **License Agreement**.
3. Read the **Information** regarding the installation process.
4. Select a path for the installation.
5. Depending on your desired HA network configuration (see page 562), select the components to be installed: **UMS Server + UMS Load Balancer** or **UMS Server**.

   > **Installing UMS Server and UMS Load Balancer on Separate Servers**
   >
   > If you install HA network components on separate servers, **UMS Server** must always be installed first. In this case, the IGEL network token, which is required for the integration of further servers into the HA network, will be created. Additionally, the UMS Console and UMS Administrator applications, necessary for the further management of the installation, will be installed too. After configuring and enabling the database via the UMS Administrator, the UMS Server will be available in the HA network.
   > If you install an individual UMS Load Balancer, neither the IGEL network token nor UMS Console nor UMS Administrator will be installed. Only the option for uninstalling the UMS will then be set up in the Windows start menu.



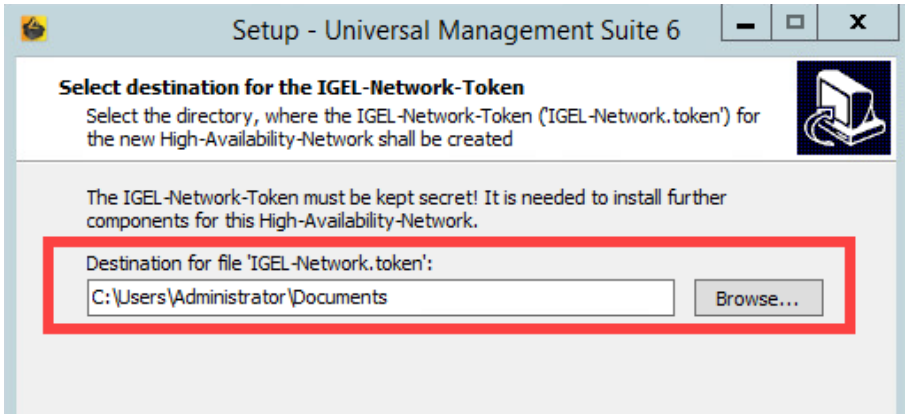
6. Select the **UMS data directory**, in which Universal Firmware Updates and files are to be saved.

7. Enable the option for creating an IGEL network token.



8. Specify a directory for saving the IGEL network token. The directory must be writeable for the administrator.

> ⚠ Be sure to keep the IGEL network token in a safe place! It will be needed for all subsequent server installations. If the IGEL network token is lost, the complete installation must be started again.



9. Optional: Under **Import existing keystore**, you can load the `tc.keystore` file from an existing UMS installation.

> ⚠ This function can destroy your UMS installation. Do not import this file unless you know exactly what you are doing.

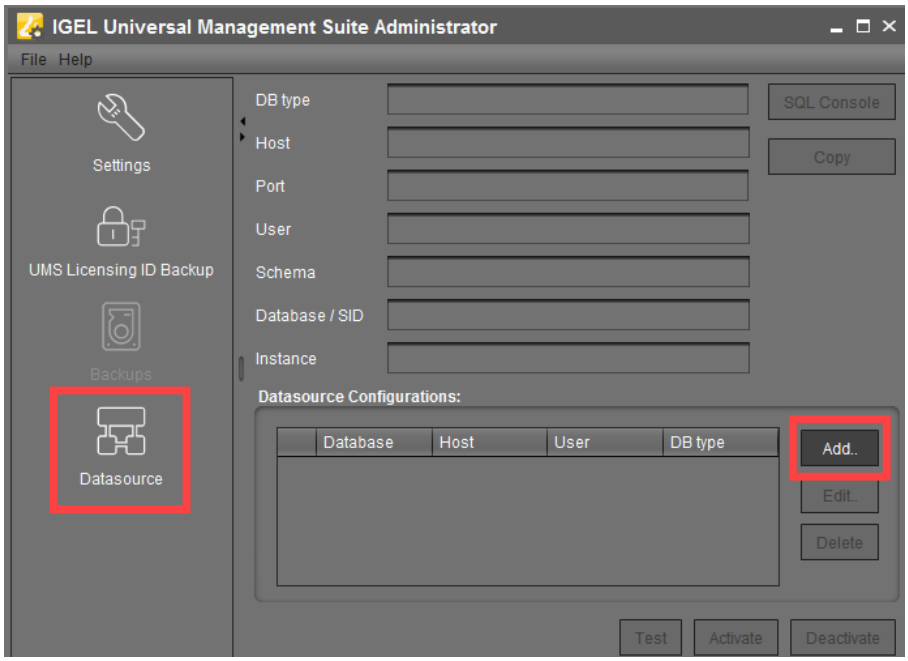
10. Specify a folder name for the shortcut.
11. Read the summary and start the installation process.
12. Close the UMS installer once the installation is complete.
    The UMS installer creates entries in the Windows software directory and the start menu. A shortcut for the UMS Console will also be placed on the desktop.

Defining the Database Connection

1. Open the UMS Administrator.

> Default path to the UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> The IGEL UMS Administrator application can only be started on the UMS Server.

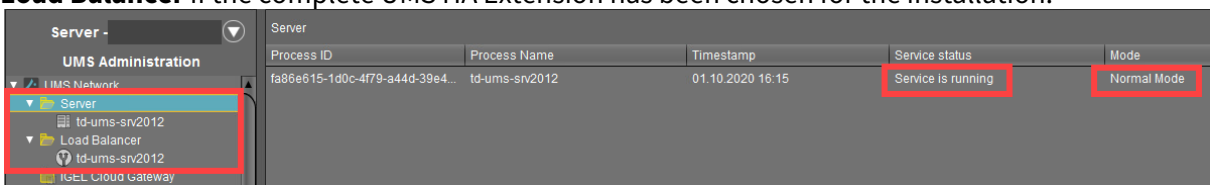
2. Select **Datasource > Add**.



3. Enter the connection properties of the prepared database schema. See also Setting up a Data Source (see page 555).
4. Click **Activate** to enable the data source. See also Activating a Data Source (see page 556).

Checking the Installation

1. Check if all processes are running. For the list of UMS HA processes, see HA Services and Processes (see page 592).
2. In the UMS Console, go to **UMS Administration > UMS Network** and check the items **Server** and **Load Balancer** if the complete UMS HA Extension has been chosen for the installation.



Saving the IGEL Network Token

▶ Save the IGEL network token, i.e. the file `IGEL-Network.token`, on a storage medium which will be accessible when installing further HA servers (e.g. on the network or on a portable storage medium such as a USB stick). Always keep the IGEL network token well protected.

Next Step

>> Proceed with adding a further server to the HA installation, see Adding Further Servers to the HA Network (see page 571).

Adding Further Servers to the HA Network

Introduction

Further HA servers – with UMS Server, UMS Load Balancer, or both – can be installed in the same way as the first one. However, you do not need to create a new IGEL network token. Instead, you must select the network token created previously during the installation of the first server in an HA network.

In addition, a connection with the same database that is used by the first server must be established. The UMS HA network only works if all servers are connected to the same database.

Prerequisites

- A High Availability (HA) installation with a configured database, see Installing the First Server in an HA Network (see page 566).

  ⚠ The database connection should be defined during the installation of the first UMS Server in an HA network. In this case, all relevant configuration information is automatically copied to the additional UMS Servers.

- The IGEL network token created during the installation of the first server in the HA network, see Installing the First Server in an HA Network (see page 567).
- A server with the operating system supported by the UMS; see the "Supported Environment" section of the release notes (see page 649).
- All installation requirements described under Installation Requirements (see page 565) are fulfilled.
- The same version of the UMS as for the first HA server is downloaded from the IGEL Download Server[19].

Instructions

To add a new server to the UMS HA installation, follow the instructions in the order given:

1. Preparing the Server (see page 571)
2. Preparing the IGEL Network Token (see page 572)
3. Starting the Installation (see page 572)
4. Checking the Installation (see page 574)

Preparing the Server

1. Verify that the server can "see" the other servers via the network.

   ⚠ All UMS Servers and UMS Load Balancers must reside on the same VLAN. Network traffic must be allowed over UDP broadcast port 6155, and TCP traffic and UDP broadcast traffic over port 61616. For more information on UMS ports, see UMS Communication Ports (see page 26).
   Note: IGEL UMS Server HA is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks.

19 https://www.igel.com/software-downloads/workspace-edition/

2. Verify that the time on all servers is synchronized.

   > ⚠ To avoid problems with your HA installation, make sure that the time on the servers of the HA network does not differ by more than one minute. After each manual time reset, the HA services on the relevant server must be restarted.

3. For Linux systems, make the directory `/root` writable for the user `root`.

Preparing the IGEL Network Token

▶ If you have not yet done so, save the IGEL network token created during the installation of the first HA server, e.g. on a portable storage medium.

> ⓘ If the path has not been changed, the file `IGEL-Network.token` can be found by default in the home directory of the administrator user on a UMS Server host.

> ⚠ If you have a fully functional UMS HA network already in use and simply want to enlarge it with one more HA server, make sure you use for the additional HA server installation the **current** IGEL network token. If you have not saved it:
>
> ▶ Restart the `IGEL RMGUIServer` service (for the instruction, see HA Services and Processes (see page 592)) and use in this case the network token created upon the UMS Server startup from the directory:
> Windows: `C:\Windows\System32\config\systemprofile\IGEL-Network.token`
> Linux: `/root/IGEL-Network.token`

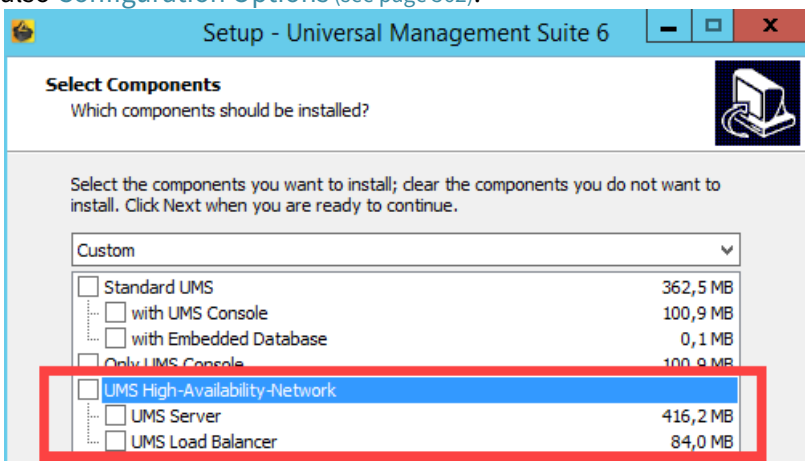
Starting the Installation

1. Launch the UMS installer.

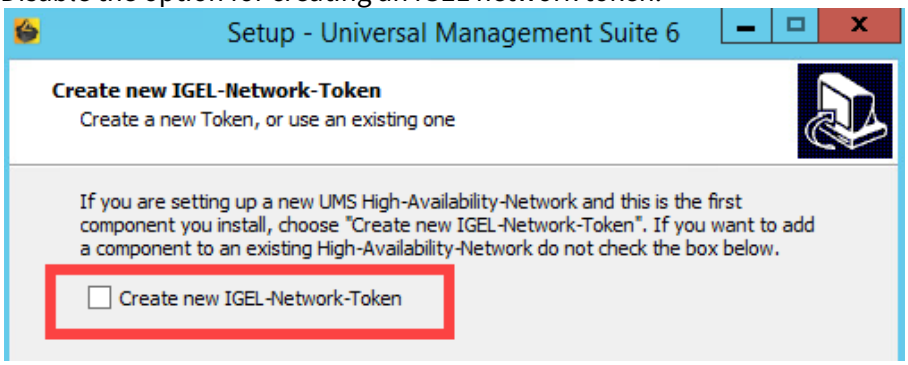
   > ⓘ You need administration rights to install the IGEL UMS HA.

2. Read and confirm the **License Agreement**.
3. Read the **Information** regarding the installation process.
4. Select a path for the installation.

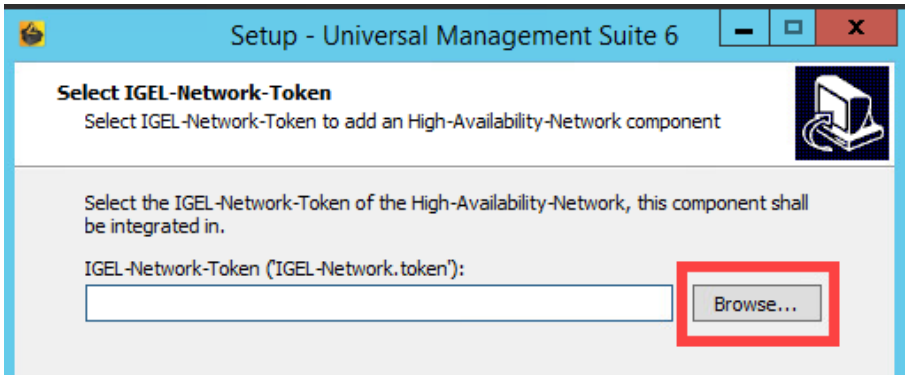
5. Select the components to be installed depending on your desired HA network configuration. See also Configuration Options (see page 562).



6. Select the **UMS data directory**, in which Universal Firmware Updates and files are to be saved.
7. Disable the option for creating an IGEL network token.



8. Select the IGEL network token to be used.



9. Specify a folder name for the shortcut.
10. Read the summary and start the installation process.
11. Close the UMS installer once the installation is complete.

If you have included a UMS Server in the installation, the UMS installer creates entries in the Windows software directory and the start menu. The UMS Console and UMS Administrator applications are installed, and a shortcut for the UMS Console is placed on the desktop.

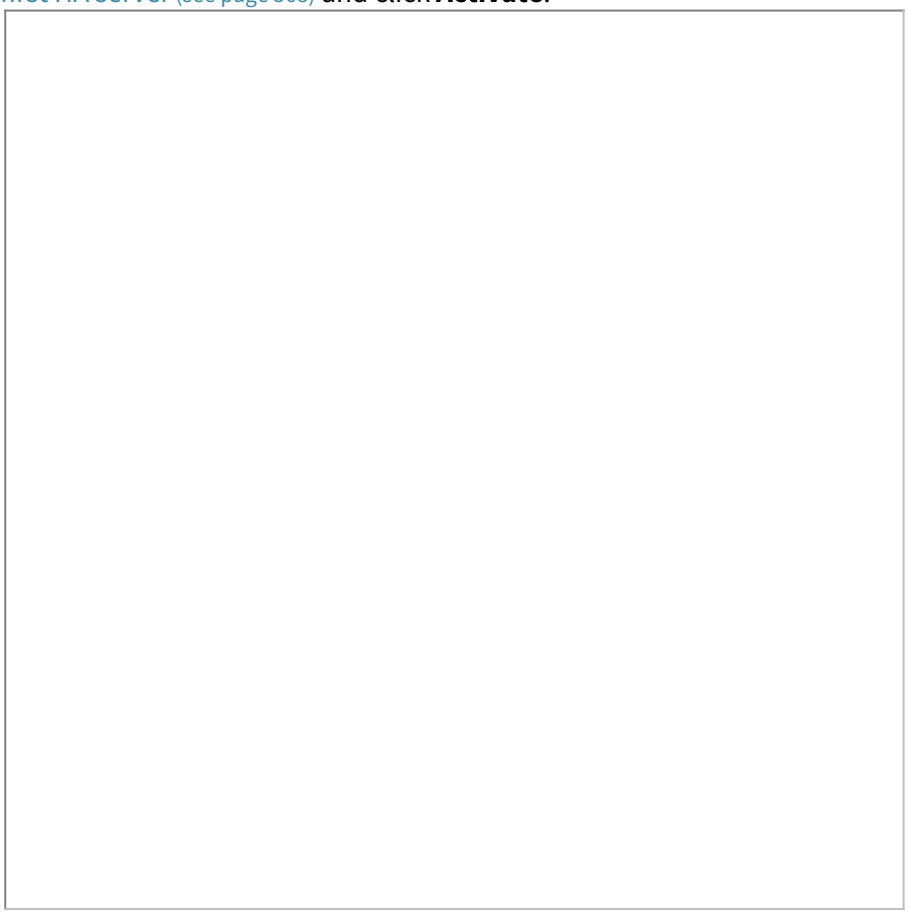
If you have installed an individual load balancer, only the option for uninstalling the UMS will be set up in the Windows start menu. No configuration on the load balancer is necessary. It connects automatically to the HA network during booting.

Checking the Installation

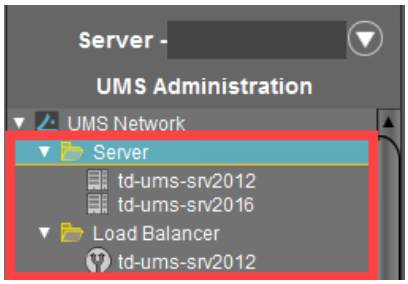
1. Check if all processes are running. For the list of UMS HA processes, see HA Services and Processes (see page 592).
2. If you have included a UMS Server in the installation, open **UMS Administrator > Datasource** and verify that the database connection has been successfully transferred from the already running UMS Server.

   > Default path to the UMS Administrator:
   > Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
   > Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
   > The IGEL UMS Administrator application can only be started on the UMS Server.

   If the database connection has not been defined automatically, enter under **UMS Administrator > Datasource > Add** exactly the same database parameters you used during the installation of the first HA server (see page 568) and click **Activate**.



3. In the UMS Console, go to **UMS Administration > UMS Network** and check the items **Server** and/or **Load Balancer**.



Updating the Installation of an HA Network

Use Case

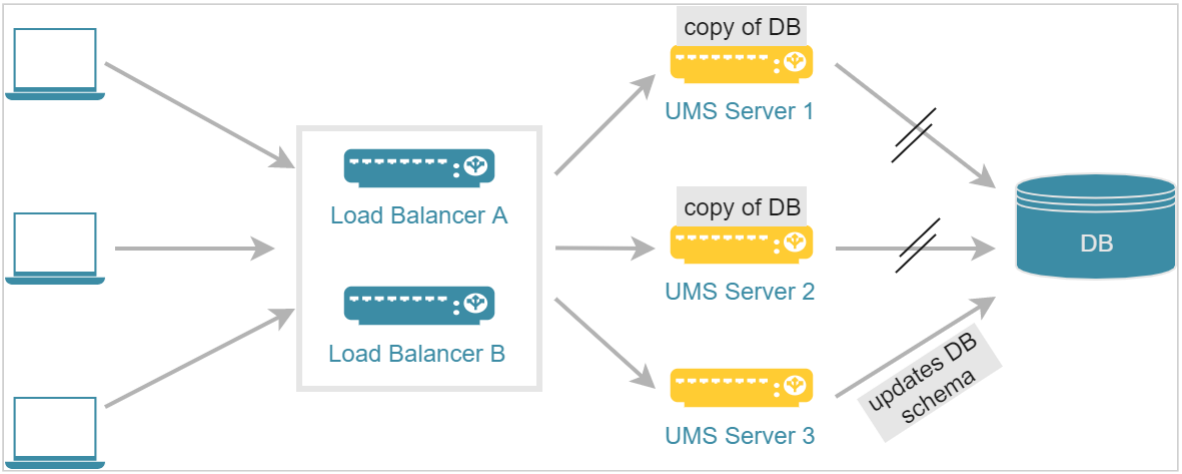
You have a UMS High Availability (HA) (see page 560) installation and need to update it.

General Overview

To update the UMS High Availability (HA) network, proceed as follows:

1. First, update all UMS Servers to a new version, one server after another.
2. Afterwards, update other components like separate UMS Load Balancers and/or UMS Consoles.

While being updated, a UMS Server disconnects itself from the productive database and stores a copy of it locally in an embedded Derby database. The last updated UMS Server will also update the schema of the productive database. After this, all other UMS Servers connect themselves again to the original productive database. In this way, all UMS Servers can be addressed by the endpoint devices at any time during the update process, e.g. to supply user-specific profiles (IGEL Shared Workplace).



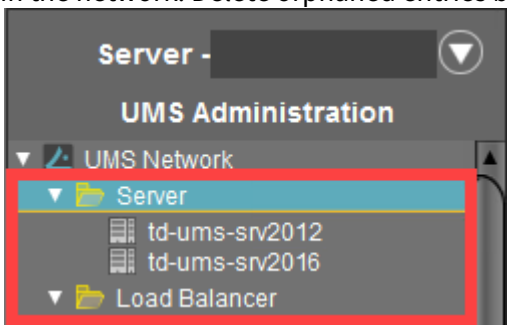
To update the HA installation, follow these instructions:

- Preparing the Update (see page 577)
- Updating UMS Servers (see page 578)
- Updating Further Components (see page 579)
- Checking the Installation (see page 580)

Preparing the Update

Perform the following steps before updating a server:

1. Download the current version of IGEL Universal Management Suite from the IGEL Download Server[20] and distribute the installer file to all systems with UMS components (UMS Server, UMS Load Balancer, UMS Consoles).
2. In the UMS Console, call up the list of UMS Servers and Load Balancers in the HA network under **UMS Administration > UMS Network** and check whether the listed components really exist in the network. Delete orphaned entries before starting the process for updating the components.



3. Create a backup of your database before starting the update installation. Use the backup procedures recommended by the DBMS manufacturer. See also Creating a Backup (see page 546).

> **Warning**
>
> It is not possible to install a UMS version which is older than the current one. If you want to change to an older version, you will need to install a separate HA network and restore a database backup of the corresponding schema. This is also one of the reasons why you should back up the running system before updating the UMS HA network.

4. Verify that the time on all servers is synchronized.

> To avoid problems with your HA installation, make sure that the time on the servers of the HA network does not differ by more than one minute. After each manual time reset, the HA services on the relevant server must be restarted.

Next Step

>> Proceed with Updating UMS Servers (see page 578).

20 https://www.igel.com/software-downloads/workspace-edition/

Updating UMS Servers

In the update mode, the UMS Servers run with a local copy of the database. This ensures that they can answer requests from the devices and transfer configuration settings and profiles to the devices.

> **Warning**
>
> Do not make changes in the productive database during the update process. This is because decoupled servers work with a copy of the database schema in the meantime. For this reason, the update of all components within the UMS HA network should be carried out immediately. Implement a test system for the first installation of new IGEL UMS versions and check their processes before transferring them to the productive system. This also applies to hotfixes, patches, etc. for server systems and databases.

Updating the First UMS Servers

You can select any UMS Server within the HA network to start the update procedure.

1. Launch the UMS installer.

   > You need administration rights to update the IGEL UMS HA.

2. Close other applications and confirm that you have done so.
3. Read and confirm the license agreement.
4. Read the explanation of the installation process.
5. Verify the components to be installed (in this case: HA network with server and load balancer installed individually).
6. Choose a name for the entry in the Windows start menu.
7. Read the summary and start the installation process.
   During the installation, the UMS Server switches to the update mode.

   > It is not possible to log in to servers via the UMS Console when in the update mode.

8. Confirm the message `n of m servers updated`.
9. Close the program once the installation is complete.
10. Continue with the update of the next UMS Server.

Updating the Last UMS Server

▶ Repeat steps 1-9 (see page 578) on the last UMS Server to be updated.

The last UMS Server updated renews the schema of the productive database after the installation. All other UMS Servers within the network which run in the update mode will be informed that the installation has finished. They will restart and reconnect themselves to the productive database. Afterwards, they will run in normal mode.

Next Step

>> Proceed with Updating Further Components (see page 579).

Updating Further Components

After updating the UMS Servers within the HA network, you have to update all other current UMS components, e.g. separate UMS Load Balancers and UMS Consoles.

1. In order to do this, run the UMS installer on the systems.
2. Verify the components to be installed.

> You cannot connect to the UMS Server with a console version that is older than the version of the UMS Server.

> Load balancers are able to interoperate with UMS Servers of newer versions, but they should have the same version as the UMS Servers for optimal performance.

See also Load Balancer Is Not Stopping during the Update of the HA Installation (see page 119).

Next Step

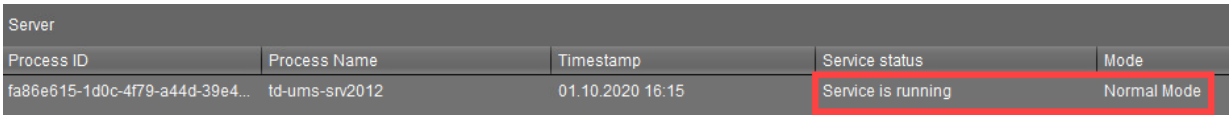
>> Proceed with Checking the Installation (see page 580).

Checking the Installation

1. Check if all processes are running. For the list of UMS HA processes, see HA Services and Processes (see page 592).
2. In the UMS Administrator (see page 539), go to **Datasource** to check if the database is activated.

   > ⚠ If the server list has not been checked at the beginning of the update (see Preparing the Update (see page 577)) and there have been more servers registered in the database than actually running, it might be the case that there is a server within the HA network that did not reconnect to the productive database.
   > In this case, you have to switch over the data source manually to the productive database.
   > The database schema will be renewed the first time an updated server connects to the productive database. Afterwards, all other servers within the network can be switched over to this database.

3. In the UMS Console, go to **UMS Administration > UMS Network** and check the items **Server** and **Load Balancer**.
   All servers and load balancers must be:
   - updated
   - running
   - in normal mode



Switching from a Standard UMS Installation to an HA Installation

Use Case

You have a standard UMS installation, but you want to switch to a High Availability (see page 560) (HA) installation.

Prerequisites

- A standard UMS installation with either an embedded or an external database
- A set of servers with the operating system supported by the UMS; see the "Supported Environment" section of the release notes (see page 649).

  ⚠ It is highly recommended to use only new servers for the HA installation, i.e. without the existing UMS installation.

- A database system supported by the UMS; see the "Supported Environment" section of the release notes (see page 649).
- All installation requirements described under Installation Requirements (see page 565) are fulfilled.
- The required version of the UMS is downloaded from the IGEL Download Server[21].

  ⚠ Do not use the UMS version older than the version of the existing UMS installation!

Instructions

The switch from a standard UMS installation to an HA installation involves the migration of the existing UMS Server to a new host and, in the case of the embedded database, the move to the external database.

The migration procedure generally involves the following steps:

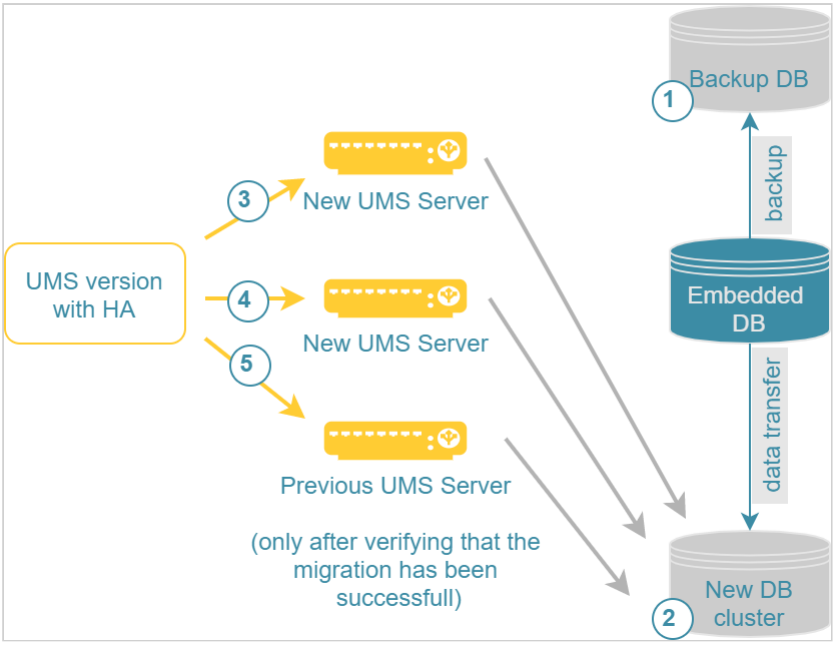
1. Backing up and, if necessary, cleaning existing data
2. If the embedded database is in use: Setting up an external database and transferring the data from the existing database to the new one
3. Installing the first HA server with the `tc.keystore` file of the previous UMS installation, connecting it to the external database and transferring the files from the previous UMS installation

   ✓ For the first HA server, take a new host machine, i.e. without the existing UMS installation. After you make sure that the migration has been successful, you can uninstall the old UMS Server and reinstall it with the HA extension.

4. Adding further components to the HA network, e.g. further UMS Servers, Load Balancers, UMS Console

Example with an Embedded DB

21 https://www.igel.com/software-downloads/workspace-edition/



Detailed instructions are provided below. Follow them in the order given:

- Preparing the Migration (see page 583)
- Setting Up the New Database and Transferring Data (If the Embedded DB is in Use) (see page 585)
- Installing the First HA Server and Transferring the Data from the Existing UMS Server (see page 587)
- Installing Further HA Components (see page 590)

Preparing the Migration

Preparing New Servers

1. Verify that each server can "see" the other servers via the network.

   > ⚠ All UMS Servers and UMS Load Balancers must reside on the same VLAN. Network traffic must be allowed over UDP broadcast port 6155, and TCP traffic and UDP broadcast traffic over port 61616. For more information on UMS ports, see UMS Communication Ports (see page 26).
   > Note: IGEL UMS Server HA is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks.

2. Verify that the time on all servers is synchronized.

   > ⚠ To avoid problems with your HA installation, make sure that the time on the servers of the HA network does not differ by more than one minute. After each manual time reset, the HA services on the relevant server must be restarted.

3. For Linux systems, make the directory `/root` writable for the user `root`.

Preparing the Existing System

> ✓ **Tip**
>
> The move provides an opportunity to remove any UMS database data which are no longer used. For example, you can
> - delete endpoint devices that no longer exist
> - delete profiles that are no longer used
> - remove files and firmware updates that are no longer needed
>
> It is highly recommended to create a backup before carrying out the cleanup (as a backup of the system running) and another one after the cleanup.

1. Create a backup before performing the move:
   - For the embedded database: Create a backup using the UMS Administrator tool, see Creating a Backup (see page 546). Include all options in the backup.
   - For external database systems: Use the backup procedures recommended by the DBMS manufacturer. For the backup of server configurations, use the UMS Administrator tool, see Creating a Backup (see page 546).
2. Save the following files, e.g. to a storage medium that can be accessed during UMS HA installation:

Certificates	• `[IGEL installation directory]/rmtcserver/*` (includes the `tc.keystore` file, which is necessary for the communication with the endpoint devices) • `[IGEL installation directory]/rmclient/cacerts` • `[IGEL installation directory]/rmguiserver/cacerts` • `[IGEL installation directory]/rmguiserver/irm_keystore`
Device licenses (up to UMS 6.07; as of UMS 6.08, licenses are included in the database)	• `[IGEL installation directory]/rmguiserver/webapps/e08ce61-d6df-4d2b-b44a-14c1ec722c44`
Files and firmware updates	• `[IGEL installation directory]/rmguiserver/webapps/ums_filetransfer`

3. Create a backup of the UMS Licensing ID using the UMS Administrator tool. For detailed instructions, see Transferring or Registering the UMS Licensing ID (see page 86).

Next Step

>> If you use the embedded database: Setting Up the New Database and Transferring Data (If the Embedded DB is in Use) (see page 585)

>> If you use the external database: Installing the First HA Server and Transferring the Data from the Existing UMS Server (see page 587)

Setting Up the New Database and Transferring Data (If the Embedded DB is in Use)

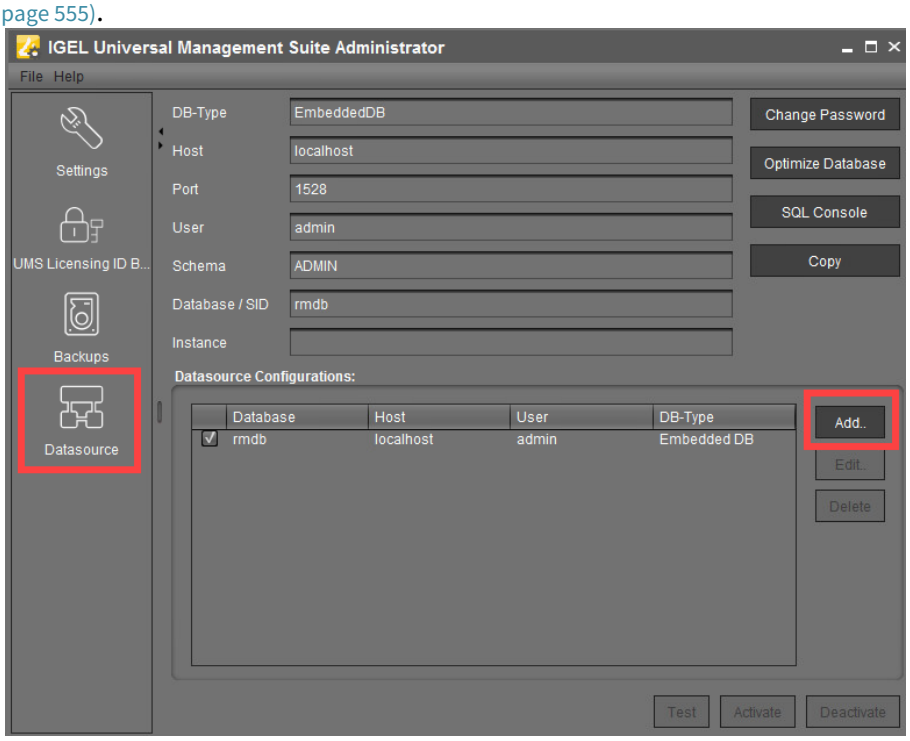
> The following steps are only required if your current UMS installation uses an embedded database.

If you use the embedded database, you have to move its data to the external database before you start with the installation of the first HA server.

1. Create a database schema and a user for the UMS. Use the relevant DBMS program and its documentation. See also Connecting External Database Systems (see page 220).
2. Open the UMS Administrator on the existing UMS Server.

   > Default path to the UMS Administrator:
   > Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
   > Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
   > The IGEL UMS Administrator application can only be started on the UMS Server.

3. Add the new database connection under **Datasource > Add**. See also Setting up a Data Source (see page 555).



4. Select the embedded database (active datasource) and click **Copy** to copy its contents to the new database.
5. Select the new database and click **Activate**. See also Activating a Data Source (see page 556).
   Now, the external database is set up as a datasource for your UMS.

For a concrete example of how to switch to an external database, see Migrating a UMS Database From Embedded DB to Microsoft SQL Server (see page 94).

Next Step

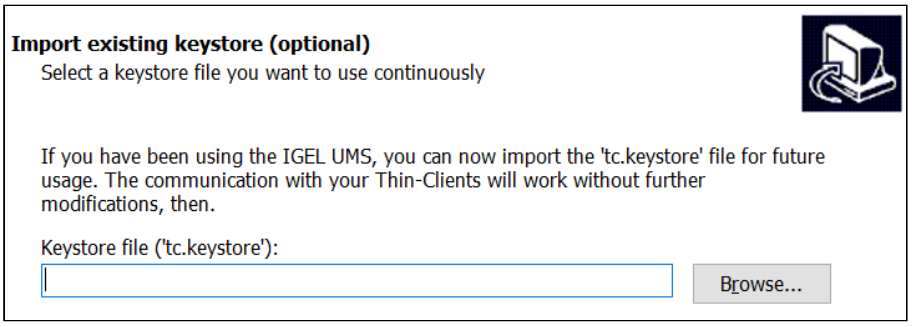
>> Installing the First HA Server and Transferring the Data from the Existing UMS Server (see page 587)

Installing the First HA Server and Transferring the Data from the Existing UMS Server

When all preparation steps have been made, you can start the migration.

Installing the First HA Server

▶ Start the UMS High Availability (HA) installation. For the instructions, see the "Starting the Installation" section under "Installing the First Server in an HA Network" (see page 567).
When asked for the keystore, use the file `[IGEL installation directory]/rmtcserver/tc.keystore` of the existing UMS installation:



Transferring the Data from the Old UMS Server

▶ Copy the files from the following folders (without the `WEB-INF` folder) to the new server:

- `[IGEL installation directory]/rmguiserver/webapps/e08ce61-d6df-4d2b-b44a-14c1ec722c44`
- `[IGEL installation directory]/rmguiserver/webapps/ums_filetransfer`

> **Universal Firmware Updates**
>
> If you have used the UMS's integrated webserver to distribute the firmware updates, the updates that are still required should be manually transferred to all servers in the HA network or the FTP server (if you configure it as the destination for the update files, see Universal Firmware Update (see page 495)). See also How to Detect Which Files Are Synchronized Automatically (see page 120).
> Or you can simply download the required firmware updates anew.

Defining the Database Connection

1. Stop the Windows service `IGEL RMGUIServer` on the old UMS Server.
2. Open the UMS Administrator on the HA server.

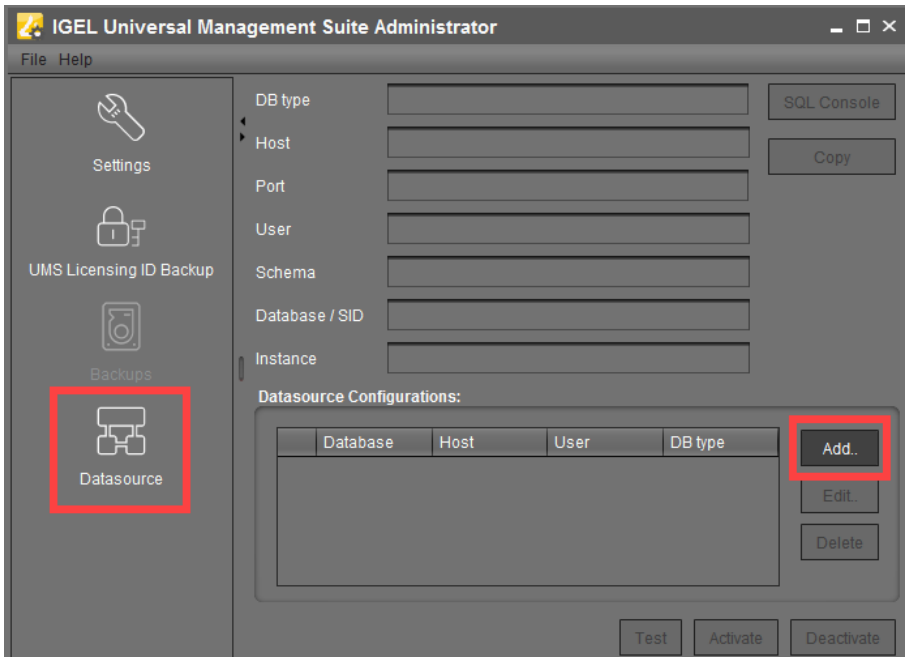
> Default path to the UMS Administrator:

Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`

Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`

The IGEL UMS Administrator application can only be started on the UMS Server.

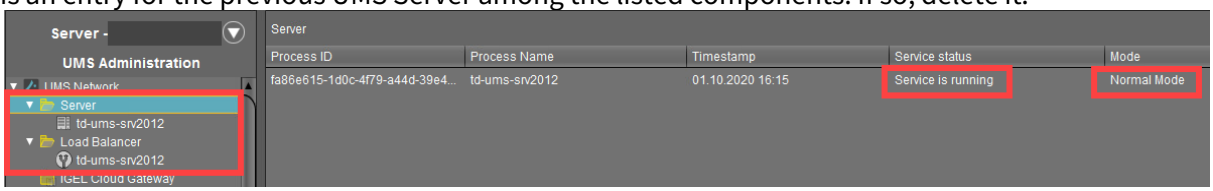
3. Select **Datasource > Add**.



4. Enter the connection properties of the prepared database. See also Setting up a Data Source (see page 555).
5. Click **Activate** to enable the data source. See also Activating a Data Source (see page 556).

Checking the Installation

1. Check if all processes are running. For the list of UMS HA processes, see HA Services and Processes (see page 592)
2. In the UMS Console, go to **UMS Administration > UMS Network** and check the items **Server** and **Load Balancer** if the complete UMS HA Extension has been selected for installation. Check if there is an entry for the previous UMS Server among the listed components. If so, delete it.



Transferring or Registering Your UMS Licensing ID

▶ Transfer the UMS Licensing ID of the previous UMS installation to the new server. Alternatively, you can register the new UMS Licensing ID, which was created during the installation of the HA server. For detailed instructions, see Transferring or Registering the UMS Licensing ID (see page 86).

Adjusting DHCP Tag and DNS Alias

▶ Adapt, if necessary, the **DHCP Tag** and the **DNS Alias** `igelrmserver` with the IP or FQDN of the new UMS Server. See Registering Devices Automatically on the IGEL UMS (see page 242).

> ⓘ The configuration of the DHCP tag and the DNS alias is not a setting that can be made within the IGEL software. You must configure these within your individual network environment on the corresponding DHCP and DNS servers.

Next Step

>> Proceed with installing the other components, i.e. further UMS Servers, UMS Load Balancers, or UMS Console: Installing Further HA Components (see page 590).

Installing Further HA Components

After the first HA server is installed and the data has been moved to it, you can install further components, i.e. further UMS Servers, Load Balancers, UMS Console.

1. Install further servers and check the installation. For the instructions, see Adding Further Servers to the HA Network (see page 571).
   The data will automatically be synchronized between the HA servers, see How to Detect Which Files Are Synchronized Automatically (see page 120).
2. After all UMS Servers have been installed, update the host assignment for job execution. For the instructions, see Updating Host Assignment for Job Execution (see page 92).

> If you have used and adjusted the DNS alias and the DHCP option, the following step is NOT required since the device can resolve the name `igelrmserver` correctly.
>
> In the local configuration, the device always remembers the IP of the UMS Server of its first registration. It is thus possible that the old IP address is displayed under **System > Remote Management**. Therefore, it makes sense to manually set an entry for remote administration after the migration:
>
> 1. Create a profile in the UMS:
>   - Go to **System > Remote Management** and click **Add**.
>   - Under **UMS Server**, enter the IP of the new UMS Server.
> 2. Apply this profile globally, to the entire structure.

Licensing the High Availability Extension

IGEL OS 11 and Higher

The IGEL UMS High Availability Extension no longer requires an additional license.

Before IGEL OS 11

The High Availability Extension comes in packages of 50 licenses. These licenses are installed in the UMS. The UMS checks if the number of licenses is at least as high as the number of devices connected to the UMS.

Each version of the IGEL UMS contains five test licenses allowing you to evaluate the function free of charge and without having to register.

▶ Register the license file you receive in the UMS Console under **UMS Administration > Global Configuration > Licenses > UMS Licenses**.

> An HA network only works with a license covering all managed devices registered in the UMS. A mixed mode (devices with HA support and devices without HA support) is not possible.

HA Services and Processes

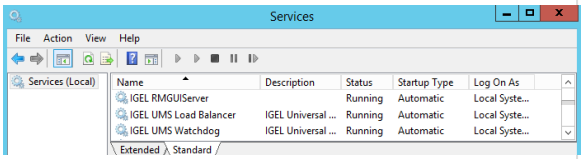
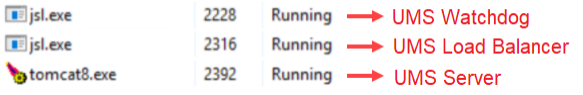
A High Availability (HA) installation consists of several processes: Each node of the HA network has either the UMS Server or the UMS Load Balancer or both running, depending on the configuration you have chosen during the installation process of the UMS HA, see also Configuration Options (see page 562). In addition, the UMS Watchdog always runs on each node.

UMS Server	• Handles all requests from the devices and the UMS Console. • Talks to the devices. • Executes jobs. • Acts as a message broker for internal messages.
UMS Load Balancer	• Forwards incoming requests from the devices to one of the UMS Servers with load balancing. The UMS Load Balancer has a list of running UMS Servers and distributes the requests to them sequentially.
UMS Watchdog	• Monitors the run status of the UMS Server and the UMS Load Balancer running on the same server and forwards it to the UMS Servers. • Starts or stops the UMS Server or the UMS Load Balancer on request from a UMS Server.

⚠ If both the UMS Server and the UMS Load Balancer are running on the same server, the UMS Server uses port 30002 and the UMS Load Balancer uses port 30001. If only the UMS Server is installed on a server, it always listens on port 30001. See UMS Communication Ports (see page 26).

The following table shows how you can find out which HA processes are running and how/where you can stop or start them.

Windows	Linux

Services:
 
 	
The processes are normally stopped here.
Task Manager:
 
 	
Emergency stop if the process cannot be stopped in the **Services**.
cmd / Command Prompt:
`sc queryex “IGELRMGUIServer”`
`sc queryex “IGEL UMS Load Balancer”`
`sc queryex “IGEL UMS Watchdog”`
Emergency stop if the process cannot be stopped in the **Services**:
• `taskkill /PID xxxx /F`
where the PID can be seen in the output of
`sc queryex “Name of the process”`
	• For the list of running processes, use the command:
	`sudo ps -ef | grep RemoteManager`
	where `RemoteManager` is the last part of the installation path; Adjust it if the installation path is different.
	Each process has two entries on the list.
	• For stopping the processes, use:
	`sudo /etc/init.d/igelUMSwatchdog stop`
	`sudo /etc/init.d/igelUMSbroker stop`
	`sudo /etc/init.d/igelRMserver stop`
	• For stopping the processes if the stop with the `init` scripts does not function:
	`sudo kill -9 xxxx`
	where the ID of the process can be seen in the output of
	`sudo ps -ef | grep RemoteManager`

Shared Workplace (SWP)

IGEL Shared Workplace (SWP) allows user-dependent configuration using profiles created in the IGEL Universal Management Suite and linked to the AD user accounts. In the process, user-specific profile settings are passed on to the device along with the device-dependent parameters. You will find an overview of the parameters that can be individually configured for a user u (see page 602)nder Parameters Configurable in the User Profile (see page 602).

Licensing with IGEL OS 11

For use with IGEL OS 11 devices, Shared Workplace requires a valid license from the IGEL Enterprise Management Pack (EMP). This license must be present on every IGEL OS 11 device on which Shared Workplace is to be used. When the license expires, users will no longer be able to login to a Shared Workplace session.

Licensing with IGEL OS 10

For use with IGEL OS 10 devices, Shared Workplace requires an add-on license for Shared Workplace. This license must be present on every IGEL OS 10 device on which Shared Workplace is to be used. The license is perpetual.

Typical Uses for Shared Workplace

- Workstations used for shift work or in call centers, where different staff members at a workstation need their own individual settings, e.g. session types or mouse-button settings for right/left-handed operation.
- Roaming environments, where users frequently switch workstations, such as in hospitals and at service/ticket counters, checkouts, or reception areas. After a user has logged in, the endpoint device licensed for Shared Workplace automatically configures itself. It does this via the UMS server using the individual or group profile stored in the UMS database. These profiles can easily be assigned to a user with the help of the IGEL Universal Management console using a convenient drag-and-drop procedure.

  > In environments with an increasing number of Shared Workplace workstations, IGEL recommends using the UMS High Availability Extension (see page 560). The high level of UMS server availability achieved ensures that users receive their user-specific profile at all times.

IGEL Tech Video

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=opgVxN791Vg

SWP Configuration in the UMS Console

In order to be able to use IGEL Shared Workplace, the following requirements must be met:

- Users who are to be given a specific profile must be set up in a Microsoft Active Directory.
- Devices which are to allow user logins must have a license for the IGEL Shared Workplace function. This can be transferred to the devices via the IGEL UMS license management system.

  > If a device has been given a license for IGEL Shared Workplace, this cannot be canceled. However, the function can be disabled via the list of available services in the device configuration. Login via IGEL Shared Workplace is then disabled.

- Although not absolutely necessary, the use of the High Availability Extension (see page 560) for the IGEL Universal Management Suite is recommended for larger installations. This will ensure a high level of availability for the user profiles in the network.

  > If you use IGEL Shared Workplace with IGEL Universal Desktop WES 7, bear in mind that the default password **"user"** must be set for the default user **"user"**, otherwise it will not be possible to log in.

  See also Display Configuration for Shared Workplace (SWP) (see page 605).

In this chapter, you can learn about:

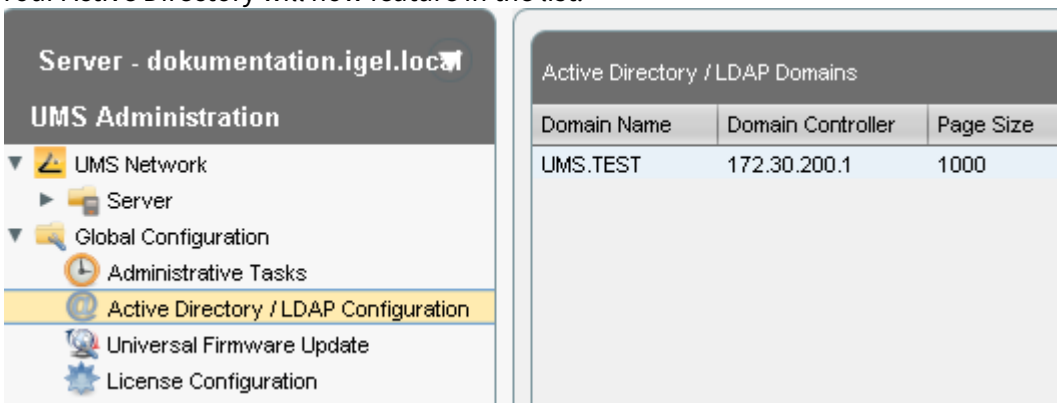
- Linking an Active Directory (see page 597)
- Assigning a User Profile (see page 598)
- Enabling IGEL Shared Workplace on the Thin Client (see page 599)
- User login (see page 600)
- Logout and Change of User (see page 601)

The priority of user-specific profiles is dealt with in Order of Effectiveness of Profiles in Shared Workplace (see page 308). See also Order of Effectiveness of Profiles (see page 305).

Linking an Active Directory

To link an Active Directory in the UMS, proceed as follows:

1. Click on **Active Directory** in the **UMS Administration** area.
2. Click on **Add**.
   The **Add Active Directory / LDAP Service** mask will open.
3. Enter the **domain name** and the access data.
4. Confirm your settings by clicking on **OK**.
   Your Active Directory will now feature in the list.



> Other LDAP servers (*Novell eDirectory*, *OpenLDAP* etc.) cannot be used for *IGEL Shared Workplace* user authentication purposes.

Assigning a User Profile

Go to your Active Directory in the UMS navigation tree under **Server > Shared Workplace User**.

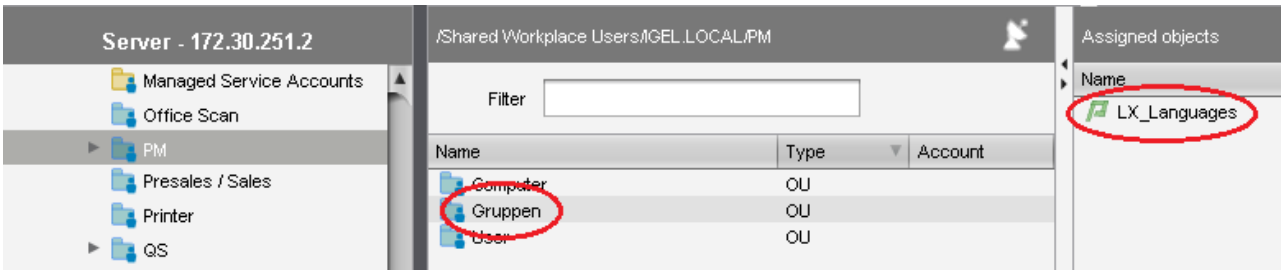
You can browse it or search for it by using this symbol:  .

▶ Select an object within the AD structure.

You will need to authenticate yourself vis-à-vis the Active Directory in order to do so.

▶ Assign the desired user profile to this object:

Server>Shared Workplace User>[Active Directory]>[Object]



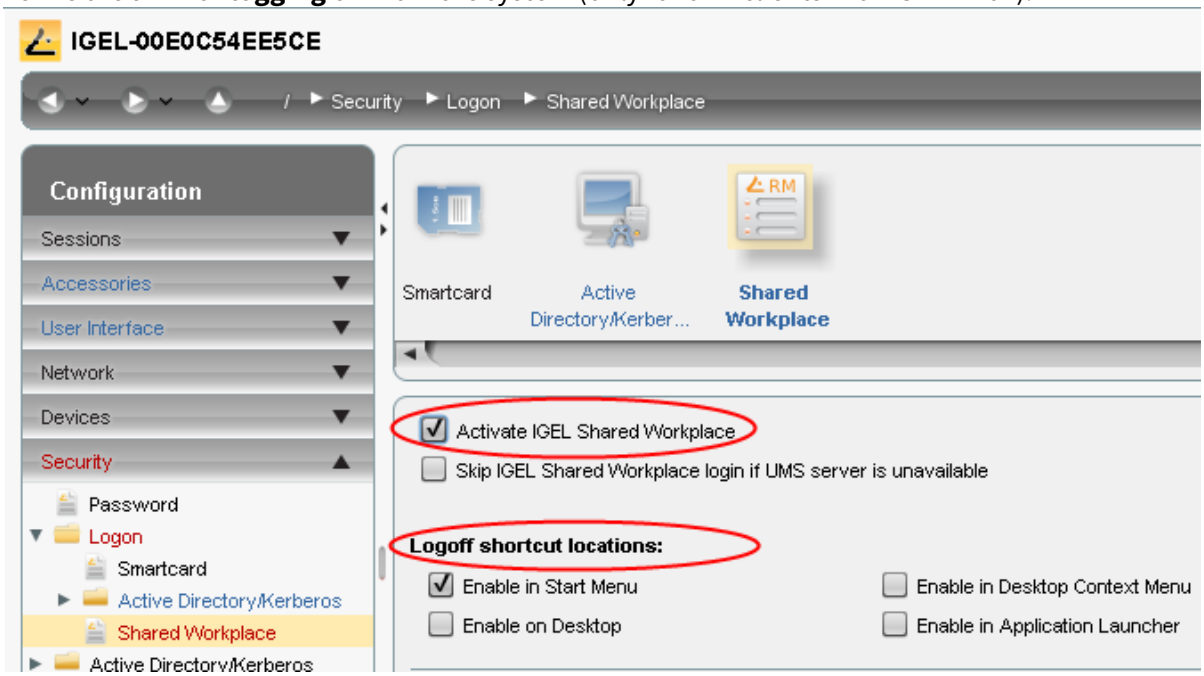
As with thin clients, a number of individual profiles can be assigned. In this case, indirectly as well as directly assigned profiles will be taken into account.

Right-click the name of a user account, to see the profile settings of a special thin client.

Enabling IGEL Shared Workplace on the Thin Client

You can configure the settings for Shared Workplace from the UMS via a profile or directly in the setup of the relevant thin client.

1. Go to **Configuration > Security > Login > IGEL Shared Workplace**.
2. Enable the **IGEL Shared Workplace** function.
3. Define the **link for logging off** from the system (only for thin clients with IGEL Linux).



User login

If you have a license, you can easily log in to a endpoint device with IGEL Shared Workplace:

1. Boot the device.
   A login window will appear.
2. Log in with your AD login data.
   You will receive the profile settings that are stored for you in the UMS.

> The device configuration which is active for the user logged in is the result of cumulating all profiles which have been assigned either directly or indirectly to the device or the user. See also Prioritization of Profiles (see page 304).

Logout and Change of User

Windows Embedded Standard

- Log out via the start menu.

IGEL Universal Desktop Linux

Under Linux, you can set up the following logout options:

- In the **Application Launcher**, define where you will place the buttons for logging off.
- Under **Security > Login > IGEL Shared Workplace** in the IGEL Setup, define a hotkey for logging off.

Parameters Configurable in the User Profile

Not all parameters available in an item of firmware can be configured on a user-specific basis.

The system settings which cannot be configured effectively by a user-specific profile are described below.

> The UMS does not check whether the settings are effective.

The device-specific system settings for the IGEL operating systems which **cannot be configured effectively** are listed below. No check takes place in the IGEL UMS.

- Universal Desktop Linux (see page 603)
- Universal Desktop Windows Embedded Standard (see page 604)

UD Linux Device-specific Parameters

The following system settings are **not** configurable in the user profile:

- Network settings including those for the network drives
- Screen configuration for IGEL Linux v5 to 5.05.100 and for IGEL Linux v4 to 4.13.100.

  > Depending on the hardware used, display errors may occur if the user changes the resolution or rotates the screen even under IGEL Linux from Release 4.14.100. See the How-To document Display Configuration for Shared Workplace (see page 605).

- Touchscreen configuration
- Update settings
- Security settings
- Remote management
- Customer-specific partition
- Server for background images

  > With IGEL *version 10.03.500* or higher, background images and the custom wallpaper server can be defined for each individual user via Shared Workplace.

- Customer-specific bootsplash
- Browser plug-ins
- SCIM entry methods, however, these can be enabled on a user-specific basis
- Three-button mouse emulation
- Appliance Mode (VMware View, Citrix XenDesktop and Spice)

UD W7 Device-specific Settings

The following system settings cannot be configured in the user profile:

- Language, standards and formats
- Network settings including those for the network drives
- Active Directory login
- USB device configuration
- List of the available features and Windows Services
- Update settings
- Setup session
- User and security settings
- File Based Write Filter
- Energy options
- Remote management
- Appliance Mode (VMware View and Citrix XenDesktop)

Display Configuration for Shared Workplace (SWP)

As of IGEL Universal Desktop Linux *version 4.14.100* and *version 5.06.100*, Shared Workplace allows user-specific screen resolutions and configurations. Resolution, layout, refresh rate, rotation, number of screens, monitor connectors (DVI, VGA, ...) can be set per user, but color depth cannot.

There are technical limitations to user-specific settings: For VIA graphics drivers/hardware, the maximum desktop size is set in the `Screen` section of the X configuration file. The name and location of the X configuration file depend on the firmware version:

- IGEL Linux *version 10*: `/config/Xserver/xorg.conf-0`
- IGEL Linux *version 5*: `/config/Xserver/xorg.conf-0` or `/etc/X11/xorg.conf` (this is a symbolic link that points to `/config/Xserver/xorg.conf-0`)
  In the `Screen` section of the above-mentioned configuration file, you can find a line such as `Virtual 1920 1200`. The size defined here cannot be changed dynamically; it is a hard limit for the overall desktop size.

Best Practice

It is recommended to set the initial desktop configuration to the maximum number of screens and the resolutions to A `utodetect`. This way, the user-specific resolutions will not be restricted.

Debugging

If the total framebuffer size of the user-specific resolutions exceeds the limits of the `Virtual [width] [height]` setting from `/config/Xserver/xorg.conf-0` (or `/etc/X11/xorg.conf`), the user-specific resolutions cannot be activated and the screen configurations are not changed dynamically.

There is no warning dialog or anything else to alert the user to this restriction. But you can find related log messages via `journalctl` or in `/var/log/messages`:

```
XRANDR: ERROR: CANNOT APPLY CHANGES ->
```

```
XRANDR: ERROR: -> Selected modes ([width]x[height]) would exceed the maximum framebuffer size ([width]x[height])
```

Asset Inventory Tracker (AIT)

For details, see View Asset Information (see page 376).

IGEL Management Interface (IMI)

See the documentation on this page: IGEL Management Interface (IMI)

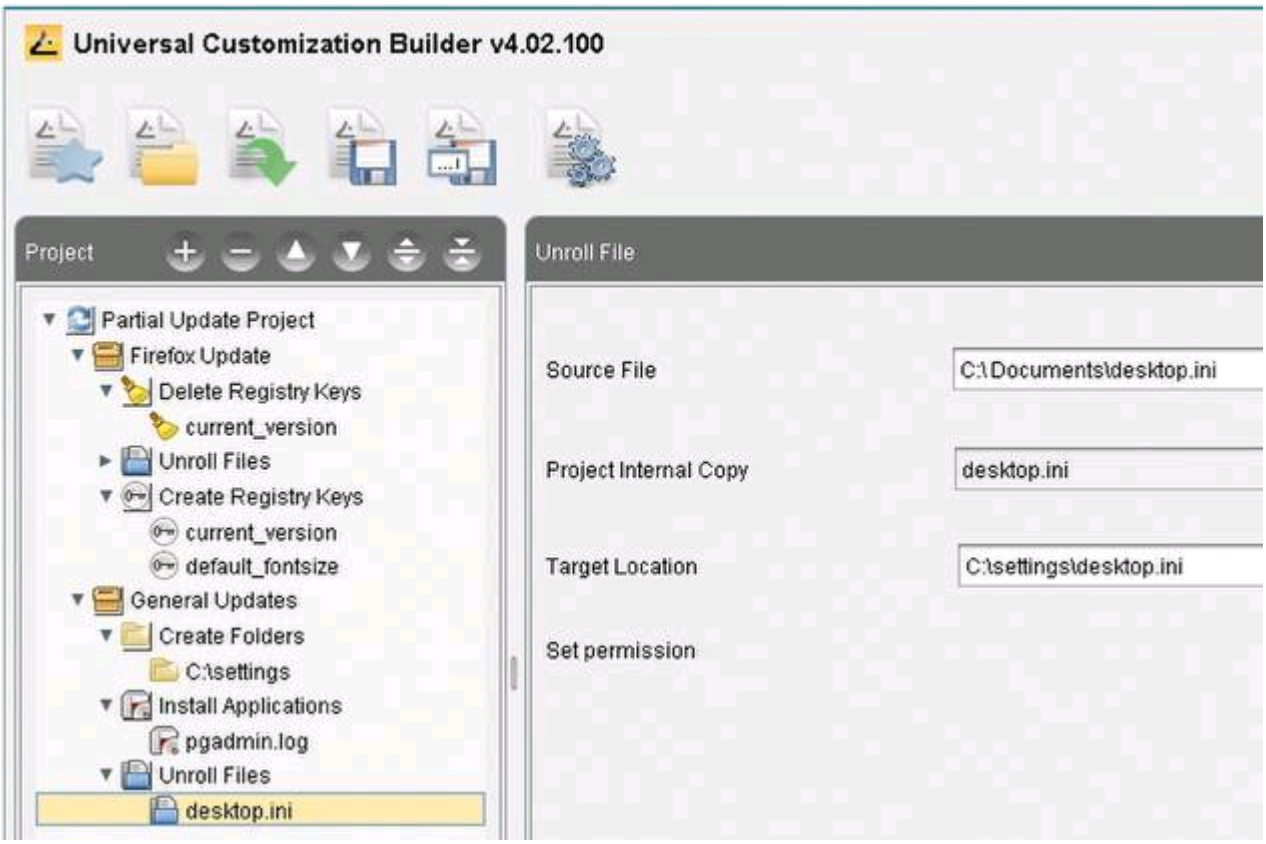
Universal Customization Builder (UCB)

UCB Reference Manual

With the Universal Customization Builder (UCB), IGEL firmware can easily and reliably be expanded and adapted to meet your needs. For example, you may choose to install local device drivers or special applications. You can even set important Windows registry keys – with no detailed knowledge of Shell or Windows scripting.

Introduction

The IGEL Universal Customization Builder (UCB) is an optional extension of the Universal Management Suite (UMS) which enables you not only to put together individual expansion packages for IGEL firmware, but also to package them and roll them out on a centralized basis. Numerous helpful features such as predefined templates or the user-friendly GUI make this reliable application easy to use. The UCB supports IGEL OS and Windows Embedded, regardless of the devices on which the firmware is installed.



Typical Usage Scenarios

- Supplementing local apps: Rolling out applications for local operations, e.g. checkout software for retailers and other sector-specific software, on a centralized basis
- Upgrading device drivers: For sector-specific peripherals or original drivers
- Setting registry keys: Individually adapting Windows Embedded Standard
- Kiosk systems: Equipping thin clients with special local applications or software clients in order to operate them independently of the company network, e.g. as time recording terminals

Features

- Simple procedures for generating, packing and rolling out firmware expansion packages for IGEL OS (custom partition) and Windows Embedded (partial update).
- Predefined templates: Task-oriented for typical application scenarios
- Debugging: Automatic package creation with syntax checks
- Automatic versioning within customization projects
- Support for the packages created available from the IGEL support team

Your Benefits

- Reduced project costs: With the UCB, you can now perform firmware expansions quickly and easily yourself (without assistance from an external service provider)
- Ease of use: User-friendly GUI with the familiar look and feel of the IGEL UMS, no detailed knowledge of Shell or Windows scripting necessary (templates)
- Quick, low-cost rollout: Convenient, remote rollouts using IGEL UMS
- Reliable processes and functions: User prompting via GUI and templates, simple debugging and support from IGEL
- Transparency: Automatic versioning within customization projects

Before distributing changes to your actual systems, it is important to test partial updates or customer-specific partitions on one or more thin clients to ensure that they are stable and function correctly.

Licensing

A UCB license is required to use the optional UCB extension for the *IGEL Universal Management Suite (UMS)*. In order to obtain this license, you must successfully take part in a paid IGEL UCB training course (in-house or classroom training).

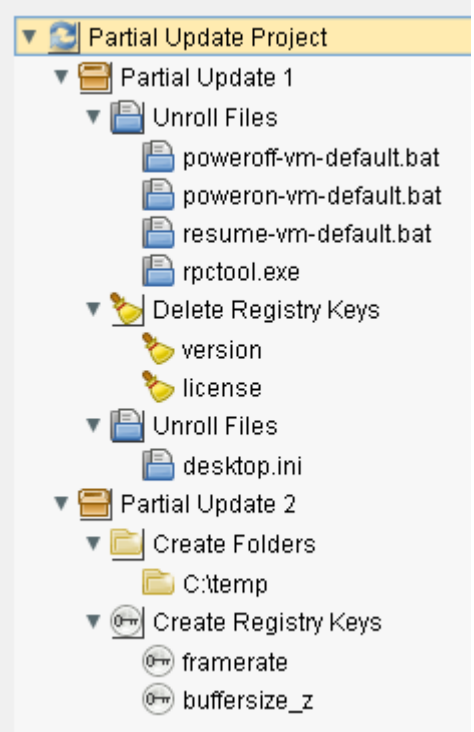
The license is registered in the administration area of the UMS Console under **Global Configuration > Licenses**.

Partial Update for IGEL Thin Clients with Windows Embedded Standard

A partial update is a collection of tasks which are grouped together in a script. This script is sent to the thin clients together with the files that are to be distributed. The script is executed on the thin client and works through the pre-defined tasks.

Various tasks such as distributing files, setting up registry keys, executing commands and many others can be defined for a partial update. Similar tasks of the equivalent type are grouped together in sections. A project can contain a number of partial updates with various sections and tasks. Using the import function, a number of partial updates can be brought together to form a project.

An example is shown here:



The following types of tasks (sections) are available in projects:

- Roll out file
- Create directory
- Set rights
- Delete file/directory
- Create registry key
- Roll out registry file
- Delete registry key
- Install application

- Execute command

When a project is being "built", all necessary scripts are generated and stored together with the required source files in a selectable project directory.

Before distributing changes to your actual systems, it is important to test partial updates or customer-specific partitions on one or more thin clients to ensure that they are stable and function correctly.

Project Functions

Launch the Universal Customization Builder in the UMS Console via **System > Universal Customization Builder**.

The following functions are available for a partial update project:

	Create new project ([Ctrl+n]) • Opened projects are saved. • The setup dialog opens. • Enter a **Project name** . • Select a **Project directory** for the project. A subfolder with this name will be created; this subfolder will contain all project files. • Select **Partial Update** as the project type. • Click **OK**.
	Load project ([Ctrl+o]) • Opened projects are saved. • The selection dialog opens. • Select a project file (partial update project `.ipu`). • Click **Open**.
	Save current project ([Ctrl+s]) • Saves the project in its current state in the project directory.
	Save current project as... • The setup dialog opens. • Enter a **Project name**. • Select a **Project directory** for the project; a sub-folder bearing the project name and containing all project files will be set up in it. • Click **OK**. • A copy of the current project with all files will be saved under the new name in the selected directory.
	Close current project ([Ctrl] + [0]) The current project is saved and then closed.
	Import project (partial update only) ([Ctrl+i]) • The selection dialog opens. • Select a project file (`.ipu`). • Click **Open**. • All parts of the selected project will be added to the current project.

	Build project ([Ctrl+b]) • The selection dialog opens. • Select a destination directory for the partial update. • **Warning** - All files in the destination directory will be deleted! • Click **Open**. All scripts and files to be sent to the thin client will be stored in the destination directory. Once the process has been completed successfully, the destination directory contains the finished partial update for distribution to the thin clients.
	Options **Default project path:** Select the URL of the current project path.
	Add new entity... ([Insert]) • Sets up a new element depending on the current element type.
	Delete entity... ([Delete]) • Deletes the selected elements.
	Move element upwards ([Page up]) • Moves the selected element up one position.
	Move element downwards ([Page Down]) • Moves the selected element down one position.
	Expand all entities • Opens all tree nodes.
	Collapse all entities • Closes all tree nodes.

Transferring the Partial Update

To transfer partial updates to the system, proceed as follows:

1. Launch the device configuration (locally or in the UMS).
2. Select **System > Update > Partial Update**.
3. Check the **Use IGEL Setup for configuring partial update settings** checkbox.
4. Select a transfer **Protocol** (HTTP, FTP, FILE).
5. Specify the source server/path on the drive (destination directory for the partial update project).
6. If necessary, enter the relevant login data.
7. Click **Apply** to save the settings.
8. Click **Search for Updates** in order to search the source for available updates (only locally on the device).

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

In the UMS, you can launch the distribution of the partial update via the device's context menu (**Update & snapshot commands > Partial Update**) or set up a planned task that will perform the distribution on a scheduled basis.

Mobile Device Management Essentials (MDM)

⚠ MDM is not further developed by IGEL.

IGEL Mobile Device Management Essentials (MDM) is a feature introduced with UMS version 5.09.100 as a technical preview.

During the technical preview phase, only five devices can be managed simultaneously. This technical preview does not require licensing.

MDM Basic Overview (see page 619)

MDM Setup Guide (see page 641)

Connecting Mobile Devices to the UMS (see page 643)

Basic Overview

This guide gives an overview of how IGEL Mobile Device Management Essentials (MDM) lets you manage iOS mobile devices.

Configuring MDM in the UMS is detailed in the MDM Setup Guide.

Apple Push Notification Service (APNs)

The UMS and iOS mobile devices communicate with each other via the Apple Push Notification service (APNs).

Also, the IGEL Cloud Gateway (version 1.04.100 or higher) is required to provide a secure communication channel between the UMS and the iOS mobile devices connecting from outside the company network (see the Communication Chart (see page 624)).

The setup procedure can be outlined as follows:

1. Set up an ICG instance and connect it to the UMS, find detailed instructions in the ICG Manual (see page 619).
2. In the UMS, create a certificate-signing request for the Apple Push Certificates portal.
3. Log in with your Apple account to the Apple Push Certificates portal to generate a certificate for the UMS using the certificate-signing request.
4. Using the generated certificate, connect the UMS to the Apple Push Notification Service (APNs).
5. You are now ready start connecting iOS mobile devices to the UMS, this is also referred to as device enrollment.

For a detailed walk-through of these setup steps, see the MDM Setup Guide.

Connecting Devices

The iOS app **IGEL MDM Enrollment** is used to connect mobile devices to the UMS. The app is available free of charge from the app store.

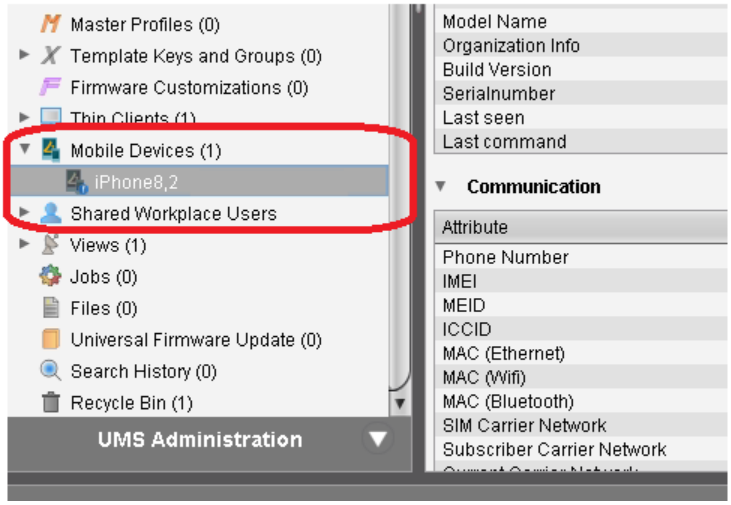
For a detailed description of the device enrollment procedure, see Connecting Mobile Devices to the UMS (see page 643).

Managing Devices

New folder "Mobile Devices" in the UMS structure tree

Mobile devices that have been added to the UMS are listed in the new **Mobile Devices** folder.

Right-clicking on a mobile device listed there will open a context menu with object-specific commands.



New profile type "Mobile Device" — mobile devices are managable via profiles only

The new profile type "Mobile Device" has been introduced, since mobile devices are managable via profiles only. The fact that you must use a profile to manage a mobile device means that, unlike with thin clients, double-clicking a mobile device object in the Mobile Devices folder will not open a configuration dialog; instead, you will have to create a profile and send the profile to the device or several devices.

In the **Profiles** folder of the UMS, mobile-device profiles can be distinguished from other types by the symbol.

- See Creating Mobile Device Profiles (see page 645).
- See Sending Profiles to Mobile Devices (see page 646).
- For general information on profiles, see Profiles.

MDM Manual

Prerequisites

Prerequisites

- Universal Management Suite (UMS) 5.09.100 or higher
- IGEL Cloud Gateway (ICG) 1.04.100 or higher
- Any of the supported mobile devices (see page 623) with the IGEL MDM Enrollment iOS app installed

Supported Mobile Devices

The following iOS versions are supported:

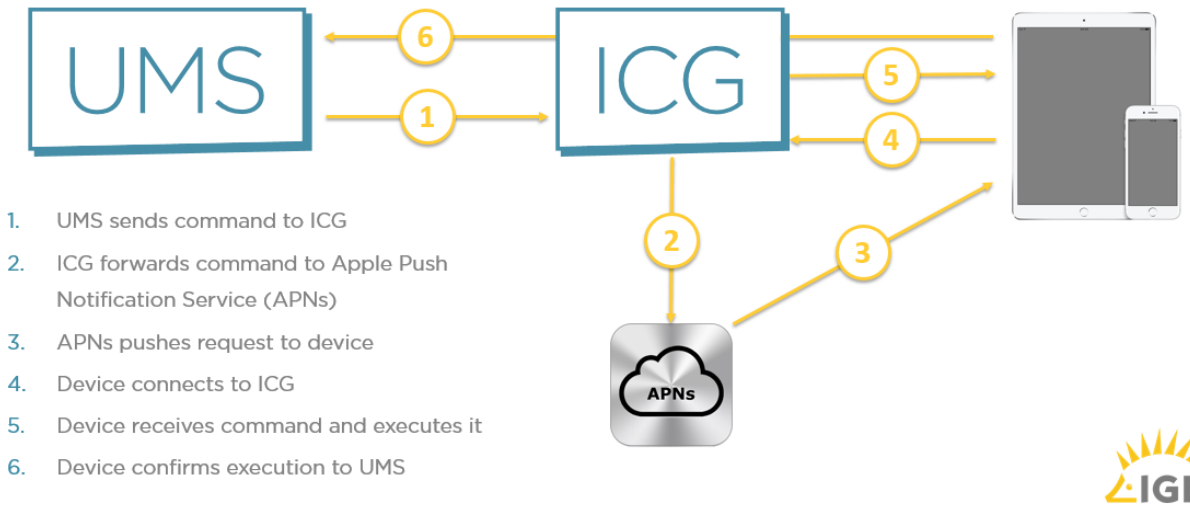
- at least iOS 10.3
- iOS 11
- iOS 12.

The following mobile devices are supported:

Device	Version(s)
Apple iPhone	5s and later
Apple iPad mini	2 and later
Apple iPad Pro	9.7 inch and later
Apple iPaid Air	1 and 2

Communication Chart

The chart belows shows the communication process between the UMS, the ICG, the Apple Push Notification Service and an iOS mobile device.



Supported Features

Some features supported by IGEL MDM are only applicable if the device has been put into **supervised mode** beforehand with Apple's tools.
Please see next section which features require supervised mode.

Mobile Devices

Menu path: **UMS Console > UMS Administration > Global Configuration > Mobile Devices**

This section gives you an overview of the status of the IGEL Could Gateway (ICG) and its connection to the Apple Push Notification service.
Users can scan the QR code with the IGEL MDM App for iOS to enroll their devices. For more information, see Connecting Mobile Devices to the UMS (see page 643).

- **Displayname**: The displayname
- **Host**: The host
- **Port**: The port
- **Apns Status**: Status of the connection to the Apple Push Notification service
- **Firmware available**: Shows if the firmware required for MDM is available
- **Enrollment URL**: The enrollment URL

Possible actions related to the QR code:

- **show**: Show the QR code in a separate window
- **send via email**: Send the QR code via email
- **save as jpg**: Save the QR code as JPG file
- **send as png**: Save the QR code

Apple iOS Devices

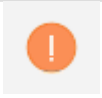
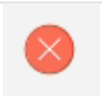
Menu path: **UMS Console > UMS Administration > Global Configuration > Mobile Devices > Apple iOS devices**

In this section, you can set up the required certificate for connecting the UMS to the Apple Push Notification Service. How you set up the certificate to connect the UMS with the Apple Push Notification Service is described in the MDM Setup Guide (see page 641).

You can perform the following actions:

Icon	Description
	Create a new certificate-signing request and save it as a *.csr file
	Open the Apple Push Certificate Portal at https://identity.apple.com in the system browser
	Import the Apple MDM Push Certificate (*.pem file)
	Create and save certificate-signing request for renewal
	Show the certificate details of the Apple MDM Push Certificate
	Cut the certificate
	Delete the certificate

Status information:

Icon	Description
	Certificate successfully set up
	Waiting for certificate upload
	Incomplete / certificate error

You may further specify:

- **Enrollment profile displayname**: Displayname for the enrollment profile
- **Enrollment profile description**: Description of the enrollment profile
- **Adjust UMS-internal name with name on device**

Context Menu

Menu path: **UMS Console > Server [IP] tab > Mobile Devices > [mobile device]**

Right-click a mobile device icon in the UMS console navigation tree to open the context menu for the device.

- **Rename**: Give the device a new name
- **Delete**: Remove device from UMS
- **Copy**: Copy the device
- **Cut**: Cut the device
- **Access control**: Configure device permissions for UMS administrators
- **Clear 'Configuration Change Status' flag:** Resets configuration change flags (blue dot next to the symbols for the thin clients).
- **Send Configuration**: Sends the configuration of the UMS to the highlighted devices (this does not happen automatically!).
- **Refresh device information:** The system information will be refreshed.
- **Refresh security information:** The security information will be refreshed.
- **Device lock**: Locks the screen of the device.
- **Clear passcode**: Clears the existing passcode for the screen locker.
- **Shutdown** (Supervised only)
- **Restart** (Supervised only)
- **Reset to factory defaults:** Resets the device to factory defaults and erases its storage contents.

  Warning

  Resetting the device to factory defaults will erase its storage contents.

- **Logging: Messages**: Opens the **Log Messages** window for messages.
- **Logging: Event Messages**: Opens the **Log Messages** window for event messages.

Mobile Device Profile Settings

Unlike thin clients, mobile devices can be configured only through profiles.

This section explains the settings available in a mobile device profile. They are also explained in the Apple Profile Manager Help.[22]

22 https://help.apple.com/profilemanager/mac/5.3/?lang=en#/

Restrictions

Menu path: **[mobile-device profile] > Restrictions**

> Features marked as **(Supervised Only)** are only manageable if the device has been put into supervised mode.

Functionality

This page allows you to disable or enable various iOS features, very similiar to the **Settings > General > Restrictions** dialog on iOS.

Apps

Enable or disable select iOS apps such as iTunes or Safari. In supervised mode you can also create a whitelist OR a blacklist of apps, using their bundle identifiers, separated by semicolon.

Media

Set your region code and age ratings for movies, TV shows and apps.

Passcode

Menu path: **[Mobile device profile] > Code**

In this area, you can change passcode settings.

- **Require Passcode on Device**: Enforce entering a passcode before using the device. (Default: enabled)
- **Allow Simple Values**: Permits users to use sequential or repeated characters in their passcodes. For example, “3333” or “DEFG”. (Default: enabled)
- **Require Alphanumeric**: Requires that the passcode contain at least one letter or number. (Default: disabled)
- **Minimum Passcode Length**: Specifies the minimum number of characters a passcode can contain.
- **Min Complex Chars**: Specifies the number of non-alphanumeric characters (such as $ and !) the passcode must contain.
- **Maximum Passcode Age:** Requires users to change their passcode at the interval you specify. It can be set to --, or from 1 to 730 days.
- **Auto-Lock**: If the device isn’t used for the period of time you specify, it automatically locks. It can be set to --, or set to lock after 1 to 5 minutes. Enter the passcode to unlock the device.
- **Passcode History**: The device refuses a new passcode if it matches a previously used passcode. You can specify how many previous passcodes are remembered and compared. It can be set to --, or from 1 to 50 passcodes.
- **Grace Period for Device Lock**: Specifies how soon the device can be unlocked again after use, without reprompting again for the passcode.
- **Max Failed Attempts**: The number of failed passcode attempts that can be made before an iOS device is erased or locked.
  If you don’t change this setting, after six failed attempts, the device imposes a time delay before a passcode can be entered again.
  The time delay increases with each failed attempt. After the final failed attempt, all data and settings are securely erased from the iOS device. The device locks after the final attempt.
  The passcode time delay begins after the sixth attempt, so if you set this value to 6 or lower, no time delay is imposed and the device is erased when the attempt limit is exceeded.

Wi-Fi

Menu path: **[mobile-device profile] > Wi-Fi**

Use the [+] icon to add a new Wi-Fi network.

Wifi Session

- **SSID**: Enter the SSID of the wireless network to connect to (must not contain spaces).
- **Hidden Network**: Defines if the network is hidden. (Default: Disabled)
- **Auto join**: Allow the device to automatically join the specified network. When this option is off, the user is asked to allow the connection. (Default: Enabled)
- **CaptiveBypass**: Users won't have an opportunity to join networks that require agreements or other information prior to network access. (Default: Disabled)

Proxy

- **Proxy Type**
  - None
  - Manual: (Enter manually the connection details **Proxy Server**, **Proxy Server Port**, **Proxy Username** and **Proxy Password**)
  - Automatic: (Enter Proxy PacUrl). For Web Proxy Autodiscovery (WPAD) configurations leave the **Proxy Server URL** field empty, and the device will request the `wpad.dat` file using DHCP (via a 252 entry) or DNS (via an A Record with the name WPAD).
- **Proxy Server**: Hostname or IP of the server
- **Proxy Server Port**: Port of the server
- **Proxy Username**: Username of the server
- **Proxy Password**: Password of the server
- **Proxy PacUrl**: The proxy PAC URL
- **Proxy PAC Fallback allowed**: (Default: Disabled)

QoS

- **QoS Marking Policy**: You can restrict QoS marking, disable it, and approve specific apps for audio and video calls. Those apps must be configured to take advantage of QoS on Cisco corporate networks. You install this payload in a configuration profile which allows specific business apps to get priority. The Cisco network looks for these markings and provides the correlated service level. (Default: Disabled)
- **Allow QoS marking** (Default: Enabled)
- **QoS marking for audio/video calls** (Default: Disabled)
- **QoS Whitelisted Apps** (bundle identifiers, separated by semicolons) (Default: Disabled)

Network

- **Choose network type**:

    - standard
    - oldhotspot
    - passpoint
- **Displayed Operator Name**: Enter the name you want displayed for the Passpoint network.
- **Domain Name**: Enter the fully qualified domain name (FQDN) of the Passpoint service provider.
- **Roaming OIs**: HotSpot 2.0 organization identifiers
- **Roaming OIs**: Enter the six-digit hex code corresponding to one of the service provider's Passpoint network.
- **Real Names:** HotSpot 2.0 NAI real names (Default: Disabled)
- **Realm Names**: Enter the known Network Access Identifier (NAI) realm names.
- **MCC/MNCs**: HotSpot 2.0 MCC/MNCs
- **MCC/MNCs**: Enter the six-digit code combining the Mobile Country Code (MCC) and Mobile Network Configurations (MNC)
- **Roaming Enable**: Specify whether to connect to additional Passpoint networks pre-approved by the service provider. (Default: Disabled)

Security

- **Encryption Type**:
    - None
    - WEP
    - WPA
    - WPA2
    - Any: The network requires either WEP, WPA or WPA2 authentication when connecting to the network, but will not connect to non-authenticated networks.
- **Password**: Password for the network

Mail

Menu path: **[mobile-device profile] > Mail**

Use the [+] icon to add a new mail account.

- **Account Description**: Display name for the account
- **Account Type**:
  - EmailTypeIMAP
  - EmailTypePOP
- **Path Prefix**: Path prefix for the IMAP mail server.
- **Account Name**: Username on mail server
- **Email Address:** E-mail address
- **Prevent Move**: Mail messages cannot be moved between mail accounts. (Default: Disabled)
- **DIsable Mail Recents Syncing:** Recently used addresses are not synced across devices. (Default: Disabled)
- **Allow Mail Drop**: Mail is not an option in the share sheet. (Default: Disabled)
- **Prevent App Sheet**: If set to true, this account will not be available for sending mail in third-party applications. (Default: Disabled)

Inbox

Menu path: **[mobile-device profile] > Mail > [session name] > Inbox**

- **Mail Server**: Hostname or IP address
- **Port**: Port number for incoming mail (Default: 993)
- **Username**: The username used to connect to the server for incoming mail
- **Incoming Mail Server Authentication**: The authentication method for the incoming mail server
  Possible values:
  - None
  - Password
  - MD5 Challenge-Response
  - NTLM
  - HTTP MD5 Digest
- **Password**: The password for the incoming mail server authentication
- **Use SSL**: Defines whether incoming mail is received through an SSL-encrypted connection (Default: Enabled)

Outbox

Menu path: **[mobile-device profile] > Mail > [session name] > Outbox**

- **Mail Server**: Hostname or IP address
- **Port**: Port number for outgoing mail (Default: 587)
- **Username**: The username used to connect to the server for outgoing mail
- **Incoming Mail Server Authentication**: The authentication method for the outgoing mail server
  Possible values:
  - None
  - Password
  - MD5 Challenge-Response
  - NTLM
  - HTTP MD5 Digest
- **Password**: The password for the outgoing mail server authentication
- **Outging Password Same as Incoming**: Defines if for SMTP authentication the same password is used as for POP/IMAP authentication. (Default: Disabled)
- **Use SSL**: Defines if mail is sent via an SSL-encrypted connection (Default: Enabled)

Air

Menu path: **[mobile-device profile] > Air**

AirPrint

- **Printer:** Use printers (Default: Disabled)
- **IP Address**: Enter IP addresses of printers, separated by semicolons
- **Resource Path**: Enter the resource paths corresponding to the IP addresses above, separated by semicolons

System

Menu path: **[mobile-device profile] > System > Registry**

In the registry, you can change firmware parameters directly.

> Changes to the registry should be made by experienced users only, because you can easily make misconfigurations.

- **Search Parameter...**: Search for setup parameters in the registry
- **Search criterion**: Criterion for searching. The following can be selected:
  - Parameter name
- **Parameter name**: Any search term
- Logical search restriction:
  - Contains
  - Exact match
  - Use regular expressions
- **Ignore case**
- **Find previous**: Go back if there are a number of hits
- **Find next**: Go forwards if there are a number of hits
  Example: If you want to find the FTP settings for updating the Linux firmware, you can search for the parameter name ftp. The parameter found in the registry structure is highlighted. Click **Find next** until you find your desired parameter:
- **Add instance**: Adds instances. This is possible with parameters which have a percent sign as their last character, e.g. nfymount%. The new instances are numbered consecutively: nfymount1, nfymount2 etc.
- **Delete instance**: Deletes a previously added instance.

MDM How-Tos

MDM Setup Guide

Prerequisites

- UMS 5.09.100 or higher
- ICG 1.04.100 or higher

> You need an **Apple account** (Apple ID and password). If you do not have one, please create an account at https://appleid.apple.com.

This how-to explains the necessary steps to set up IGEL Mobile Device Management Essentials (MDM) in the UMS. Perform the steps in the given order.

Step 1: Import the iOS Firmware Metadata File

Import the iOS firmware metadata into the UMS:

1. Download `IGEL Firmware for iOS <version>.xml`.

> MDM is not further developed by IGEL. Only the profile for enabling the management of devices with iOS 10.3 is available.
> Direct download link: IGEL Firmware for iOS[23].

2. Start the **UMS Console**.
3. In the upper left, click **System** and select **Import ... > Import Firmwares**.
4. In the file chooser dialog, select the `IGEL Firmware for iOS <version>.xml` file.
5. Click **Open**.
   The firmware will be imported. Upon success, a confirmation window will appear.

Step 2: Connect the UMS to the Apple Push Service

(1) Generate a certificate-signing request for the Apple Certificates Portal:

1. Start the **UMS Console**.
2. Go to **UMS Administration > Global configuration > Mobile Devices > Apple iOS devices**.
   You will find the status message set to **Incomplete**.
3. Click the  icon (**Create and Save Certificate Signing Request for MDM Apple Push Certificate**).
   You will be prompted to save a *.csr file, which contains the generated certificate-signing request.
4. Save the *.csr file to a location you can remember.
   When completed, the status message will change to **Waiting for upload of the Apple MDM Push Certificate**.

23 https://publicbuilds.blob.core.windows.net/files/IGEL_UNIVERSAL_MANAGEMENT_SUITE/MDM/IGEL%20Firmware%20for%20iOS%2010.3.11.xml.zip

Now you need to create an Apple MDM Push Certificate and import it, as described in the next two steps (2) and (3).

(2) Generate an Apple Push Certificate in the Apple Push Certificates Portal:

1. Open the Apple Push Certificates Portal at https://identity.apple.com/pushcert/ and log in with your Apple ID and password.
2. Click **Create a Certificate**.
3. Accept the **Terms & Conditions**.
4. Upload the certificate-signing request (*.csr file) which you created in step (1).
5. Download the resulting push certificate (*.pem file) to a location you can remember.

(3) Import the Apple Push Certificate in the UMS Console to connect the ICG with the Apple Push Service.

- Click the  icon (**Import Apple MDM Push Certificate**) to import the MDM Apple Push Certificate into the UMS.
  When the certificate was successfully imported, the status message will change to **Complete - Certificate expires at [date]**.
  Via the ICG, the UMS will try to establish a connection to the Apple Push Service.

  > When the connection between the ICG and the Apple Push Service was successfully established, in the UMS, under **UMS Administration > Global configuration > Mobile Devices**, the **Appns Status** field will be **Connected**.

You are now ready to start connecting mobile devices to the UMS, see Connecting Mobile Devices to the UMS (see page 643).

Connecting Mobile Devices to the UMS

Prerequisites

- UMS 5.09.100 or higher
- Any of the devices listed under Supported Devices (see page 623)
- The IGEL iOS app IGEL MDM Enrollment must be installed on your device.

  > The **IGEL MDM Enrollment** app is available free of charge from the Apple App Store.

  Download on the App Store
- The UMS must be connected to the Apple Push Service, see the MDM Setup Guide (see page 641).

This how-to explains the necessary steps to connect iOS mobile devices to the UMS using the IGEL Mobile Device Enrollment app.

Steps

To connect a mobile device to the UMS, proceed as follows:

1. Switch on your mobile device and start the **IGEL MDM Enrollment** app.
   You will be presented with a screen to choose between **Scan QR-Code** and **Manual Input**:

2. Tap **Scan QR-Code**:
3. With your mobile device's cam, scan the QR code under **UMS Administration > Global Configuration > Mobile Devices**.

   > If for any reason you cannot use your mobile device's cam, please use **Manual Input** and manually enter the connection details available under **UMS Administration > Global Configuration > Mobile Devices**. The required format is `https://[host or IP]:port`

4. Click **Enroll**.
   Your device's default browser (usually Apple Safari) will open a link to automatically download the MDM profile file.

   > When presented an HTTPS error, select **Show details > Visit website**.

5. Accept all warnings and allow installing the enrollment profile ("Remote Management").

   > If you receive the error "Profile Installation Failed", see the troubleshooting article Profile Installation Fails When Connecting Mobile Device to the ICG (see page 648).

6. In the UMS Console, reload the navigation tree.
   Your mobile device is now listed in the **Mobile Devices** folder.

Creating Mobile Device Profiles

This how-to assumes that you have set up IGEL Mobile Device Management Essentials (MDM). If not, see MDM Basic Overview (see page 619).

To create a mobile device profile, proceed as follows:

1. Right-click **Profiles** in the UMS structure tree; from the context menu, choose **New Mobile Device Profile**.
2. Enter a **Profile Name**
3. Enter a **Profile Description**
4. For **Based on**, choose **IGEL Firmware for iOS 10.3.x**
5. Click **OK**.
   The settings window for the profile will open.
6. In the settings window, you can make settings and apply them immediately (send the configuration to mobile devices), or click **Save** and apply settings later.

For a general overview of UMS profiles, see Creating Profiles (see page 282).

Sending Profiles to Mobile Devices

This how-to assumes that you have set up IGEL Mobile Device Management Essentials (MDM). If not, see MDM Basic Overview.

To send a profile to a mobile device, proceed as follows:

1. Assign a profile to a device by dragging and dropping the profile onto the mobile-device object in the **Mobile Devices** tree node.
2. Right-click the device and select **Send Configuration**.

MDM Troubleshooting

Profile Installation Fails When Connecting Mobile Device to the ICG

Issue

You are trying to connect a mobile device to the UMS as described under Connecting Mobile Devices to the UMS (see page 643).

You can download the profile for MDM, but its installation fails.

Solution

This issue occurs because you already installed a profile in the past.

When you try to install a new profile, the old one is not automatically overwritten.

You have to manually delete the old profile.

To do this, on your mobile device, go to **Settings > General > Device Management** and delete the old profile.

UMS Release Notes

Notes for Release 6.10.140

Software:	Version 6.10.140
Release Date:	2022-12-13
Release Notes:	RN-610140-1
Last update:	2022-12-13

Supported Environment 6.10.140

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Microsoft Windows Server 2022	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Ubuntu 22.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows 11	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Microsoft Windows Server 2022	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	

Ubuntu 22.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 12c	(with Cluster Support)
PostgreSQL	9.6 and 10 - 13
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 10 - 13)

See also Devices Supported by IGEL Universal Management Suite (UMS).

New Features 6.10.140

UMS common

- Updated: **Spring Framework** to the latest LTS version

Resolved Issues 6.10.140

Profiles

- Fixed: The profile setting '**OpenVPN - Set Auto**' did not persist after copying or importing a profile, where the setting was enabled.

IGEL Cloud Gateway (ICG)

- Fixed: In some cases, **when using multiple ICGs, the UMS was no longer able to send commands to the devices**, so the **devices** could become **unmanageable**.

Notes for Release 6.10.130

Important Information for Release IGEL UMS 6.10.130
IGEL UMS version **6.10.130** has been **removed** from the IGEL Download Server https://www.igel.com/software-downloads/workspace-edition/.
Reason: In some cases, **when using multiple ICGs, the UMS is no longer able to send commands to the devices, so the devices can become unmanageable**.
Please **update to UMS 6.10.140** to resolve the issue.

Software:	Version 6.10.130
Release Date:	2022-10-05
Release Notes:	RN-610130-1
Last update:	2022-10-05

Supported Environment 6.10.130

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Microsoft Windows Server 2022	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Ubuntu 22.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows 11	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Microsoft Windows Server 2022	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	

Ubuntu 22.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 12c	(with Cluster Support)
PostgreSQL	9.6 and 10 - 13
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostrgreSQL (compatible with PostgreSQL 10 - 13)

See also Geräte, die von der IGEL Universal Management Suite (UMS) unterstützt werden.

New Features 6.10.130

Server, common

- Updated: **Apache Tomcat** from version 8.5.75 to **8.5.82**

Devices

- Added: Two options for the **device settings export**, to either include all **passwords** or replace them with a placeholder. See Export Device Settings in the IGEL UMS.

Resolved Issues 6.10.130

High Availability Feature

- Fixed: UMS HA installation still contained a **Log4j 1.x** reference.

Console, common

- Fixed: **Delete option** in the context menu of management tree items was disabled when **recycle bin** was deactivated.
- Fixed: The **number of deployed licenses** was not shown correctly when devices were **licensed manually**.
- Fixed: **Import** of device settings if it contains **duplicate values**. The duplicates are ignored and a warning message is shown.

UMS, common

- Fixed: Server **performance** dropped if **scanning for devices** ran into an error.

Views

- Fixed: **Error** occurred for views consisting of several device **license criteria** combined with **'AND'** and **'OR'**.

IGEL Cloud Gateway (ICG)

- Fixed: **Primary key violation** occurred while processing connection status information of ICG-managed devices.

Notes for Release 6.10.120

Software:	Version 6.10.120
Release Date:	2022-06-29
Release Notes:	RN-610120-1
Last update:	2022-06-29

Supported Environment 6.10.120

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Microsoft Windows Server 2022	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows 11	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Microsoft Windows Server 2022	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	

Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 12c	(with Cluster Support)
PostgreSQL	9.6 and 10 - 13
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostrgreSQL (compatible with PostgreSQL 10 - 13)

See also Devices Supported by IGEL Universal Management Suite (UMS).

Resolved Issues 6.10.120

Secure Terminal

- Fixed: Secure Terminal was **broken after replacing Log4j with Logback** in UMS 6.10.110

Notes for Release 6.10.110

Software:	Version 6.10.110
Release Date:	2022-05-31
Release Notes:	RN-610110-1
Last update:	2022-05-30

Supported Environment 6.10.110

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Microsoft Windows Server 2022	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows 11	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Microsoft Windows Server 2022	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	

Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 12c	(with Cluster Support)
PostgreSQL	9.6 and 10 - 13
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostrgreSQL (compatible with PostgreSQL 10 - 13)

See also Devices Supported by IGEL Universal Management Suite (UMS).

New Features 6.10.110

Server, common

- Changed: The outdated **logging framework Log4j 1.x** was **replaced with Logback 1.2.11**.

IGEL Management Interface (IMI)

- Added: IMI call to **return all devices in view**.

Notifications

- Added: **Notifications for Rolling and Stable Releases** of Firmware Updates.

Console, administration section

- Added: **Customizable timeout** (**UMS Administration > Global Configuration > Device Network Settings**) for the action to upload device files for the support (**Help > Save device files for support**).

Admin tasks

- Added: Datasource configuration for **MS SQL Server allows setting of performance optimization**.

Resolved Issues 6.10.110

UMS common

- Changed: The processing **performance of AssetInfo notification** from **Devices** was improved.

Devices

- Fixed: **Sorting** of column '**Last Contact**' in device table.

Views

- Fixed: **Result list** was **empty** when a view contained **several device license criteria combined with 'AND'**.

Server, common

- Fixed: **Secure Terminal/Secure shadowing** failed for **devices connected over ICG** when the devices were configured to send **periodic heartbeat signal**.

IGEL Cloud Gateway (ICG)

- Fixed: **ICG Gateways** are **not removed from the UMS** when installed on the same host with different ports.

Jobs

- Fixed: Job's **next scheduled execution** is now set properly when the **start date is set in the future**.

IGEL UMS Web App

Devices

- Fixed: **GUI** was extremely **slow when navigating to "Devices" tab** in the UMS Web App. This fix mainly relates to deep AD-Trees but will improve performance for all customers.

Searches

- Fixed: It was not possible to **sort a search result based on custom device attributes**.

Misc

- Fixed: In rare cases, an **error** could be thrown **when loading firmwares**.

Notes for Release 6.10.100

Software:	Version 6.10.100
Release Date:	2022-03-15
Release Notes:	RN-610100-1
Last update:	2022-03-15

Supported Environment 6.10.100

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Microsoft Windows Server 2022	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows 11	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Microsoft Windows Server 2022	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	

Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 12c	(with Cluster Support)
PostgreSQL	9.6 and 10 - 13
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostrgreSQL (compatible with PostgreSQL 10 - 13)

See also Devices Supported by IGEL Universal Management Suite (UMS).

New Features 6.10.100

UMS, common

- Added: Support of **Amazon AWS Aurora datasources**
- Added: **Admin CLI commands** to start, stop, restart and end update mode of the UMS Server.
- Deprecated: **Deprecated the old Admin CLI option 'restart-server'.** This is now a subcommand of 'server'.
- Updated: **Apache Tomcat** from version 8.5.72 to **8.5.75**
- Updated: **Azul Zulu JRE** from version 8u302 to **8u322**

Administrator Application

- Changed: **Postgres datasources with empty database name** can now be defined

High Availability Feature

- Added: Communication between **UMS Servers in HA environment installed on distributed subnets**.

Custom Device Attributes

- Changed: **Values of device attributes can** also **be set by devices**. It can be configured, whether UMS/UMS Web App/IMI, devices, or both are allowed to change the values (**UMS Administration > Global Configuration > Device Attributes**).

Console, common

- Added: **Information about all available network adapters** of a device (**lx 11.07.100 or higher**) is sent to and displayed in the UMS Console and the UMS Web App. This information can **also be accessed via the IMI**.

IMI, server

- Changed: Added more session information to **login logging of IMI and UMS Web App**

IGEL Cloud Gateway (ICG)

- Changed: Updated bundled **Zulu JRE** from version 8u302 to **8u322**
- Changed: Updated **Spring Boot** to version **2.6.2** (embedded Tomcat version 9.0.56)

UMS Web App

Devices

- Added: Implemented handling of **"Device only" device attributes**. (See "Custom Device Attributes" (see page 672) above)
- Added: New tab for **Network Adapters** information. (See "Console, common" (see page 672) above)

Resolved Issues 6.10.100

UMS, common

- Changed: Updated **Apache Log4j 2** library to version **2.17.1**

Console, common

- Fixed: The **retrieval of all or some ICG log files could be prevented** if one ICG could not be reached while the log files were collected (**Help > Save support information...**)

AD / LDAP integration

- Changed: **Increased** maximum **password length for imported Active Directory users**.

High Availability Feature

- Fixed: **Windows service 'IGELRMGUIServer'** will not be recreated but updated during UMS update installation to preserve service user (service log on account, e.g. required for SQL Server JDBC authentication) and heap size (Xmx).
- Changed: For connections to message broker using SSL only, **TLSv1.2 is allowed**.

Installer (Linux)

- Fixed: UMS installer failed to install **qt5-qtbase dependency on Amazon Linux 2**

IGEL Cloud Gateway (ICG)

- Changed: Removed **unused dependency to log4j** (Version 1.2.17)
- Changed: Removed **unnecessary logging of temporary file transfers**

UMS Web App

Security

- Fixed: Fixed security issue where it was possible to **access and manipulate log messages without proper authorization**.
- Changed: **Log4j** was updated to **2.17.1**
- Changed: **Export of Device Information as CSV** was **hardened against DDE injection**.

Common

- Fixed: Some settings were **only initially cached and never updated**.

Logging

- Fixed: **Commands "Reboot", "Shutdown"** and **"Suspend"** resulted in **misleading log messages**.
- Changed: **Clearing (old) data** is now **possible even if logging itself is disabled**.

Notes for Release 6.09.120

Software:	Version 6.09.120
Release Date:	2021-12-22
Release Notes:	RN-609120-1
Last update:	2021-12-22

The Release Notes for UMS 6.09.120 are available in plain text format: Readme 6.09.120.txt

Notes for Release 6.09.100

Software:	Version 6.09.100
Release Date:	2021-11-15
Release Notes:	RN-609100-1
Last update:	2021-11-15

Supported Environment 6.09.100

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Microsoft Windows Server 2022	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows 11	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Microsoft Windows Server 2022	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	

Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 12c	(with Cluster Support)
PostgreSQL	9.6 and 10 - 13
Apache Derby	10.9 - 10.14

See also Devices Supported by IGEL Universal Management Suite (UMS).

New Features 6.09.100

UMS common

- Added: Support for **Microsoft Windows Server 2022**. See https://docs.microsoft.com/en-us/windows/release-health/windows-server-release-info.
- Added: **Monitoring** endpoint for **requesting the status of UMS Server / ICG**.
- Updated: **Apache Tomcat** from version 8.5.66 to **8.5.72**
- Updated: **Azul Zulu JRE** from version 8u282 to **8u302**

Console, common

- Added: **Microsoft Windows 11** to the supported environment for **UMS Client**.
- Added: **Basic information of used ICG certificates** is now part of the support information (**Help > Save support information...**).

IGEL Cloud Gateway (ICG)

- Added: It is now possible to **add existing ICGs to newly installed UMS** when the messaging is not working.

Administrator application

- Added: **Command-line interface for UMS Administrator** with full feature set (except SQL console)
  Note: The **functionality** of the command line tools '**embackup**', '**installNetworkToken**', and '**ksbackup**' is **completely included in** the new tool '**umsadmin-cli**'. Therefore, these tools will no longer be available in future UMS releases.

UMS Web App

Security

- Added: **Login brute-force protection**.

  A1. **Multiple failed login attempts** will lead to a **temporary ban for the user account**.
  A2. This **includes accounts that do not exist** to prevent probing.
  B1. Inserted **dynamic login delay** (milliseconds) to prevent probing.
  (Response-time could otherwise be an indicator for the (non-)existence of an account.)

Resolved Issues 6.09.100

UMS, common

- Fixed: **No message templates** available for **Postgres** installations.
- Fixed: **Heavy WebDav access** may cause **poor AD login performance** due to authentication checks.
- Fixed: In some circumstances, the **directory's information for Firmware Customizations and Files** in the UMS-Cache could be out of date.
- Changed: Improved **performance of online check**.

Console, common

- Fixed: **Log Message dialog** did not show any results if the '**Selected Objects**' option was left empty (**System > Logging > Log Messages**).

Console, web start

- Fixed: **UMS Console** couldn't be started **via Java Web Start**.

Views

- Changed: Improved **execution of views** with the condition '**device (NOT) IN directory**'.

Console, administration section

- Fixed: **License file registration failed** when UMS Server and UMS Console are not installed on the same machine (**UMS Administration > Global Configuration > Licenses > Device Licenses**).

Permissions

- Changed: **Passwords saved in the database are hashed with SHA-512** for optimal security.

IGEL Cloud Gateway (ICG)

- Fixed: **ICG with display name with more than 200 characters** can no longer be installed.

Server, common

- Fixed: Devices were **displayed offline after** the used **network adapter** had been **changed**.
- Fixed: Internal issue that resulted in **redundant error log-entries of inability to parse asset inventory events**.

High Availability Feature

- Fixed: **Load balancer** on Linux does not show the full OS version.
- Fixed: **Assigned files** of imported Firmware Customizations **weren't synchronized** within the HA network.

Installer (Linux)

- Fixed: **Upgrade from non-HA to HA** installation on Linux servers.

UMS Web App

Configuration

- Changed: **Folders in the configuration tree** now show the **amount of contained profile**s.
- Fixed: Wrong **naming for number of contained profiles** for a profile directory.
- Fixed: Wrong **German translation** for '**Site**'.
- Fixed: Device **icon not aligned** in filter.

Devices

- Changed: **German translations** for detaching objects.
- Changed: The **order of assigned objects** is improved.
- Fixed: **Color** and **text of attachment cards** are incorrect during a drag operation.

Misc

- Changed: **Assign Object icon** now persistent throughout the Web App.
- Changed: **Values** are now **checked before the creation of a new directory**.
- Fixed: **Gaps in the header**.
- Fixed: **Header alignment**.
- Fixed: **Missing icons** in various dropdown components.

Notes for Release 6.08.120

Software:	Version 6.08.120
Release Date:	2021-09-27
Release Notes:	RN-608120-1
Last update:	2021-09-24

Supported Environment 6.08.120

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	

Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 12c	(with Cluster Support)
PostgreSQL	9.6 and 10 - 13
Apache Derby	10.9 - 10.14

See also Devices Supported by IGEL Universal Management Suite (UMS).

Resolved Issues 6.08.120

Security

- Fixed: CRITICAL SECURITY ISSUE
  UMS Web App can be made to **reveal critical information**, including the UMS Superuser password.
  The critical security vulnerability in UMS Web App affects the following IGEL products:
  - **UMS 6.8.x** with UMS Web App installed
  - **UMS 6.7.x** with UMS Web App installed
  - **UMS 6.6.x** with UMS Web App installed
  - **UMS 6.5.x** with UMS Web App installed

  IGEL strongly recommends that all affected users (UMS Web App installed) **update/upgrade to UMS 6.08.120**.
  If you have reasons not to do that, you can do the following:
  1. Make a UMS data backup.
  2. Re-run your current installer and re-install the UMS without the UMS Web App.

Notes for Release 6.08.110

Software:	Version 6.08.110
Release Date:	2021-09-13
Release Notes:	RN-608110-1
Last update:	2021-09-13

Supported Environment 6.08.110

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	

Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 12c	(with Cluster Support)
PostgreSQL	9.6 and 10 - 13
Apache Derby	10.9 - 10.14

See also Devices Supported by IGEL Universal Management Suite (UMS).

New Features 6.08.110

Views

- Added: The text mode in the enhanced expert mode can now **auto-complete** supported operators and recognize unsupported operators as **syntax errors**.

Resolved Issues 6.08.110

Views

- Fixed: **Views that contain a 'is true' or 'is false'** constraint could not be edited in the expert mode.

Console, administration section

- Fixed: It was not possible to edit a **device attribute** without also **changing the internal identifier**.
- Fixed: License file registration failed when UMS Server and UMS Console were not installed on the same machine (**UMS Administration > Global Configuration > Licenses > Device Licenses**).

High Availability Feature

- Fixed: Assigned files of **imported Firmware Customization**s were not synchronized within the HA network.

Notes for Release 6.08.100

Software:	Version 6.08.100
Release Date:	2021-07-15
Release Notes:	RN-608100-1
Last update:	2021-07-15

Supported Environment 6.08.100

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	

Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 12c	(with Cluster Support)
PostgreSQL	9.6 and 10 - 13
Apache Derby	10.9 - 10.14

See also Devices Supported by IGEL Universal Management Suite (UMS).

Known Issues 6.08.100

UMS common

- **CAUTION**: For **Oracle** database installations, **verify the 'open_cursors'** setting **prior to an upgrade**. The **recommended** setting is **3000**. For more information, see Oracle (see page 221).

License Deployment

- **Manual registration** of license files fails if UMS Console and server are **not installed on the same machine**. The following error message is displayed to the user: `“Unable to register the license file. The license is invalid.”`
  Workaround: Start the UMS Console from the same server where the UMS is installed.

New Features 6.08.100

Views

- Added: **Enhanced expert mode** to create and adjust complex views using a comfortable text input field.

Admin tasks

- Added: It is possible to specify a **custom view export name for the administrative tasks** "Export view result via mail" and "Save view results in the file system" (**UMS Administration > Global Configuration > Administrative Tasks)**.

UMS common

- Updated: **Apache Tomcat** from version 8.5.61 to **8.5.66**

UMS Web App

Master Profiles

- Added: Master profile tree
- Added: Master profile list
- Added: Master profile details

Quick Jump

- Added: Quick Jump **from profile** and **master profile to devices**
- Added: Quick Jump **from device to the assigned profiles**

Configuration

- Added: **Profile directory details** in the **Configuration** app
- Added: **Filtering of activated settings** is now possible.

Devices

- Added: **Last Contact** (last time an endpoint successfully communicated with the UMS) is now displayed **in the device properties section**.

Misc

- Changed: **New icon set** has been implemented to improve accessibility.

Resolved Issues 6.08.100

UMS common

- Fixed: **Restore of embedded database** sometimes fails with **database timeout**.
- Fixed: **Delete actions in UMS Console fail** if the used **MS SQL Server** database is set up **in 'contained' mode**.
- Fixed: **Heavy WebDav** access may cause **poor AD login performance** due to authentication checks.

Console, common

- Fixed: **Only** the **UMS superuser** was **allowed to make changes to Access Control** of certain tree nodes.

Devices

- Fixed: Added missing **check for write permission** for certain device actions

Views

- Changed: Small text changes of view/search criterium '**Configuration Changes pending**'

Jobs

- Fixed: **Some jobs were not executed** when the **"retry next boot"** option was selected.

Automatic License Deployment (ALD)

- Changed: **Created device licenses are now containing only one Unit ID** and the **license files are stored in the database** instead of the file system. From now on, **it is no longer possible to create a separate license file backup** since the license files are part of the database.

Console, administration section

- Fixed: **Refresh** was **needed after adding/removing device attributes** in order to see the correct list of attributes.

AD / LDAP integration

- Fixed: Improved **AD logon performance** when the option **'Include all configured AD domains for search and import of AD users / groups'** (**UMS Administration > Global Configuration > Active Directory/LDAP**) is active.
- Fixed: In the dialog '**Administrator accounts**', the action "**Members**" **now search users for the selected group in all configured ADs** when the option **'Include all configured AD domains for search and import of AD users / groups'** (**UMS Administration > Global Configuration > Active Directory/LDAP**) is active.

WebDAV

- Fixed: WebDAV was **no longer accessible after the Web server port** had been **changed**.

IGEL Cloud Gateway (ICG)

- Fixed: **Login to Shared Workplace** failed if the **password** contained **certain special characters or umlauts**.

IMI, server

- Fixed: **Device network name** was **not updated** when the device name was **changed via IMI** and option '**Adjust network name if UMS-internal name has been changed**' (**UMS Administration > Global Configuration > Device Network Settings > Adjust Names of Devices**) was active.

Server, common

- Changed: **Administrative tasks are suspended during database backup task** in order to prevent deadlocks.
- Fixed: **Some UMS features and services** e.g. download of Universal Firmware Updates **didn't work properly after an update** installation for UMS 6.05.120 (or prior) to UMS 6.06.100 or higher was performed or after restoring a backup with schema 6.5 or lower for UMS 6.06.100 or higher.
- Changed: Because of security reasons, the **UMS version information** has been **removed from the '.../info'** page.
- Fixed: The **hostname** was **not editable** in case of Web certificate renewal (**UMS Administration > Global Configuration > Certificate Management > Web**)

High Availability Feature

- Fixed: **Internal version number of UMS Load Balancer** was shown **in the health check**.
- Fixed: **Adding a new process to a HA network** failed if a **network token created** with **UMS 6.05.120 or lower** was used for the installation.

UMS Web App

Configuration

- Added: **Detach assigned objects** is enabled in the **Configuration** app.
- Added: **Quick Assign** is now **available also on 'Enter'** after selecting an assignable object with a keyboard.
- Changed: **Activated Settings Values overwritten by template keys** are now represented as template key icons.

Devices

- Added: If **online check** is activated, GLOBAL_ONLINE_CHECK_INTERVAL is used for device online status update.
- Added: If **online check** is disabled, more components are aware of that setting. Server load is reduced.
- Added: For **Activated Settings** that are **marked as using a template key**, but no template key was set, a warning icon is shown.
- Changed: If **no changes** occurred **in "Edit Custom Properties" dialog**, then the **Save** button is **disabled**. (No more empty change requests)
- Changed: It is now possible to **filter Template Key Relations**.
- Changed: **Template key icons** in **Activated Settings Values** are now **clickable**.
- Changed: "**Editable Properties**" are renamed to **"Custom Properties"**.
- Fixed: The session parameters inside the **Template Key Relation** tab (Profile) will now show the **correct session instance number**.
- Fixed: **Permissions for move and copy device directory** now follow the UMS.
- Fixed: Improved **styling** of **Template Key Relation** table (alternating rows).

Misc

- Changed: **Performance updates** on various sub-systems.
- Changed: Redesigned **"About" dialog**
- Changed: **Quotation marks** for device and directory names and configurations **in logs**.
- Changed: **Quotation marks** for object names **in confirmation dialogs and logging entries**.
- Fixed: Items in **Quick Assign** list were not restricted for **profile rights Assign Device and Assign File**.
- Fixed: Removed **redundant and not translated values** inside the **Logging** app.
- Fixed: **Unused actions and categories** were shown in the **Logging** app.

Notes for Release 6.07.100

Software:	Version 6.07.100
Release Date:	2021-03-29
Release Notes:	RN-607100-1
Last update:	2021-03-29

Supported Environment 6.07.100

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	

Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 12c	(with Cluster Support)
PostgreSQL	9.6 and 10 - 13
Apache Derby	10.9 - 10.14

See also Devices Supported by IGEL Universal Management Suite (UMS).

Removed Support 6.07.100

- PostgreSQL 9.5
- Oracle 11g R2

Added Support 6.07.100

- PostgreSQL 11 - 13

Known Issues 6.07.100

UMS common

- **CAUTION**: For **Oracle** database installations, **verify the 'open_cursors'** setting **prior to an upgrade**. The **recommended** setting is **3000**. For more information, see Oracle (see page 221).

New Features 6.07.100

UMS common

- Added: New feature to enable **devices** to **send heartbeat signals** in regular intervals. See Monitoring Device Health and Searching for Lost Devices.
- Added: Better integration for **Azure & AWS**. See Installing IGEL UMS on Microsoft Azure.
- Updated: Apache **Tomcat** from version 8.5.58 to **8.5.61**
- Updated: **Zulu JRE** from version 8u265 to **8u282**

Asset Inventory Tracker (AIT)

- Added: A (global) **switch to enable** or **disable** the Asset Inventory Tracker (**UMS Administration > Global Configuration > UMS Features**)

AD / LDAP integration

- Added: **Extended** the Active Directory / LDAP-Service **connection test** to give better feedback (**UMS Console > Administration Tree > Global Configuration > Active Directory/LDAP**)
- Added: Option to **resolve AD user group dependency** within multiple domains (**UMS Administration > Global Configuration > Active Directory/LDAP**)

Server, common

- Added: **Active Directory database users for SQL Server Cluster** database type
- Changed: The **Elasticsearch log files** are now also regarded when collecting the log files

High Availability Feature

- Added: Much faster upgrade installation sequence for HA installation. See Updating the Installation of an HA Network.

Views

- Added: New view/search criterion: **Configuration changes pending**. It's now possible to filter for devices which did not get the newest configuration changes.

UMS Web App

- Added: Introduced a **new global permission "Device Bulk Action"**. This permission **only affects the UMS Web App**. Users without this permission cannot perform actions on multiple devices at once.
- Added: **New section** introduced: **Configuration** Management. See Configuration.
    - Added: **Profile tree**
    - Added: Base information for **profiles**: **settings**
    - Added: Base information for **profiles**: **template key relations**
    - Added: Base information for **profiles**: **contained files**
    - Added: Base information for **profiles**: **assigned devices**
    - Added: **QuickAssignment** via profile section
    - Added: Editing of **profile properties** (not settings!)

Resolved Issues 6.07.100

UMS, common

- Fixed: The **size limit of log files** on some **Windows** installation **did not affect the log files**.
- Fixed: **Deadlock** occurred when runtime information of devices was updated d**uring copying database to Embedded DB**.
- Fixed: **Some log files** did get **very big** and were **not truncated**.
- Fixed: **Upload of Universal Firmware Updates via FTPS** was not possible because of a certificate error.

UMS Web App

- Fixed: The **search** does no longer **crash handling a massive number of devices**.
- Fixed: A **bug** inside the **License Check Service** (UMS Web App) for **Windows10 devices** resulted in **an error that stopped the index** service.
- Fixed: The **renaming of Windows 10 devices** caused an error inside the Web Application.
- Fixed: **Logging** section inside the UMS Web App was **hidden from AD Group Users and Superusers**.
- Fixed: **New log messages** could sometimes **not** be **deleted** if the **days-value was set to zero**.

Console, common

- Fixed: In rare scenarios, the **last tree selection** in UMS Console **could not be restored**, and as a result the **UMS Console could not start**.

Jobs

- Fixed: **Start date field** is **sometimes not filled** when a **new scheduled job** is created.

Automatic License Deployment (ALD)

- Fixed: Configuration **changes for Automatic License Deployment** were **not synchronized within HA** network.

Configuration Dialog

- Fixed: The UMS Console configuration dialog **didn't show correct settings for parameters configured parallel by FWCs and indirectly assigned master profiles**. The settings of **Shared Workplace users** were **also affected**.

Admin Tasks

- Changed: "**Delete administrative execution data**" admin task: deleted executions are now saved to multiple CSV files for large execution numbers.

AD / LDAP integration

- Fixed: In an HA environment, **LDAPS certificates** are **now loaded automatically to all HA servers**.
- Fixed: **Change Password** for **Shared Workplace users** with **more than one domain controller** didn't work.

IGEL Cloud Gateway (ICG)

- Fixed: It is now **forbidden to import end-certificates without** a **subject alternative name** (**UMS Administration > UMS Network > IGEL Cloud Gateway > Install new IGEL Cloud Gateway** and **Update Keystore**)
- Fixed: **Wildcard certificate host name validation** in ICG update keystore dialog (**UMS Administration > UMS Network > IGEL Cloud Gateway**)
- Fixed: Feature **'Send ICG Configuration'** (**Device > [context menu] > ICG Configuration > Send ICG Configuration**) always sends the internal ICG Hostname and Port.

Server, common

- Fixed: Some **global configuration settings changes** were **not synchronized within the HA** network.
- Fixed: **Automatic License Deployment** mechanism was **improved** in order **to prevent deadlocks**.
- Fixed: **Registering device** in UMS from the device itself required the user to have **'Move' permission instead of** the correct **'Scan' permission**.

High Availability Feature

- Fixed: **Files of a WebDAV subdirectory** were **not synchronized within a HA** environment.

Views

- Fixed: **Devices** where **"Boot Time" and "Last contact" are empty** are now **also considered in views and searches** if the criterion is relative and the filter is "Date more than X days ago".

Notifications

- Changed: Improved notification **messages for expiring licenses, packs, and certificates**

Administrator application

- Fixed: **DB update** failed in case of a **specific certificate configuration**
- Fixed: After **changing** the **password of the database user**, the application had to be restarted to change the settings of the UMS superuser.

Installer (Windows)

- Fixed: **RMClient.exe** and **RMAdmin.exe** did not have a digital signature.
- Fixed: **Changed ports** (in **UMS Administrator > Settings**) are now **reflected in the firewall exclusions**.

Notes for Release 6.06.110

Software:	Version 6.06.110
Release Date:	2021-01-25
Release Notes:	RN-606110-1
Last update:	2021-01-25

Supported Environment 6.06.110

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	

Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.5 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

See also Devices Supported by IGEL Universal Management Suite (UMS).

Resolved Issues 6.06.110

UMS Web App

- Fixed: The **search** does no longer **crash handling a massive number of devices**.
- Fixed: A bug inside the **Licence Check Service (UMS Web App) for Windows 10 devices** resulted in an error that **stopped the index service**.
- Fixed: The r**enaming of Windows 10 devices** threw an error inside the Web Application.
- Fixed: **Logging section** inside the UMS WebApp was **hidden from AD Group users** and **superusers**.
- Fixed: The **device online check** was incorrect if the user had **insufficient permissions for the corresponding Cloud Gateway**.
- Fixed: New **log messages** could sometimes **not** be **deleted** if the **days value** was **set to zero**.

Views

- Fixed: Possible errors in **views with license criterion** combination.

UMS common

- Fixed: The **size limit of log files** on some Windows installation did not affect the log files.
- Fixed: **Deadlock** occurred when runtime information of devices was updated during **copying database to Embedded DB**.
- Fixed: Some log files get **very big** and are **not truncated**.

Universal Firmware Update

- Fixed: Universal Firmware Updates are **no longer deleted from UMS WebDAV** if the protocol is **changed from HTTP(S) (UMS WebDAV) to another protocol**.

AD / LDAP integration

- Fixed: **Shared workplace login** was **not possible** if the user had **no settings assigned**.
- Added: Extended the **Active Directory / LDAP service connection test** to give **better feedback**. (**UMS Console -> Administration Tree -> Global Configuration -> Active Directory/LDAP**)

IGEL Cloud Gateway (ICG)

- Fixed: **Wildcard certificates** were **not selectable in the ICG Update KeyStore** dialog.

Server, common

- Fixed: **Automatic license deployment** mechanism was **improved** to **prevent deadlocks**.

High Availability Feature

- Added: **Upgrade installation sequence** for HA installations with **big databases**.

Default Directory Rules

- Fixed: **Default Directory Rules with an IGEL Cloud Gateway criterion** could, if applied while registering the device, provide wrong results.

Notes for Release 6.06.100

Software:	Version 6.06.100
Release Date:	2020-11-16
Release Notes:	RN-606100-1
Last update:	2020-11-16

Supported Environment 6.06.100

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	

Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.5 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

See also Devices Supported by IGEL Universal Management Suite (UMS).

New Features 6.06.100

UMS, common

- Added: Management for the **Web Certificate**. This certificate is used for transferring files to the devices, all WebDAV actions, inter-server communication, the IMI, and the UMS Web App. **Own certificates** can be created and managed, as well as **third-party certificate**s, including those from **public CAs**. For details, see Web.
- Added: Ability to **exchange the IGEL Cloud Gateway root certificate** (IGEL Cloud Gateway version 2.02.100 or later) via the '**Update Keystore**' dialog (**UMS Administration > UMS Network > IGEL Cloud Gateway**).
  The dialog now contains an **extra page** to give the **possibility to create and automatically navigate to views** showing the affected devices.

  > **Warning**
  >
  > **For all UMS installations with a legacy ICG certificate**: After updating devices to IGEL OS 11.04.100 and higher, the devices will no longer be manageable because the new firmware does not accept the legacy ICG certificate anymore. See Device Does Not Connect to ICG after Update to IGEL OS 11.04 or Higher.

- Added: **New device commands** were added to **define the device ICG configuration remotely** from the UMS (devices with IGEL OS version 11.04.240 and 11.05.100 or higher). For details, see Moving an Endpoint Device to an ICG.
- Added: New column **"Send-by" in events view** with filter option (**UMS Console > UMS Administration > UMS Network > Events >** e.g. **Today**)
- Added: The **permission** to use the **UMS HA Health Check** feature can be set under **System > Administrator accounts**.
- Updated: **Apache Tomcat** from version 8.5.56 to **8.5.58**
- Updated: **Bundled Zulu JRE** from version 8u252 to **8u265**

UMS Web App

- Changed: **UMS Web App login** is **filled with the current UMS Console user** when **opening** it via the **toolbar link**.
- Added: Support for several **new commands** (Send settings to device, Receive settings from device, Reset to factory defaults, Update, Update on shutdown, Refresh system information, Refresh license information)
- Added: **Device commands** can be executed **on directory level**.
- Added: **Support** of custom **device attributes**
- Added: **Presentation o**f all **assigned objects** (profiles, master profiles, files, firmware customizations, template keys, value groups, and Universal Firmware Updates) of a device or a device directory
- Added: **Possibility to assign or detach objects** to or from a device or a device directory
- Added: **Responsive design** (min. supported width: **768 px**)

Unified Logging

- Added: New application to **log all user events in the UMS Web App** (only if feature is activated in **UMS Console > UMS Administration > Global Configuration > Logging**)
- Added: New page in the **UMS Web App** to **search and filter all log events**

Template Keys and Groups

- Added: **Template key option for Citrix StoreFront setup parameter**: server location settings, application autostart, quick start and display filter settings

Views

- Added: New **operators "not beneath"** and **"not in**" for the directory criterion
- Added: New **criterion "Indirect Profile Assignment"** and **renamed** existing "**Profile Assignment**" criterion to "**Direct Profile Assignment**"
- Added: New **criterion** "**Feature**"
- Added: New **criterion** "**Has ICG Certificate with SHA1 fingerprint**"

Universal Firmware Update

- Added: Option to **synchronize** downloaded **Universal Firmware Updates** in all UMS **WebDAV directories in HA** networks (**UMS Administration > Global Configuration > Universal Firmware Update**)

Asset Inventory Tracker (AIT)

- Added: **Devices with** a '**Starter License**' are **licensed for the Asset Inventory Tracker** feature in the UMS.

Installer (Windows)

- Added: **Firewall ports preselection** depending on installation type

Default Directory Rules

- Added: New **operators "not beneath"** and **"not in"** for the directory criterion
- Added: New **criterion "Indirect Profile Assignment"** and **renamed** existing "**Profile Assignment**" criterion to "**Direct Profile Assignment**"
- Added: New **criterion "Feature"**

Resolved Issues 6.06.100

UMS, common

- Changed: Improved **third party license information dialog** (**UMS Console > Help > Third party licenses**)
- Changed: Improved **device communication check** for manipulated commands
- Fixed: **Config change flag** was not set for **file** and **firmware update assignments**.
- Fixed: **Config change flag** was often not set on object in the **device's assigned/indirect assigned objects** table.
- Fixed: Sometimes, **template values** were **missing** in template groups if both were **restored from the recycle bin** at the same time.
- Fixed: In rare cases, it could happen that some **administrator accounts**, except the UMS superuser, were **not editable**.

UMS Web App

- Fixed: **Devices** were **not displayed** on a screen with **1200 px** resolution
- Fixed: **'Runtime since last Boot'** and **'Total Operating Time'** are presented in a human-readable format (Device > System information).
- Fixed: The **Elastic Search service stopped** due to an error on certain machines

Console, common

- Fixed: **"Check template definition"** can flood the server if activated in parallel
- Changed: **SQL Console output as HTML file** now always with white background and black text color
- Fixed: Issues with the **filename extension** of the saved result files from SQL Console (**UMS Console > Misc > SQL Console > Save Result**)

Template Keys and Groups

- Fixed: Template keys and groups **could not be changed** under certain conditions (**Oracle** database **only**)

Universal Firmware Update

- Fixed: In rare instances, the **firmware update server** was **overwritten by old settings**.

Configuration Dialog

- Fixed: After editing the page permission pages in a configuration dialog/profile, all **other profiles/ TC configurations showed not their own but the previous configuration**.
- Fixed: Sometimes, it was not possible to **remove all page permissions in a configuration dialog** or **profile**.

Console, administration section

- Changed: **Events views** are now **refreshed automatically** (**UMS Administration > UMS Network > Events**)
- Fixed: The **'Generate a new key pair' dialog** inside the **Device Communication** section could be **finished successfully only by the UMS superuser** (**UMS Administration > Global Configuration > Certificate Management > Device Communication**).

- Fixed: Added missing **ICG certificate permission check** for **Remote ICG install** and **ICG Update Keystore** dialog (**UMS Administration > UMS Network > IGEL Cloud Gateway**)

Admin Tasks

- Fixed: **Renamed views** were shown with **old name** in admin task configuration (delete devices)
- Fixed: **Deleted views / views moved to the bin** are no longer present in admin task configuration (delete devices)

AD / LDAP integration

- Fixed: **In HA environments** and for **multiple domains**, AD certificates were **not loaded** sometimes.

Firmware

- Changed: Improved the **GUI workflow** of firmware import / registration (**UMS Console > System > Import > Import Firmwares**)

WebDAV

- Removed: **Tomcat version** in directory listing
- Changed: Improved **security for WebDAV communication** between UMS components

SSH

- Fixed: Reconnecting a failed **secure terminal session over ICG** failed

High Availability Feature

- Fixed: Upgraded **HA messaging** to the **newest version of ActiveMQ** to resolve security issues

Installer (Windows)

- Fixed: "**install.log" file** was **not created** if only UMS Console was installed.
- Fixed: **Silent installation** with **"Console only" selection** always installed the UMS Web App.
- Fixed: Installer **offered** automatic **embedded database backup** after the previous uninstallation.
- Fixed: **Deselecting** the **UMS Web App** in the Windows installer **also deselected "Standard UMS" server**, including subcomponents.
- Fixed: The **UMS Web App** will **no longer** be **preselected on "Console only"** update installation (Windows installer).
- Fixed: **Previous selection of the UMS Web App** was not taken into account during the **update installation**.
- Fixed: The **UMS Web App** was **re-selected** upon selection of standard or HA server component.

Installer (Linux)

- Fixed: **"install.log" file** was **not created** if only UMS Console was installed.
- Changed: **Replaced SysVinit** scripts **with systemd** unit files for UMS Server, Load Balancer, and Watchdog during Update to 6.06.100 (Linux only)
- Fixed: **Database passwords with special characters** were misformatted during database setup, leading to password mismatch when used in UMS Console login (Linux only)
- Changed: **Improved support for special characters** (e.g. umlauts) in all input dialogs in Linux installer
- Fixed: The **UMS Web App did not start on Ubuntu 20.04** due to a missing library in Tomcat configuration

Notifications

- Fixed: When **all licenses of a pack are used up**, a warning notification is shown, not an error notification.
- Changed: Improved **notification classification and management**
- Changed: Improved **notification** messages for **expiring licenses, packs, and certificates**

UI / Look&Feel

- Changed: **Button order for Access Control** dialog is now: **Apply, OK, Cancel**.

Default Directory Rules

- Fixed: **Rules with a "Device License" criterion** did not generate the correct results.

Known Issues 6.06.100

UMS Web App

- **UMS superuser** does not have the permission to access the **Logging** application.

Notes for Release 6.05.110

Software:	Version 6.05.110
Release Date:	2020-10-08
Release Notes:	RN-605110-1
Last update:	2020-10-07

Supported Environment 6.05.110

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	

Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.5 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

See also Devices Supported by IGEL Universal Management Suite (UMS).

Resolved Issues 6.05.110

UMS, common

- Fixed: **Plain messages** (sent to the device) are **not visible**. (**UMS Console > Global Configuration > Messages to Devices**)

UMS Web App

- Fixed: **Shadowing** not working with **Internet Explorer**. (**UMS Web App > Device > Shadowing**)

Devices

- Fixed: Under rare circumstances, **manual license deployment** did not work **via Java Web Start**. (**Device context menu > License manually...**)

AD / LDAP integration

- Fixed: If **multiple Active Directories with LDAP Service** configuration were used, only one of the domains was working correctly. (**UMS Console > Global Configuration > Active Directory / LDAP**)

Server, common

- Fixed: Having **multiple device certificates** could result in a **5 seconds delay for all commands**. (**UMS Console > Global Configuration > Certificate Management**)

Administrator application

- Fixed: **Database ports** for **SQL Server AD** connections are not editable. (**UMS Administrator > Datasource**)

Notifications

- Fixed: When **all licenses of a pack are in use**, a **warning notification** will be shown instead of an error notification. (**UMS Console > Help > Notifications**)
- Changed: Improved notification messages for **expiring licenses, packs,** and **certificates**. (**UMS Console > Help > Notifications**)
- Changed: **Notification classification and management** were improved. (**UMS Console > Help > Notifications**)

Notes for Release 6.05.100

Software:	Version 6.05.100
Release Date:	2020-07-15
Release Notes:	RN-605100-1
Last update:	2020-07-15

Supported Environment 6.05.100

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.5 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

See also Devices Supported by IGEL Universal Management Suite (UMS).

Removed Support 6.05.100

UMS Server

- Microsoft Windows Server 2008 (64 bit and with SP2) -> EOL 14.01.2020
- Microsoft Windows Server 2008 R2 (64 bit and with SP1) -> EOL 14.01.2020

UMS Client

- Microsoft Windows Server 2008 (64 bit and with SP2) -> EOL 14.01.2020
- Microsoft Windows Server 2008 R2 (64 bit and with SP1) -> EOL 14.01.2020
- Microsoft Windows 7 (64 bit and with SP1) -> EOL 14.01.2020

Backend database (DBMS)

- PostgreSQL 9.4 -> EOL Feb 2020

Added Support 6.05.100

UMS Server

- Amazon Linux 2
- Ubuntu 20.04 (64 bit)

UMS Client

- Amazon Linux 2
- Ubuntu 20.04 (64 bit)

Known Issues 6.05.100

UMS Web App

- **Shadowing** is not working with **Internet Explorer**.

New Features 6.05.100

UMS, common

- Added: Support of **Active Directory authentication for MS SQL Server** database.
- Added: New UMS superuser for initial UMS setup. This '**UMS superuser**' is automatically **created during installation** and receives **the same username and password as the database user**.
- **DB user has no longer the rights for** accessing **UMS**, **UMS Web App**, **IMI**; UMS superuser has to be used instead. The **UMS superuser** can be **configured with IGEL UMS Administrator** (Settings).
- Updated: **Apache Tomcat** from version 8.5.50 to **8.5.56**.
- Updated: **Java** from version 8u242 to **8u252**.

UMS Web App

- Added: **Web-based user interface** for managing IGEL OS endpoints (**early feature set**)
  - Managing device tree
  - See device details (System information, License information, User login history)
  - Sending power control commands (Reboot, Shutdown, Suspend, Wakeup)
  - Shadow devices
  - Powerful search
  - Network and server overview

See https://kb.igel.com/ums/webapp/en for more details.

Console, common

- Added: **Toolbar** in the UMS Console provides **the link for the UMS Web App**.

Console, administration section

- Changed: **The '-' sign is now optional and editable** in the prefix of the network name (**UMS Administration > Global Configuration > Device Network Settings > Naming Convention**). Prefixes that generate a non-standard network name are not allowed if **Adjust Names of Devices > Adjust network name if UMS-internal name has been changed** is selected.

IGEL Cloud Gateway (ICG)

- Added: It is now possible to run **ICG on port 443** (ICG 2.02.100 and higher).
- Added: A **limit for possible device connections** can be defined for an ICG; ICG with version 2.02.100 or higher is required (**UMS Administration > UMS Network > IGEL Cloud Gateway > Edit Connection Limit**)

High Availability Feature

- Added: Tool to check the status of an HA environment (**Help > UMS HA Health Check**)

Installer (Windows)

- Added: New Setup Page to configure **Firewall port exclusions** (only **incoming connections**)
- Added: New **option to select the UMS Web App** component for installation
- Changed: Installer shows information and a weblink for the UMS Web App if it is selected for installation.

Resolved Issues 6.05.100

UMS, common

- Removed: **Command Devices > Other commands > Delete file from device**.
- Changed: **Import** of keystore files **supports** also **JKS keystores** (**UMS Administration > Global Configuration > Certificate Management**).
- Changed: **Certificate chains** could be imported although they are not supported. An import is now prevented (**UMS Administration > Global Configuration > Certificate Management**).
- Fixed: The **user manual** couldn't be opened with the **UMS internal PDF viewer** (**Help > User Manual (offline)**)
- Added: Option for **choosing the PDF viewer** used for the offline manual (**Misc > Settings > General**)

Console, common

- Fixed: **Universal Firmware Update** assignments of devices were not visible in some cases.
- Fixed: Some **scrollbars**, mostly horizontal ones, were extremely slow.
- Fixed: Missing **German translations** in request chart dialog of a selected IGEL Cloud Gateway (**Show History**)
- Fixed: **Rich Message Editor** had wrong background color in **Information/Help** tab
- Fixed: **Save device files for support** (**Help** menu) and **Export Device Settings** (**System > Export...**) dialogs opened very slowly when no device was selected and therefore all devices were loaded.
- Fixed: In rare circumstances, the **device specific command** list was not complete.
- Changed: **Online check interval** (**Misc > Settings > Online check**) has a valid range between 100 ms and 1 hour. For existing installations, values outside this range will be adjusted to the closest valid value.
- Changed: Modified **permissions**. A '**Deny**' **can't be overwritten by** an '**Allow**', see https://kb.igel.com/ums/no-permissions-after-ums-update

Devices

- Fixed: **License model information** was not updated on up-/downgrade, affecting legacy licenses for ICG, HA, and AIT. Information is **now updated on each boot**.
- Changed: **ICG administrated devices without valid IGEL Enterprise Management Pack** license are now shown with the 'device isn't licensed' icon.

Firmware Customization

- Fixed: Some **exported firmware customizations** could not be imported if they were created with **Oracle Database**.

Profiles

- Fixed: Error occurred when executing '**Take over settings from...**' for devices.

Views

- Fixed: **Update time of views and searches** was not displayed in a localized format.
- Fixed: Error occurred when **a view with a relative date criterion** was created and **a value of 0 days** was specified.
- Changed: '**Device license**' criterion now contains the **possibility to search for all license types**.
- Changed: **Special characters** in **MAC** address search are **ignored**.

Jobs

- Fixed: A **missing library** could lead to failing jobs on **headless installations**.
- Fixed: Jobs **could not be edited/selected** (The error message was '**Error Unable to load details for the tree nodes. Original error message: null**').

Automatic License Deployment (ALD)

- Fixed: Devices **don't receive** a **renewal license automatically** if the renewed subscription pack is assigned to the UMS Licensing ID and the pack has no ALD Token.

Universal Firmware Update

- Fixed: The **check for** available **firmware updates** does no longer fail if some of the **firmware properties files** are invalid.
- Fixed: **User name could be edited** in the settings of Universal Firmware Updates for special system users.

Searches

- Fixed: User was not told to do a **necessary restart of the UMS Console** if certain configurations changed.
- Fixed: **Search History** used **lifetime settings of views** instead of its own lifetime settings.

Admin tasks

- Changed: Exported **views are split into multiple files** if the file size exceeds 25 MB. This **affects** the administrative tasks '**Save view results in the file system**' and '**Export view result via mail**' (**UMS Administration > Global Configuration > Administrative Tasks**) and the context menu action '**Send view result as mail**' of views.
- Added: **Context menu** action '**Save as...**' offers now the option to **save views or searches as ZIP** file.

VNC

- Fixed: **No confirmation dialog** was displayed if **multiple VNC session tabs** were about to be closed.

IGEL Cloud Gateway (ICG)

- Fixed: **Shadowing over ICG** failed if a **proxy** server was configured.
- Fixed: Selection of a configured IGEL Cloud Gateway took very long when it was not reachable (**UMS Administration > UMS Network > IGEL Cloud Gateway**)
- Fixed: **Shadowing/Secure terminal over ICG** didn't regard **proxy** configuration.
- Fixed: ICG was **displayed online** when it was running, but the **websocket** connection **wasn't established** yet.
- Fixed: **Job** option '**Retry next boot**' was **ignored** if the device is connected via ICG (requires firmware LX 11.03.500 or newer).
- Fixed: Not all **HA Servers** were connected to a newly registered ICG.
- Changed: **Hostname/IP** text field is now **disabled** if '**CA Certificate**' is selected as a certificate type (**UMS Administration > Global Configuration > Cloud Gateway Options > Create signed certificate**).
- Changed: Information about the **last contact** of an IGEL Cloud Gateway is shown in **UMS Administration > UMS Network > IGEL Cloud Gateway > Gateway details**.

Asset Inventory Tracker (AIT)

- Changed: Improved the **loading** of Asset Information.

Administrator application

- Changed: Reduced the list of **available cipher suites** for **GUI server port** (default: 8443)(**UMS Administrator > Settings > Cipher (Server-side) > Configure Ciphers**).
- Fixed: **Shortcut** for IGEL **UMS Administrator** didn't work after the update of UMS installation.

Database schema

- Fixed: **No upgrade** possible if the **MS SQL Server** database has a **schema name** with **dashes**.

High Availability Feature

- Fixed: **Special characters '.' and '-' in database user name** caused problems during HA update.
- Fixed: In some cases, **database configuration** was **not synchronized within the HA** network depending on the available UMS Servers.
- Fixed: **Deletions of files in WebDAV folder** were not synchronized in the UMS HA network.
- Changed: **Changes** referring to the **configured certificates** are now **automatically synchronized** within the HA network and **no longer require a restart** of the **IGEL RMGUIServer** (**UMS Administration > Global Configuration > Certificate Management**).

Installer (Linux)

- Fixed: On some dialogs, the **installation couldn't** be **aborted** with [**ESC**] key.

Notifications

- Added: When the available **amount of licenses of a License Pack** is **below the limit** or when it **exceeds the total amount**, a notification is shown.

Notes for Release 6.04.120

Software:	Version 6.04.120
Release Date:	2020-05-06
Release Notes:	RN-604120-1
Last update:	2020-05-06

Supported Environment 6.04.120

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)

Microsoft SQL Server 2019	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.5 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

See also Devices Supported by IGEL Universal Management Suite (UMS).

Removed Support 6.04.120

UMS Server

- Microsoft Windows Server 2008 (64 bit and with SP2) -> EOL 14.01.2020
- Microsoft Windows Server 2008 R2 (64 bit and with SP1) -> EOL 14.01.2020

UMS Client

- Microsoft Windows Server 2008 (64 bit and with SP2) -> EOL 14.01.2020
- Microsoft Windows Server 2008 R2 (64 bit and with SP1) -> EOL 14.01.2020
- Microsoft Windows 7 (64 bit and with SP1) -> EOL 14.01.2020

Backend database (DBMS)

- PostgreSQL 9.4 -> EOL Feb 2020

New Features 6.04.120

- Support of **OSCW** (IGEL OS Creator for Windows)

Resolved Issues 6.04.120

Console, common

- Fixed: **Universal Firmware Update assignments** of devices were **not visible** in some cases.
- Fixed: In rare circumstances, the d**evice-specific command list** was **not complete**.

IGEL Cloud Gateway (ICG)

- Fixed: **Shadowing/SecureTeminal via ICG** always **used the internal ICG address and port** instead of the external address and port (if available).

Notes for Release 6.04.110

Software:	Version 6.04.110
Release Date:	2020-03-12
Release Notes:	RN-604110-1
Last update:	2020-03-12

Supported Environment 6.04.110

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	with SP1
Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

See also Devices Supported by IGEL Universal Management Suite (UMS).

Resolved Issues 6.04.110

Jobs

- Fixed: **Jobs could not be edited/selected**. (Error Message was "`Error Unable to load details for the tree nodes. Original error message: null`")
- Fixed: A **missing library** could lead to **failing jobs on headless installations**.

Automatic License Deployment (ALD)

- Fixed: **Devices did not receive a renewal license** automatically if the renewed subscription pack was assigned to the UMS Licensing ID and the pack had no ALD Token.

Universal Firmware Update

- Fixed: The check for available firmware updates failed with a null pointer message if one of the downloaded firmware properties was invalid.

Searches

- Fixed: **Search History used lifetime settings of views** instead of its own lifetime settings.

Database schema

- Fixed: The **UMS could not be updated** if the used **schema name** contained **dashes**. (Only for Microsoft SQL Server databases)

Notes for Release 6.04.100

Software:	Version 6.04.100
Release Date:	2020-02-17
Release Notes:	RN-604100-1
Last update:	2020-02-17

Supported Environment 6.04.100

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	with SP1
Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

See also Devices Supported by IGEL Universal Management Suite (UMS).

New Features 6.04.100

UMS, common

- Added: **Shared Workspace** can be deactivated.
- Added: Support for **Secure Terminal via IGEL Cloud Gateway** (ICG 2.01.100 or higher and IGEL OS 11.02.100 or higher are required).
- Added: **Installer** and **UMS Administrator** perform **database version check** when a database is selected.
- Changed: It is possible to **log in to the UMS Server** via the UMS Console i**f the UMS Server is in HA update mode**.
- Added: '**Manual Licenses Dialog**' – Table with licensable devices shows the **list of licensing pack IDs** in the comment if the information is available in the UMS.
- Updated: Apache **Tomcat** from version 8.5.45 to **8.5.50**.
- Updated: **Java** from version 8u222 to **8u242**.

Universal Customization Builder (UCB)

- Added: **Universal Customization Builder** (for Windows) is now **available for free** (No license required).
- Removed: Obsolete **Linux part of Customization Builder**.

Jobs

- Added: **New Job** command '**Send Message**' added.

Universal Firmware Update

- Added: The UMS Server supports **FTP passive mode for Universal Firmware Upload**.
- Added: **Check for free disk space** on the file system **before downloading firmware updates**.

Console, administration section

- Added: Show **UMS Licensing ID fingerprint** in the **UMS Console** (**UMS Administration > Global Configuration > Licenses > UMS Licensing ID**).
- Changed: Option to enable **Master Profiles**, **Template Profiles** and **Recycle Bin moved to** new node **UMS Features** (**UMS Administration > Global Configuration > UMS Features**).
- Changed: It is now possible to choose **a specific port for the online check (UMS Administration > Server Network Settings > Online Check Parameters > Specify online check port (UDP)**).

Administrator application

- Added: Show **UMS Licensing ID fingerprint** in the **UMS Administrator** (Administrator application > **UMS Licensing ID Backup**).
- Added: **Multiselect** option **for cipher selection** (UMS Administrator > **Settings > Cipher > Configure Ciphers**).
- Added: **Confirmation dialog** after the database password change.

Notifications

- Added: Notifications for **expiring** and **expired certificates** (**Help > Notifications**).
- Added: Notifications for **expiring** and **expired packs** (**Help > Notifications**).
- Added: Option to **show archived notifications (Help > Notification**).
- Added: Option to **restore archived notifications**.
- Changed: Replaced the **"Do not show again" checkbox** for multiple notification selection with **a dropdown action selector** in the Notification dialog (**Help > Notifications**).
- Changed: **Notifications are automatically restored from the archive** when the Info Type is updated to a higher level (from warning to error).

Devices

- Added: **Device file location can now be edited** before sending a file to a device (Device context menu **> Other commands > 'File UMS > Device'**)

Views

- Added: If '**Send view result as mail**' ('View' context menu) fails, **an error message** is **displayed in the 'Messages'** area.
- Added: It is now **possible to send view results as mail** even **if the result is not loaded** in the detail view.

VNC

- Added: **Secure Terminal confirmation dialog** shows whether the terminal feature enabled status for each device.

IGEL Cloud Gateway (ICG)

- Added: The **Events table in the UMS Administration** view is always visible in the management tree. **ICG events will be logged in the table** (**UMS Administration > UMS Network > Events**)

Installer (Windows)

- Updated: **Bundled Microsoft Visual C++ 2017 Redistributable** from version 14.15 to **14.16**.

Resolved Issues 6.04.100

UMS, common

- Changed: **Activation/Deactivation of template profiles/master profiles has to be confirmed now** when at least one key value/master profile exists.
- Fixed: Several **file choosers did not remember the last selected directory**.

Console, common

- Fixed: '**Messages**' area sometimes **forgot its previous size**.
- Fixed: Various **windows did not remember their last size**, **position** or had an unfavorable default size.
- Fixed: **Save support information** could sometimes not be generated due to the unnecessary size check.
- Added: **Cross-check of a user and group name** when adding a new administrator account.

Server, common

- Fixed: Removed misleading **logging information on updating network name for Linux** clients (`network.interfaces.ethernet.use_igel_setup`)

Devices

- Fixed: '**Runtime since last Boot**', '**Total Operating Time**', and '**Battery Level**' were **not always refreshed** on Refresh/F5.
- Fixed: **Changes to a device or a profile were lost** when switching to UMS Administrator in UMS Console.
- Fixed: **Update on network name (DNS) was not triggered** if name was changed via system information.

Firmware Customization

- Fixed: **Files** or **folders with spaces in the name** could not be used in **Firmware Customizations** or **file upload**.

Jobs

- Fixed: **Log messages for jobs** were not displayed.

Universal Firmware Update

- Changed: Snapshot upload in **'Universal Firmware Update' only allows** files with `.snp` **filename extension**.

Searches

- Fixed: **Changes to the Search result** page behavior (**Misc > Settings > Views and Searches > Page Behavior**) were **not applied immediately** after saving the settings and selecting a search result.

Configuration Dialog

- Fixed: "**Always apply settings on reboot...**" checkbox was **missing in Update time dialog** when saving Device/Profile configuration.

Console, administration section

- Fixed: The **split position of the panels** in the detail view of a server (**UMS Administration > UMS Network > Server**) was not persistent.
- Fixed: **Connect/Disconnect operation of ICGs to UMS HA** had inconsistent behavior.
- Changed: **Online Check Response Timeout input** restricted to **100 ms up to 10.000 ms** (**UMS Administration > Global Configuration > Server Network Settings**).

AD / LDAP integration

- Changed: For an administrator account import of users from an AD/LDAP directory (**System > Administrator account > Import**), the **selection for 'Add user/group' was improved**.
- Fixed: **Inherited permissions of an imported AD user** were **not displayed correctly** in the 'Effective Rights' section of the 'Administrator accounts' window (**System > Administrator accounts > Effective Rights**)

Console, web start

- Fixed: An issue introduced in UMS 6.03.120 prevented the **execution of the UMS Console via Java Web Start**.

VNC

- Fixed: **VNC Viewer always started on the primary screen** instead of the last screen (multidisplay environment).
- Fixed: The **VNC Certificate Dialog could be off-screen** and so blocked the user from interactions.

IGEL Cloud Gateway (ICG)

- Removed: Misleading **log message during ICG installation**.

Mobile Device Management (MDM)

- Fixed: **Synchronization with ICG** failed if the MDM push certificate had expired.

Administrator application

- Fixed: **Backup sizes smaller than 1 KB** were not displayed correctly.

- Added: **Additional check for the existing database schema** before activating a database connection.
- Added: **Check for supported database versions**.

High Availability Feature

- Fixed: **Misc settings** configurations (**UMS Administration > Global Configuration > Misc Settings**) were **not synchronized with all HA servers**.
- Fixed: **WebDAV subfolders** were **not synchronized with other HA servers**.
- Fixed: **Adding an HA server after adding an ICG server** to the environment **caused ICG connection problems**.
- Fixed: The created **support file**, from triggering 'Save support information' (**Help > Save support information**), **did not** always **contain** the **information of remote components**.

UI / Look&Feel

- Fixed: **Visibility** of various (disabled) **menu icons**.
- Removed: Deprecated **bevel bar from legacy themes**.

Notifications

- Fixed: **Notification dialog** did sometimes not show notifications **when global notifications were enabled**.

Notes for Release 6.03.130

Software:	Version 6.03.130
Release Date:	2019-12-10
Release Notes:	RN-603130-1
Last update:	2019-12-10

Supported Environment 6.03.130

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	with SP1
Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

See also Devices Supported by IGEL Universal Management Suite (UMS).

New Features 6.03.130

UMS Common

- Changed: **All IGEL services** and resources like the **firmware update server** (which was fwu.igel.com and is now fwus.igel.com) and the **IGEL Knowledge Base** (kb.igel.com[24]) are now contacted via **HTTPS**. **It is now important to allow the https port (default 443) and the new address (fwus.igel.com) in the firewall rules and the proxy rules**.

24 http://kb.igel.com

Resolved Issues 6.03.130

IGEL Cloud Gateway (ICG)

- Fixed: **ICG root certificates** created with UMS version 6.01.130 or with an older version **can be used again for creating a signed certificate**.

Console, common

- Fixed: **The file transfer status** of firmware customizations without read permission was not displayed in the device detail window.

Firmwares

- Fixed: **Generic commands** could not be triggered by the UMS Console.

Notes for Release 6.03.110

Software:	Version 6.03.110
Release Date:	2019-10-30
Release Notes:	RN-603110-1
Last update:	2019-10-30

Supported Environment 6.03.110

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	with SP1
Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

See also Devices Supported by IGEL Universal Management Suite (UMS).

Resolved Issues 6.03.110

UMS, common

- Fixed: Files are now applied correctly when assigned to multi-level device folders.

Console, common

- Fixed: Removed unnecessary log entries which occured if the user had no permission set.
- Fixed: Issue where the 'configuration changed' indicator (blue exclamation mark) was not updated correctly if shared workplace assignments existed.

Views

- Fixed: Amount of hidden devices did not get refreshed if devices were added by another console.

Notes for Release 6.03.100

Software:	Version 6.03.100
Release Date:	2019-10-15
Release Notes:	RN-603100-1
Last update:	2019-10-15

Supported Environment 6.03.100

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	with SP1
Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

See also Devices Supported by IGEL Universal Management Suite (UMS).

Known Issues 6.03.100

- **Updating IGEL Windows 10 devices via UMS webdav folder** can result in **an endless update loop** of the devices. Please contact IGEL Support in this case.
  To avoid this problem, we recommend distributing the Windows 10 firmware updates via an external FTP or HTTPS server.

New Features 6.03.100

UMS, common

- Added: New display of **legend of UMS icons** (UMS Console **> Help > Legend**).
- Added: Support of **MS SQL Server Always On Availability Groups**.
- Added: Allow **TLS protocol** version **1.1 or 1.2 selection for SMTP server** communication in UMS.
- Changed: UMS with **external Derby database** supports only **Derby** versions **10.9 up to 10.14**.
- Changed: Increased the **maximum memory usage** of **UMS Console** (1024mb -> 3072mb), **UMS Server** (2048mb -> 4096mb) and **RMAdmin** (512mb -> 1024mb).
- Changed: Redesign of the UMS cache. The **cache is now always switched on**. The corresponding configuration dialogs were removed.
- Updated: **Apache Tomcat** from version 8.5.43 to **8.5.45**.
- Updated: **Azul Zulu JRE** from version 1.8.0_212 to **1.8.0_222**.

Console, common

- Added: **Configuration dialog for Views** and **Searches** (**Misc > Settings > Views and Searches**).
- Added: **Digit grouping** to improve the readability of large numbers (e.g. devices in a folder).
- Added: When creating a new administrator account, the **user name** or **group name** is **checked for duplicate names** prior to saving (**System > Administrator accounts > New**).

Devices

- Added: Option to **copy device information** to clipboard **in ASCII format** (**Device** > Detail View > Bottom > **Copy to Clipboard (ASCII)**).
- Changed: **Import Devices** uses the **Unit ID** instead of the MAC address as the client descriptor **for the long and short import formats**.
- Changed: **States of Device information lists** ("open" or "close") are now saved.

Views

- Added: **Option to cache View results** for more convenience.

Universal Firmware Update

- Changed: **Windows Firmware Updates** are now provided **with https**.
- Added: **Universal Firmware Update** supports **FTPS** and **SFTP** (**UMS Administration > Global Configuration > Universal Firmware Update**).

Searches

- Added: **New View/Search criterion** 'Structure Tag'.
- Added: Option to **save Searches** as **CSV, XML, HTML**, and **XSL**.
- Added: **Option to cache Search result**s for more convenience.

Console, administration section

- Added: **Choice** between **rich** and **plain text messages** to a device (**UMS Administration > Global Configuration > Messages to Devices**).
- Changed: Available **filter criteria** for registered device licenses (**UMS Administration > Global Configuration > Licenses > Device's Licenses**).
- Changed: It is now possible to **create/import certificates** in the **remote ICG installer/updater**. (UMS Console > **UMS Administration > UMS Network > IGEL Cloud Gateway**).

High Availability Feature

- Added: **'Stop Service' option** in process detail view (**UMS Administration > UMS Network > Server/Load Balancer**).

Installer (Linux)

- Added: **UMS** can be installed **on Red Hat Enterprise Linux 8**.
- Added: Installer will now also **check for a running instance of UMS Administrator** during an update installation.
- Added: **New wizard page** after component selection, **displaying the memory (RAM) requirements** for the selected components.

Installer (Windows)

- Added: **New wizard page** after component selection, **displaying the memory (RAM) requirements** for the selected components.

Resolved Issues 6.03.100

UMS, common

- Fixed: **Deleting a firmware update snapshot** also **deleted the** `ums_filetransfer` **folder**. (Only occurred if the firmware update has been stored directly in the UMS webdav folder without parent folder).

Console, common

- Fixed: **Indicator that the device settings have change**d (blue exclamation mark) **did not always appear** when an assigned profile was changed or indirectly assigned to a device.
- Fixed: When using an Oracle database, after moving files/views to a subfolder **the file/view count display of the subfolder was not updated**.
- Fixed: The **"Show Message" button** (UMS Console > Bottom right hand corner) **in "smart contrast"** behaves now analogously to the other themes.
- Fixed: The **UMS firmware statistics** overview (**Misc > Firmware Statistics**) could display **a wrong number of devices** when UD Pocket devices were managed in the UMS.
- Fixed: When a firmware customization has been assigned to a device, this device and all other already assigned devices got a **notification that the settings have changed**. Now only the new device will get the notification.
- Fixed: **Overwriting an existing zip file** when exporting firmware, firmware customizations, template keys / groups and device settings **created an unusable file** (**System > Export...**).

Devices

- Changed: The value o**f 'Last IP' in 'System Information'** of a device **is no longer editable** and has been moved from the editable section to the non-editable section.
- Fixed: Possible problems with the **File Transfer Status** if the device is **connected via ICG**.
- Changed: **Renamed** the field 'Expiration Date of Maintenance Subscription' **to** '**Expiration Date of OS10-Maintenance Subscription'** in the device detail view to avoid confusion (**Device** > Detail View > **Advanced System Information**).

Profiles

- Fixed: '**New Profile' dialog did not resize** if expert mode was closed (UMS Console > **Profiles** > context menu > **New Profile**).

Views

- Fixed: **Creating a view with criterion 'Monitor size'** caused an **error with the SQL Server database**.

Configuration Dialog

- Fixed: In the configuration dialog of a device on the **Security > Password** page, the "**Change Password" buttons** are now **properly enabled/disabled** to match the enable states of the corresponding parameters.
- Fixed: In profile configuration dialog (**Devices > Storage Hotplug**), the "Storage Hotplug" selection was not saved.

Console, administration section

- Fixed: Display of **wrong status** after renaming a server (**UMS Administration > UMS Network > Server**).
- Added: **Syntactic check of email address** before sending email in Cloud Gateway Options (**UMS Administration > Global Configuration > Cloud gateway options > First authentications keys > Send first Email authentications keys by Email**).

Firmware Customization

- Fixed: **Importing a firmware customization** without assigned files resulted in a "permission denied" warning.

Mobile Device Management (MDM)

- Fixed: **MDM** is working again **with LDAP users**.

Server, common

- Changed: Server details (**UMS Administration > Server**) will now show the **actual name of the Linux operating system** if it provides the file `/etc/os-release`.

High Availability Feature

- Fixed: **Support information for HA feature** no longer generates error-entry on other servers.
- Fixed: Issue with data directory in HA update. **HA update changed the data directory** (`ums_filetransfer`) to `c:\programData\igel` **without notice**. All files were automatically moved to the new directory. On Linux systems, the issue could lead to loss of files in `ums_filetransfer` folder.

UI / Look&Feel

- Fixed: **Console used wrong tooltip color** after sending RichMessages.

Installer (Linux)

- Fixed: After an **upgrade installation of the UMS Load Balancer**, it did not talk to the UMS Server anymore.

Notes for Release 6.02.110

Software:	Version 6.02.110
Release Date:	2019-08-14
Release Notes:	RN-602110-1
Last update:	2019-08-14

Supported Environment 6.02.110

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	New: only with SP2
Microsoft Windows Server 2008 R2	(64 bit)	New: only with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	New: only with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	New: only with SP1
Microsoft Windows 8.1	(64 bit)	New: only with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	New: only with SP2
Microsoft Windows Server 2008 R2	(64 bit)	New: only with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	New: only with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

- **Backend Database (DBMS):**

Oracle 11g R2	
Oracle 12c	

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10

See also Devices Supported by IGEL Universal Management Suite (UMS) (see page 25).

New Features 6.02.110

Server, common

- Updated **Apache Tomcat** from version 8.5.40 to **8.5.43**

IGEL Cloud Gateway (ICG)

- Added: Support for **Shadowing via IGEL Cloud Gateway** (ICG 2.01.100 or higher and IGEL OS 11.02.100 or higher are required)

Resolved Issues 6.02.110

AD / LDAP integration

- Fixed: **AD authentication** was not possible in a mixed domain/subdomain environment.

Thin clients

- Fixed: **Firmware update settings** of a device shown in UMS differed from the settings the device received when a **Universal Firmware Update** and a **profile with configured firmware update settings** were assigned to the device.

Views

- Added: The **timeout for the online check of devices** that is set in **UMS Administration > Global Configuration >Server Network Settings > Online Check Parameters** will be used for the **Online criterion** in **Views**.

IGEL Cloud Gateway (ICG)

- Changed: Due to structural changes between ICG 1.04 and ICG 2.01 **a downgrade is not possible**. It is also disabled in the ICG remote installer.
- Fixed: **Changing the name** of an ICG or a UMS Server does no longer result in an error message.

DB command line tools

- Fixed: The **embackup command line tool didn't find the backup file in restore mode** although it existed.

Server, common

- Fixed: Downloading global notifications (by UMS itself or via the **Send notification information via mail** administrative task) failed with Microsoft databases.

Installer (windows)

- Fixed: **Updating a UMS installation (4.09.x or older) directly to versions between 5.09.100 and 6.02.100 (inclusive) did not work completely**. In these cases, the installer asked for the data directory (which already existed) and even if the user entered the same path as the UMS used before, the folder was completely overwritten. Additionally, if the UMS used an embedded database before the update, a manual reactivation was sometimes required after the update.

Notes for Release 6.02.100

Software:	Version 6.02.100
Release Date:	2019-06-14
Release Notes:	RN-602100-1
Last update:	2019-06-14

Supported Environment 6.02.100

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	New: only with SP2
Microsoft Windows Server 2008 R2	(64 bit)	New: only with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	New: only with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	New: only with SP1
Microsoft Windows 8.1	(64 bit)	New: only with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	New: only with SP2
Microsoft Windows Server 2008 R2	(64 bit)	New: only with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	New: only with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

- **Backend Database (DBMS):**

Oracle 11g R2	
Oracle 12c	

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10

See also Devices Supported by IGEL Universal Management Suite (UMS) (see page 25).

New Features 6.02.100

UMS (common)

- Added: **Disk Usage** notification type for the UMS notification system. (**Help > Notifications**)
- Added: **Global notification** type for the UMS notification system to inform the user of important news like maintenance times, bugfixes, etc. (**Help > Notifications**)
- Changed: When a device is renamed, the setting **Adjust network name if UMS-internal name has been changed** is automatically set to enabled (**UMS Administration > Global Configuration > Device Network Settings > Adjust Names of Devices**).
- Changed: The administrative task **Assign objects to the devices of views** now provides the possibility to **assign firmware customizations**, **files** and **firmware updates** to the devices of views.

Console (common)

- Added: **Administrative tasks** notification type for the UMS notification system. (**Help > Notifications**)
- Added: The UMS now **displays all connected monitors** of a device. It previously displayed only two.

Console (administration section)

- Added: Option to create **ICG wildcard certificates**. (**UMS Administration > Cloud Gateway Options > Create signed certificate**)

Server (common)

- Changed: Suppress **server identity** in tomcat headers and by disabling default error pages.

AD / LDAP integration

- Added: **LDAPS** support **for AD** configuration.

Mobile Device Management (MDM)

- Added: **Public port** and **address** are now part of the MDM enrollment codes.

Security Fixes 6.02.100

High Availability Feature

- Fixed: HA installation unnecessarily **opened a debug port** (**ISN 2019-05**).

Resolved Issues 6.02.100

UMS (common)

- Fixed: **Resetting** a device **to factory defaults** could lead to various errors. (**UMS > Device > [Device's context menu] > Other commands > Reset to Factory Defaults**)
- Fixed: Missing **configuration state change flag** for template value and value group assignments.
- Fixed: Text **color of warning hints** when some/none of the selected devices have **Secure Terminal** enabled.
- Removed: Unused icons.
- Changed: **Tomcat access log files** are now also collected as a part of the support information. (**UMS > Help > Save support information**)
- Changed: The bundled Oracle JRE was replaced with **Azul Zulu JRE 8 Update 212**.
- Updated: **Apache Tomcat** from version 8.5.37 to **8.5.40**.
- Updated: UMS-bundled Java version from **Java 8** Update 202 to **Update 212**.

Console (common)

- Fixed: Already existing **archive of a profiles export** could not be overridden.
- Fixed: **UMS console login dialog** was not properly focused.
- Fixed: **Notifications** cannot be deactivated for **users of an imported AD group**.
- Fixed: Some texts could not be read because the text and the background had the same color.
- Added: Functionality to **assign objects** (profiles, FWCs, etc.) to more than one device at once.
- Fixed: Error message when **exporting result in SQL** console. (**Misc > SQL Console > Save Result**)
- Changed: In the UMS **Scan for devices** dialog, when the **Rescan** action is executed, the current filter is maintained and applied again to the new scan results. (**UMS > Scan for devices > Scan > Rescan**)
- Fixed: Double click on **Indirect assigned objects** redirects you to the Object and on right-click a pop-up window opens.
- Fixed: Selecting '**Don't show again**' on a notification in the **Notification** dialog had no effect. (**Help > Notifications**)
- Fixed: Wrong color in **Move to recycle bin** confirmation dialog.
- Fixed: Issue when devices were erroneously shown as unlicensed.
- Fixed: Issue when the **Close** button was sometimes invisible in the **Update Check** dialog. (**Help > UMS Update Check**)
- Changed: **Notification pop-up** on start-up is hidden if there are no notifications.

Devices

- Changed: **Save device files for support** dialog was redesigned and completed with the possibility to save files of multiple devices and devices of views. (**Help > Save device files for support**)
- Changed: **Wake up** commands are not sent to devices when they are registered in the UMS through an ICG.

Profiles

- Fixed: Re-added a missing **file picker** for the field **File name** on page **System > Update > Snapshots > Download**. File picker is now properly enabled after resetting the file name parameter with enabled template keys checkbox.
- Fixed: Changes of the **screen rotation**, i.e. rotating a screen with the left/right arrow buttons on the **User Interface > Display** page, could not be saved in profiles.
- Fixed: Re-added a missing **FTP password** field in W7 profile configuration dialog. (**System > Snapshots > Upload/Download**)
- Changed: Simplified dialog to create a new profile.

Template Keys and Groups

- Fixed: **Variable expressions** in template keys are now supported for **devices registered into directories**.

Firmware Customization

- Fixed: The **FWC import** did not upload the provided files.
- Changed: The **Firmware Customization import file** is validated and the import process is aborted if the imported parameters are not supported by the current UMS version.

Views

- Fixed: **CSV-exports** did not include the **column headers** of custom device attributes. (Admin task: Export view as...)
- Fixed: **Special characters from Eastern Europe** are shown incorrectly within **view exports**. (**View context menu > Save as...**)
- Fixed: Reduced processing time of assignment/detachment of profiles to/from the devices of a view.
- Added: A new **View** criterion for **device licenses**.

Jobs

- Changed: By **deleting a server** in **UMS Administration > UMS Network > Server**, the assigned devices are assigned to another available server and the **Job** execution data is deleted.

Automatic License Deployment (ALD)

- Fixed: An **empty error message** is shown if the configuration of **UDC2 Deployment** is changed and the configuration page is left without saving the changes.
- Fixed: A **Product Pack** is occasionally shown twice in the **Registered packs** section. (**UMS Administration > Global Configuration > Licenses > Deployment**)
- Changed: The **default automatic distribution method of new packs** (except for Workspace Edition packs) altered from 'Enabled' to 'Enabled (with conditions)'.

Universal Firmware Update

- Fixed: A **device directory** cannot be assigned to a **Universal Firmware Update** if the directory has already such an assignment.

- Changed: The **progress bar** shows the **download process** of Universal Firmware Update with **a better accuracy**.

Configuration Dialog

- Fixed: Configuration dialog combobox **Multimonitor full-screen mode** was missing in UMS 6 for **clients with firmware 10.4.100**. (**Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Window**)

Console (administration section)

- Changed: A test mail configured under **UMS Administration > Mail Settings > Send Test Mail** can now be sent to different recipients.
- Fixed: The **Certificate Management Node** was only visible to the **DB administrator**. (**UMS Administration > Global Configuration > Certificate Management**)
- Fixed: Issue when multiple **ICGs** were shown in the wrong order. (**UMS Administration > UMS Network > Igel Cloud Gateway**)
- Updated: **DSA** export graphic. (**UMS Administration > Global Configuration > Licenses > Device's Licenses > Export Unit ID list**)
- Fixed: In the device's **Rich Message Editor**, the **Reject changes** message does not appear anymore if you switch the template and the previous template had no changes. (**UMS > Device > [Device's context menu] > Other commands > Send Message**)
- Fixed: **UMS Licenses** with more than one corresponding notification could not be deleted. (**UMS Administration > Global Configuration > Licenses > UMS Licenses**)
- Added: **Wait dialog during ICG certificate creation** to indicate progress. (**Global Configuration > Cloud Gateway Options**)
- Added: **Server** and **broker icons** now show status.
- Changed: Renamed '**Remove'** buttons in the **ICG configuration dialog** to avoid misunderstanding. (**UMS Administration > UMS Network > Igel Cloud Gateway**)
- Added: **Dialog to Naming Convention** feature to guide the user. (**Global Configuration > Device Network Settings > Naming Convention**)
- Fixed **display** of correct **operating system name** for Windows Server 2016/2019 in administration section.

Console (web start)

- Fixed: Webstart sometimes showed **outdated splash screen**.
- Added: **Expressive error and log messages** when uploading files to UMS server fail due to **invalid server hostname**.

WebDAV

- Fixed: **WebDAV credentials** were not recognized under certain circumstances.

IGEL Cloud Gateway (ICG)

- Fixed: **UMS lost ICG connection** if a lot of devices were ICG administrated (device count> 500).

- Changed: When a device is registered on ICG, **ICG credentials** are **cached** before the device is removed from the **Recycle Bin** and then stored again. It only applies for devices that are in the Recycle Bin at the moment of ICG registration.
- Added: **New safeguard** to the ICG certificate dialog to prevent inexperienced users from making mistakes. (**UMS Administration > Global Configuration > Cloud Gateway Options**)
- Added: Option for the **certificate creation dialog** whether a new certificate should be **CA** or **End Entity**.
- Added: Check to prevent users from signing a certificate with a non-CA certificate.
- Added: **X.509 extensions** to show certificate dialog.

Server (common)

- Updated: **Microsoft SQL Driver** to support **TLS 1.2** in Microsoft SQL database connection.
- Fixed: Issue with an **incorrect identification** of the operating system of **Windows Server 2016/2019**. (**UMS Administration > UMS Network > Server > [UMS Server] > Attribute 'Operating System'**)
- Fixed: A **valid Workspace Edition license / Enterprise Management license** was not recognized because of not properly formatted timestamps.
- Fixed: Bug in the device authentication.
- Changed: All tables of the database schema are optimized. (Optimize Database)
- Updated: **EULA** text.

High Availability Feature

- Fixed: HA installation unnecessarily **opened a debug port**. (**ISN 2019-05**)
- Fixed: Communication issues within a HA network.
- Fixed: **Update installation wizard** contained misleading user prompt.
- Fixed: Commands for servers, load balancers and ICGs could create an **unreadable balloon tip**.
- Changed: Now support files also contain **watchdog log files** in **Save support information** function. (**UMS > Help > Save Support Information**)

Installer (Linux)

- Fixed: **Uninstaller on Linux** can be executed from now on only with **root privileges** and shows the correct UMS version.
- Fixed: **Splash screen** was shown as "**win0**" on panel in GNOME desktop on **RHEL7** and **Oracle Linux 7**.
- Added **check for running UMS** Console in Linux installer.
- Fixed: **UMS binaries** (e.g. RemoteManager.bin) do not start on **RHEL 7.x** or **Oracle Linux 7** due to ABI compatibility issue.

UI / Look&Feel

- Fixed: **Rich Message Templates** could spill their colors into the UMS.

Notes for Release 6.01.100

Software:	Version 6.01.100
Release Date:	2019-02-15
Release Notes:	RN-601100-1
Last update:	2019-02-15

Supported Environment 6.01.100

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	New: only with SP2
Microsoft Windows Server 2008 R2	(64 bit)	New: only with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	New: only with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	New: only with SP1
Microsoft Windows 8.1	(64 bit)	New: only with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	New: only with SP2
Microsoft Windows Server 2008 R2	(64 bit)	New: only with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	New: only with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

- **Backend database (DBMS):**

Oracle 11g R2	
Oracle 12c	
Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10

See also Devices Supported by IGEL Universal Management Suite (UMS).

New Features 6.01.100

Automatic License Deployment (ALD)

- Added: Support of new **IGEL OS 11 licensing mechanism** and new license distribution method **Automatic with Condition**. With this option, the device will get a license automatically only when the device accords to one or more of the selected conditions. The conditions can be folder memberships or views.
- Added: New **UMS Licensing ID** for easier license deployment. (**UMS Administrator > UMS Licensing ID** and **UMS Console > UMS Administration > Global configuration > Licenses > UMS Licensing ID**)

UMS (common)

- Updated: **Apache Tomcat** from **version 8.5.32 to 8.5.37**.
- Updated: UMS-bundled Java version **from Java 8 Update 181 to Update 202**.
- Added: Support for **Windows Server 2019**.
- Added: It is now possible to **license devices via context menu** (**License manually ...** in context menu of **Devices**, **Device Directories** and **Views**).
- Added: **Device-specific commands** that can be executed in the device's context menu (**UMS > Structure Tree > Devices**) and in the **device's menu bar**. The list of the available commands depends on the current selection. Therefore, a command is only listed when it is possible to execute by at least one of the devices in the current selection. The specific commands can be also selected in **Jobs**. (**UMS Console > Management Tree > Jobs**)

Resolved Issues 6.01.100

UI / Look&Feel

- Changed: **New bootsplash and theme** for UMS 6.01.100

IGEL Cloud Gateway (ICG)

- Changed: **Stabilized ICG connections** in UMS High-Availability Environments (UMS HA)
- Fixed: **Sub-Certificates (ICG) were not visible** right after creation. A refresh was necessary.
- Fixed: A **used mass deployment key** was not exportable. (**UMS Console > Global Configuration > Cloud Gateway Options**)
- Fixed: The **usage count of first-authentication keys** did not change. (Affected: Only the GUI representation in **UMS Console > Global Configuration > Cloud Gateway Options**)

UMS (common)

- Fixed: All **certificate management actions**, which generate a new network token, failed to save the network token. (Only in HA environment)
- Changed: **Thin Clients** have been renamed "**Devices".**

Console (common)

- Fixed: The download link in **UMS Update Check** could not be opened on some operating systems. (**UMS Console > Help > UMS Update Check**)

Devices

- Fixed: The function **Take over settings from...** did not work, when the UMS was connected to a PostgreSQL database. (**UMS Console > device > context menu**)
- Fixed: Sometimes an **empty error dialog** occurred by selecting a device (happened only if an assigned file has been deleted before).

Firmware Customization

- Fixed: The **manual import of firmware customizations** from older UMS versions was not possible. (**UMS Console > System > Import > Import Firmware Customizations**)

Automatic License Deployment (ALD)

- Fixed: **Changing the default proxy in the GUI did not change the default proxy in the backend** sometimes. (Only a server restart fixed the bug)
- Changed: Improved the **token validation dialog** to be more user friendly. (**UMS Console > Global Configuration > Licenses > Deployment > Register Pack**)

Console (administration section)

- Changed: Improved **certificate validation mechanism** (**UMS Console > Global Configuration > Certificate Management**)
- Fixed: The **'host' entry in ICG remote installer dialog** is now editable for **wildcard certificates** (e.g.: *.xyz.com[25]). (**UMS Console > Administration Tree > UMS Network > Igel Cloud Gateway > Install new ICG Cloud Gateway**)

Administrative tasks

- Fixed: The administrative task **Create backup** failed for external databases when the task was configured to **include licenses and files**, which is only possible for the **embedded database**. (**UMS Console > Administration Tree > Global Configuration > Administrative Tasks**)
- Fixed: An issue where the **next execution time of admin tasks** was not properly calculated. (**UMS Console > Administration Tree > Global Configuration > Administrative Tasks**)

Server (common)

- Fixed: The **certificate key pair import fails**, if the UMS data directory differs from the default. (**UMS Console > Administration Tree > Global Configuration > Certificate Management**)

Administrator application

- Fixed: It was not possible to **delete created database backups** even after a restart of the UMS Administrator.

Installer (Linux)

- Fixed: The **update installation** on Linux OS will no longer ask for the **installation directory**.

25 http://xyz.com

Notes for Release 5.09.100

Software:	Version	5.09.100
Release Date:	2018-10-08	
Release Notes:	Version	RN-509100-1
Last update:	2018-10-08	

The following formatting is used in the 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

Supported Environment 5.09.100

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 16.04	(64 bit)
Ubuntu 18.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **UMS Client:**

Microsoft Windows 7	(64 bit)
Microsoft Windows 8	(64 bit)
Microsoft Windows 10	(64 bit)
Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 16.04	(64 bit)
Ubuntu 18.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **Backend database (DBMS):**

Oracle 11g R2	
Oracle 12c	
Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)

Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10

See also Devices Supported by IGEL Universal Management Suite (UMS).

Warnings 5.09.100

- Following 32-bit environment is no longer supported:
  (Support removed because of software change to 64 bit)

  UMS Server:

  Ubuntu 14.04 (32 bit)
  Ubuntu 16.04 (32 bit)
  Red Hat Enterprise Linux (RHEL) 6 (32 bit)

  UMS Client:

  Microsoft Windows 7 (32 bit)
  Microsoft Windows 8 (32 bit)
  Microsoft Windows 10 (32 bit)
  Ubuntu 14.04 (32 bit)
  Ubuntu 16.04 (32 bit)
  Red Hat Enterprise Linux (RHEL) 6 (32 bit)

- Microsoft SQL Server 2008 / 2008 R2 support removed because of incompatible SSL certificates (not supported by Java)
- Ubuntu 14.04 (64 bit) support removed because of incompatible libraries (too old for the new UMS installation files)
- Increased maximal memory usage:

  UMS Server: 1024 MB to 2048 MB
  UMS Client: 768 MB to 1024 MB
  UMS Administrator: 384 MB to 512 MB

- Removed function to create a thin client license with smartcard. (**UMS Administration -> Global Configuration -> Licenses -> Thin Client Licenses -> Hardware**)

> **Care:**
>
> Licenses can still be created via Thin Client Smartcard License Server. (**UMS Administration -> Global Configuration -> Licenses -> UDC2 Deployment**)

New Features 5.09.100

UMS Common

- **New EULA**: This UMS version is licensed under a new end user license agreement (EULA). Please read it carefully.
- Added: **Notifications**. Now the UMS Console shows a notification pop-up (default: on each console connect) which informs about the latest firmware updates and expiration of UMS or client licences. Notifications can be deactivated (for all users) in **UMS Console -> Administration Tree -> Global Configuration -> Misc**, and the relevant notification types can be set in **UMS Console -> Misc -> Settings -> Notifications** (user specific). Notifications can also be sent via Mail. (**UMS Console -> Administration Tree -> Global Configuration -> Administrative Tasks**)
- Added: It is now possible to **configure the used cipher suites for the UMS SSL port**. This setting is server specific and not part of the database backup. For UMS HA: Cipher suite selection has to be made on each node separately. (**UMS Administrator -> Settings -> Configure Ciphers**)
- Added: New feature **Certificate Management**: It is now possible to replace the certificate, which is mainly used for thin client to UMS communication. Changing the default certificate triggers a mechanism which consistently tries to store the new certificate on each thin client. This can only be done for online thin clients.

  > **Warning**
  >
  > Incautious usage can lead to loss of the management connection to thin clients. The management functionality can only be restored by deleting the UMS certificate manually (local access) from each affected thin client. Certificate management can be found in **UMS Console -> UMS Administration -> Global Configuration -> Certificate Management**. (Only visible for the database administration user)

- Updated: The UMS is now bundled with a 64 bit JRE. The new JAVA version is 1.8.0_181.

Thin Clients

- Added: **Automatic Wake On LAN Proxy Detection**. The UMS will try to find a thin client that is able to relay the wake up call automatically to the target thin client without configuring thin clients as Wake On Lan Proxy. A thin client can automatically relay the wake up call, if the thin client is online, has a firmware version of LX 5.09.100 or newer and can 'see' the target thin client (same network, subnet ...). This feature can be activated in **UMS Console -> UMS Administration -> Global Configuration -> Wake on LAN -> Automatic Wake On LAN Proxy Detection** (default: off).
- Added: The thin client panel now contains a section **File Transfer Status** which gives status information about the assigned files.
- Added: New field **boot mode** in thin clients system information section.

Profiles

- Added: **Changes in UMS profiles can now be seen in their registry**. (Same colors as in the configuration tree).

Template Keys and Groups

- Added: **Static template keys**: For these template keys it is no longer necessary to configure and assign a template value since the thin client provides the values at runtime. The following three keys are available: MACADDRESS, HOSTNAME and UNITID. (Visible in each **Choose Template Key** dialog)

Firmware Customization

- Added: It is now possible to **assign wallpapers and boot splashes to W10 thin clients** (version 4.02.100 and higher) via firmware customizations.

Configuration Dialog

- Added: Additional **setup admin** user and permission layer on page **Accessories -> Setup -> User Page Permission**
- Added: Each parameter has got a new **reset button** which resets the value to factory defaults. The button is disabled when the parameter already has its default value.

Mobile Device Management (MDM)

- Added: **Mobile Device Management Preview**. Now it is possible to manage up to 5 mobile iOS devices with iOS version 10.3 or newer in the UMS.

UI / Look & Feel

- Added: If a tree node (folder, profile, master profile, firmware customization, view, ...) gets copied, and the target folder already contains an object with this name, the new displayed name will be marked with a **modifier ("COPY")**.

Resolved Issues 5.09.100

UMS, Common

- Removed: **It is no longer possible to create UDC 2 licenses manually from smartcard** (Smartcard was directly connected to the UMS Console). It is still possible to configure and use a thin client as UDC 2 smartcard license server. (Automatic Licensing)
- Removed: **Support for SQL Server 2008 and SQL Server 2008 R2 databases**. (Incompatible SSL certificates)
- Fixed: Bug in **Automatic License Deployment** which occurred with **UD Pocket** devices. If the amount of registered unlicensed UD Pocket devices was higher than the amount of available licenses of one token, no license could be deployed.
- Fixed: **Automatic UDC2 license deployment created several identical licenses for the same thin client**.
- Fixed: **Offline user manual in UMS Console did not open on Linux OS**.
- Fixed: **install.log file** could not be added to the support information.
- Changed **default signature algorithm** for certificates to SHA512withRSA.
- Changed: The knowledge base links point now to kb.igel.com[26] instead of edocs.igel.com[27]
- Changed: **Apache Tomcat** from version 8.0.47 to version 8.5.32.

Console, Common

- Removed: Unused graphical effects parameters for configuration dialog. (**UMS Console -> Misc -> Settings -> Configuration Dialog**)
- Fixed: **UMS Console window did not request focus anymore** while a firmware update is downloaded.
- Fixed: **Splash screen and accept certificate dialog can be hidden** behind other windows on Linux.
- Fixed: **Clearing the recycle bin** took much too long.
- Fixed: The **ID of non-displayable tree objects** is no longer shown with a thousands separator.
- Fixed: The **cache management dialog** in UMS Console did not open on Linux OS.
- Fixed: A **custom thin client attribute** which is linked to a default directory rule **could falsely be deleted**.
- Changed: **Users without the WebDav Access permission now get** a **more detailed hint** (message or tooltip) why they can´t perform some actions (e.g. creating a UMS file).
- Added: **All file choosers in the UMS Console can now remember their last used directory** (Except the WebDAV file choosers). This can be disabled in **UMS Console -> Misc -> Settings**.

Thin Clients

- Fixed: **User login history** had no entries for UD Pocket devices. (**UMS Console -> Management Tree -> Thin Clients -> Thin Client Content Panel**)
- Fixed: The actions **rename** and **delete** were selectable on the thin client root node. (**UMS Console -> Management Tree**)

26 http://kb.igel.com
27 http://edocs.igel.com

- Fixed: After resetting a thin client to factory defaults, the **UMS Console still showed the thin client in the assigned objects**.
- Fixed: **After scanning several thin clients at once** (with specified target directory) **some of the scanned thin clients were not visible in the tree** until a refresh was done.
- Fixed: The thin **client settings cache** was not updated by assignment changes coming from administrative task **Assign profiles to the thin clients of views**.
- Fixed: Although the flag **Adjust network name if UMS-internal name has been changed** had been set, the thin client rename function ignored the maximum name length of 15 characters. (Rename via content panel)
- Fixed: The **Lock screen** icon (Advanced Thin Client Health Status) was permanently set if the thin client was remotely suspended.
- Changed: I**mproved usability** of thin client import dialog. (**UMS Console -> System -> Import -> Thin clients**)
- Changed: **Order of entries** in thin client context menu **Update & Snapshot Commands**.
- Changed: The **default thin client name** is now TC-MAC instead of IGEL-MAC to be fully DNS capable.

Profiles

- Fixed: Re-added missing file picker for field **file name** on page **System -> Update -> Snapshots -> Download**
- Fixed: Bug in **display configuration** where the second screen could not be saved on the left of screen one. (Only if both screen resolutions were set to **Autodetect**)

Template keys and groups

- Fixed: The **template check showed a missing value alert** (because no template value had been assigned to the thin client) although the setting in question had been overwritten by a correct profile/master profile and therefore did not affect the thin client.

Firmware Customization

- Fixed: **The config change flag in the thin client assignment panel was not displayed** if firmware customization was changed without sending the changes directly to the assigned thin clients.
- Fixed: In firmware Customizations, **the cancel button of the select file dialog did the same as the OK button**. When clicking the cancel button, changes will now be discarded instead of accepted.

Jobs

- Changed: Improved user interaction for **creating/editing a job where the execution time is in the past**.

Files

- Fixed: File **directories** could be renamed, but **after a refresh received the old name again**. (**UMS Console -> Management Tree -> Files**)

Configuration Dialog

- Fixed: The windows profile setting **Use IGEL Setup for configuration display settings** could be disabled, but after saving and reopening the configuration dialog, the **flag was still enabled**. (**Setup -> Configuration -> User Interface -> Display**)
- Fixed: **Huge memory consumption** in the configuration dialog of display page with high monitor resolutions.

Console, Administration Section

- Fixed: **Windows Server 2016 was not recognized as such**. OS name was displayed as "Windows NT (unknown)". (Visible in **UMS Console -> Administration Tree -> UMS Network -> Server -> Server Content Panel**)
- Fixed: Changes in the **Active Directory / LDAP** configuration didn't affect the management tree node **Shared Workplace Users** until the next connect.
- Fixed: **The thin client license node showed an access denied error on selection**, if the user had the permission to access the thin client license node, but not the UMS license node.
- Added: **Checkbox** to show only the last 20 executions in administrative task execution history to performance-friendly. (**UMS Console -> UMS Administration Tree -> Global Configuration -> Administrative Tasks**)
- Changed: **Configuration of concurrent thin client request threads** is now more user-friendly. (**UMS Console -> Administration Tree -> Global Configuration -> Thin Client Network Settings**)

Administrative Tasks

- Fixed: **Performance problem** which occurred if a newly created administration task with action **Delete logging data** had an incorrect export path set.
- Fixed: The two administrative tasks **Delete job execution data** and **Delete administrative job execution data** had wrong default values (Keep no more than x executions per job).
- Fixed: The administrative task **Delete job execution data** was not able to handle a very large amount of database entries (several millions).
- Fixed: A few 'old' administrative tasks could not be opened/reconfigured anymore.

IGEL Cloud Gateway (ICG)

- Fixed: The **usage date of mass-deployment keys** was not set. (**UMS Console -> Administration Tree -> Global Configuration -> Cloud Gateway Options**)
- Added: **Remote installer** for IGEL Cloud Gateway

Asset Inventory Tracker (AIT)

- Fixed: Asset names in **Asset Inventory Tracker** weren't appropriately truncated
- Added: **New administration task** to delete outdated asset history data. (**UMS Console -> Administration Tree -> Global Configuration -> Administrative Tasks**)

Server, Common

- Fixed: Bug which led to **high CPU-load of the UMS Server**, if the **Advanced Health Check** was enabled (**UMS Console -> Misc -> Settings -> Appearance**).

Administrator Application

- Fixed: The action **restore from backup** failed and the user got an error message. After the user acknowledged it, a wrong message **Database successfully restored** was displayed.
- Fixed: **Error while copying data into an oracle database**. (Only if **Asset Inventory Tracker** was used)
- Fixed: The **UMS Administrator database copy action aborted in some cases** (depending on the values in the database) with the following error: 'An attempt was made to get a data value of type 'BINARY' from a data value of type 'BLOB' '.
- Changed: **It is no longer possible to create a separate certificate backup in UMS Administrator**. The certificates are now contained in the database backup. The certificates (UMS to thin client communication) can be imported/exported in the new tree node **Certificate Management**. (**UMS Console -> Administration Tree -> Global Configuration**)

Installer (Linux)

- Added: Support for **Ubuntu 18.04**

UI / Look & Feel

- Fixed: **Broken row-sorter** in the license section
- Changed: **New Splash Screen** for UMS Console and UMS Administrator
- Changed: The UMS Console and UMS Administrator received **new task bar icons** and **application icons**.

Notes for Release 5.08.120

Software:	Version	5.08.120
Release Date:	2018-06-22	
Release Notes:	Version	RN-508120-1
Last update:	2018-06-22	

The 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

Supported Environment 5.08.120

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 14.04	(32 bit) (64 bit)
Ubuntu 16.04	(32 bit) (64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 6	(32 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **UMS Client:**

Microsoft Windows 7	(32 bit) (64 bit)
Microsoft Windows 8	(64 bit)
Microsoft Windows 10	(64 bit)
Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 14.04	(32 bit) (64 bit)
Ubuntu 16.04	(32 bit) (64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 6	(32 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **Backend database (DBMS):**

Oracle 11g R2	(with RAC support)
Oracle 12c	(with RAC support)

Microsoft SQL Server 2008	
Microsoft SQL Server 2008 R2	
Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
PostgreSQL 9.3 - 9.6 and 10.1	
Apache Derby 10	

See also Devices Supported by IGEL Universal Management Suite (UMS).

Resolved Issues 5.08.120

UMS (common)

- Fixed: Automatic UDC2 deployment creates unnecessarily several identical licenses for the same thin client. (Did not influence the smartcard license amount)

Notes for Release 5.08.110

Software:	Version	5.08.110
Release Date:	2018-05-11	
Release Notes:	Version	RN-508110-1
Last update:	2018-05-11	

The 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

Supported Environment 5.08.110

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 14.04	(32 bit) (64 bit)
Ubuntu 16.04	(32 bit) (64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 6	(32 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **UMS Client:**

Microsoft Windows 7	(32 bit) (64 bit)
Microsoft Windows 8	(32 bit) (64 bit)
Microsoft Windows 10	(32 bit) (64 bit)
Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 14.04	(32 bit) (64 bit)
Ubuntu 16.04	(32 bit) (64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 6	(32 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **Backend database (DBMS):**

Oracle 11g R2	(with RAC support)
Oracle 12c	(with RAC support)

Microsoft SQL Server 2008	
Microsoft SQL Server 2008 R2	
Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
PostgreSQL 9.3 - 9.6 and 10.1	
Apache Derby 10	

See also Devices Supported by IGEL Universal Management Suite (UMS).

New Features 5.08.110

UMS (common)

- Added: This UMS version is licensed under a **new end user license agreement (EULA)**. Please read it carefully!

Resolved Issues 5.08.110

UMS (common)

- Fixed: A **custom thin client attribute** which is linked to a default directory rule could falsely be deleted.
- Fixed: Bug in **Automatic License Deployment** which occurred with UD Pocket devices. If the number of registered unlicensed UD Pocket devices was higher than the number of available licenses of one token, no license could be deployed.
- Fixed: The **thin client settings cache** has not been updated by assignment changes coming from the administration task **Assign profiles to the thin clients of views**.

Console (common)

- Fixed: **UMS Console window doesn't request focus** anymore while a firmware update is downloaded.
- Fixed: Although the flag **Adjust network name if UMS-internal name has been changed** has been set, the **thin client rename function** ignored the maximum name length of 15 characters. (Rename via content panel)
- Fixed: **Cache management dialog in UMS Console** did not open on Linux.
- Fixed: **Offline user manual** in UMS Console did not open on Linux.

Console (administration section)

- Fixed: A few 'old' **administrative tasks** could not be opened/ reconfigured anymore.

Profiles

- Fixed: Bug in the **display configuration** where the second screen could not be saved on the left of screen one. (Only if both screen resolutions are set to 'Autodetect').

Configuration Dialog

- Fixed: The Windows profile setting **Use IGEL Setup for configuration display settings** could be disabled, but after saving and reopening the configuration dialog, the flag was still enabled. (**Setup > Configuration > User Interface > Display**).

Notes for Release 5.08.100

Software:	Version	5.08.100
Release Date:	2018-01-29	
Release Notes:	Version	RN-508100-1
Last update:	2018-01-29	

The 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

Supported Environment 5.08.100

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 14.04	(32 bit) (64 bit)
Ubuntu 16.04	(32 bit) (64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 6	(32 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **UMS Client:**

Microsoft Windows 7	(32 bit) (64 bit)
Microsoft Windows 8	(64 bit)
Microsoft Windows 10	(64 bit)
Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 14.04	(32 bit) (64 bit)
Ubuntu 16.04	(32 bit) (64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 6	(32 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **Backend database (DBMS):**

Oracle 11g R2	(with RAC support)
Oracle 12c	(with RAC support)

Microsoft SQL Server 2008	
Microsoft SQL Server 2008 R2	
Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
PostgreSQL 9.3 - 9.6 and 10.1	
Apache Derby 10	

See also Devices Supported by IGEL Universal Management Suite (UMS).

New Features 5.08.100

Console (administration section)

- Added: **Automatic license deployment** for UDC3, UMA and UD Pocket. (**UMS Administration > Global Configuration > Licenses > Deployment**)

  > If the feature is enabled (disabled by default) and appropriate tokens have been registered in the UMS, licenses for unlicensed UDC3 devices, UMA devices and UD Pockets are deployed automatically.

- Added: New tree node **Proxy Server** (**UMS Console > UMS Administration > Global Configuration**), to administrate several proxies in an easy way.
  As yet, a proxy could be configured for firmware updates only. A proxy now can be used for ICG´s and the new **Automatic License Deployment** feature too.

Thin Clients

- Added: **Snapshot upload/download support** for UMA devices with version 3.01.100 or higher.

Server (common)

- Changed: Because of security reasons, the **https connector of the UMS Server** does now provide **TLSv1.2** only.

UMS (common)

- Updated: **Apache Tomcat** version from 8.0.42 to **8.0.47**.
- Updated: **Java Version** from 1.8.0_121 to **1.8.0_152**.

Resolved Issues 5.08.100

Console (common)

- Fixed: The **UMS Update Check** is now able to use a proxy. When a firmware update proxy is defined, the **Update Check** uses this proxy to verify whether there is a new UMS version available.
- Fixed: **Plenty wrong server log entries**. Occurred when the UMS user had no permission to see the license tree node in the **UMS Administration** tree and the **Advanced thin client health check** was active.
- Changed: Renamed the global permission **Snapshot** into **WebDAV access** (UMS file transfer).
- Changed: Users without the **WebDav Access** permission get now **a more detailed hint** (message or tooltip) why they cannot perform some actions (e.g. creating a UMS file).

Server (common)

- Fixed: Bug which led to high CPU load of the UMS server when the **Advanced Health Check** (**UMS Console > Misc > Settings > Appearance**) was enabled.
- Updated: PostgreSQL database driver to support **PostgreSQL v9.3 - v9.6 and v10**.

Firmware Customization

- Fixed: With **certain permission combinations**, users were not allowed **to assign files** to newly created firmware customizations.
- Fixed: **FileUpload via FWC-Wizard could lead to errors** when the user had insufficient permissions.
- Fixed: In **Firmware Customizations**, the **Cancel** button of the 'select file' dialog did the same as the **OK** button. By clicking the **Cancel** button, changes will now be discarded instead of accepted.

Universal Firmware Update

- Fixed: The **firmware update text viewer** remembers now its size, and the text font has been changed to a monospaced font to support text formation.

IGEL Cloud Gateway

- Fixed: **Root certificates** are now marked as a **certificate authority**.
- Fixed: After a connection to an **Igel Cloud Gateway** failed with a certificate error, some threads could not be closed.

Administrative Tasks

- Fixed: The **execution time of administration tasks** was reported to be in the past, although it was in the future.

  > This issue occurred only for new or changed administrative tasks with execution time after 12:00 p.m. and before 12:00 a.m.

- Fixed: **Performance problem occurred** when a created administrative task with action **Delete logging data** got an incorrect export path set.

Console (administration section)

- Changed: Stored all license tree nodes into a new **Licenses** folder (**UMS > UMS Administration > Global Configuration**) and updated their icons.

Notes for Release 5.07.110

Software:	Version	5.07.110
Release Date:	2017-10-19	
Release Notes:	Version	RN-507110-1
Last update:	2017-10-19	

The Linux installation was tested on the following distributions:
- Ubuntu 16.04 64-bit
- RedHat Enterprise 7.3
- Oracle Linux Server 7.3

The 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

Resolved Issues 5.07.110

Console (common)

- Fixed: **Plenty server log entries** if the UMS user had no permission to see the license tree node in the UMS Administration and if the '**Advanced thin client health check**' was active.
- Fixed: **Firmware customizations could be manipulated** by a user without write permission.
- Changed: Renamed the global permission '**Snapshot**' into **WebDAV access (ums-filetransfer)**.

Firmware Customization

- Fixed: With certain permission combinations, users were not allowed to **assign files to newly created FWCs**.
- Fixed: **FileUpload via FWC-Wizard** could lead to errors if the user had insufficient permissions.

Administrative tasks

- Fixed: The **execution time of administration tasks** was reported to be in the past although it was in the future. This issue occurred only for new or changed administrative tasks with execution time after 12:00 p.m. and before 12:00 a.m.

AD / LDAP integration

- Fixed **AD login issue**: Login to UMS console failed with an AD user that had been indirectly imported to UMS via AD group. This issue occurred only if there was no browse user set in the AD configuration.

Notes for Release 5.07.100

Software:	Version	5.07.100
Release Date:	2017-08-30	
Release Notes:	Version	RN-507100-1
Last update:	2017-08-30	

The 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

New Features 5.07.100

UMS (common)

- Added: New Feature **Asset Inventory Tracker**.
  With a valid Asset Inventory license, it enables the user to collect Asset Inventory data from thin clients with Linux firmware 10.03.100 and higher.
  The data is displayed as part of the thin client details panel.

Console (common)

- Added: Function to **check for new UMS updates**. (**UMS > Help > UMS Update Check**)
- Added: **Export and import actions** for template keys, value groups, and firmware customizations.

Server (common)

- Updated: **Apache Tomcat** from version 8.0.41 to **8.0.44**.

Thin Clients

- Added: New thin client attribute **Battery Level**.
- Added: **Advanced thin client state icons**.
  The feature is activated by default and can be disabled via **Misc > Settings > Appearance > Use Advanced Health Status Icons**.
  In addition to the existing states (online and offline) four new states have been added: **Never communicated with UMS**, **License violated**, **In Lockscreen,** and **In Firmware Update**.
  The states **In Lockscreen** and **In Firmware Update** are only visible if the thin client firmware supports it and if the following option is set in the UMS (activated by default): **UMS Administration > Global Configuration > Thin Client Network > Thin Clients send updates**. This feature requires Linux firmware 10.03.100 or newer.
- Added: **Advanced message functionality**.
  The **Send Message** action in the thin client context menu opens a new editor to send customized messages and templates.
  Several default templates have been added and can be seen/changed in **UMS > UMS Administration > Global Configuration >TC Rich Message Templates**.
  Thin clients which do not support the feature are showing the plain message like before.
- Added: **Clear value button** for thin client attributes with type "DATE".

Universal Firmware Update

- Added: Filter option to show only the latest available firmware version in firmware update dialog. (**UMS Console > Universal Firmware Update Tree Node >** Context Menu **> Check for new firmware updates**)

Console (UMS Administration)

- Added: Possibility to use a list of **predefined thin client attribute values**. (**UMS Console > UMS Administration Tree > Global Configuration > Thin Client Attribute**)
- Changed: The **order of the tree nodes** in **UMS Console > UMS Administration > Global Configuration**.

Administrative Tasks

- Added: Administrative tasks can now be **executed monthly**.
- Added: New administration task to **save a UMS view on the file system**.

Firmwares

- Changed: Unused firmware can now be removed separately. (**UMS Console > Misc > Remove Unused Firmwares**)

IGEL Cloud Gateway (ICG)

- Changed: The **file and user synchronization process** after connecting an Igel Cloud Gateway is now executed in the **background**.

IGEL Management Interface (IMI)

- Added: IMI V3 supports now **Asset Inventory Information**.
- Added: IMI V3 supports now **Reset to factory defaults** for thin clients.
- Added: The thin client details do now contain the field **Battery Level** in IMI V3.

Installer (Linux)

- Added: Enhanced functionality for UMS installations on Linux. **Required libraries can now be installed automatically during UMS installation**.

Resolved Issues 5.07.100

UMS (common)

- Fixed: **Licenses can't be registered at the UMS** if the licenses are located on a network drive.
- Fixed: **UMS installations with more than three domain controllers** were not able to update to UMS version 5.05.100. After the update, each UMS login failed with a "truncation error" message.
- Fixed: The **Confirm deletion** dialog showed nested objects twice.
- Fixed: The **Restore backup** action failed for renamed `.pbak` backup files.
- Changed: If the internal thin client name is set to **overwrite the network name of the thin client**, there is now a check to make sure that the name is **DNS capable**.

Console (common)

- Changed: All **export actions** in the main menu are now always **enabled**, irrespective of the selected tree-object.
- Fixed: Bug in **UMS Linux installations** where hyperlinks could not be opened. (e.g. **UMS > UMS Administration > Misc Settings**)
- Added: The **thin client** content panel shows **icon corresponding to the current status** (online/offline/advanced health status)

Profiles

- Fixed: **Exporting profiles** (as archive) on a mapped network drive resulted in an unreadable file.
- Fixed: **Inconsistent results in profile comparison** when comparing two profiles in different directions (e.g. A-B vs B-A).

Template Keys and Groups

- Fixed: An error occurs if a template key or value group with **empty description** is edited and the **UMS database is an Oracle DB**.

Firmware Customization

- Fixed: **Display error in thin client directory assignments**. After a reload, the FWC assignments were not visible.
- Added: **FWC directories can now be copied** (including descendants).

Universal Firmware Update

- Fixed: Bug which was responsible for a **very low FTP firmware download rate**.

Configuration Dialog

- Fixed: After assigning two profiles (each with a default printer) to a thin client, the **thin client has now only one default printer set** (coming from a profile with higher priority).

- Fixed: **Coloring** for following changed and saved setup parameter:
  User Interface > Desktop
  Security > Logon > Active Directory / Kerberos
  Security > Smartcard > Middleware

Console (UMS Administrator)

- Fixed: After a change in **UMS Console > UMS Administration > Global Configuration > Server Network Settings > Broadcast IP** the user is not asked to save the change.
- Fixed: The **Igel Cloud Gateway configuration node** depended on permissions of Igel Cloud Gateway server node.
- Fixed: The dialog **Export all Unit IDs from a view** showed duplicated thin client entries in the result list. (**UMS Console > UMS Administration > Global Configuration > Thin Client Licenses > Export Unit ID list**)

Administrative Tasks

- Fixed: **Maximum amount of backups** has been ignored by database backup task.
- Fixed: The **reporting of a database backup job** showed a failed task even if the task was completed successfully.
- Changed: Handling of **immediate execution time** for administrative tasks.

AD / LDAP Integration

- Fixed: **Active Directory login error** for domain names without a separating dot.

IGEL Cloud Gateway (ICG)

- Fixed: **Reregistration of an ICG managed thin client** (before rebooting the ICG) leads to a connection error between the thin client and the ICG.
- Fixed: **UMS lost ICG connection** randomly.
- Fixed: Thin Client **license files could not be downloaded** via IGEL Cloud Gateway.
- Fixed: **File transfer via ICG fails** if a custom UMS file transfer folder location is used.
- Fixed: The **Igel Cloud Gateway configuration node** depended on permissions of Igel Cloud Gateway server node.
- Fixed: After an ICG administrated thin client got changed settings, **the configuration flag has not been cleared** for assigned objects (e.g. profiles).
- Fixed: The thin client **license upload fails** if the ICG license is expired.

Administrator Application

- Fixed: The **backups** section in the UMS Administrator was only active for embedded databases. Now the **backups** section is always enabled to give the possibility to create and restore certificates and server configurations with all databases.

Installer (Windows)

- Changed: To avoid incorrect input, **the backup file path in Windows installer can now only be set by the file chooser dialog**.

Installer (Linux)

- Fixed: Removed **irritating log4j warnings** during database backup process in Linux installer.
- Fixed: Removed **irritating jsvc_server.pid error** message in Linux installer summary.

UI / Look & Feel

- Added: **New splash screen** for UMS Console and UMS Administrator.