



UMS Reference Manual

- [What is New - Knowledge Base Updates for IGEL UMS 12.04.100](#) (see page 3)
- [Overview of the IGEL UMS](#) (see page 6)
- [UMS Installation and Update](#) (see page 12)
- [Connecting the UMS Console to the IGEL UMS Server](#) (see page 162)
- [Registering the IGEL UMS](#) (see page 164)
- [Registering IGEL OS Devices on the UMS Server](#) (see page 165)
- [UMS Console User Interface](#) (see page 182)
- [Profiles in the IGEL UMS](#) (see page 207)
- [Priority Profiles in the IGEL UMS](#) (see page 253)
- [Template Profiles in the IGEL UMS](#) (see page 256)
- [Firmware Customizations in the IGEL UMS](#) (see page 274)
- [Devices](#) (see page 286)
- [Shared Workplace Users](#) (see page 327)
- [Views](#) (see page 328)
- [Jobs - Sending Automated Commands to Devices in the IGEL UMS](#) (see page 355)
- [Files - Registering Files on the IGEL UMS Server and Transferring Them to Devices](#) (see page 366)
- [Universal Firmware Update](#) (see page 377)
- [Search History](#) (see page 381)
- [Recycle Bin - Deleting Objects in the IGEL UMS](#) (see page 383)
- [UMS Administration](#) (see page 386)
- [Importing Active Directory Users](#) (see page 515)
- [Create Administrator Accounts](#) (see page 519)
- [User Logs](#) (see page 537)
- [Save Support Information / Send Log Files to Support](#) (see page 544)
- [Save Device Files for Support](#) (see page 548)
- [The IGEL UMS Administrator](#) (see page 550)

What is New - Knowledge Base Updates for IGEL UMS 12.04.100

In this article you will find a summary of documentation updates with direct links to the updated articles.

- ⓘ You will find the release notes for IGEL Universal Management Suite 12 both as a text file in the same folder as the installation programs on our [download server](#)¹ and in the Knowledge Base.
You can also find information about the released features in the [UMS 12.04.100 Release Video](#) (see page 5).

- ⚠ Before the installation / update of the IGEL UMS, please read [How to Start with IGEL COSMOS](#).
You cannot manage IGEL OS 12 devices without the UMS Web App. Thus, the UMS Web App must be selected during the installation of the UMS.

Reverse Proxy / Load Balancer Example Configurations

Example network configurations with the use of third party reverse proxies got verified. For more information, see:

- [IGEL Universal Management Suite Network Configuration](#)
- [NGINX: Example Configuration for as Reverse Proxy in IGEL OS with SSL Offloading](#)
- [F5 BIG IP: Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading](#)
- [Azure Application Gateway: Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading](#)

Using Advanced Search in Jobs and Administrative Tasks

The advanced searches created in the IGEL UMS Web App can be used now in Jobs and Administrative Tasks in the UMS Console. For more information, see [Search for Devices in the IGEL UMS Web App](#), and [Jobs - Sending Automated Commands to Devices in the IGEL UMS](#) (see page 355), and [Administrative Tasks - Configure Scheduled Actions for the IGEL UMS](#) (see page 436).

Remote Security Logging for UMS Web App and IMI

Security relevant events of the UMS Web App and the IGEL Management Interface (IMI) can now be logged in files, that can be picked up by a configured log collector (for example, Graylog). For more information, see [Remote Security Logging in IGEL](#) (see page 504).

The logging of security relevant events can be enabled through the GUI. For more information, see [Logging](#) (see page 501).

¹ <https://www.igel.com/software-downloads/cosmos/>

Migrate from HA UMS to Distributed UMS

Description added to perform the migration. For details, see [How to Migrate an UMS High Availability Installation to a Distributed UMS](#).

Updated Secure Shadowing and Secure Terminal Description

The process descriptions and graphs are updated for the Unified Protocol use case OS 12. For more information, see the OS 12 sections of UMS and Devices: Secure Shadowing and UMS and Devices: Secure Terminal.

New File Type: App Signing Certificate

A new file type can be uploaded through UMS Console and UMS Web App. For more information, see [Files - Registering Files on the IGEL UMS Server and Transferring Them to Devices](#) (see page 366) and [Upload and Assign Files in the IGEL UMS Web App](#).

New Commands in Command-Line Interface

New commands added to Manage Web Certificates. For more information, see [IGEL UMS Administrator Command-Line Interface](#) (see page 582).

UMS Web App

General User Interface Update

Left panel is collapsible. For more information, see [IGEL UMS Web APP User Interface](#).

App Dependencies Tab

A new tab is added showing the dependencies of the selected app version. For more information, see [Apps - Import and Configure Apps for IGEL OS 12 Devices via the UMS Web App](#).

App Versions Tab

Links are added to a list of devices on which the selected app / app version is installed. For more information, see [Apps - Import and Configure Apps for IGEL OS 12 Devices via the UMS Web App](#).

Communication Token in Network Area

Communication Token for onboarding is made easily available. For details, see [Network Settings in the IGEL UMS Web App](#).

Using Template Profiles in IGEL UMS Web App

Template keys and values can be created and assigned through the IGEL UMS Web App. For details, see [How to Use Template Profiles in IGEL UMS Web App](#).

Profile Information in Device Configurator

In the Device Configurator, a tooltip shows which profile defines the given parameter. For details, see [How to Check which Profiles Define Parameters in the IGEL UMS Web App](#).

Information on Parameter Use in Registry

Pages that contain the same parameter are listed and linked under the registry parameter. For details, see [Registry in IGEL OS 12](#).

Case Sensitive Search

A parameter is added to enable/disable case sensitivity in searches. For details, see [Search for Devices in the IGEL UMS Web App](#).

IGEL Community Video - UMS 12.04.100 – What's New



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

<https://www.youtube.com/watch?v=GveZVrw8-dY>

Overview of the IGEL UMS

With the IGEL Universal Management Suite (UMS), you can remotely configure and control IGEL OS devices. For an overview of devices supported by the IGEL UMS, see Devices Supported by IGEL Universal Management Suite (UMS).

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

Typical Areas of Use of the IGEL UMS

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

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.

Access independent of the operating system:

The UMS Console runs on any device with the Java Runtime Environment. The UMS Web App can be opened on any supported browser.

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:

If you configure default directory rules, IGEL OS devices can be automatically placed in a required directory, e.g. on the basis of the relevant subnet. The devices will automatically receive the configuration settings that you have defined for this directory.

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 device screens, enabling them to rapidly identify problems and demonstrate solutions directly to users.

IGEL UMS Components

The IGEL Universal Management Suite (UMS) comprises the following components:

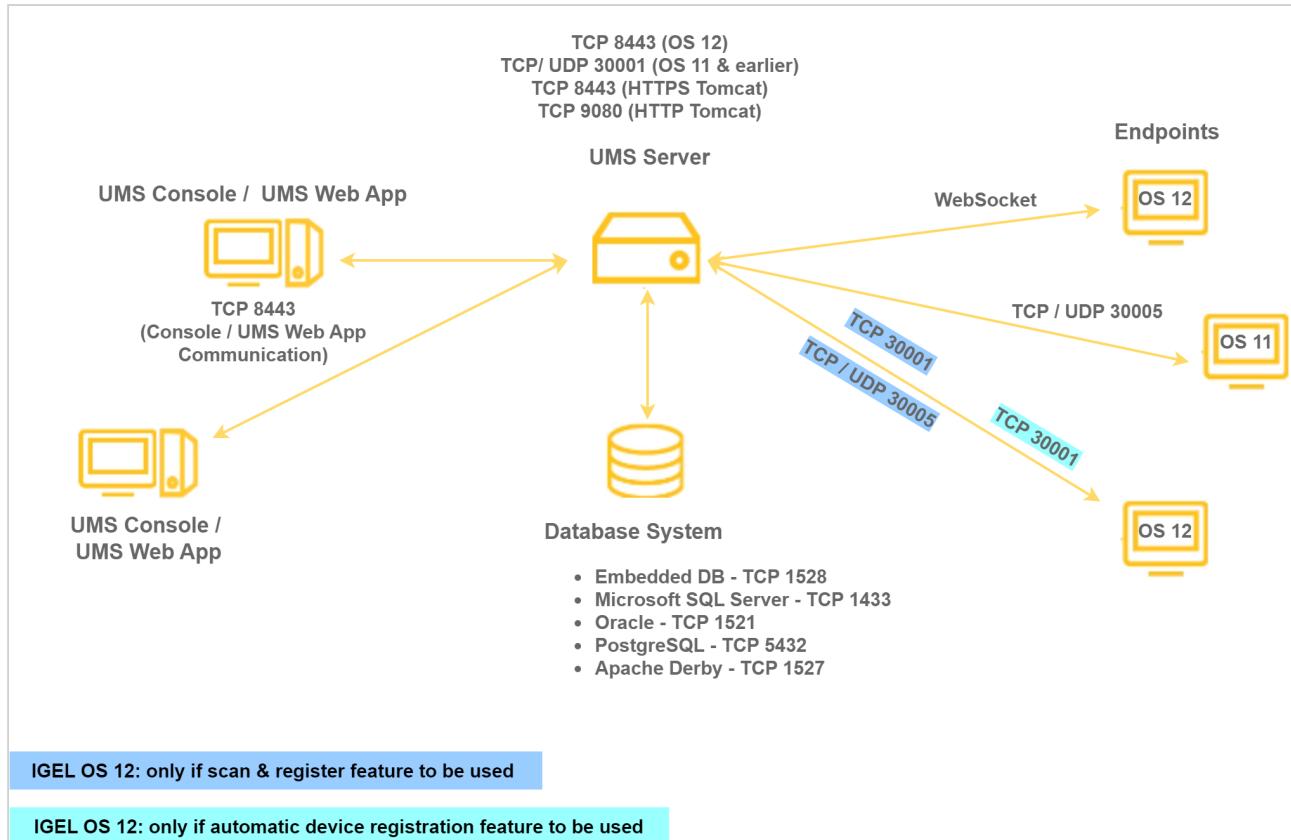
- UMS Server
- UMS Administrator
- UMS Console / UMS Web App

UMS Server

The UMS Server is a server application which requires a database management system (RDBMS). The database can be installed on the server itself or on a remote host. Detailed information on the supported environment can be found in the release notes. See also [Installation Requirements for the IGEL UMS \(see page 17\)](#).

Typically, the UMS Console and UMS Server are installed on different computers.

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



Data transmission between the UMS Server and devices as well as between the UMS Server and UMS Console / UMS Web App is encrypted.

For communication with IGEL OS 11 devices, there are two protocols running on separate communication ports (30001 and 30005) – one for devices to communicate with the UMS and another for the UMS to communicate with the device. With the introduction of IGEL Cloud Services, also the Unified Protocol has been introduced. The Unified Protocol is used for all communication between the UMS and OS 12 devices. This single path of communication is now accomplished with a WebSocket connection, enabling persistent, bi-directional, full-duplex TCP connectivity between UMS 12 and OS 12 devices. Using a WebSocket connection makes it possible to reduce network traffic due to the compression of commands, increase security by using client certificates and security tokens for device onboarding, and introduce a new Device Connector service on the UMS and IGEL Cloud Gateways that prepares your IGEL environment for future cloud capabilities. For more information on ports, see [IGEL UMS Communication Ports](#).

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)
- Database configuration (data sources, backups)

Further information regarding the UMS Administrator can be found under [The IGEL UMS Administrator \(see page 550\)](#).

UMS Console / UMS Web App

The IGEL OS devices and their configuration are administered via the GUI of the UMS Console and the UMS Web App.

The key tasks of the UMS Console and the UMS Web App are as follows:

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

UMS Console

The UMS Console is the Java-based user interface to the UMS Server. You will find detailed information regarding the UMS Console under [UMS Console User Interface \(see page 182\)](#).

For how to log in to the UMS Console, see [Connecting the UMS Console to the IGEL UMS Server \(see page 162\)](#).

UMS Web App

The UMS Web App is a web-based user interface to the UMS Server. For detailed information about the application, see [IGEL UMS Web App](#). For how to connect to the UMS Web App, see [How to Log In to the IGEL UMS Web App](#).

⚠ The UMS Web App can currently be used only in addition to the UMS Console. Some features are currently available only in the UMS Web App (e.g. creating profiles for IGEL OS 12 devices, managing IGEL OS Apps), others – only in the UMS Console (e.g. scheduled jobs, user permissions and access control). See the feature matrix below.

Feature Matrix: UMS Web App vs. UMS Console

Configuration Dialog, Profiles, Assignments, and Apps

		UMS Console	UMS Web App
Edit configuration	OS 12 devices	✓	✓
Assignments	IGEL OS 12 devices	✓	✓
Profiles	IGEL OS 12 devices	✓	✓

	OS 11 devices	✓	✓
Create and edit profiles	OS 12 devices	✗	✓
	OS 11 devices	✓	✓
Copy profiles	OS 12 devices	✗	✗
	OS 11 devices	✓	✗
Delete profiles		✓	✗
Manage assignments		✓	✓
Manage IGEL OS Apps		✗	✓
Export devices as profiles	OS 12 devices	✗	✓
Import devices as profiles ("Import profiles" in the UMS Web App)	OS 11 devices	✓	✗
	OS 12 devices	✗	✓
Export/Import profiles	OS 11 devices	✓	✗
Export/Upload IGEL OS Apps		✗	✓

Device Commands

	UMS Console	UMS Web App
Shadowing	✓	✓
Secure terminal	✓	✗
Power control commands	✓	✓
Synchronization commands	✓	✓
Reset to factory defaults	✓	✓
Extended commands	✓	✗

Device commands available in the UMS Console can be found under [Menu Bar of the IGEL UMS Console](#) (see page 185).

For the detailed list of device commands available in the UMS Web App, see [Devices - View and Manage Your Endpoint Devices](#) in the IGEL UMS Web App.

Extended Management

	UMS Console	UMS Web App

Delete devices	✓	✗
Scan for devices and register	✓	✓
Views (= "Search" in the UMS Web App)	✓	✓
Jobs	✓	✗
Administrative tasks	✓	✗
URL-file management	✓	✓
Recycle Bin	✓	✗
User permissions and access control	✓	✗
UMS Administration (Manage UMS Network & Global Configuration settings)	✓	✗

Logs and Support Information

	UMS Console	UMS Web App
View logs of the UMS Web App	✗	✓
View logs of the UMS Console	✓	✓ (partly)
Enable logging	✓	✓
Delete logs	✓	✓
Save support information	✓	✗
Save device files for support	✓	✗

Search

	UMS Console	UMS Web App
Search for devices	✓	✓
Search for views	✓	✗
Search for profiles	✓	✗
Export search results	✓	✓

UMS Installation and Update

In this chapter, you can find information on the following topics:

- Basics of IGEL Universal Management Suite (UMS) installation types and their use cases: [IGEL UMS Installation \(see page 13\)](#)
- Software and hardware requirements to install UMS components: [Installation Requirements for the IGEL UMS \(see page 17\)](#)
- Guidelines and recommendations for setting up your UMS environment: [Installation and Sizing Guidelines for IGEL UMS \(see page 63\)](#)

You can find detailed instructions to perform the following:

- Installation of the standard UMS with embedded database: [IGEL UMS Installation under Linux \(see page 20\)](#) and [IGEL UMS Installation under Windows \(see page 50\)](#)
- [Installing the Distributed IGEL UMS \(see page 59\)](#)
- [IGEL UMS Update \(see page 88\)](#)
- [Connecting External Database Systems to UMS \(see page 98\)](#)

 Further information on specific topics can be found in the articles under UMS Installation and UMS Environment.

IGEL UMS Installation

This article describes possible installation options for the IGEL Universal Management Suite (UMS) and it provides general installation recommendations and instructions. For further guidelines about the UMS environment, see [Installation and Sizing Guidelines for IGEL UMS \(see page 63\)](#).

A UMS installation can consist of a single UMS Server instance or multiple UMS Servers.

In a single-instance installation (also called "**standard UMS**"), only one UMS Server performs all tasks and is the single access point for the endpoint devices.

A multi-instance installation has several UMS Servers – each can perform all tasks, but some tasks are distributed across the UMS Servers. The endpoint devices can connect to any of the UMS Servers and are not fixed to them. Multi-instance installations require messaging between the components to support organizational tasks. The IGEL UMS supports two realizations of multi-instance installations:

- **Distributed UMS**

In a Distributed UMS installation, all UMS Servers are installed as standalone servers, but with the Distributed UMS feature enabled, these UMS Servers work just as if they were installed as a High Availability environment. Messages between the UMS Servers use the database bridge: With this, all core features of distributed tasks are available.

A Distributed UMS installation has the following requirements:

- Common external database
- 8443/TCP for WebDav file exchange

Characteristic features: Cross-subnet communication and installation in cloud environments like Azure / AWS are possible. For load distribution, DNS-Round-Robin load balancing of the server IP address should be used since IGEL UMS Load Balancers are not supported. The DNS-Round-Robin for `igelrmserver` should point to all servers.

- i** Alternatively, you can use a reverse proxy / external load balancer for load distribution as of UMS 12; the FQDN and port of the external load balancer / reverse proxy must be specified as a Cluster Address, see [Server Network Settings in the IGEL UMS \(see page 420\)](#).

Note the following:

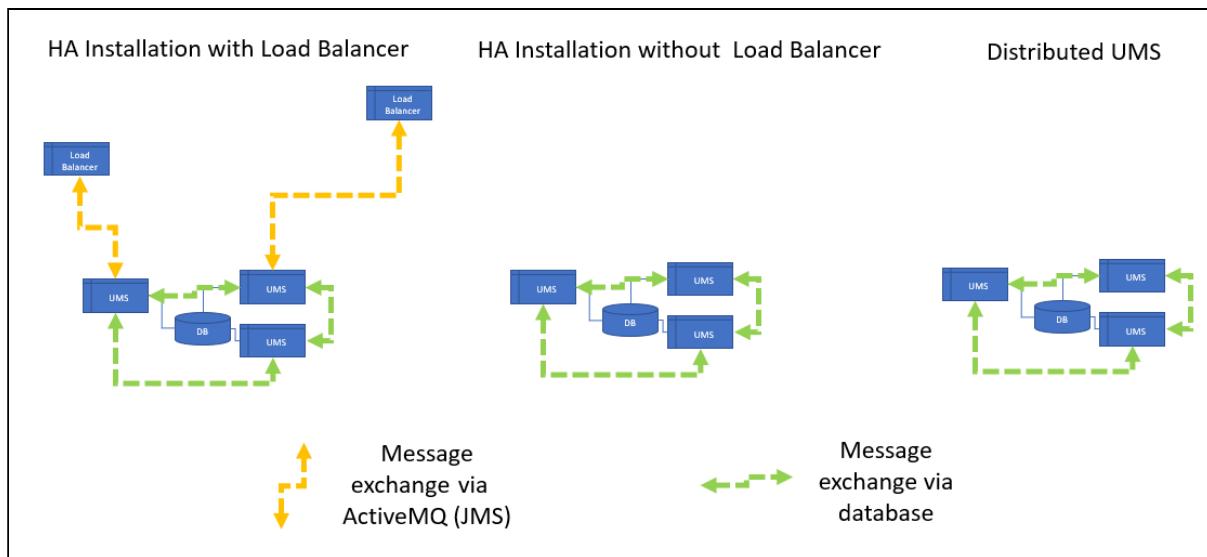
- The Cluster Address is only for communication via the [web server port \(see page 552\)](#) (default: 8443).
- SSL can be terminated at the reverse proxy / external load balancer (see NGINX: Example Configuration for as Reverse Proxy in IGEL OS with SSL Offloading) or at the UMS Server.

- **UMS High Availability (HA) Extension**

The UMS HA provides all features from the Distributed UMS but comes with the possibility to install UMS Load Balancers. Communication between the components of the UMS HA installation, i.e. UMS Servers, UMS Load Balancers, is possible due to the use of the same IGEL network token.

As of UMS version 6.10 (no matter if it is an HA installation with UMS Load Balancers or without), messages between the UMS Servers use the database bridge, and not ActiveMQ like on earlier UMS versions. Nevertheless, ActiveMQ messaging still remains active: on HA installations without Load Balancers, it is active only in the background; on HA installations with UMS Load Balancers, ActiveMQ messaging is, however, further used for the message exchange with Load Balancers, and exactly this poses restrictions on the cross-subnet communication and possibility to install UMS HA with Load Balancers in cloud environments. For further information on messaging, see UMS HA Health Check - Analyse Your IGEL UMS High Availability and Distributed UMS Systems.

More on message exchange...



A UMS HA installation has the following requirements:

- Common external database
- 8443/TCP for WebDav file exchange
- For HA installations with IGEL UMS Load Balancers: 6155/UDP, 61616/TCP ActiveMQ messaging. For the list of the UMS ports, see IGEL UMS Communication Ports.

Characteristic features of HA installations with IGEL UMS Load Balancers: All UMS Servers and UMS Load Balancers must reside on the same VLAN; there is no support for cloud environments like Azure / AWS.



Cross-subnet Communication for UMS HA Installations without UMS Load Balancers

Existing UMS HA installations without UMS Load Balancers can be further used – there is no need to reinstall them as Distributed UMS. UMS Server communication over subnets will automatically be possible when you update to UMS 6.10 or higher.

There is no need for reinstallation also because a UMS HA without Load Balancers operates essentially as the Distributed UMS - both are identical in terms of the synchronization of files, firmware, certificates, licenses, and jobs; both use the database bridge for the message exchange.

How to Choose between the Standard UMS, Distributed UMS, and UMS High Availability

General Installation Recommendations

For small installations, a single UMS Server instance (standard UMS) with an embedded database is usually sufficient. If required, a single-instance installation can be easily extended anytime to a Distributed UMS installation by installing additional servers (and in the case of an embedded database, by switching preliminarily to an external data source).

Large installations should use either the UMS High Availability or the Distributed UMS (preferable for new installations, e.g. because you do not have to configure additional firewall exclusions). For large installations, it is also recommended to use DNS-Round-Robin load balancing or IGEL Cloud Gateway.

See also [Installation and Sizing Guidelines for IGEL UMS](#) (see page 63).

- You are an **existing customer** and have a single-instance UMS installation but want to run additional UMS Servers...
=> Install UMS 12.01 or higher ("standard UMS" in the UMS installer) on the first server and enable the Distributed UMS feature. After that, you can install additional servers (as Distributed UMS) and connect them to the same database (NOT embedded database).
- You are an **existing customer** and have the UMS High Availability installed...
=> Install UMS 12.01 or higher (UMS High Availability Network components in the UMS installer; see Updating the Installation of an HA Network) and leave everything as it is.
- You are a **new customer** and want a single-instance UMS installation...
=> Install standard UMS 12.01 or higher.
- You are a **new customer** and want to run the UMS with multiple servers, but you do not need IGEL UMS Load Balancers because you deploy DNS-Round-Robin load balancing...
=> Install UMS 12.01 or higher ("Distributed UMS" in the UMS installer) on the first server. After that, you can install the other servers, also as Distributed UMS, and connect them to the same database (NOT embedded database).
- You are a **new customer** and want to run the UMS with multiple servers and to use the IGEL UMS Load Balancers...
=> Install UMS 12.01 or higher as High Availability with Load Balancers. But first, ask IGEL if it would be better to refrain from deploying IGEL UMS Load Balancers because they may be not optimal for large installations. For management of devices outside the company network, use also IGEL Cloud Gateway.
- You are a **new customer** and want the UMS with multiple servers in the cloud...
=> Install UMS 12.01 or higher ("Distributed UMS" in the UMS installer) on the first server. After that, you can install the other servers, also as Distributed UMS, and connect them to the same database (NOT embedded database).

How to Install the IGEL UMS



- For the management of the UMS installation, you require the UMS Console. In multi-instance installations, the UMS Console does not necessarily have to be installed on every UMS Server.
Note: For security, performance, or other reasons, the UMS Console is often additionally installed on a separate host.
- You cannot manage IGEL OS 12 devices without the UMS Web App. Thus, the UMS Web App must be selected during the installation of the UMS. In multi-instance installations, the UMS Web App does not necessarily have to be installed on every UMS Server, see [Important Information for the IGEL UMS Web App](#).
- The UMS Administrator application, which is necessary for the management of the UMS installation, will be automatically installed during the installation of the UMS Server.

For information on the UMS components, see [Overview of the IGEL UMS](#) (see page 6).

Standard UMS

If you decided on a single-instance UMS installation, see the following articles. They describe the complete procedure for installing the standard UMS with an embedded database. If your required installation differs, you can select individual components, e.g. for an individual console installation.

- [IGEL UMS Installation under Linux](#) (see page 20)
- [IGEL UMS Installation under Windows](#) (see page 50)

Distributed UMS

If you want to install the Distributed UMS or extend your existing standard UMS installation to the Distributed UMS, see [Installing the Distributed IGEL UMS](#) (see page 59).

UMS High Availability

If you want to install the UMS HA Extension, see [HA Installation](#).

Installation Requirements for the IGEL UMS

This article lists the minimum requirements your hardware and software must meet to successfully install the components of the IGEL Universal Management Suite (UMS) environment. For details on the IGEL UMS components, see [Overview of the IGEL UMS](#) (see page 6).

System 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.

Standard UMS Installation Requirements

UMS Server and UMS Administrator

Standard UMS means that you have a single UMS Server. To host the **UMS Server** and the **UMS Administrator**, your hardware and software must meet the following minimum requirements:

- At least 5 GB of RAM
- At least 22 GB of free disk space
- 4 CPUs

- ⓘ 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.

- ⚠
 - 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 not recommended.

Installation Requirements of UMS Components

You can decide to install other UMS components on the same host as the UMS Server and UMS Administrator. In this case, the components have the following minimum requirements:

- **UMS Web App**
 - At least 1 GB of RAM

- **UMS Console**
 - At least 3 GB of RAM
 - At least 1 GB of free disk space
- **Embedded Database**
 - At least 2 GB of free disk space

Standard UMS With UMS Console and Embedded Database

Installation requirements in total for a Standard UMS with UMS Console and Embedded Database:

- At least 8 GB of RAM
(5 GB for UMS Server and UMS Administrator + 3 GB for UMS Console)
- At least 25 GB of free disk space
(22 GB for UMS Server and UMS Administrator + 1 GB for UMS Console + 2 GB for Embedded DB)
- 4 CPUs

Standard UMS With UMS Console, Embedded Database, and UMS Web App

Installation requirements in total for a Standard UMS with UMS Console, Embedded Database, and UMS Web App:

- At least 9 GB of RAM
(5 GB for UMS Server and UMS Administrator + 3 GB for UMS Console + 1 GB for UMS Web App)
- At least 25 GB of free disk space
(22 GB for UMS Server and UMS Administrator + 1 GB for UMS Console + 2 GB for Embedded DB)
- 4 CPUs

Standalone UMS Console Requirements

To install a standalone UMS Console on a separate host machine, your hardware and software must meet the following minimum requirements:

- At least 3 GB of RAM
- At least 1 GB of free disk space
- 2 CPUs

Database Systems (DBMS) Requirements

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

High Availability Requirements

The High Availability (HA) extension is designed to address the needs of large environments by implementing a network of several UMS Servers. For details on HA, see [High Availability](#).

For installation requirements, see [Installation Requirements](#).

- ⓘ 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.

- ⚠ High Availability with IGEL UMS Load Balancers: All UMS Servers and UMS Load Balancers must reside on **the same VLAN**.

For High Availability (UMS HA) with IGEL UMS Load Balancers, network traffic must be allowed over UDP broadcast port 6155, and TCP traffic and UDP broadcast traffic over port 61616. For further port configuration, see [IGEL UMS Communication Ports](#).

Note: IGEL UMS HA installation with IGEL UMS Load Balancers is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks. The HA installation without IGEL UMS Load Balancers (as well as the [Distributed UMS](#) (see page 13)) is, however, supported in cloud environments as of UMS version 6.10.

IGEL UMS Installation under Linux

This article describes the complete procedure for installing the standard IGEL Universal Management Suite (UMS) with an embedded database under Linux. If your required installation differs, you can select individual components, e.g. for a standalone UMS Console installation. You can check the installation requirements under [Installation Requirements for the IGEL UMS](#) (see page 17).

-  For the supported operating systems, see the "Supported Environment" section of the release notes.

The procedure for installing the IGEL UMS under Linux is as follows:

1. Download the current version of the IGEL Universal Management Suite from the [IGEL Download Server](#)².

-  For integrity and security purposes, it is recommended to verify the checksum of the downloaded software.



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 installation file is executable. If not, it can be made executable with the following command:

```
chmod u+x setup*.bin
```

-  You will need `root / sudo` rights to carry out the installation.

² <https://www.igel.com/software-downloads/>

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 included Java Virtual Machine, and removes the temporary files once the installation has been completed.

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. Under **Destination directory**, select the directory in which the UMS is to be installed. (Default: `/opt/IGEL/RemoteManager`)
8. If you are updating an existing UMS installation: Under **Database backup**, select a file for the backup of the embedded database. If you have already created a backup, you can select **No (continue)** in order to skip this step. See also [Updating the IGEL UMS under Linux](#) (see page 90).

For Update Installations Only

- As of UMS 12, MDM feature is no longer available. Cancel the upgrade to UMS 12 if you still need the MDM feature:



- Only if you have a Distributed UMS installation: During the update installation, it will be checked whether only one UMS Server is running and the others are stopped. If not, stop all UMS Servers except one and proceed with the update; otherwise, you risk losing data. After the update on this server is complete, you can update the remaining UMS Servers, either simultaneously or one after another.

9. Under **Installation type**, select the scope of installation:

- Complete:** UMS Server and UMS Console
- Distributed UMS:** [Distributed UMS installation](#) (see page 13)
- HA Net:** High Availability configuration

- **Client only:** UMS Console only

10. Choose whether the **IGEL UMS Web App** should be installed. See [Important Information for the IGEL UMS Web App](#).

11. Confirm the **system requirements** dialog if your system fulfills them.

12. Under **Confirm server IP address**, confirm or enter the IP address of the UMS Server. This IP address will be used for the creation of the UMS Server certificate on the initial startup. This dialog is shown only on the first installation of a UMS version that includes this feature.

⚠ If you do not adjust the IP address during the installation of the UMS, the web certificate of your UMS Server will contain the wrong IP, which results in problems with device registration, etc. To solve the issue, a new web certificate will have to be generated. See [Invalid Web Certificate and Errors by Device Registration after the Installation of the IGEL UMS 12 on Linux](#).

13. Under **Data directory**, select the directory in which Universal Firmware Updates and files are to be saved. (Default: /opt/IGEL/RemoteManager)

❗ Files and firmware updates are stored in the `ums_filetransfer` directory. Custom file transfer directories are not supported.

14. Under **Database selection**, select the desired database system.

- **Internal:** The embedded database
- **Other:** An external database server

ⓘ The embedded database is suitable for most purposes. It is included in the standard installation. 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 or the Distributed UMS solution.

For more information regarding the use of the IGEL UMS with external databases, see [Connecting External Database Systems](#) (see page 98).

15. Under **User name**, enter a **user name** and **password** for the database connection.

The credentials for the database connection are created.

ⓘ The user name and password are case-sensitive.

Initially, the credentials entered here are also the credentials of the UMS superuser. After the installation, the credentials for the database user and those for the UMS superuser can be changed independently from each other. For more information about the UMS superuser, see [Changing the UMS Superuser](#) (see page 579).

16. Specify whether you would like to create **shortcuts** for the UMS Console and UMS Administrator on the menu.

17. 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 embedded database will be installed and started.

18. Once the installation procedure is complete, open the UMS Console via the menu or with the command `/opt/IGEL/RemoteManager/RemoteManager.sh`

i It is generally NOT recommended to execute the command `RemoteManager.sh` with `sudo`.
On Red Hat Enterprise Linux 8, `RemoteManager.sh` can be executed only without `sudo`.

19. Connect the UMS Console to the UMS Server by entering the login data for the database that you specified during the installation. For more information, see [Connecting the UMS Console to the IGEL UMS Server \(see page 162\)](#).

To connect to the UMS Web App, see [How to Log In to the IGEL UMS Web App](#).

i It is recommended to check your antivirus software and, if installed, other management software like HP Device Manager for possible conflicts if

- the installation of the IGEL UMS fails
- the UMS Server service does not start when the installation is complete, and the manual start of the service fails. For details on how to start services, see [IGEL UMS HA Services and Processes](#).
- there are problems when connecting the UMS Console to the UMS Server

i **UMS 12 Communication Ports**

If you are going to make network changes, consider the following ports and paths:

- For IGEL OS 12 devices, TCP 8443 `/device-connector/*` is required.
SSL can be terminated at the reverse proxy / external load balancer (see [IGEL UMS Configuration for the External Load Balancer / Reverse Proxy: Example for NGINX with SSL Offloading](#)) or at the UMS Server.
- For importing IGEL OS 12 Apps to the UMS from the IGEL App Portal, the URL <https://app.igel.com/> (TCP 443) is required.
- For the UMS Web App, TCP 8443 `/webapp/*` and `/wums-app/*` are required.
- For the UMS Console, the root is required, i.e. TCP 8443 `/*`
- For IGEL OS 11 devices, TCP 30001 and TCP/UDP 30005 are required.

For more information on UMS ports, see [IGEL UMS Communication Ports](#).

ⓘ **If You Use an External Load Balancer / Reverse Proxy**

The FQDN and port of your external load balancer / reverse proxy must be specified in the UMS Console under **UMS Administration > Global Configuration > Server Network Settings > Cluster Address**. Information on the Cluster Address can be found under [Server Network Settings in the IGEL UMS](#) (see page 420).

ⓘ For the management of IGEL OS 12 devices, it is necessary to register your UMS after the installation, see [Registering the IGEL UMS](#) (see page 164).

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=p52CxtB_0ok

- Preparing Amazon Linux 2 for UMS Installation (see page 25)
- Installing UMS on Red Hat Enterprise Linux (RHEL) 8 (see page 26)
- Installing UMS on Red Hat Enterprise Linux (RHEL) 7.3 (see page 28)
- Installing UMS on Oracle Linux Server (see page 30)
- Installing IGEL UMS on Microsoft Azure (see page 32)

Preparing Amazon Linux 2 for UMS Installation

Overview

You can install the UMS on Amazon Linux 2, both in the cloud and on-premises.

If you want to use the UMS Console or the UMS Administrator on your Amazon Linux 2 machine, you must install and set up the Mate desktop environment. The procedure is described in this article.

Environment

This description is valid for the following environment:

- UMS 6.05 or higher
- Amazon Linux 2, cloud or on-premises

Instructions

1. Log in to Amazon Linux 2 as a user with `sudo` permissions.
2. Update all package repositories:
`sudo yum update`
3. Install the Mate desktop environment:
`sudo amazon-linux-extras install mate-desktop1.x`
4. Go to `/etc/sysconfig/` and create a file named `desktop` with a text editor.
5. Enter the following content into the `desktop` file:
`PREFERRED=/usr/bin/mate-session`
6. Save the file.
7. Go to your home directory and create a file named `.Xclients`
8. Enter the following content into the `.Xclients` file:
`/usr/bin/mate-session`
9. Save the file.
10. Make the `.Xclients` file executable:
`chmod +x ~/.Xclients`

You can now install the UMS; for instructions, see [IGEL UMS Installation under Linux \(see page 20\)](#).

Installing UMS on Red Hat Enterprise Linux (RHEL) 8

You want to install the UMS on the 64-bit version of Red Hat Enterprise Linux (RHEL) 8.

-  The installation of the UMS on RHEL 8 can be done on a plain RHEL 8 system (Server with a GUI).

Before installing the UMS (or UMS HA, see HA Installation), the following steps have to be done:

1. As `root`, update the local package database and reboot the server.

```
# yum -y update
```

The UMS installation will load additional modules if they have not yet been installed: `qt5-qtbase`

2. Set the `TERM` variable as follows, especially if a GUI is installed on the server.

```
# export TERM=xterm
```

3. Make the `/root` directory writable.

By default, the `/root` directory has no write flag set. As the default installation of UMS HA creates the network configuration archive in this directory, this directory must get the write flag for the `root` user.

```
# sudo chmod u+w /root
```

4. Configure the firewall.

RHEL 8 comes with an activated firewall. For the UMS and UMS HA to work properly, the following ports have to be opened in the active profile (see also IGEL UMS Communication Ports):

```
# 8443/tcp 9080/tcp 30001/tcp 30002 tcp 61616/tcp 61616/udp 1528/tcp  
6155/udp
```

To open these ports, the following commands must be executed:

```
# sudo firewall-cmd --zone=public --add-port=8443/tcp --permanent  
# sudo firewall-cmd --zone=public --add-port=9080/tcp --permanent  
# sudo firewall-cmd --zone=public --add-port=30001/tcp --permanent
```

```
# sudo firewall-cmd --zone=public --add-port=30002/tcp --permanent  
# sudo firewall-cmd --zone=public --add-port= 61616/tcp --permanent  
# sudo firewall-cmd --zone=public --add-port= 61616/udp --permanent  
# sudo firewall-cmd --zone=public --add-port= 1528/tcp --permanent  
# sudo firewall-cmd --zone=public --add-port= 6155/udp --permanent
```

5. Proceed with the UMS installation as described in [IGEL UMS Installation under Linux](#) (see page 20).

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 [IGEL UMS Communication Ports](#).
2. Complete the installation as described in [IGEL UMS Installation under Linux \(see page 20\)](#).

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 [IGEL UMS Communication Ports](#).
2. Complete the installation as described in [IGEL UMS Installation under Linux \(see page 20\)](#).

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 [IGEL UMS Communication Ports](#).

5. Complete the installation as described in [IGEL UMS Installation under Linux](#) (see page 20).

-  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 [IGEL UMS Installation under Linux \(see page 20\)](#).

1. Adjust the Oracle Linux Server firewall settings to allow the network ports used by the UMS, see [IGEL UMS Communication Ports](#).
2. Complete the installation as described in [IGEL UMS Installation under Linux \(see page 20\)](#).

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 [IGEL UMS Communication Ports](#).
2. Complete the installation as described in [IGEL UMS Installation under Linux \(see page 20\)](#).

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 [IGEL UMS Communication Ports](#).
5. Complete the installation as described in [IGEL UMS Installation under Linux](#) (see page 20).

Installing IGEL UMS on Microsoft Azure

This article describes a standard IGEL Universal Management Suite (UMS) single server installation (not High Availability) along with IGEL Cloud Gateway (ICG). The database is reachable via Azure or is hosted in Azure.

ⓘ High Availability (HA)

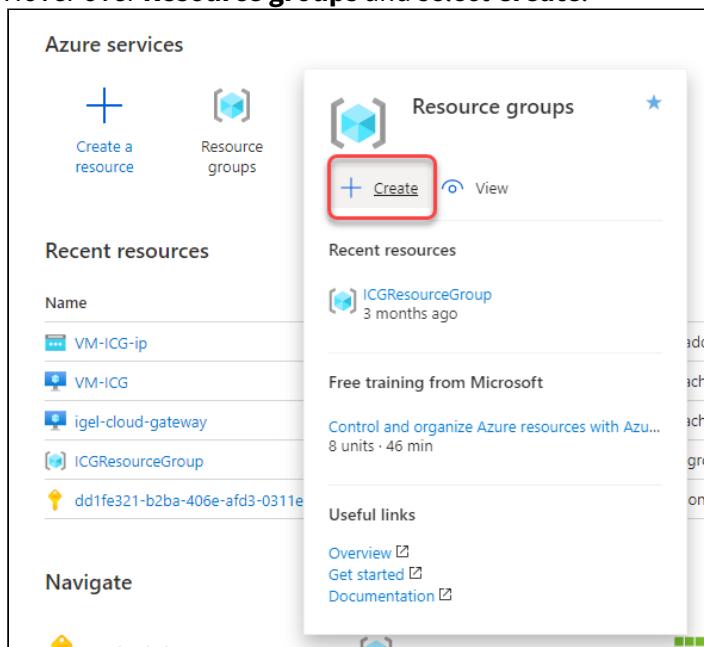
IGEL UMS Server HA is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks.

IGEL Requirements

- Microsoft Azure account
 - UMS 6.07.100 or higher

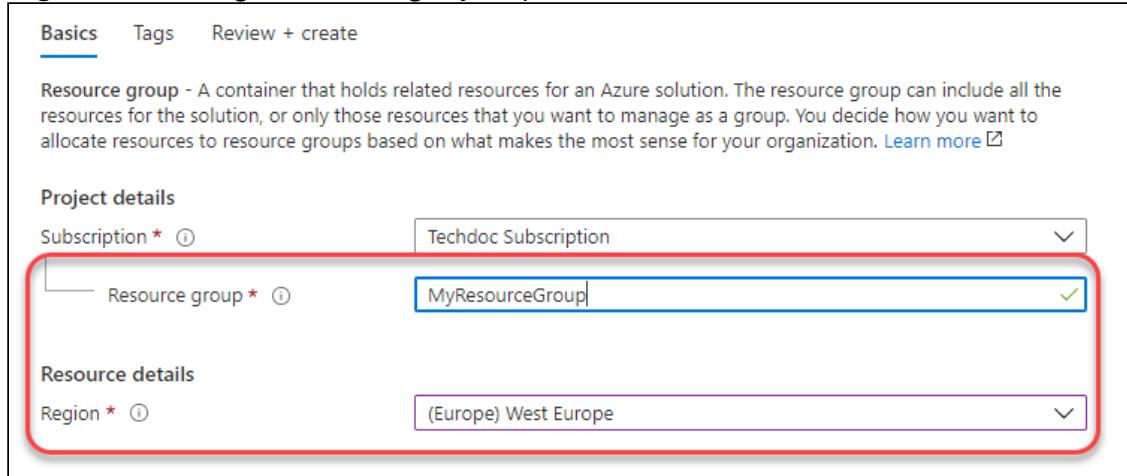
Creating a Virtual Machine for the IGEL UMS

1. Log in to Microsoft Azure.
 2. Hover over **Resource groups** and select **Create**.



3. Edit the data as follows:
 - **Resource group:** Enter a name for the resource group, e.g. "MyResourceGroup".

- **Region:** Select a region, according to your preferences.



Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

Project details

Subscription * ⓘ Techdoc Subscription

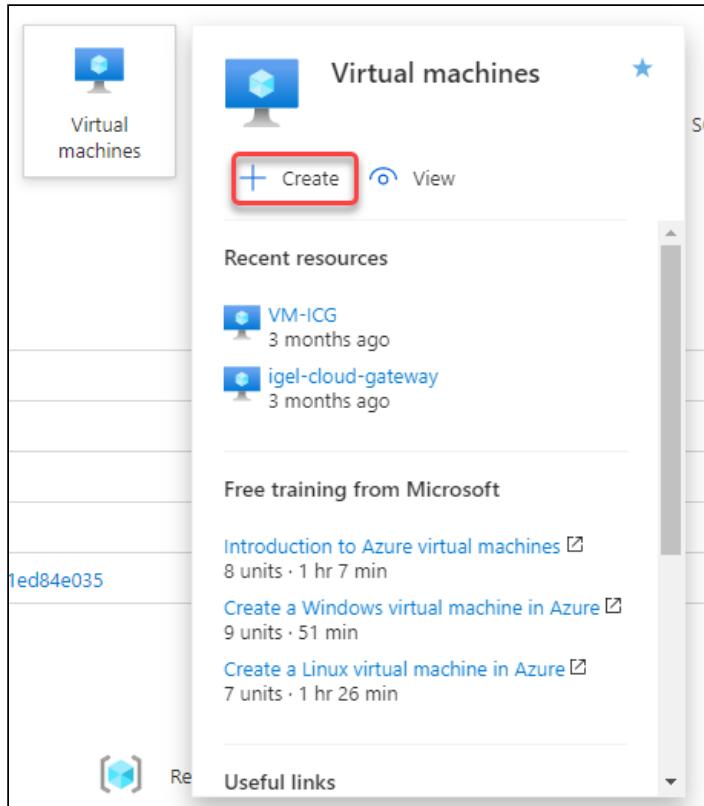
Resource group * ⓘ MyResourceGroup ✓

Resource details

Region * ⓘ (Europe) West Europe

4. Click **Review + create**.
- Your resource group is validated.
5. Click **Create**.
- Your resource group is created.
6. Click **Home** to get to the overview.

7. Hover over **Virtual machines** and select **Create**.



8. Edit the data as follows:

- **Resource group:** Select the resource group you have created before.
- **Virtual machine name:** Enter a name for the virtual machine on which your UMS is to be installed.
- **Image:** Select "Windows Server 2016 Datacenter".
- **Size:** Select the size for your virtual machine. If all components will be running at the same time, we recommend "Standard B4ms" (4cpu/16 GiB). The components and their RAM requirements are as follows:
 - UMS Server: 4 GB
 - UMS Administrator: 2 GB
 - UMS Console: 3 GB
 - UMS Web App: 1 GB
 - Embedded database: 2-3 GB
- **Select inbound ports:** Select "HTTP (80)", "HTTPS (443)", and "RDP (3389)". As an alternative, you can add the ports later on; see [Configuring the Virtual Machine](#) (see page 36).

Subscription * ⓘ Techdoc Subscription

Resource group * ⓘ MyResourceGroup [Create new](#)

Instance details

Virtual machine name * ⓘ MyUmsMachine ✓

Region * ⓘ (Europe) West Europe

Availability options ⓘ Availability zone

Availability zone * ⓘ 1

Image * ⓘ Windows Server 2016 Datacenter - Gen1 [See all images](#)

Azure Spot instance

Size * ⓘ Standard_B4ms - 4 vcpus, 16 GiB memory (\$151.84/month) [See all sizes](#)

Administrator account

Username * ⓘ UmsAdmin ✓

Password * ⓘ ***** ✓

Confirm password * ⓘ ***** ✓

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ Allow selected ports None

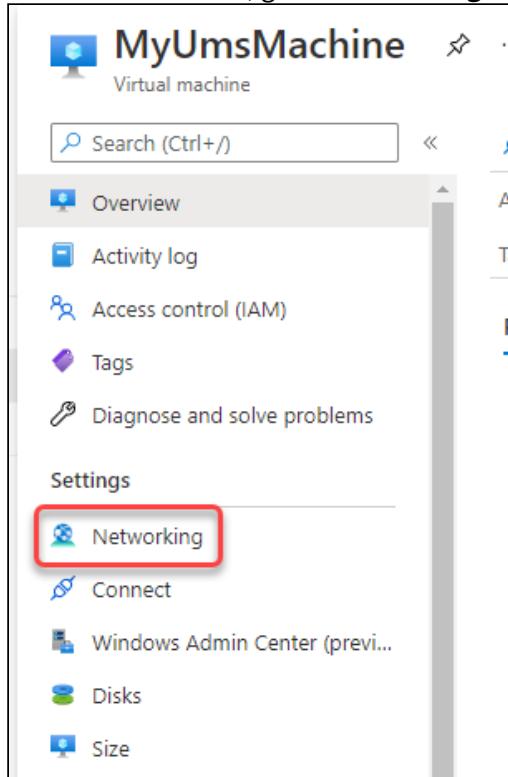
Select inbound ports * ⓘ [HTTP \(80\), HTTPS \(443\), RDP \(3389\)](#)

9. Click **Review + create**.

10. Click **Create**.

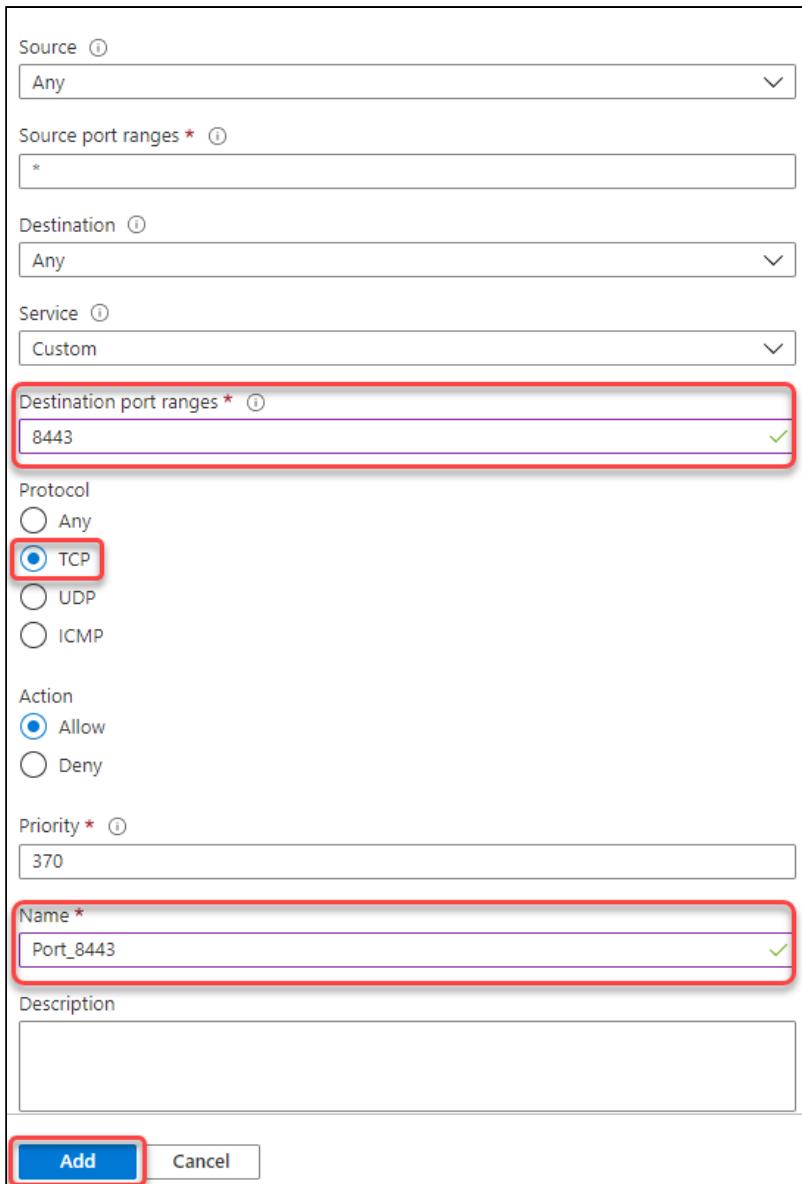
Configuring the Virtual Machine

1. In the sidebar menu, go to **Networking**.



2. Click **Add inbound port rule**.
3. Edit the data as follows:
 - Destination port ranges: Enter "8443".
 - Protocol: Select **TCP**.
 - Name: Change to "Port_8443".

4. Click **Add**.



The screenshot shows the 'Add' configuration dialog for a new rule. The fields are as follows:

- Source:** Any
- Source port ranges:** *
- Destination:** Any
- Service:** Custom
- Destination port ranges:** 8443 (highlighted with a red box)
- Protocol:** TCP (selected, highlighted with a red box)
- Action:** Allow (selected, highlighted with a red box)
- Priority:** 370
- Name:** Port_8443 (highlighted with a red box)
- Description:** (empty)

At the bottom are the **Add** and **Cancel** buttons, with **Add** highlighted with a red box.

 After the installation is complete, do not forget to disable ports 3389 and 22!

5. Select **Outbound port rules**.

Virtual network/subnet: MyResourceGroup-vnet/default NIC Public IP: 51.124.127.0 NIC Private IP: 10.0.1.4 Accelerated networking: Disabled

Inbound port rules	Outbound port rules	Application security groups	Load balancing			
	Network security group MyUmsMachine-nsg (attached to network interface: myumsmachine8) Impacts 0 subnets, 1 network interfaces					
			Add inbound port rule			
Priority	Name	Port	Protocol	Source	Destination	Action
300	▲ RDP	3389	TCP	Any	Any	Allow
320	HTTPS	443	TCP	Any	Any	Allow
340	HTTP	80	TCP	Any	Any	Allow

6. Click **Add outbound port rule**.

7. Using the procedure described in steps 2 and 3, add the following ports:

- 8443 (TCP)
- 22 (TCP)
- Database port: The port that will be used for communication with the database. For more information, see UMS with External Database.
- 443 (TCP)

8. Review your settings.

Inbound port rules **Outbound port rules** Application security groups Load balancing

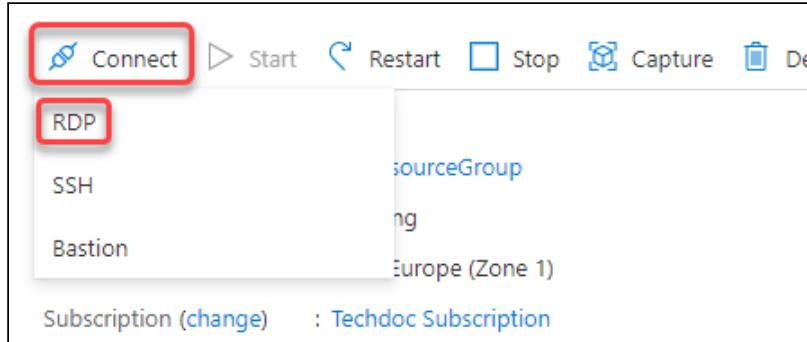
Network security group MyUmsMachine-nsg (attached to network interface: myumsmachine8)
Impacts 0 subnets, 1 network interfaces

Inbound port rules	Outbound port rules	Application security groups	Load balancing			
	Network security group MyUmsMachine-nsg (attached to network interface: myumsmachine8) Impacts 0 subnets, 1 network interfaces					
			Add outbound port rule			
Priority	Name	Port	Protocol	Source	Destination	Action
100	Port_out_8443	8443	TCP	Any	Any	Allow
110	Port_out_22	22	TCP	Any	Any	Allow
120	Port_out_1433	1433	TCP	Any	Any	Allow
130	Port_out_443	443	TCP	Any	Any	Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Installing the IGEL UMS

1. Ensure that your virtual machine is running.

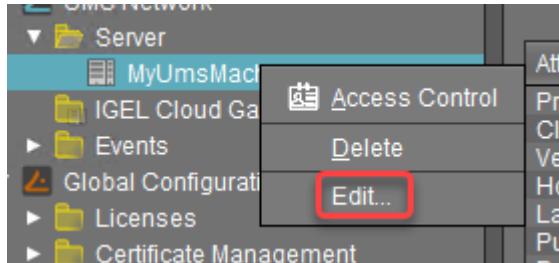
2. Click **Connect** and then select **RDP**.



3. Enter the displayed data in your RDP client or click **Download RDP File** and use the RDP file.
4. With a web browser, download the UMS installer from the [IGEL Download Server³](#) > **UNIVERSAL MANAGEMENT SUITE > WINDOWS**. (Example: `setup-igel-ums-windows_6.07.100.exe`)
5. Install the UMS as described in [IGEL UMS Installation under Windows](#) (see page 50) with the following settings:
 - Activate **Standard UMS**.
 - Activate **with UMS Console**.
 - Deactivate **with Embedded Database** if you are going to use the external database.
 - Deactivate **Only UMS Console**.
 - Activate **UMS Web App**.
6. When the installation is finished, open the UMS Administrator and follow the instructions under [How to Set Up a Data Source in the IGEL UMS Administrator](#) (see page 572).

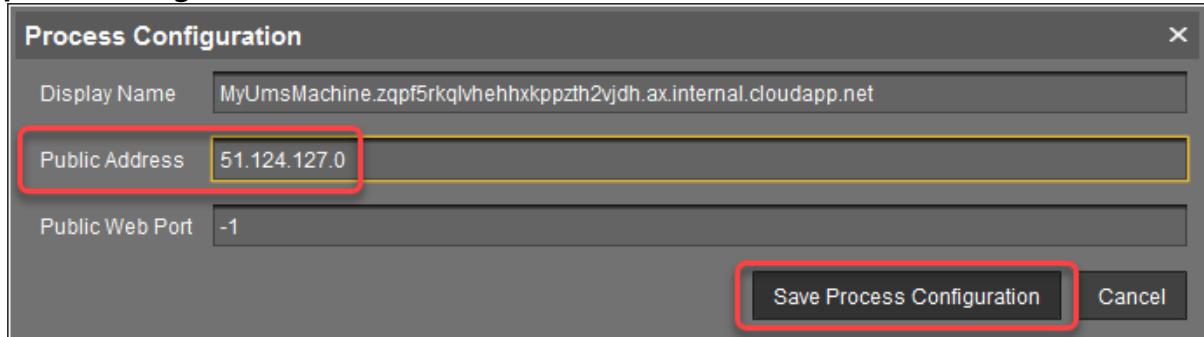
Setting the Public Address on the IGEL UMS Server

1. Start the UMS Console and log in.
2. Go to **UMS Administration > UMS Network > Server**, open the context menu and select **Edit**.



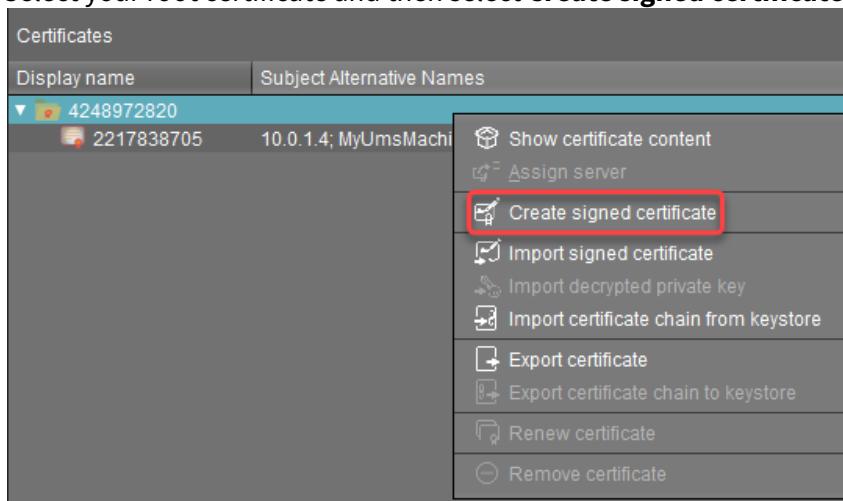
³ <https://www.igel.com/software-downloads/>

3. Enter the public ID of your virtual machine (displayed on the overview page) and click **Save process configuration**.

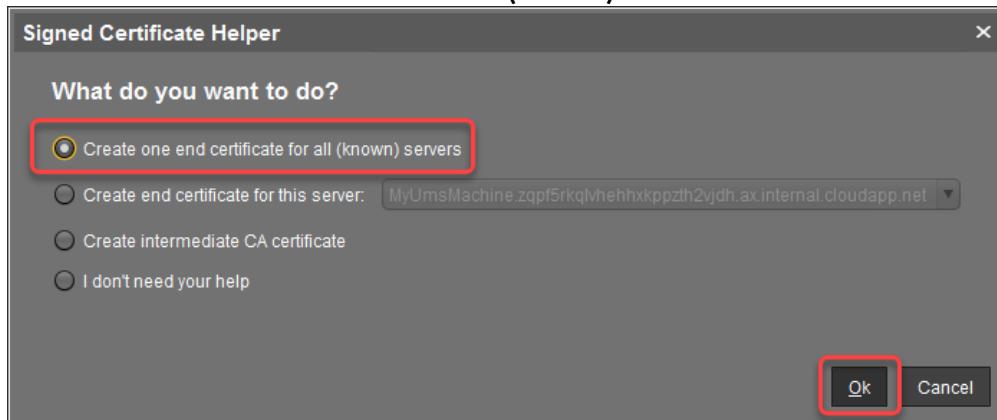


Create Web Certificates

1. In the UMS Console, go to **UMS Administration > Global Configuration > Certificate Management > Web**.
2. Select your root certificate and then select **Create signed certificate** from the context menu.

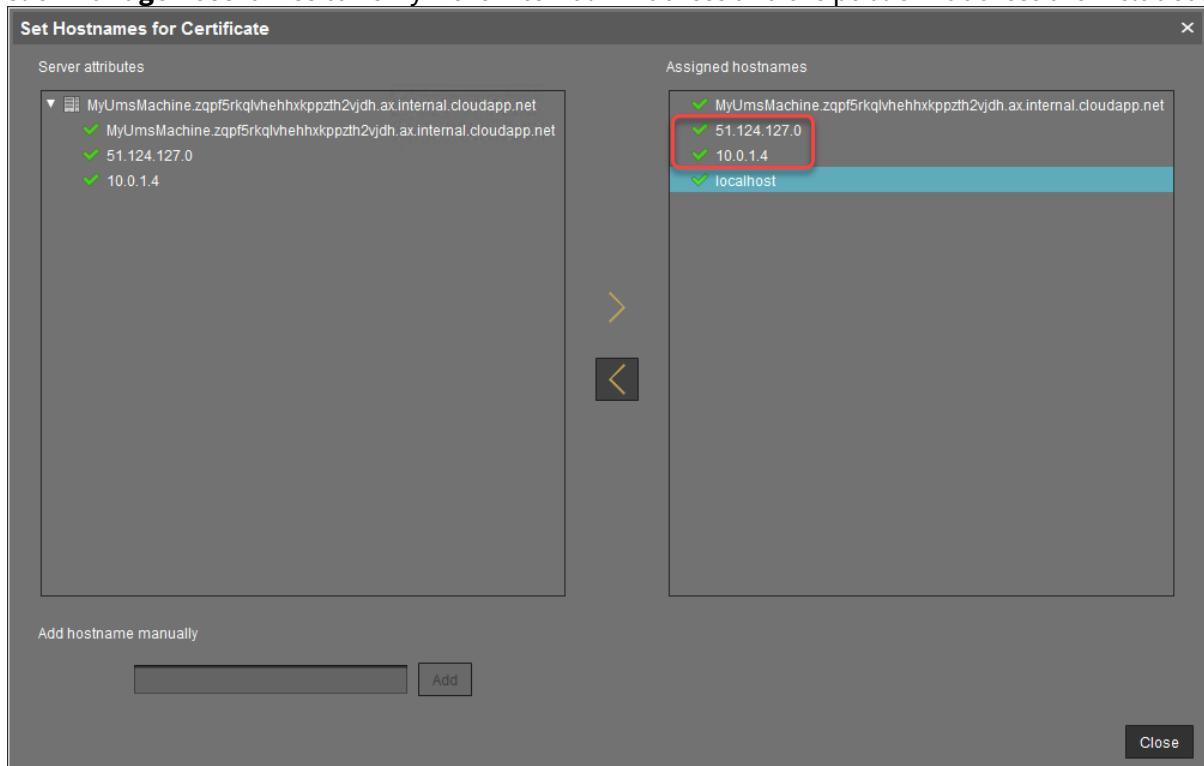


3. Select **Create one end certificate for all (known) servers** and then confirm with **Ok**.

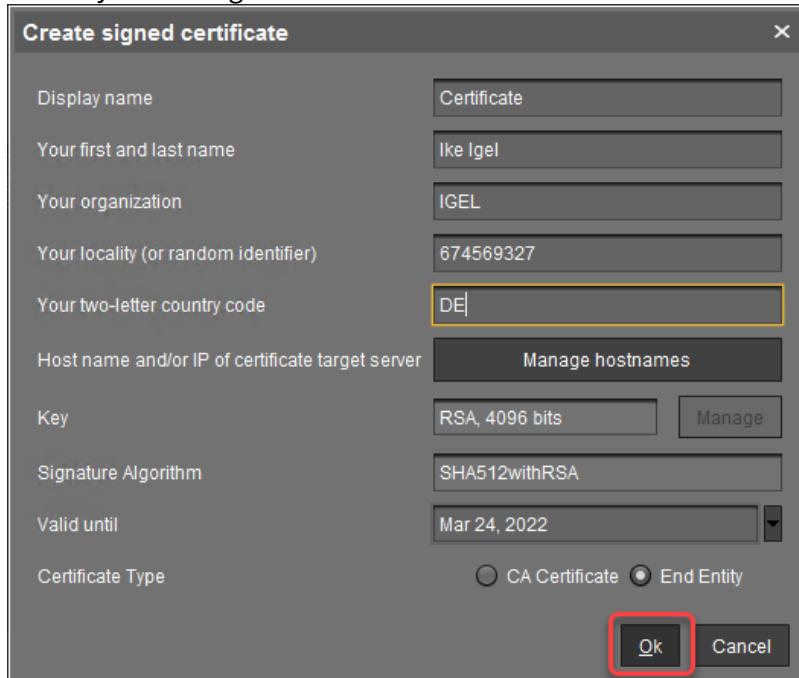


4. Fill in the details as appropriate.

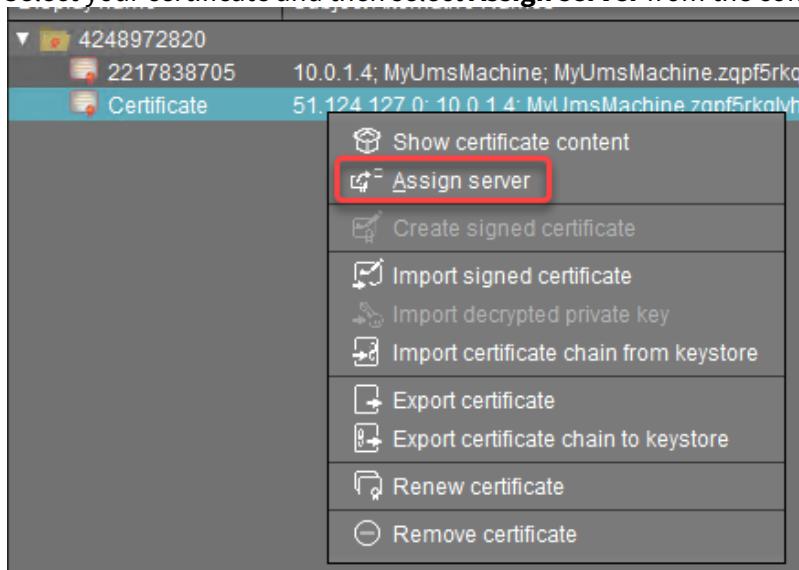
5. Click **Manage hostnames** to verify if the internal IP Address and the public IP address are included.

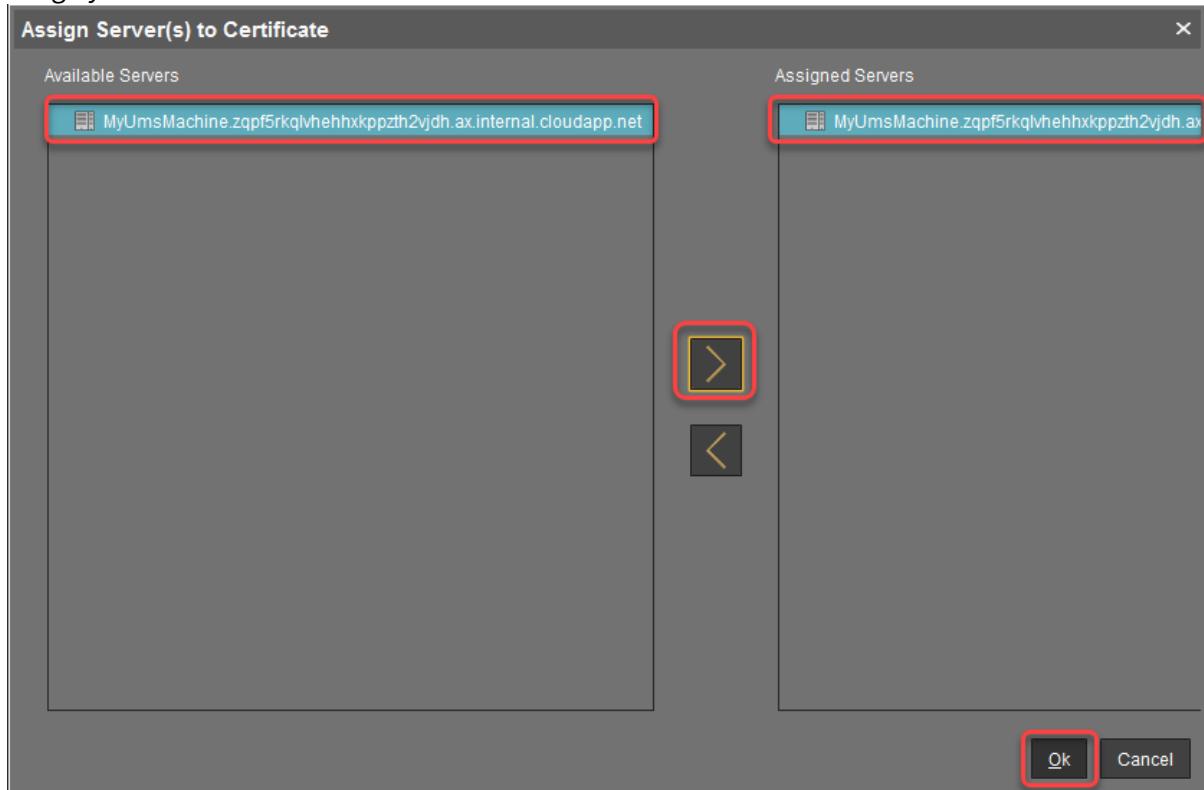
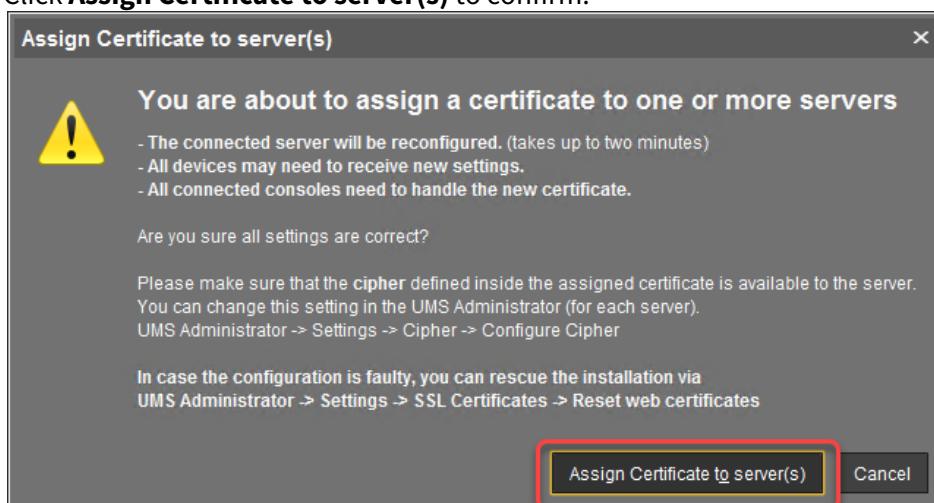


6. Review your settings and click **Ok**.



7. Select your certificate and then select **Assign server** from the context menu.



8. Assign your server to the certificate and confirm with **Ok**.9. Click **Assign Certificate to server(s)** to confirm.

10. Check if the certificate is marked as **Used**.

Display name	Subject Alternative Names	Expiring date	Key Specificati...	Signature	Used	Pr...
4248972820		Mar 24, 2041	RSA (4096 bits)	SHA512withR...	<input checked="" type="checkbox"/>	
2217838705 10.0.1.4; MyUmsMachine; MyUmsMachine.zqpf5rkqlvhehxkppzth2vjdh.ax.internal.cl...		Mar 24, 2022	RSA (4096 bits)	SHA512withR...	<input checked="" type="checkbox"/>	
Certificate 51.124.127.0; 10.0.1.4; MyUmsMachine.zqpf5rkqlvhehxkppzth2vjdh.ax.internal.cl...		Mar 24, 2022	RSA (4096 bits)	SHA512withR...	<input checked="" type="checkbox"/>	

At this point, you can safely connect to your UMS from a local machine as well as from remotely installed UMS Consoles. For clarity purposes, we will still use the UMS Console on Azure.

Downloading the Installer for IGEL Cloud Gateway (ICG)

- With a web browser, download the ICG installer from the [IGEL Download Server⁴](#) > **IGEL CLOUD GATEWAY (ICG)**. (Example: `installer-2.02.110.bin`) You can do this on the virtual machine or use your local machine and then copy the file to your virtual machine via RDP (clipboard).

Creating a Virtual Machine for IGEL Cloud Gateway (ICG)

1. In your Azure portal, go to your resource group (in our example: MyResourceGroup) and add a new **Ubuntu Server 18.04 LTS**.

⁴ <https://www.igel.com/software-downloads/>

2. Edit the settings as follows:

- **Resource group:** This must be set to the resource group we have created before (in our example: MyResourceGroup).
- **Virtual machine name:** Enter a name for the virtual machine.
- **Size:** “D2s v3” (2 CPUs/8 GiB RAM) or higher is recommended.
- **Authentication type:** Select **Password**.
- **Username:** Enter a username for SSH access. This user account will be used for ICG installation by the UMS.

 For security reasons, the username should be long (20 to 30 characters) and cryptic.

 **Username "icg" Is Reserved**

Do not use "icg" as a username for the remote installer; this is the username under which the Tomcat server is running.

- Under **Password** and **Confirm password**, enter a strong password (20 to 30 characters are recommended)

Create a virtual machine

Instance details

Virtual machine name *	MyIcg
Region *	(Europe) Germany West Central
Availability options	Availability zone
Availability zone *	1
Image *	Ubuntu Server 18.04 LTS - Gen1
See all images	
Azure Spot instance	<input type="checkbox"/>
Size *	Standard_D2s_v3 - 2 vcpus, 8 GiB memory (\$83.95/month)
See all sizes	

Administrator account

Authentication type	<input type="radio"/> SSH public key <input checked="" type="radio"/> Password
Username *	cryptic-icg-admin
Password *	*****
Confirm password *	*****

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports *	<input type="radio"/> None <input checked="" type="radio"/> Allow selected ports
Select inbound ports *	SSH (22)
⚠️ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab.	

Review + create < Previous Next : Disks >

3. Click **Review + create** and review the settings.

4. Click **Create**.

5. Click **Go to resource** and note the **Public IP address**.

Essentials	
Resource group (change) :	MyResourceGroup
Status	: Running
Location	: Germany West Central (Zone 1)
Subscription (change)	: Techdoc Subscription
Subscription ID	: dd1fe321-b2ba-406e-af3d-0311ed84e035
Availability zone	: 1
Tags (change)	: Click here to add tags
Operating system	: Linux (ubuntu 18.04)
Size	: Standard D2s v3 (2 vcpus, 8 GiB memory)
Public IP address	20.52.18.90
Virtual network/subnet	: MyResourceGroupvnet118/default
DNS name	: Configure

Configuring the IGEL Cloud Gateway Server

1. In the sidebar menu, go to **Networking**.

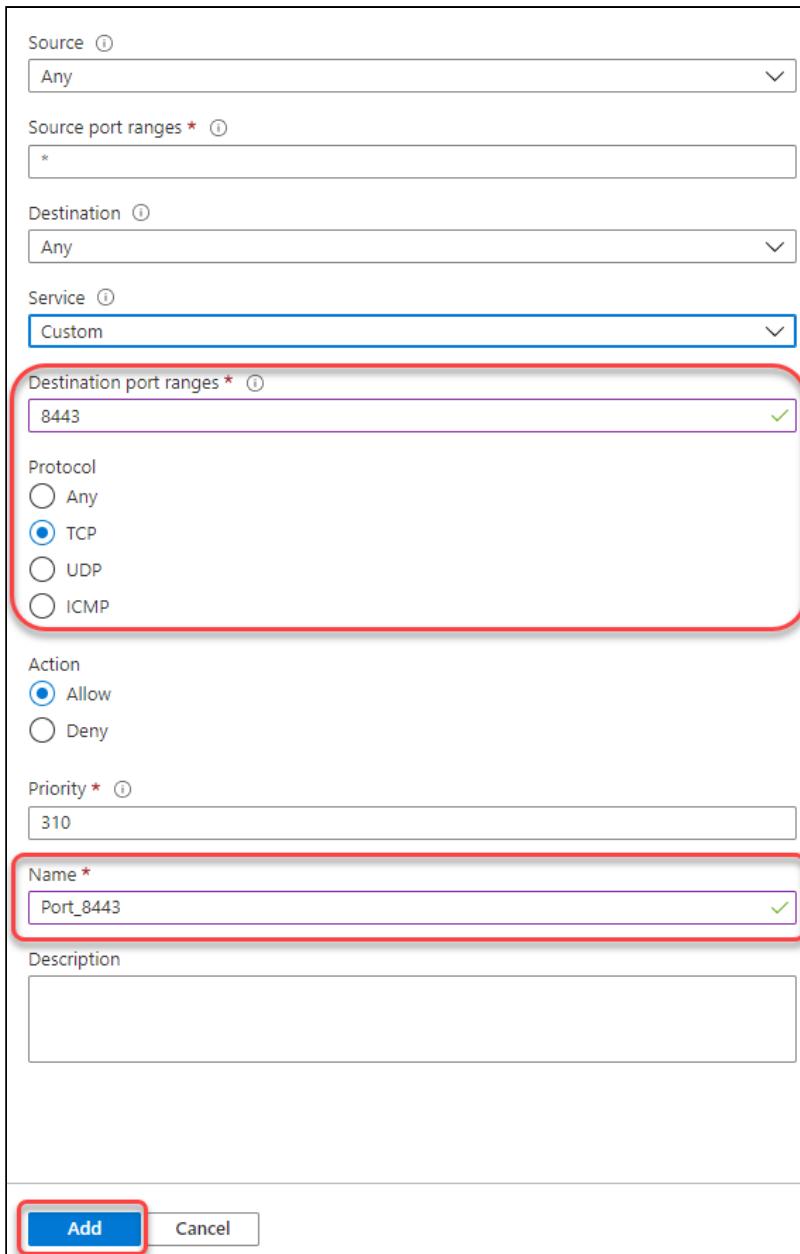
- Mylcg** ⚡ ...
- Virtual machine
- Search (Ctrl+ /)
- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
- Networking**
- Connect
- ...

2. Click **Add inbound port rule**.

3. Edit the data as follows:

- Destination port ranges: Enter "8443".
- Protocol: Select **TCP**.
- Name: Change to "Port_8443".

4. Click **Add**.



The screenshot shows a configuration dialog for adding a new firewall rule. The fields are as follows:

- Source:** Any
- Source port ranges:** *
- Destination:** Any
- Service:** Custom
- Destination port ranges:** 8443 (highlighted with a red box)
- Protocol:** TCP (selected, highlighted with a red box)
- Action:** Allow
- Priority:** 310
- Name:** Port_8443 (highlighted with a red box)
- Description:** (empty)

At the bottom, there are two buttons: **Add** (highlighted with a red box) and **Cancel**.

Installing the IGEL Cloud Gateway

1. Follow the instructions under Providing the Certificates.
2. Follow the instructions under Installing the IGEL Cloud Gateway.

Connecting the Devices

- ▶ Follow the instructions under Connecting the Devices.

IGEL UMS Installation under Windows

This article describes the complete procedure for installing the standard IGEL Universal Management Suite (UMS) with an embedded database under Windows. If your required installation differs, you can select individual components, e.g. for a standalone UMS Console installation. You can check the installation requirements under [Installation Requirements for the IGEL UMS](#) (see page 17).

 For the supported operating systems, see the "Supported Environment" section of the release notes.

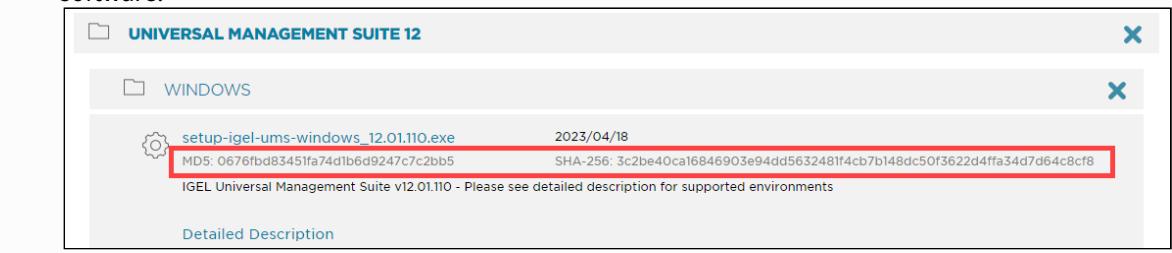
 The Server Core installation option of the Microsoft Windows Server is not supported.

Standard Installation of the UMS

To install the IGEL UMS under Windows, proceed as follows:

1. Download the current version of the IGEL Universal Management Suite from the [IGEL Download Server](#)⁵.

 For integrity and security purposes, it is recommended to verify the checksum of the downloaded software.



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. Only if this is an update installation: 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 the IGEL UMS under Windows](#) (see page 94).

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

i For Update Installations Only

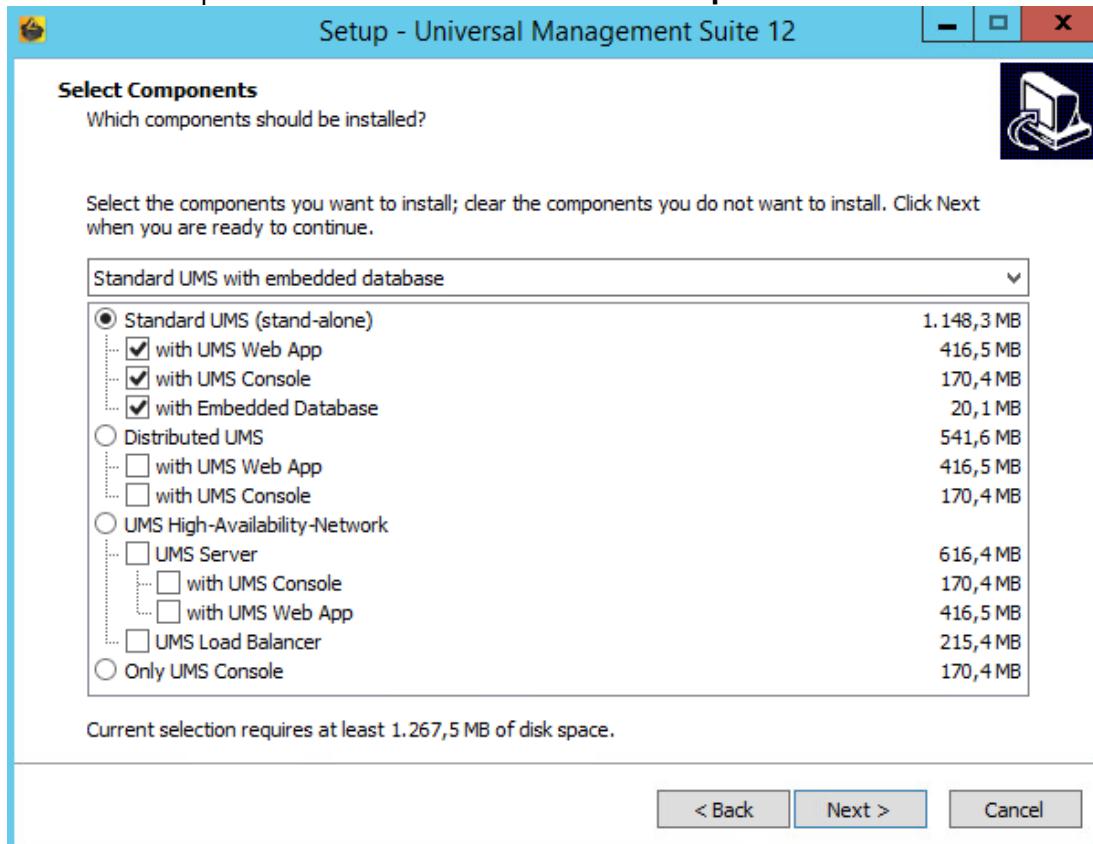
- As of UMS 12, MDM feature is no longer available. Cancel the upgrade to UMS 12 if you still need the MDM feature:



- Only if you have a Distributed UMS installation: During the update installation, it will be checked whether only one UMS Server is running and the others are stopped. If not, stop all UMS Servers except one and proceed with the update; otherwise, you risk losing data. After the update on this server is complete, you can update the remaining UMS Servers, either simultaneously or one after another.

- Only if this is a new installation: Select the folder for the installation under **Select Destination Location**. (Default: C:\Program Files\IGEL\RemoteManager)

7. Choose the components to be installed under **Select Components**.



- **Standard UMS**
 - **with UMS Web App**
 - **with UMS Console**
 - **with Embedded Database**
- **Distributed UMS**
 - **with UMS Web App**
 - **with UMS Console**
- **UMS High Availability Network**
 - **UMS Server**
 - **with UMS Console**
 - **with UMS Web App**
 - **UMS Load Balancer**
- **Only UMS Console**

For information on the UMS installation types, see [IGEL UMS Installation](#) (see page 13).

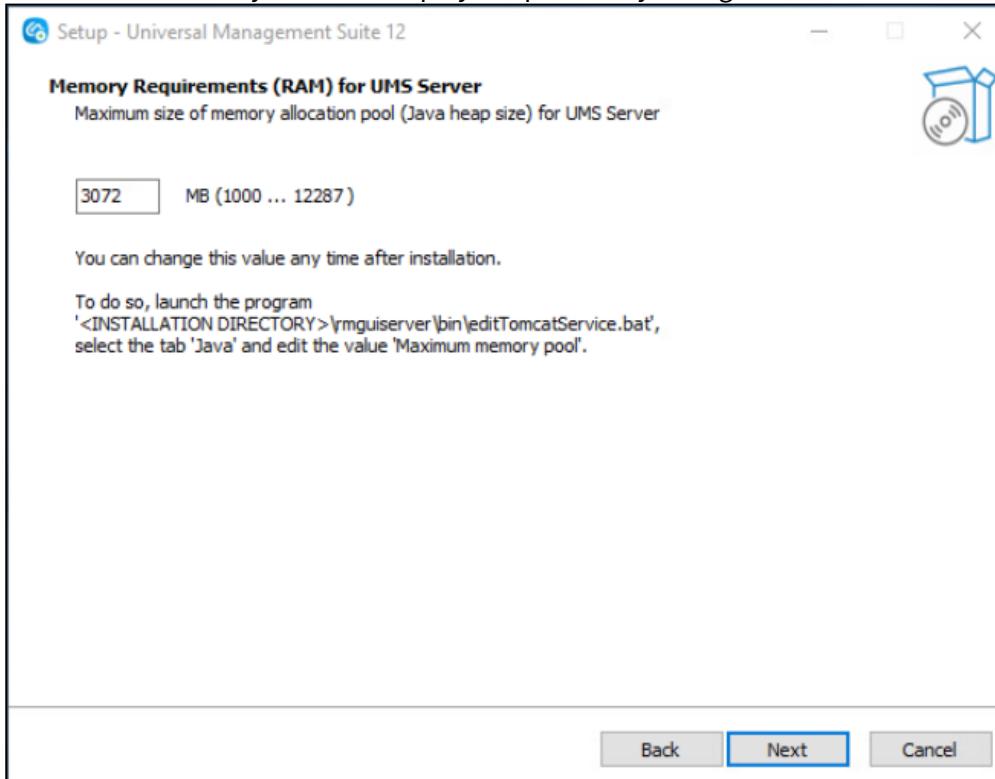
For information on the UMS components, see [Overview of the IGEL UMS](#) (see page 6).

- i** 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:

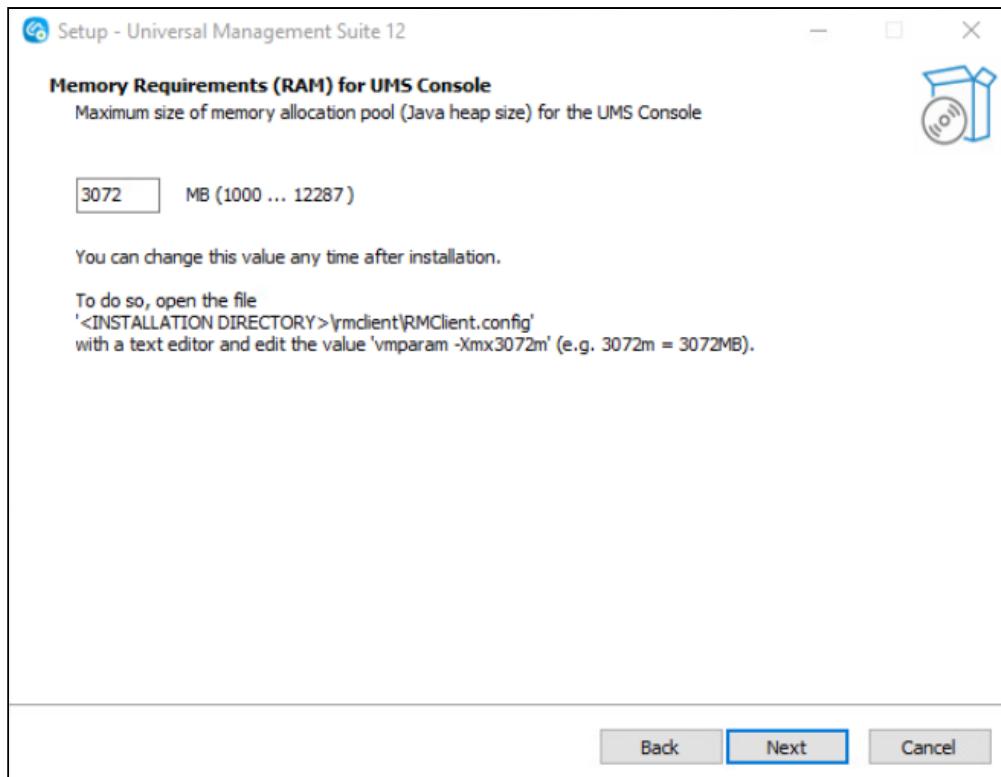
- You manage a large network of devices.
- A dedicated database system is already in use in your company.
- You integrate the High Availability or the Distributed UMS solution.

For more information regarding the use of the IGEL UMS with external databases, see [Connecting External Database Systems](#) (see page 98).

8. Set the maximum memory consumption (Java heap size) for the UMS Server depending on your environment. For the first installation, you can leave the default value (3072 MB), and change it later based on How to Configure Java Heap Size for the UMS Server. If you are updating the UMS, the installer will carry over and display the previously configured value.



9. Set the maximum memory consumption (Java heap size) for the UMS Console depending on your environment. For the first installation, you can leave the default value (3072 MB), and change it later based on How to Configure Java Heap Size for the UMS Console. If you are updating the UMS, the installer will carry over and display the previously configured value.



10. Read the **Memory (RAM) requirements** and click **Next** if your system fulfills them.
11. Select the **UMS data directory**. (Default: C:\Program Files\IGEL\RemoteManager)
12. Under **User Credentials for DB-connect**, enter the user name and password for the database connection – unless you are planning to connect the UMS to an MS SQL Server via Active Directory. For more information on connecting via AD, see [Connecting the UMS to an SQL Server via Active Directory \(see page 50\)](#).
The credentials for the database connection are created.

i The user name and password are case-sensitive.
Initially, the credentials entered here are also the credentials of the UMS superuser. After the installation, the credentials for the database user and those for the UMS superuser can be changed independently from each other. For more information about the UMS superuser, see [Changing the UMS Superuser \(see page 579\)](#).
13. If the internal Windows firewall is active on your host: Review the settings under **Windows firewall settings** and change them where necessary. Each port that is activated here will be set as rule in the Windows firewall.

i **UMS 12 Communication Ports**
If you are going to make network changes, consider the following ports and paths:

- For IGEL OS 12 devices, TCP 8443 `/device-connector/*` is required.
SSL can be terminated at the reverse proxy / external load balancer (see IGEL UMS Configuration for the External Load Balancer / Reverse Proxy: Example for NGINX with SSL Offloading) or at the UMS Server.
- For importing IGEL OS 12 Apps to the UMS from the IGEL App Portal, the URL <https://app.igel.com/> (TCP 443) is required.
- For the UMS Web App, TCP 8443 `/webapp/*` and `/wums-app/*` are required.
- For the UMS Console, the root is required, i.e. TCP 8443 `/*`
- For IGEL OS 11 devices, TCP 30001 and TCP/UDP 30005 are required.

For more information on UMS ports, see IGEL UMS Communication Ports.

14. Choose a folder name under **Select Start Menu Folder**.
15. Under **Select Additional Tasks**, specify whether you would like to create shortcuts for the UMS Console and [UMS Administrator](#) (see page 550) on the desktop.
16. 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, if selected, will place shortcuts for the UMS Console and UMS Administrator on the desktop.
17. 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.
18. Start the UMS Console.
19. Connect the UMS Console to the UMS Server using the access data for the database that you entered during the installation. For more information, see [Connecting the UMS Console to the IGEL UMS Server](#) (see page 162).
20. Start the UMS Web App. See [How to Log In to the IGEL UMS Web App](#).

- i** It is recommended to check your antivirus software and, if installed, other management software like HP Device Manager for possible conflicts if
- the installation of the IGEL UMS fails
 - the UMS Server service does not start when the installation is complete, and the manual start of the service fails. For details on how to start services, see [IGEL UMS HA Services and Processes](#).
 - there are problems when connecting the UMS Console to the UMS Server

i [If You Use an External Load Balancer / Reverse Proxy](#)

The FQDN and port of your external load balancer / reverse proxy must be specified in the UMS Console under **UMS Administration > Global Configuration > Server Network Settings > Cluster Address**. Information on the Cluster Address can be found under [Server Network Settings in the IGEL UMS](#) (see page 420).

- ⓘ For the management of IGEL OS 12 devices, it is necessary to register your UMS after the installation, see [Registering the IGEL UMS](#) (see page 164).

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>

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. For further information, see [Unattended / Silent Installation of the UMS Console](#) (see page 57).

- ⓘ Silent installation is only possible for the UMS Console. It is not possible for the UMS Server, the UMS Administrator, or the UMS Web App.

Unattended / Silent Installation of the UMS Console

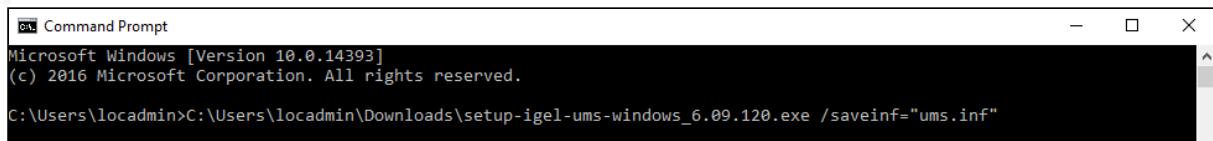
For performance, security, or other reasons like [the great size of your IGEL Universal Management Suite \(UMS\) installation](#) (see page 65), you have decided to install the UMS Console on a separate client machine, not on the UMS Server host. But you want to carry out the installation silently. In this case, you can use the following instructions for an unattended / silent installation of the UMS Console. They are also applicable when you updated the UMS Server and, thus, need to update the UMS Console on the client machines.

- ⓘ Silent installation is only possible for the UMS Console. It is not possible for the UMS Administrator, the UMS Server, or the UMS Web App.
- ⓘ These instructions apply only to the UMS installer for Windows.

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

1. Download the IGEL UMS from the [IGEL Download Server](#)⁶. Select the same version you used for the installation / update of the UMS Server.
2. In `cmd` or `powershell`, create a config file using the following command:

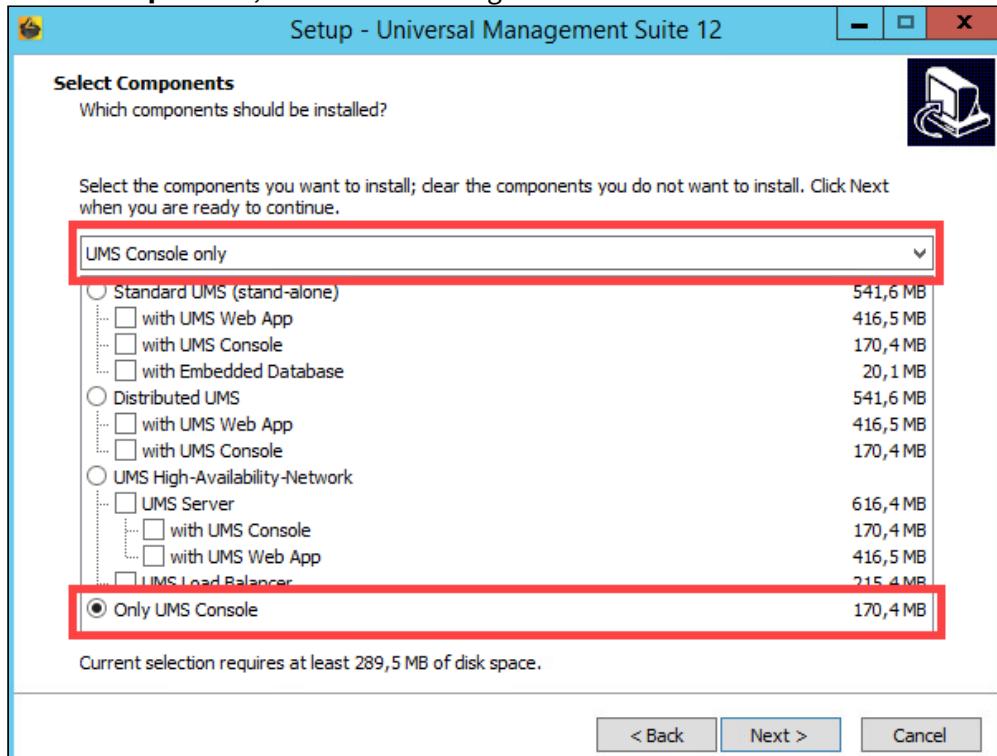
```
C:\[download directory]\setup-igel-ums-windows_x.y.z.exe /  
saveinf="[config-file]"
```



3. Confirm the dialog "Do you want to allow this app to make changes to your device?"

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

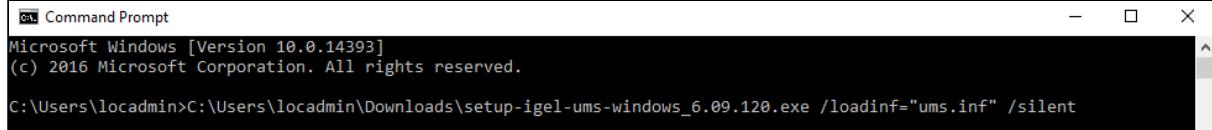
4. Use the wizard displayed to complete the installation while recording it to the config file. Under **Select Components**, make the following selection:



Info: If there are already other UMS components installed on the client machine, the **Only UMS Console** option will be deactivated and, thus, cannot be selected for the installation.

5. Transfer the UMS installation file and the created config file to the client machines, on which the UMS Console has to be installed / updated.
6. Use the following command to install the UMS Console:

```
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.

Installing the Distributed IGEL UMS

This article describes how to install the Distributed IGEL Universal Management Suite (UMS). Detailed information on the Distributed UMS can be found under [IGEL UMS Installation \(see page 13\)](#). The following instructions can be used:

- if you plan a new installation of the Distributed UMS
- if you already have a standard UMS installation but want to switch to the Distributed UMS

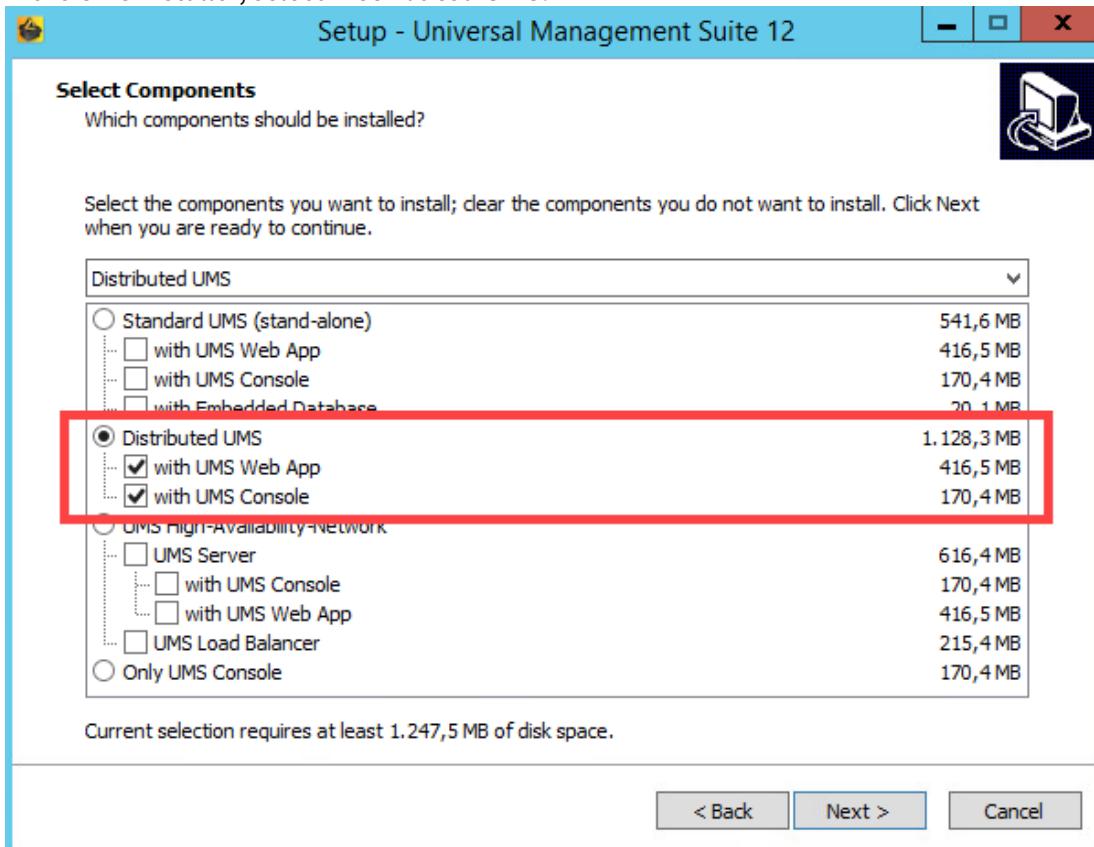
i For load distribution, DNS-Round-Robin load balancing of the server IP address should be used. The DNS-Round-Robin for `igelrmserver` should point to all servers.

New Installation of the Distributed UMS

To install the Distributed UMS, proceed as follows:

1. Install the first UMS Server. For the instructions, see [IGEL UMS Installation under Windows \(see page 50\)](#) or [IGEL UMS Installation under Linux \(see page 20\)](#).

In the UMS installer, select **Distributed UMS**.



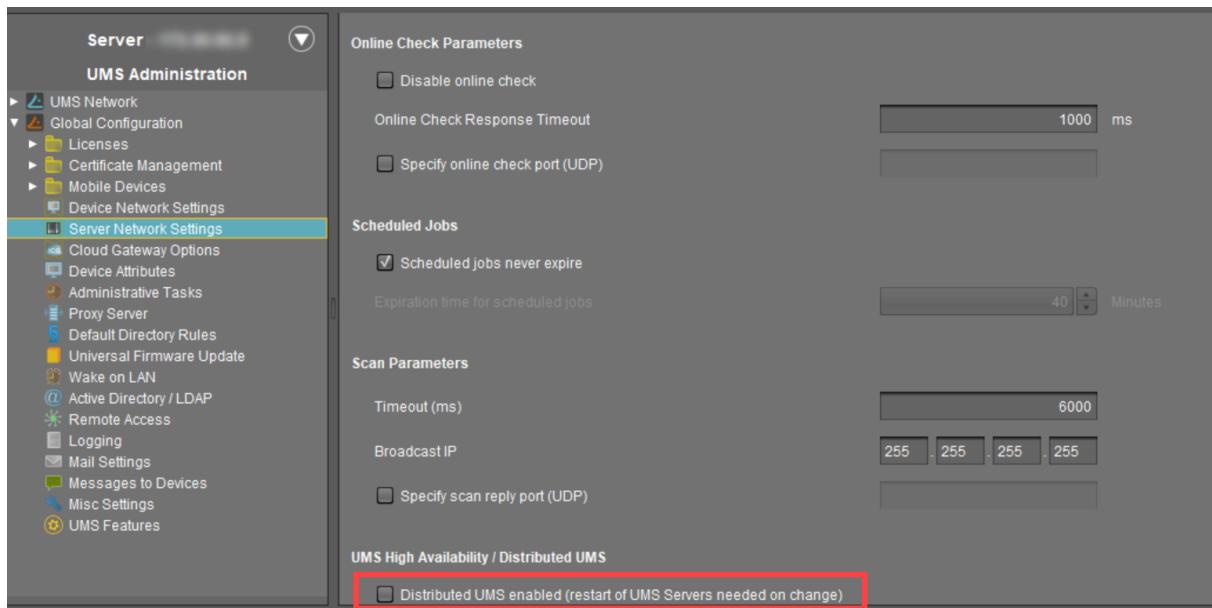
2. Configure an external database, see [Connecting External Database Systems \(see page 98\)](#).
3. Add this database as a data source in the **UMS Administrator > Datasource > Add** and **activate** it. See [How to Set Up a Data Source in the IGEL UMS Administrator \(see page 572\)](#).
4. Open the UMS Console and go under **UMS Administration > UMS Network > Server** to check that the server is up and running.
5. Install other UMS Servers (select **Distributed UMS** in the UMS installer) and connect them to the same database.

⚠ If you activated the Distributed UMS feature and have multiple UMS Servers, take care in case you decide to disable the feature. If the Distributed UMS feature is deactivated but more than one UMS Server is using the same database, no synchronization will be done between the UMS Servers.

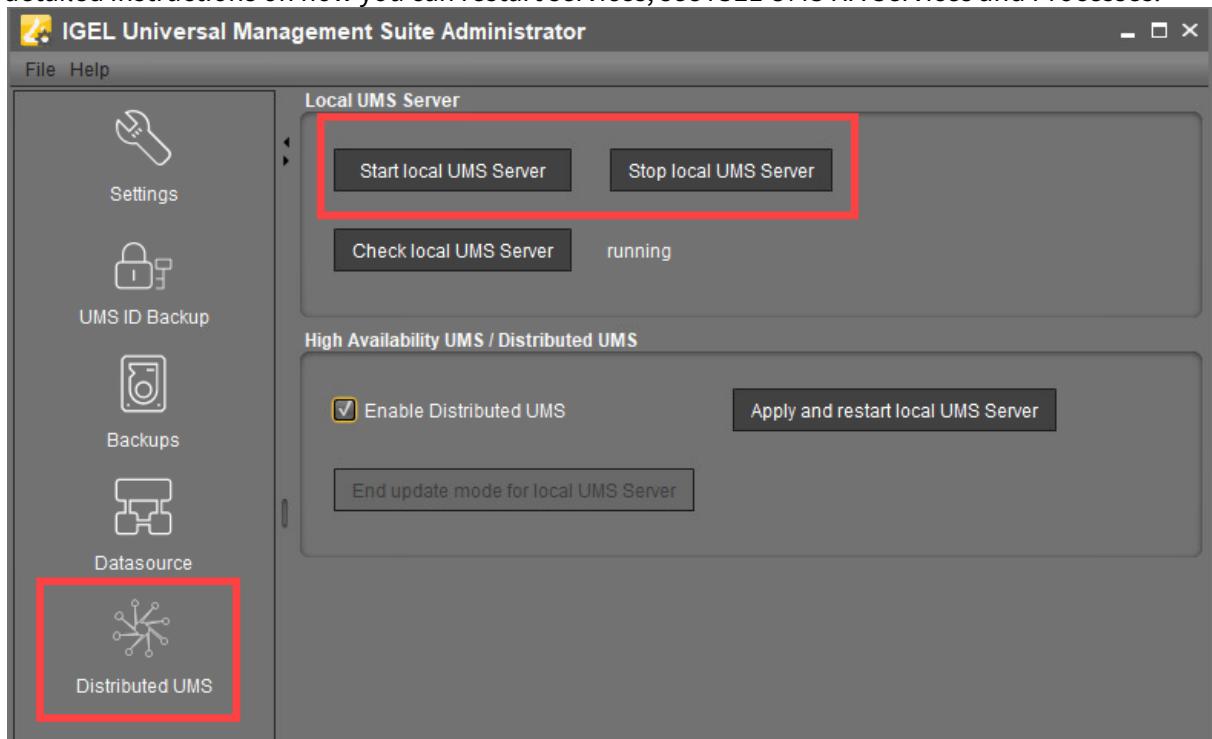
Switching from the Standard UMS to the Distributed UMS

If you want to extend your existing standard UMS installation to the Distributed UMS, proceed as follows:

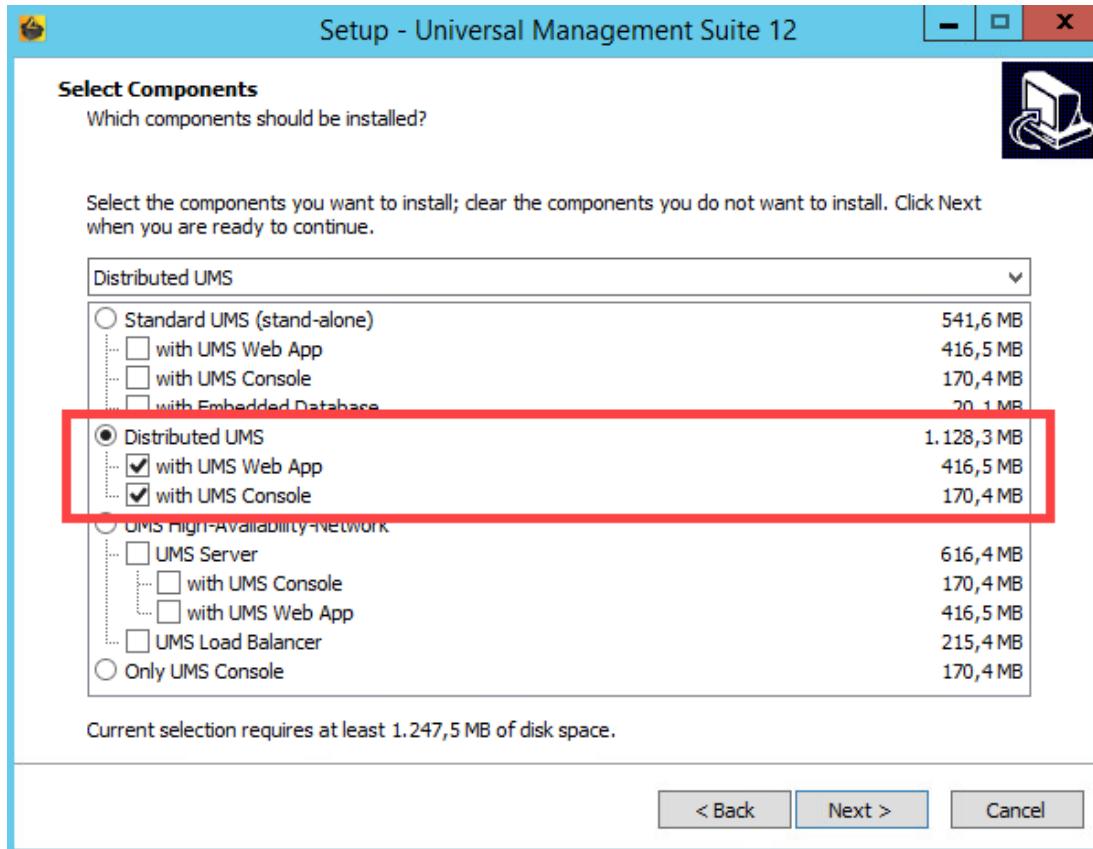
1. If you have a standard UMS installation with an external database: Start with step 4.
If you have a standard UMS installation with an embedded database: Create a new external database (see [Connecting External Database Systems \(see page 98\)](#)) and add this database as a data source in the **UMS Administrator > Datasource > Add** (see [How to Set Up a Data Source in the IGEL UMS Administrator \(see page 572\)](#)).
2. Copy the embedded database to the new external data source, see [Copying a Data Source \(see page 577\)](#), and **activate** the new data source.
3. Open the UMS Console and go under **UMS Administration > UMS Network > Server** to check that the server is up and running.
4. Go under **UMS Administration > Global Configuration > Server Network Settings** and activate **Distributed UMS enabled**.



5. Restart the UMS Server service, e.g. via [UMS Administrator > Distributed UMS](#) (see page 580). For detailed instructions on how you can restart services, see [IGEL UMS HA Services and Processes](#).



6. Install other UMS Servers (select **Distributed UMS** in the UMS installer) and connect them to the same database.



⚠ If you activated the Distributed UMS feature and have multiple UMS Servers, take care in case you decide to disable the feature. If the Distributed UMS feature is deactivated but more than one UMS Server is using the same database, no synchronization will be done between the UMS Servers.

Installation and Sizing Guidelines for IGEL UMS

The following installation and sizing guidelines are intended to support you with setting up the IGEL Universal Management Suite (UMS) environment – UMS Server, UMS Console & UMS Web App, database, and, if required, load balancer and ICG instances. For information on the installation requirements, see [Installation Requirements for the IGEL UMS](#) (see page 17).

The size and structure of the UMS setup depend mainly on the following criteria:

- Number of devices
- High Availability
- ICG connection for devices outside of your company network

General Preconditions

The Installation and Sizing Guidelines apply for a standard UMS setup and describe the most common UMS environments. Any individual exceptions or requirements may not be covered by these scenarios.

- System requirements: UMS 6.05 and newer, ICG 2.02 and newer
- UMS Console may be located **inside the same (V)LAN as UMS Servers** (no NAT, no proxies) or **outside the VLAN** with firewalls/routing configured according to IGEL UMS Communication Ports.
- Devices **directly connected to the UMS Server** are in **the same (V)LAN as UMS Servers** (no NAT, no proxies). If there is a firewall, it must be configured according to IGEL UMS Communication Ports.
- Devices **outside of the internal LAN** are connected **via ICG**.
- Devices are **not booted/rebooted frequently** (once a day on average).
- **A maximum of 10 different firmware versions** is managed via UMS.
- UMS backups and exports are **not permanently stored on the UMS server** host.
- In the case of automatic device registration (see [Registering Devices Automatically on the IGEL UMS](#) (see page 179)): The **DNS** alias `igelrmserver` or the **DHCP** tag can only point to ONE UMS installation. Therefore, the installation of several separate UMS Servers (without the High Availability Extension) in one network is not recommended.

⚠️ **High Availability with IGEL UMS Load Balancers:** All UMS Servers and UMS Load Balancers must reside on **the same VLAN**.
For High Availability (UMS HA) with IGEL UMS Load Balancers, network traffic must be allowed over UDP broadcast port 6155, and TCP traffic and UDP broadcast traffic over port 61616. For further port configuration, see IGEL UMS Communication Ports.
Note: IGEL UMS HA installation with IGEL UMS Load Balancers is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks. The HA installation without IGEL UMS Load Balancers (as well as the [Distributed UMS](#) (see page 13)) is, however, supported in cloud environments as of UMS version 6.10.

i Recommended Additional Information

- IGEL UMS Communication Ports: Find a list with all ports that are relevant for the communication with the UMS.
- Latest release notes: Find in the Supported Environment section the list of supported servers, clients, and backend databases.
- High Availability (HA): Find useful how-tos and the reference guide around your HA installation.
- IGEL Cloud Gateway: Find how-tos, the reference guide, and additional information concerning the management of endpoints outside the company network.

-
- [IGEL UMS Sizing Guidelines & Architecture Diagrams](#) (see page 65)
 - [Performance Optimizations in IGEL UMS](#) (see page 78)
 - [IGEL Cloud Gateway vs. Reverse Proxy for the Communication between UMS 12 and IGEL OS Devices](#) (see page 84)

IGEL UMS Sizing Guidelines & Architecture Diagrams

The following sizing guidelines are intended to support you with setting up the IGEL Universal Management Suite (UMS) environment – UMS Server, UMS Console & UMS Web App, database, and, if required, load balancer and ICG instances.

General Installation Recommendations

For small installations, a single UMS Server instance (standard UMS) with an embedded database is usually sufficient. If required, a single-instance installation can be easily extended anytime to a Distributed UMS installation by installing additional servers (and in the case of an embedded database, by switching preliminarily to an external data source).

Large installations should use either the UMS High Availability or the Distributed UMS (preferable for new installations, e.g. because you do not have to configure additional firewall exclusions). For large installations, it is also recommended to use DNS-Round-Robin load balancing or IGEL Cloud Gateway.

For more information, see [IGEL UMS Installation \(see page 13\)](#).

Installation Size	#Devices	#UMS Server Host (+ Load Balancer)	UMS Server	UMS Console Standalone	#Load Balancer Standalone	Load Balancer Standalone	Database* * ICG
S < 5.000	1 server	8 GB RAM (UMS Web App + 1 GB) 4 CPUs 25 GB free disk space	Optional* 3 GB RAM 2 CPUs 1 GB free disk space			Embedded database	1 ICG instance per 2,500 devices
M < 15.000	1 server	8 GB RAM (UMS Web App + 1 GB) 4 CPUs 25 GB free disk space	Optional* 3 GB RAM 2 CPUs 1 GB free disk space		External database 10 GB	Server generally: 8 GB RAM 2 CPUs 20 GB free disk space	
M / S < 15.000 (HA or Distrib uted UMS)	2 servers 2 load balancers	9 GB RAM (Web App +1GB) 6 CPUs 25 GB free disk space	Optional* 3 GB RAM 2 CPUs 1 GB free disk space		External database 10 GB	Only ICG service: 4 GB RAM 2 CPUs 2 GB free disk space	
L (HA or 50.000 Distrib uted UMS)	2 servers 2 load balancers	6 GB RAM*** (Web App +1GB) 4 CPUs 25 GB free disk space	Mandatory 3 GB RAM 2 CPUs 1 GB free disk space		External database 10 GB		
XL (HA or 300.0 Distrib uted UMS)* ***	Up to 6 servers (1 server / 50,000 devices)	9 GB RAM (Web App +1GB) 6 CPUs 25 GB free disk space	Mandatory 6 GB RAM 4 CPUs 1 GB free disk space	Up to 3 Load Balancer (1 LB / 3 Server)	4 GB RAM 4 CPUs 2 GB free disk space	External database 20 GB	

* UMS Console can be installed on UMS Server host.

** Follow the recommendation of the external database system on RAM and CPU.

*** RAM and CPU requirements are less than in the case of **M / S (HA)** installation since the UMS Console is installed on a separate host machine (**UMS Console Standalone = Mandatory**).

**** General recommendation: 1 UMS Server per 50,000 devices, 1 load balancer for 3 UMS Servers.

For the architecture diagrams of the installations, see:

- [Small Environment: UMS S \(see page 68\)](#)
- [Medium Environment: UMS M \(see page 70\)](#)
- [Small and Medium Environments: UMS M/S \(HA\) \(see page 72\)](#)
- [Large Environment: UMS L \(HA\) \(see page 74\)](#)
- [Extra Large Environment: UMS XL \(HA\) \(see page 76\)](#)

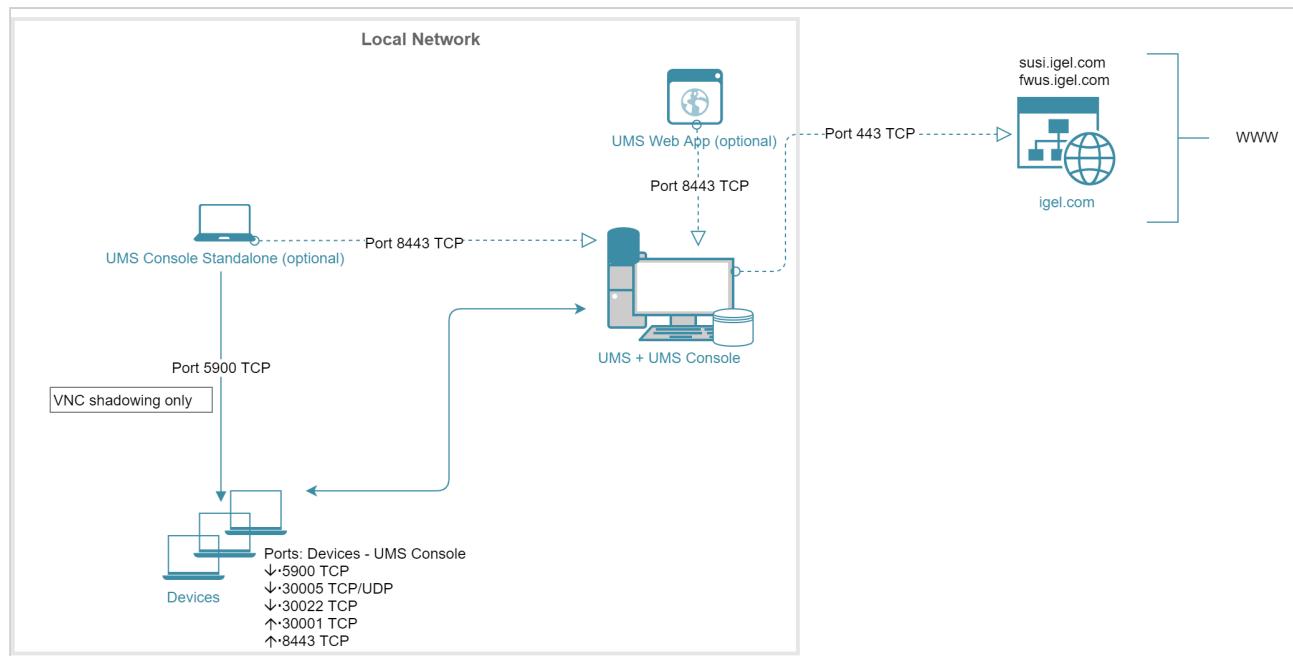
Small Environment: UMS S

Small Size UMS Installation (<5k Devices) or Demo/POV Environment with an Embedded Database

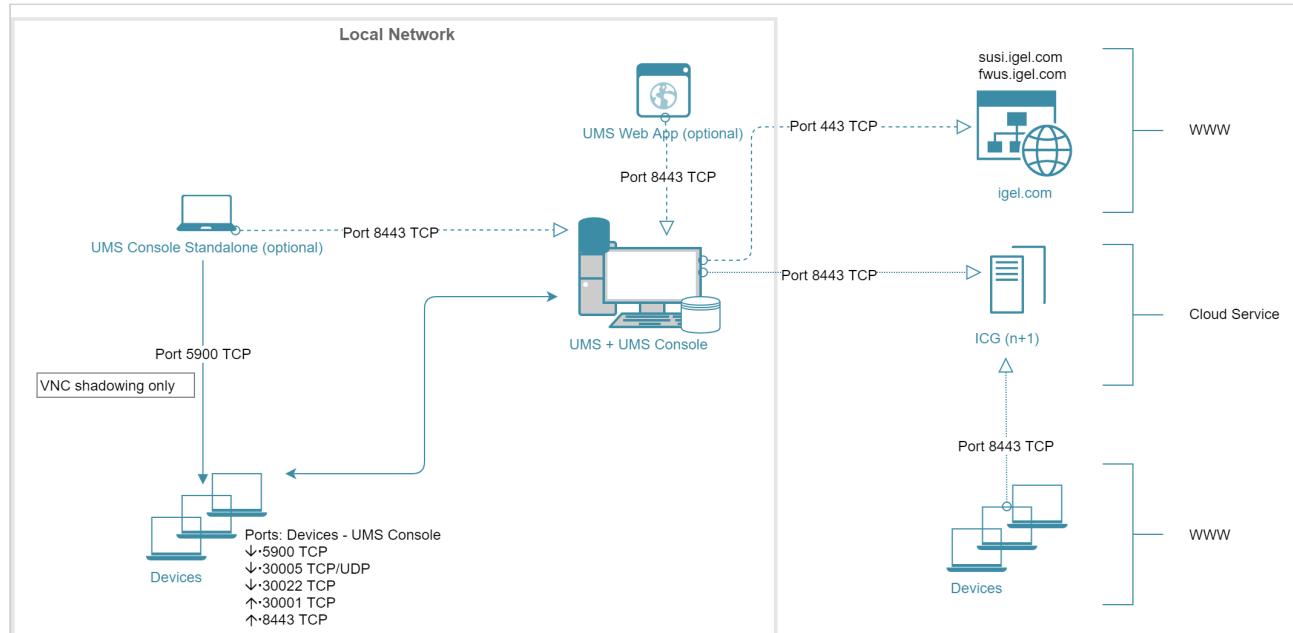
Installation Size	#Devices	#UMS Server Host	UMS Server	UMS Console Standalone	#Load Balancer Standalone	Load Balancer Standalone	Database	ICG
S	< 5.000	1 server	8 GB RAM (UMS Web App + 1 GB) 4 CPUs 25 GB free disk space	Optional* 3 GB RAM 2 CPUs 1 GB HDD			Embedded database	1 ICG instance per 2,500 devices Server generally: 8 GB RAM 2 CPUs 20 GB HDD Only ICG service: 4 GB RAM 2 CPUs 2 GB HDD

* UMS Console can be installed on UMS Server host.

Architecture: Small Environment



Architecture: Small Environment + ICG in Cloud



Medium Environment: UMS M

Medium Size UMS Installations (up to ~15k Devices); No High Availability

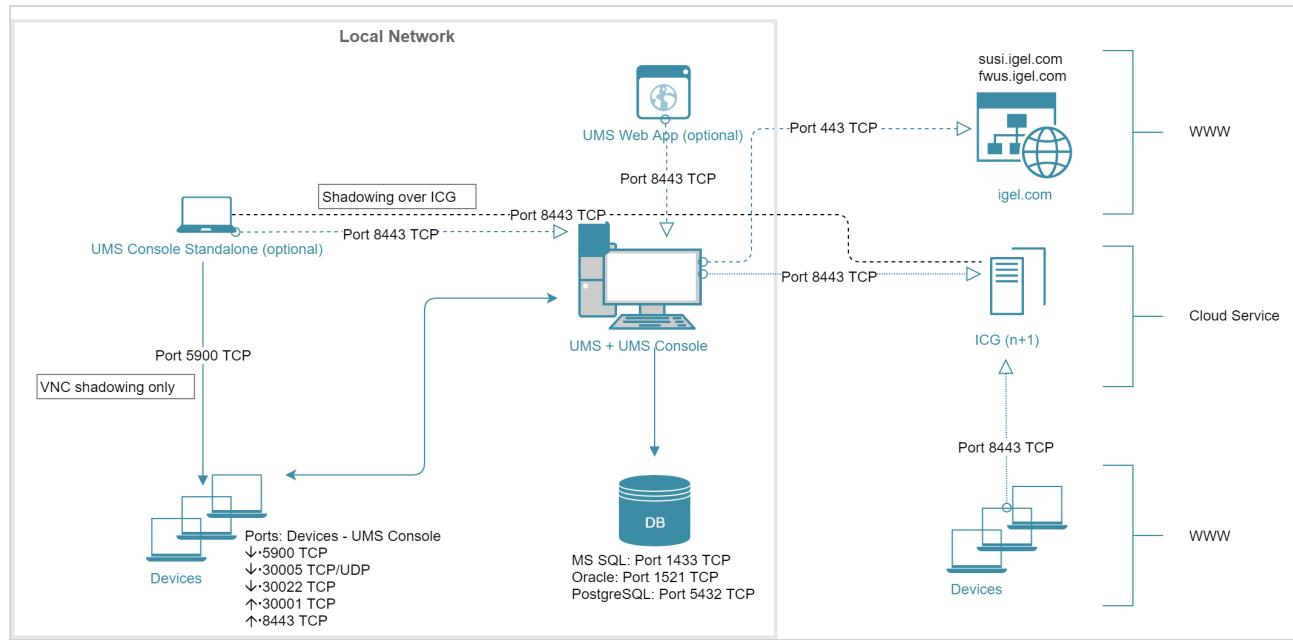
Installation Size	#Devices	#UMS Server Host	UMS Server	UMS Console Standalone	#Load Balancer Standalone	Load Balancer Standalone	Database*	ICG
M	< 15.000	1 server	8 GB RAM (UMS Web App + 1 GB) 4 CPUs 25 GB free disk space	Optional* 3 GB RAM 2 CPUs 1 GB HDD			External database 10 GB	1 ICG instance per 2,500 devices Server generally: 8 GB RAM 2 CPUs 20 GB HDD Only ICG service: 4 GB RAM 2 CPUs 2 GB HDD

* UMS Console can be installed on UMS Server host.

** Follow the recommendation of the external database system on RAM and CPU.

 For High Availability, see [Small and Medium Environments: UMS M/S \(HA\) \(see page 72\)](#).

Architecture: Medium Environment + ICG



Small and Medium Environments: UMS M/S (HA)

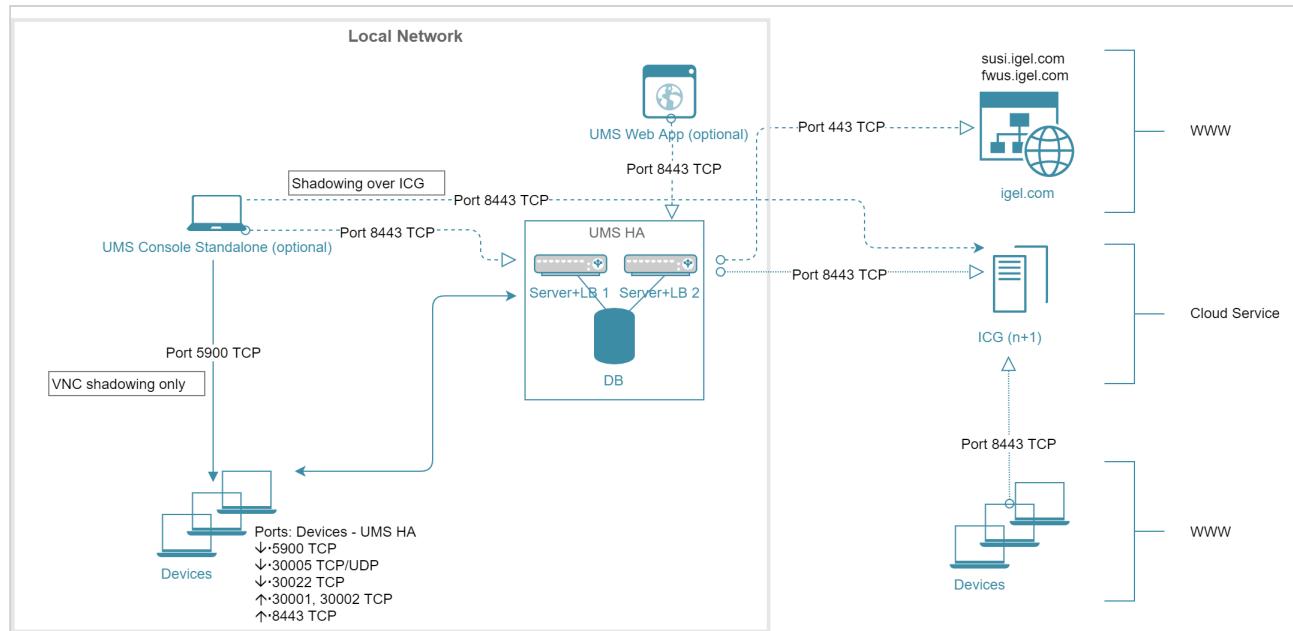
Small and Medium Size UMS Installations (up to ~15k devices); High Availability

Installation Size	#Devices	#UMS Server Host (+ Load Balancer)	UMS Server	UMS Console Standalone	#Load Balancer Standalone	Load Balancer Standalone	Database*	ICG
M / S (HA or Distributed UMS (see page 13))	< 15.00	2 servers 2 load balancers	9 GB RAM (Web App +1 GB) 6 CPUs 25 GB HDD	Optional* 3 GB RAM 2 CPUs 1 GB HDD			External database 10 GB	1 ICG instance per 2,500 devices Server generally: 8 GB RAM 2 CPUs 20 GB HDD Only ICG service: 4 GB RAM 2 CPUs 2 GB HDD

* UMS Console can be installed on UMS Server host.

** Follow the recommendation of the external database system on RAM and CPU.

Architecture: Small and Medium Environment (HA) + ICG



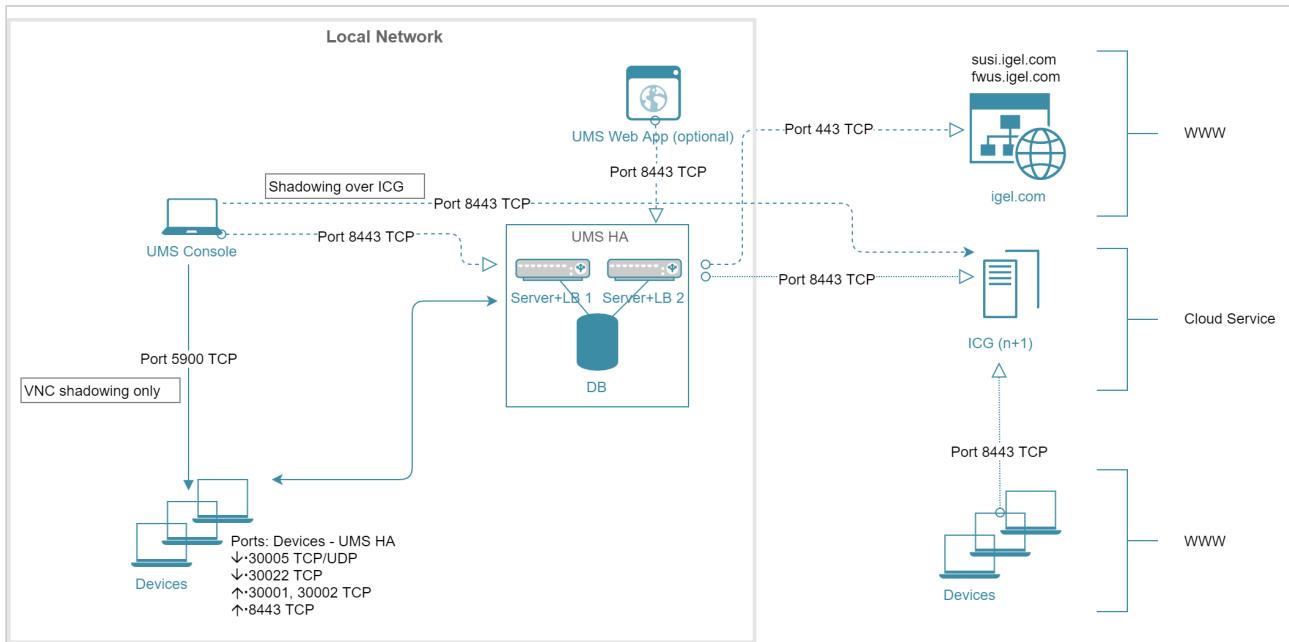
Large Environment: UMS L (HA)

Large UMS Installations with up to 50k Devices; High Availability + ICG

Installation Size	#Devices	#UMS Server Host (+ Load Balancer)	UMS Server	UMS Console Standalone	#Load Balancer Standalone	Load Balancer Standalone	Database*	ICG
L (HA or Distribute UMS (see page 13))	< 50.00	2 servers 2 load balancers	6 GB RAM (Web App +1GB) 4 CPUs 25 GB HDD	Mandatory 3 GB RAM 2 CPUs 1 GB HDD			External database 10 GB	1 ICG instance per 2,500 devices Server generally: 8 GB RAM 2 CPUs 20 GB HDD Only ICG service: 4 GB RAM 2 CPUs 2 GB HDD

* Follow the recommendation of the external database system on RAM and CPU.

Architecture: Large Environment (HA) + ICG



Extra Large Environment: UMS XL (HA)

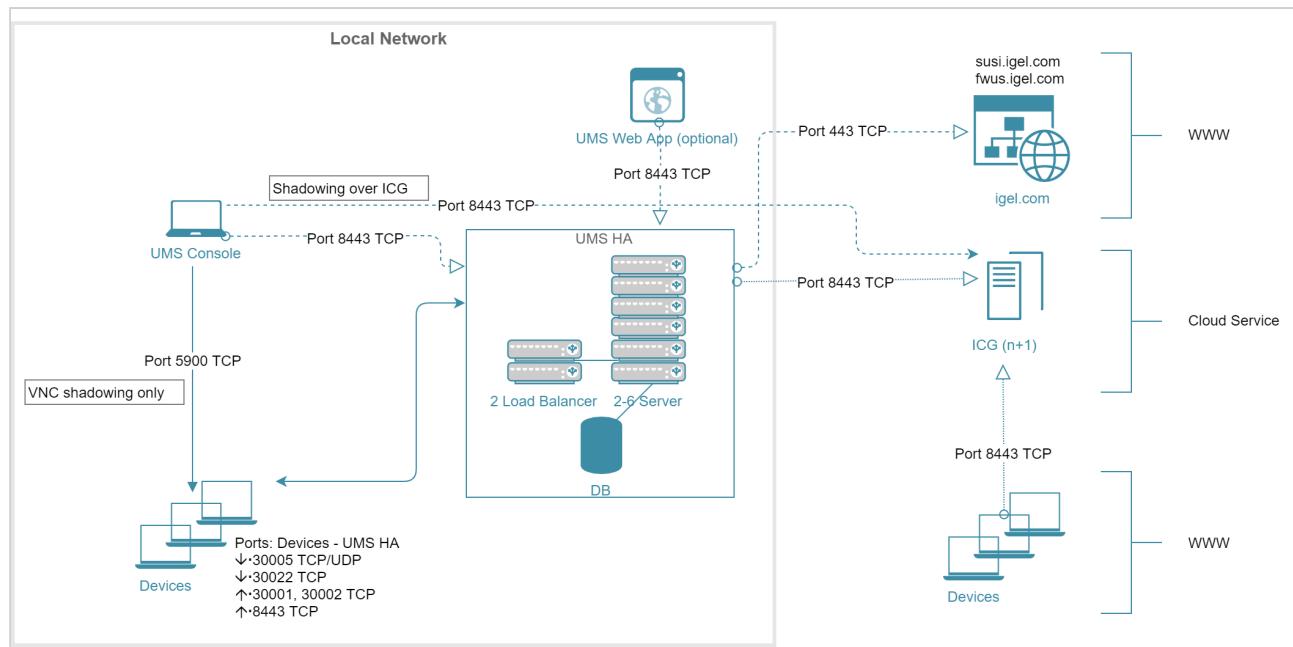
Extra Large UMS Installations with up to 300k Devices; High Availability + ICG

Installation Size	#Devices	#UMS Server Host	UMS Server	UMS Console Standalone	#Load Balancer Standalone	Load Balancer Standalone	Database*	ICG
XL (HA or Distributed UMS (see page 13))**	< 300.00	Up to 6 servers (1 server / 50,000 devices)	9 GB RAM (Web App +1GB) 6 CPUs 25 GB HDD	Mandatory y 6 GB RAM 4 CPUs 1 GB HDD	Up to 3 load balancers (1 load balancer / 3 servers)	4 GB RAM 4 CPUs 2 GB HDD	External database 20 GB	1 ICG instance per 2,500 devices Server generally: 8 GB RAM 2 CPUs 20 GB HDD Only ICG service: 4 GB RAM 2 CPUs 2 GB HDD

* Follow the recommendation of the external database system on RAM and CPU.

** General recommendation: 1 UMS Server per 50,000 devices, 1 load balancer for 3 UMS Servers.

Architecture: Extra Large Environment (HA) + ICG



Performance Optimizations in IGEL UMS

Data Sizing

- The number of registered firmware versions has the **largest impact** on the size of the database. (Listed in UMS Console under **Misc > Firmware Statistics**)
- The number of devices or profiles has a **minor impact**.
- Average size per...
 - Firmware configuration: ~15 MB
 - Profile (depends on the number of active parameters): ~100 kB
 - Device: ~100 kB
- Reserve 500 MB up to 1 GB for database transaction logs of excessive database calls like **Remove unused Firmware**. Please note that the usage depends on the database system used.

Latencies

If you are struggling with long-distance connections and high latency, please consider the following recommendations:

- Minimize latency between...
 - Database <-> UMS Server: <= 20 ms
 - Several UMS Servers: <= 50 ms
 - Load balancer <-> UMS Server: <= 50 ms
- High latency between the database and the UMS Server has a **huge impact** on the performance. The communication between the device and the UMS Console will slow down, the UMS Console itself will become lazy.
- High latency between the device and the UMS Server has **little impact** on overall performance.

Performance Optimizations

- **UMS logs:**
Use [administrative tasks](#) (see page 436) to automatically clean up logs (logging data, job execution data, execution data of administrative tasks, process events, asset information history) or remove old UMS log files (/rmguiserver/logs) when storage space runs out.
- **Firmware:**
Remove unused firmware regularly.
- **Embedded database only:**
 - Optimize database regularly (UMS Administrator application, e.g. once a month)
 - Check for free storage space and expand the storage size if necessary (keep at least 1 GB free at all times)
- **Number of devices:**
 - If the device count is high (>10k) and overall performance is low, increase UMS Server and UMS Console memory. See [How to Configure Java Heap Size for the UMS Server](#) and [How to Configure Java Heap Size for the UMS Console](#).
 - Avoid too many devices (>5k) in one folder.

- **Assignments:**

Keep the number of assignments per device (direct and indirect) at a low level (<25).

- **Administrative tasks and jobs:**

The more administrative tasks and jobs are created, the more heap is "eaten up", so it may be necessary to increase UMS Server memory. See How to Configure Java Heap Size for the UMS Server.

- **Default directory rules:**

Do not use default directory rules with the **Apply rule when device boots** option unless they are required.

- **Concurrent device requests:**

If you are experiencing problems with many concurrent device requests (delays in configuration deployment or logging on to the device), open the UMS Console and use the options under **UMS Administration > Global Configuration > Device Network Settings > Device Requests** (thread and queue size) to control the throughput of the device requests. Contact support for recommendations.

Limitations: UMS HA

- Device actions that are manually triggered in the UMS Console are performed by **one UMS Server** (the one the UMS Console is currently connected to); there is no load balancing for these actions.

IGEL UMS Maintenance Tasks

There are a few items that are recommended to configure after your IGEL Universal Management Suite (UMS) server(s) are set up to make sure they are properly maintained and running as efficiently as possible. This article outlines some recommended configurations that should be made to make sure your UMS database and file structure are maintained properly.

Recommended Administrative Tasks (Scheduled Jobs)

There are multiple tasks that should be scheduled to properly maintain a UMS server/cluster and database.

- ⚠ As part of the tasks, you will be asked to provide a location to back up the data before deleting them. This can be done on a mapped (lettered) drive in Windows, or a mounted remote location on Linux if required.

Scheduling

It is recommended to schedule each task on a different day, two hours after any backups are made. This will give each task enough time to complete and allow for a rollback via the backup if data is removed that is required.

Recommended Tasks

	Task Name	Task Details	Task Notes
1	Delete job execution data	UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action Delete job execution data	With this administrative task, you can delete the job execution results listed under Jobs > [job name] . For details, see Delete Job Execution Data (see page 448).
2	Delete process events	UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action Delete process events	With this administrative task, you can delete the process events displayed under UMS Administration > UMS Network > Events > [timespan] . For details, see Delete Process Events (see page 454).

	Task Name	Task Details	Task Notes
3	Delete administrative task execution data	UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action Delete administrative task execution data	With this administrative task, you can delete the results of the execution of administrative tasks listed under UMS Administration > Global Configuration > Administrative Tasks > [task name]. For details, see Delete Administrative Task Execution Data (see page 451).
4	Delete asset info history	UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action >Delete asset info history	With this administrative task, you can delete the stored asset information that is displayed under Devices > [device name] . For details, see Delete Asset Information History (see page 472).
5	Delete logging data	UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action >Delete logging data	With this administrative task, you can delete the log messages that can be configured under UMS Administration > Global Configuration > Logging . For details, see Delete Logging Data (see page 444).

Example:

Administrative Tasks							
Name	Job	Last Execution	Next Execution	Execution Status	Active	Send result	
Nightly - Backup	Create backup	Jul 15, 2023, 10:00 PM	Jul 16, 2023, 10:00 PM	completed	✓		
Monday - Delete Job Execution Data	Delete job execution data	Jul 17, 2023, 10:59 PM	Jul 17, 2023, 11:59 PM	completed	✓		
Tuesday - Delete Process Events	Delete process events	Jul 18, 2023, 10:59 PM	Jul 18, 2023, 11:59 PM	completed	✓		
Wednesday - Delete Administrative	Delete administrative task execution data	Jul 19, 2023, 11:00 PM	Jul 19, 2023, 11:59 PM	completed	✓		
Thursday - Delete Asset Inventory H	Delete asset info history	Jul 20, 2023, 10:58 PM	Jul 20, 2023, 11:59 PM	completed	✓		
Friday - Delete Logging Informa	Delete logging data	Jul 21, 2023, 10:59 PM	Jul 21, 2023, 11:59 PM	completed	✓		

UMS Server Backups

Backup Schedule

It is recommended to schedule a backup at least once a week of the UMS database and local file repositories.

- This could be scheduled as frequently as once a day during device deployment or mass configuration changes.

This backup should be scheduled to occur at a minimum of two hours after any other Administrative Tasks are scheduled to run.

External Database

For external / third-party databases, such as Postgres and Microsoft SQL, you will need to utilize their respective backup options, or a third-party software to manage database backups.

For the internal IGEL database, see [IGEL Embedded Database \(see page 82\)](#).

Local Files

For UMS, the IGEL database is the most critical component that needs to be backed up, and this should be handled via a third-party application connected to your external database. However, some local directories should be backed up outside of UMS. These locations are noted below.

Directory	Usage
%INSTALL_DIR%/ RemoteManager/ rmguiserver/webapps/ ums_filetransfer	Contains all transfer files deployed via UMS including Universal Firmware Packages, wallpaper files, icon files, and SSL certificates, etc.
UMS12 and later: %INSTALL_DIR%/ RemoteManager/ rmguiserver/persistent/ ums-appproxy	Contains OS 12 application packages for the local UMS Web Proxy

⚠ By default the IGEL install directory (%INSTALL_DIR%) will be located in one of the locations below. If UMS was installed to a different directory, please update the path accordingly.

Operating System	Location(s)
Windows	C:\Program Files\IGEL\ or C: \Program Files(x86)\IGEL\
Linux	/opt/IGEL/

IGEL Embedded Database

For the embedded database, there are a couple more items that are recommended to perform.

⚠ IGEL recommends moving to an external database for production environments, so this should only be required in POC / Lab environments. However, some smaller environments may still utilize the embedded database in production.

Local Database Optimization

If you are using the IGEL embedded database, it is recommended to run a database optimization at least every 3 months, and maybe more depending on the size of your environment. You can find more details on this process under [Optimizing the Active Embedded DB \(see page 578\)](#), but keep in mind that this will halt services on UMS and the console will be unavailable until it completes.

Local Database Backup

If you are using the IGEL embedded database, then you will want to schedule an additional administrative task in UMS to perform this action.

Task Name	Task Details	Notes
Database Backup	Creates a backup of the database, and other optional components.	<ul style="list-style-type: none">Recommended to backup only the database, but you can also select the transfer files as well. Doing so may take a long time, and will create a larger backup file.Backing up the server configuration is not required or recommended

IGEL Cloud Gateway vs. Reverse Proxy for the Communication between UMS 12 and IGEL OS Devices

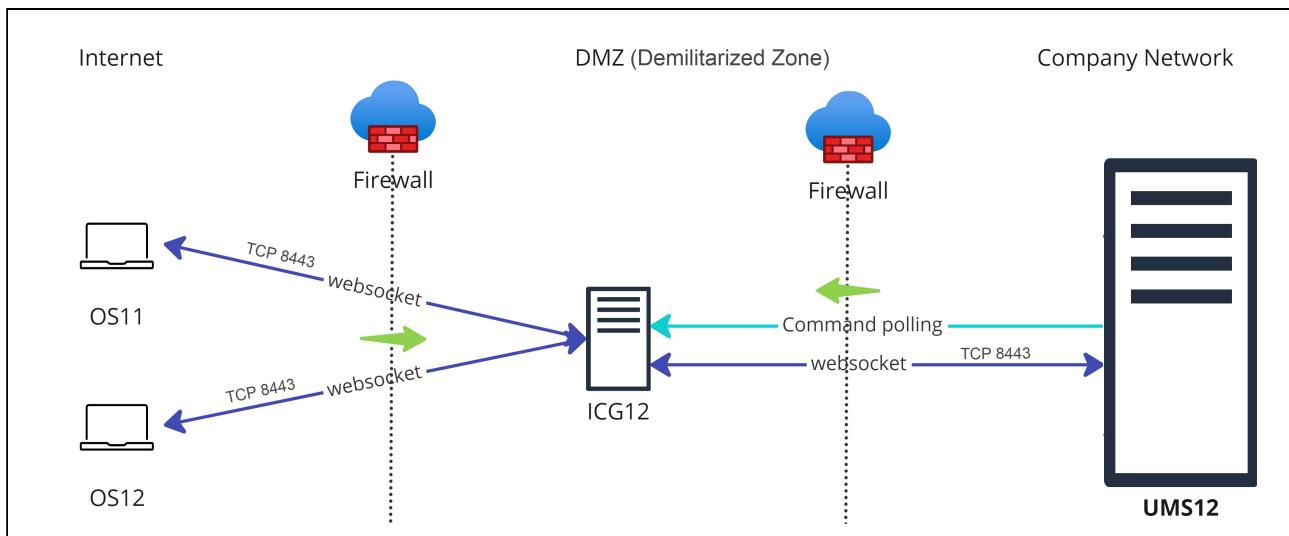
With the launch of IGEL Universal Management Suite (UMS) 12, the Unified Protocol used for all communication between the UMS and IGEL OS 12 devices was introduced, see [Overview of the IGEL UMS \(see page 6\)](#). The Unified Protocol is a secure protocol that uses TCP 8443, see IGEL UMS Communication Ports. However, depending on the structure of your UMS environment, company's security policies, etc., it may be insufficient, and the use of the IGEL Cloud Gateway (ICG) or reverse proxy may be required. In the following article, you will find pros and cons of each solution.

i In general UMS/ICG only needs routing for the configured web port between the device and the UMS/ICG. If any of the network components terminates SSL, the client cert needs to be forwarded in a HTTP header.

⚠ The example configurations in the pictures are for general illustrative purposes. Each network configuration will vary depending on the network setup, i.e. whether the UMS is in a DMZ or not.

Option 1: ICG 12

In the case of the ICG, endpoint devices connect to the ICG as well as the UMS connects to the ICG, see [Devices and UMS Server Contacting Each Other via ICG](#). The WebSocket communication between the ICG and the UMS as well as between the ICG and the device is only established after mutual authentication, and the communication is encrypted with TLS. All data is routed through this WebSocket.



Advantages:

- Suitable for mixed environments when you manage both IGEL OS 12 and IGEL OS 11 devices

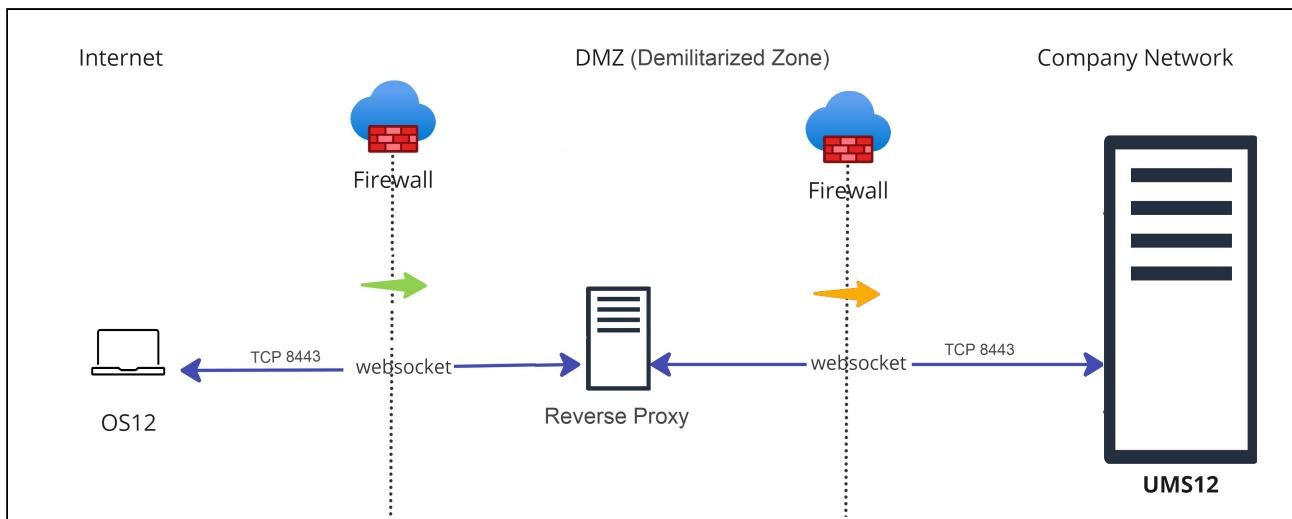
- No inbound connection from the device to the UMS
- Only the ICG is exposed to the Internet. Thus, if compromised, the UMS is NOT compromised at the same time.
- Simple and lightweight, which minimizes the attack surface

Disadvantages:

- UMS as an Update Proxy feature cannot currently be used, i.e. IGEL OS devices can download the apps from the App Portal only, not from the UMS Server. See [Configuring Global Settings for the Update of IGEL OS Apps](#).
- Higher latency and longer command execution in comparison to the reverse proxy. For large enterprise environments, the use of a reverse proxy may be considered.

Option 2: Reverse Proxy

Another possibility to route the traffic via port 8443 is to use a reverse proxy. The reverse proxy will forward the requests from devices to the UMS.



Technical details:

- Reverse proxy with SSL offloading is possible as of UMS 12.02. See [NGINX: Example Configuration for as Reverse Proxy in IGEL OS with SSL Offloading](#).
- The FQDN and port of the reverse proxy must be specified as a Cluster Address, see [Server Network Settings in the IGEL UMS](#) (see page 420).

i A reverse proxy / load balancer can also be used to distribute traffic from devices within the company network. For more information on network component integration, see [IGEL Universal Management Suite Network Configuration](#).

- It is advisable to use TLS 1.3 for the reverse proxy configuration.

Advantages:

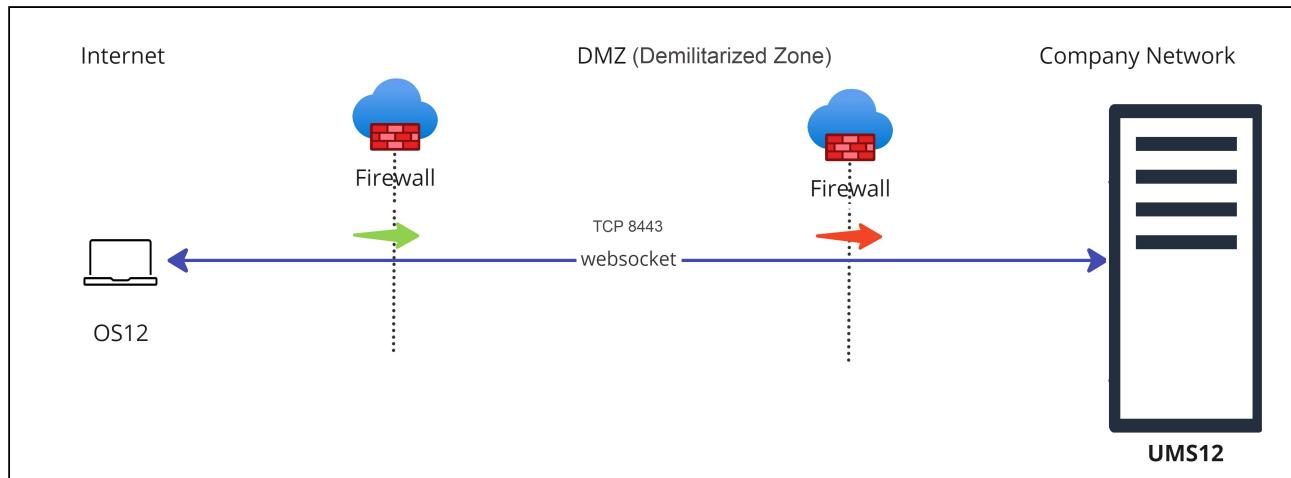
- Load balancing
- UMS as an Update Proxy feature can be used, i.e. IGEL OS devices can download the apps from the UMS Server. See Configuring Global Settings for the Update of IGEL OS Apps.

Disadvantages:

- Can be used if you manage IGEL OS 12 devices only.
- Proper configuration and maintenance of the reverse proxy is required. For security reasons, you may want to restrict access to any components you do not require, but note that the following paths must be enabled:
 - For IGEL OS 12 device onboarding and communication: TCP 8443 /device-connector/*
 - For IGEL OS 12 and UMS as an Update Proxy feature: TCP 8443 /ums-appproxy/*
 - For the UMS Web App: TCP 8443 /wums-app/* and /webapp/*
- If used to connect devices from outside the company network, the devices have an inbound connection to the UMS. In comparison, with the ICG, there is no inbound connection from the devices to the UMS.
- Adds an extra layer of security (depending on the configuration), but, if compromised, the reverse proxy can provide access to the UMS. In comparison, the ICG does not expose the UMS to the Internet.

Option 3: Direct Connection of the Devices to the UMS via Unified Protocol (No ICG, No Reverse Proxy)

In this case, IGEL OS 12 devices communicate directly with the UMS, see Devices Contacting UMS.



Advantages:

- port 8443 (can be changed under [UMS Administrator > Settings > Web server port \(see page 552\)](#)) must be opened in a firewall, but no other configuration is required
- suitable for communication with devices within the company network

Disadvantages:

- Inbound connection from the device to the UMS
- For communication with devices outside the company network, it is advised to consider the use of a reverse proxy or the ICG

 IGEL Onboarding Service (OBS) is NOT a substitute for an ICG or a reverse proxy and is only meant to authenticate and register the endpoint device with the correct UMS during the onboarding. For more information on the OBS, see Initial Configuration of the IGEL Onboarding Service (OBS) and Onboarding IGEL OS 12 Devices.

Legend to the images:

 : Shows that the traffic in the WebSocket runs in both directions.

 (multicolored): Shows from which side firewalls etc. must be opened.

IGEL UMS Update

In this chapter, you will find how to update the IGEL Universal Management Suite (UMS) under Windows or Linux. Update instructions for the UMS High Availability (HA) installation can be found under Updating the Installation of an HA Network.

Update Instructions

- [Updating the IGEL UMS under Linux](#) (see page 90)
- [Updating the IGEL UMS under Windows](#) (see page 94)

Update Preparations

- ⚠ Before the installation, check that your hardware and software fulfill the [installation requirements](#) (see page 17). See also [Devices Supported by IGEL Universal Management Suite](#).
- ⚠ 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 562) and [Creating a Backup of the IGEL UMS](#) (see page 563).
- ✓ 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.

- ⓘ WebDAV downloads (e.g. files, firmware updates) are stored in the `ums_filetransfer` directory. Custom file transfer directories are not supported.
- ⓘ During a UMS upgrade, e.g. from 6.09 to 6.10 or from 6.x to 12.x, 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 the IGEL UMS under Linux

Before starting the update of the IGEL Universal Management Suite (UMS), read [IGEL UMS Update \(see page 88\)](#).

- ⚠ Create a [backup of the database \(see page 562\)](#)** 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.

To perform an update under Linux, proceed as follows:

1. Download the current version of the IGEL Universal Management Suite from the [IGEL Download Server](#)⁷.

- ⓘ For integrity and security purposes, it is recommended to verify the checksum of the downloaded software.**



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.

⁷ <https://www.igel.com/software-downloads/>

3. Check whether the installation file is executable. If not, it can be made executable with 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
```

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.

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. 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.

For Update Installations Only

- As of UMS 12, MDM feature is no longer available. Cancel the upgrade to UMS 12 if you still need the MDM feature:



- Only if you have a Distributed UMS installation: During the update installation, it will be checked whether only one UMS Server is running and the others are stopped. If not, stop all UMS Servers except one and proceed with the update; otherwise, you risk losing data. After the update on this server is complete, you can update the remaining UMS Servers, either simultaneously or one after another.

8. Under **Installation type**, select the scope of installation:

- Complete:** UMS Server and UMS Console

- **Distributed UMS:** [Distributed UMS installation \(see page 13\)](#)
- **HA net:** High Availability configuration
- **Client only:** UMS Console only

9. Choose whether the **UMS Web App** should be installed. See [Important Information for the IGEL UMS Web App](#).
10. Confirm the **system requirements** dialog if your system fulfills them.
11. Under **Confirm server IP address**, confirm or enter the IP address of the UMS Server. This IP address will be used for the creation of the UMS Server certificate on the initial startup. This dialog is shown only on the first installation of a UMS version that includes this feature.

⚠ If you do not adjust the IP address during the installation of the UMS, the web certificate of your UMS Server will contain the wrong IP, which results in problems with device registration, etc. To solve the issue, a new web certificate will have to be generated. See [Invalid Web Certificate and Errors by Device Registration after the Installation of the IGEL UMS 12 on Linux](#).
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 6.09 to 6.10 or from 6.x to 12.x, 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`

ⓘ It is generally NOT recommended to execute the command `RemoteManager.sh` with `sudo`. On Red Hat Enterprise Linux 8, `RemoteManager.sh` can be executed only without `sudo`.
15. Connect the UMS Console to the UMS Server with the help of the existing access data. To connect to the UMS Web App, see [How to Log In to the IGEL UMS Web App](#).

ⓘ UMS 12 Communication Ports

If you are going to make network changes, consider the following ports and paths:

- For IGEL OS 12 devices, TCP 8443 `/device-connector/*` is required. SSL can be terminated at the reverse proxy / external load balancer (see [IGEL UMS Configuration for the External Load Balancer / Reverse Proxy: Example for NGINX with SSL Offloading](#)) or at the UMS Server.

- For importing IGEL OS 12 Apps to the UMS from the IGEL App Portal, the URL <https://app.igel.com/> (TCP 443) is required.
- For the UMS Web App, TCP 8443 /webapp/* and /wums-app/* are required.
- For the UMS Console, the root is required, i.e. TCP 8443 /*
- For IGEL OS 11 devices, TCP 30001 and TCP/UDP 30005 are required.

For more information on UMS ports, see IGEL UMS Communication Ports.

Updating the IGEL UMS under Windows

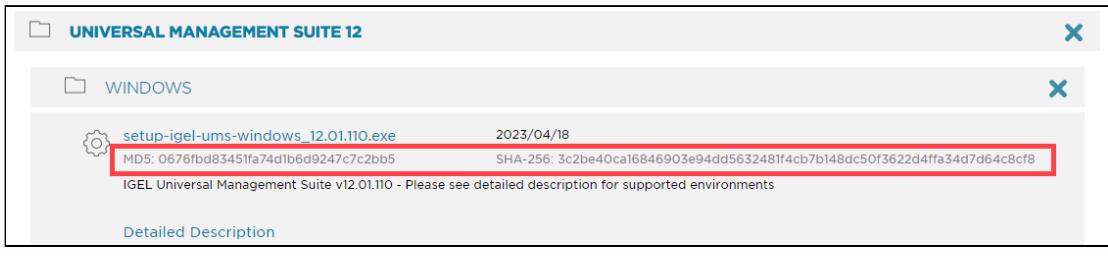
Before starting the update of IGEL Universal Management Suite (UMS), read [IGEL UMS Update \(see page 88\)](#).

- ⚠** Create a [backup of the database \(see page 562\)](#) 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](#)⁸.

- i** For integrity and security purposes, it is recommended to verify the checksum of the downloaded software.



2. Close any other applications and launch the installer.

- i** 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.

- i** **For Update Installations Only**

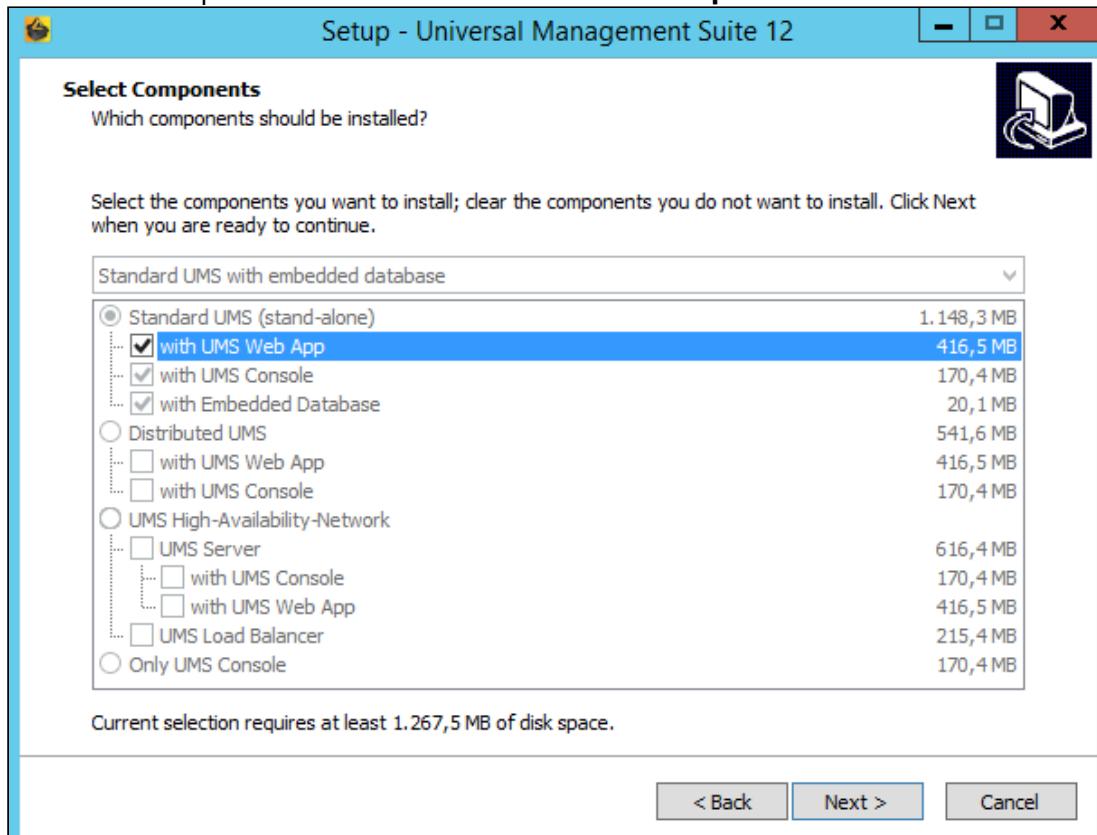
⁸ <https://www.igel.com/software-downloads/>

- As of UMS 12, MDM feature is no longer available. Cancel the upgrade to UMS 12 if you still need the MDM feature:



- Only if you have a Distributed UMS installation: During the update installation, it will be checked whether only one UMS Server is running and the others are stopped. If not, stop all UMS Servers except one and proceed with the update; otherwise, you risk losing data. After the update on this server is complete, you can update the remaining UMS Servers, either simultaneously or one after another.

6. Choose the components to be installed under **Select Components**.



- Standard UMS**
 - with UMS Web App**

- **with UMS Console**
- **with Embedded Database**
- **Distributed UMS**
 - **with UMS Web App**
 - **with UMS Console**
- **UMS High Availability Network**
 - **UMS Server**
 - **with UMS Web App**
 - **UMS Load Balancer**
- **Only UMS Console**

For information on the UMS installation types, see [IGEL UMS Installation](#) (see page 13).
For information on the UMS components, see [Overview of the IGEL UMS](#) (see page 6).

7. Read the **Memory (RAM) requirements** and click **Next** if your system fulfills them.
8. Under **Select Additional Tasks**, specify whether you would like to create shortcuts for the UMS Console and [UMS Administrator](#) (see page 550) on the desktop.
9. If the internal Windows firewall is active on your host: Review the settings under **Windows firewall settings** and change them where necessary. Each port that is activated here will be set as rule in the Windows firewall.

 **UMS 12 Communication Ports**

If you are going to make network changes, consider the following ports and paths:

- For IGEL OS 12 devices, TCP 8443 /device-connector/* is required.
SSL can be terminated at the reverse proxy / external load balancer (see [IGEL UMS Configuration for the External Load Balancer / Reverse Proxy: Example for NGINX with SSL Offloading](#)) or at the UMS Server.
- For importing IGEL OS 12 Apps to the UMS from the IGEL App Portal, the URL <https://app.igel.com/> (TCP 443) is required.
- For the UMS Web App, TCP 8443 /webapp/* and /wums-app/* are required.
- For the UMS Console, the root is required, i.e. TCP 8443 /*
- For IGEL OS 11 devices, TCP 30001 and TCP/UDP 30005 are required.

For more information on UMS ports, see [IGEL UMS Communication Ports](#).

10. 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, if selected, will place shortcuts for the UMS Console and UMS Administrator on the desktop.

-  During a UMS upgrade, e.g. from 6.09 to 6.10 or from 6.x to 12.x, 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.

11. Close the program once the installation is complete by clicking on **Finish**.
12. Start the UMS Console.
13. Connect the UMS Console to the UMS Server with the help of the existing access data.
To connect to the UMS Web App, see How to Log In to the IGEL UMS Web App.

For information on the silent installation of the UMS Console, see [Unattended / Silent Installation of the UMS Console](#) (see page 57).

- i** If you use an external database, check the database connection in the [UMS Administrator](#) (see page 550) > [Datasource](#) (see page 571).
If [SQL Server AD Native](#) (see page 94) is used, you must also set the correct startup type and logon settings for the "IGEL RMGUIServer" service and restart the service. For details, see "[Configuring the UMS Server Windows Service](#)" under "[Setting Up the UMS for SQL Server AD Native](#)" (see page 94).

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 or the [Distributed UMS](#) (see page 13) solution.
- In other cases, the use of the embedded database is suitable. It is included in the standard UMS installation, see [IGEL UMS Installation under Windows](#) (see page 50) or [IGEL UMS Installation under Linux](#) (see page 20).
- ⓘ For details on the supported database systems, see the "Supported Environment" section of the release notes. 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 550) > [Datasource](#) (see page 571).
- ⚠ 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 of the IGEL UMS](#) (see page 563).

See also Migrating a UMS Database From Embedded DB to Microsoft SQL Server.

-
- [Oracle](#) (see page 99)
 - [Oracle RAC](#) (see page 100)
 - [Microsoft SQL Server/Cluster with Native SQL Authentication](#) (see page 101)
 - [Microsoft SQL Server/Cluster with Native Active Directory \(AD\) Authentication](#) (see page 117)
 - [Microsoft SQL Server/Cluster with Active Directory \(AD\) Authentication via Kerberos](#) (see page 137)
 - [PostgreSQL](#) (see page 157)
 - [Apache Derby as a Data Source for the IGEL UMS](#) (see page 159)
 - [Using an AWS Aurora PostgreSQL Database with IGEL Universal Management Suite \(UMS\)](#) (see page 161)

Oracle

Configuration Hints

The UMS Server runs several services in parallel to provide the functionality. These services establish connections to the database. The database must therefore allow a certain number of connections. The expected maximum number of connections is
 $128 * [\text{number of UMS Servers}]$
Please make sure that your database can handle these connections.

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 550), 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.

i 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 550) to set up a new **Oracle RAC** type data source for each server.

Microsoft SQL Server/Cluster with Native SQL Authentication

This article describes the setup of a UMS database using a Microsoft SQL server, the configuration of the database login, and the connection of the IGEL Universal Management Suite (UMS) to the database using native SQL authentication.

Creating the UMS Database

It is recommended to create a separate database with a specific schema for the UMS.

Configuration Hints

The UMS Server application runs several services in parallel to provide the required functionality. These services establish separate connections to the database. The database must therefore allow a certain number of connections. The expected maximum number of connections is $128 * [\text{number of UMS Servers}]$. Please make sure that your database can handle these connections.

Using the SQL Management Console

- In the SQL Management Console, select **New Query** and enter the script below; replace the placeholders accordingly.

Do NOT use the schema **dbo** for the UMS database tables!

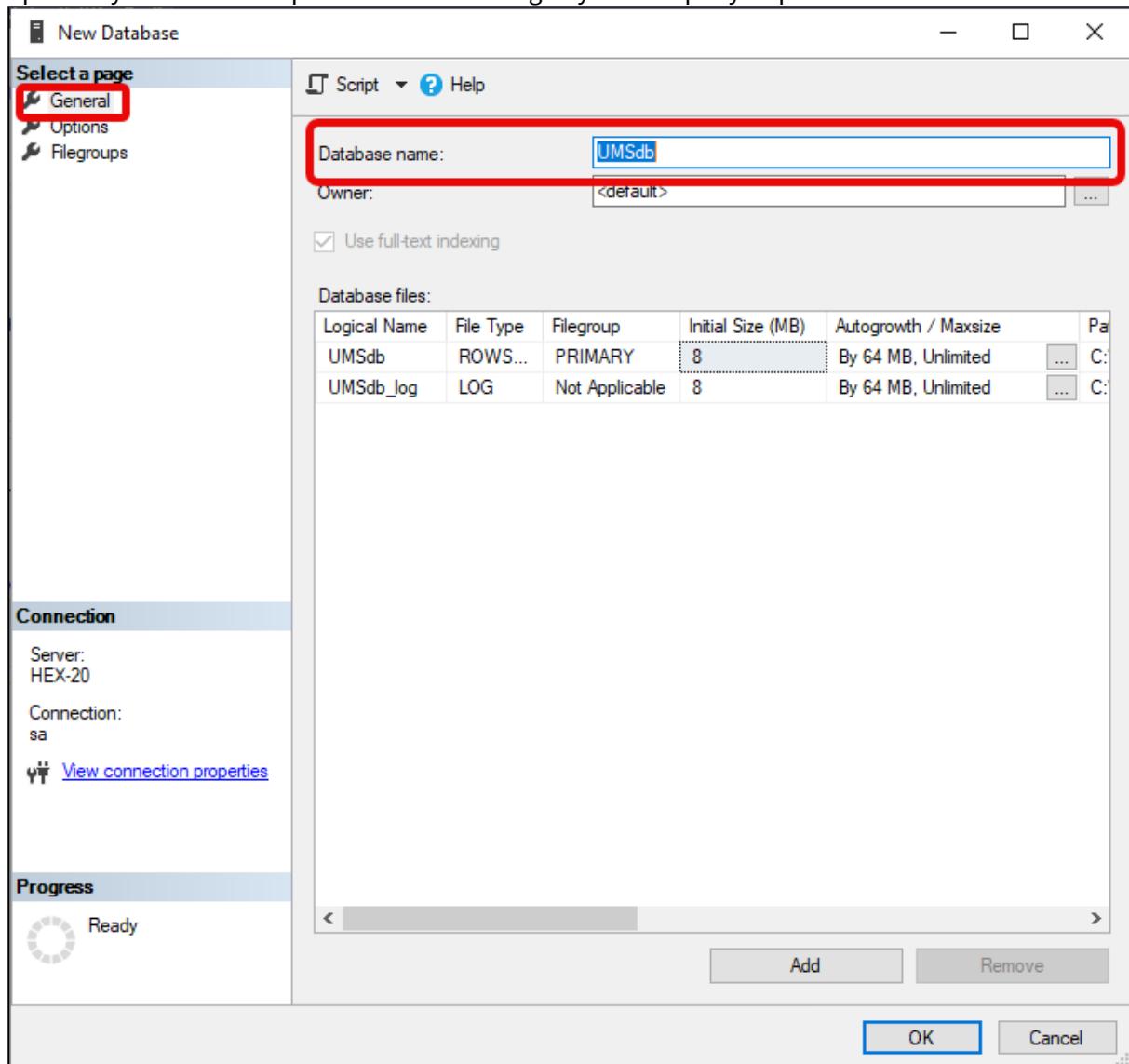
- <database_name> : The name for the UMS database
- <schema_name> : The name of the schema for the UMS database

```
USE [master]
GO
CREATE DATABASE [<database_name>];
GO
USE [<database_name>];
GO
CREATE SCHEMA [<schema_name>];
GO
```

Using the GUI

1. In SQL Server Management Studio, right-click **Databases** and select **New Database**.
2. Under **General**, give the database a name.

3. Optionally set additional parameters according to your company requirements.



Configuring the UMS User, Schema, and Database Permissions

Using the SQL Management Console

- ▶ In the SQL Management Console, select **New Query** and enter the script below; please note the following.
 - <ums_user> : The local alias in the database <database_name> of the real user <sql_user>

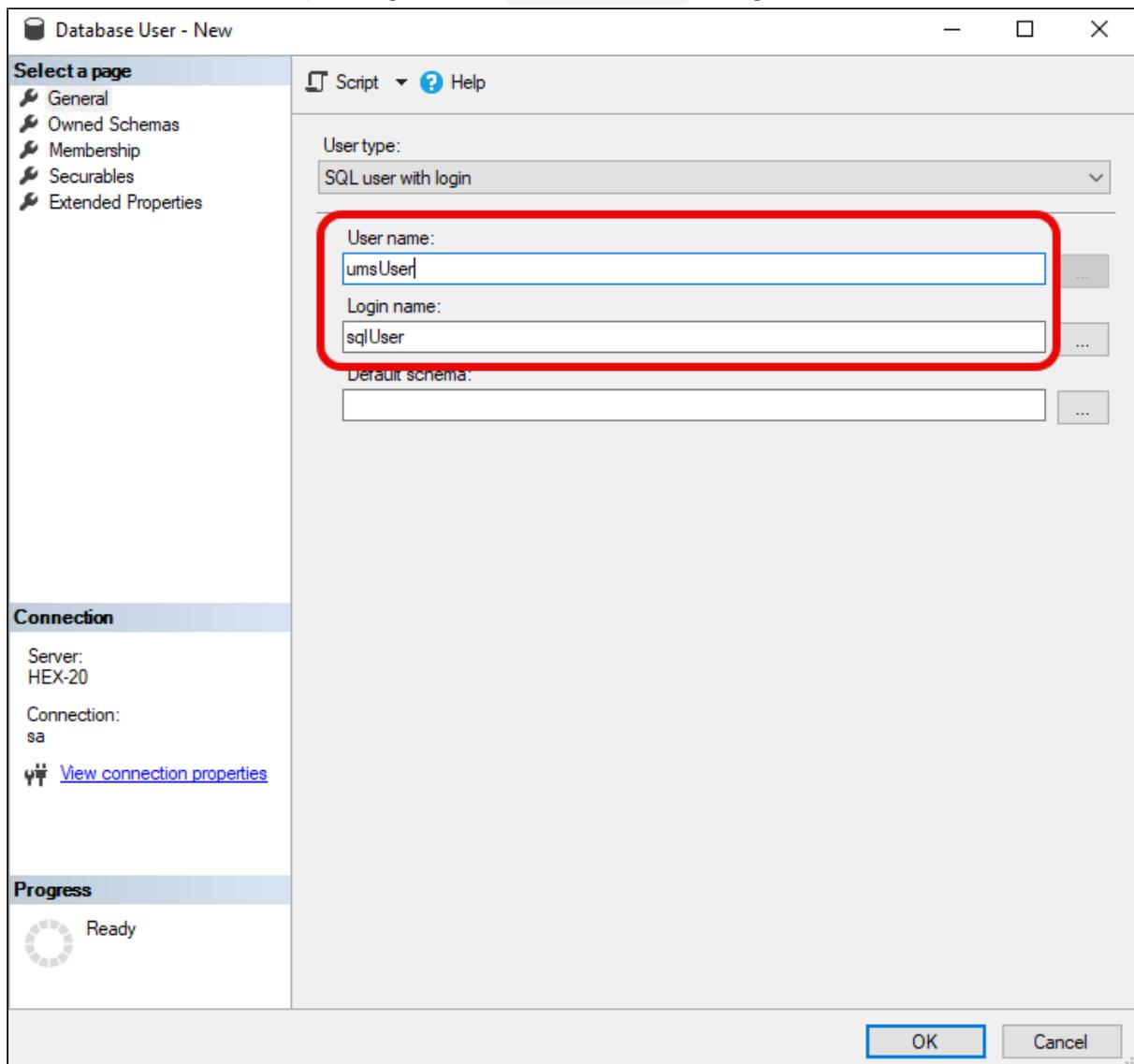
- According to the Microsoft SQL Server documentation, the <ums_user> must be db_owner to create and alter tables.

```
USE [<database_name>]
GO
CREATE USER [<ums_user>] FOR LOGIN [<sql_user>];
GO
ALTER ROLE [db_owner] ADD MEMBER [<ums_user>];
GO
ALTER USER [<ums_user>] WITH DEFAULT_SCHEMA = [<schema_name>];
GO
ALTER AUTHORIZATION ON SCHEMA::[<schema_name>] TO [<ums_user>]
GO
```

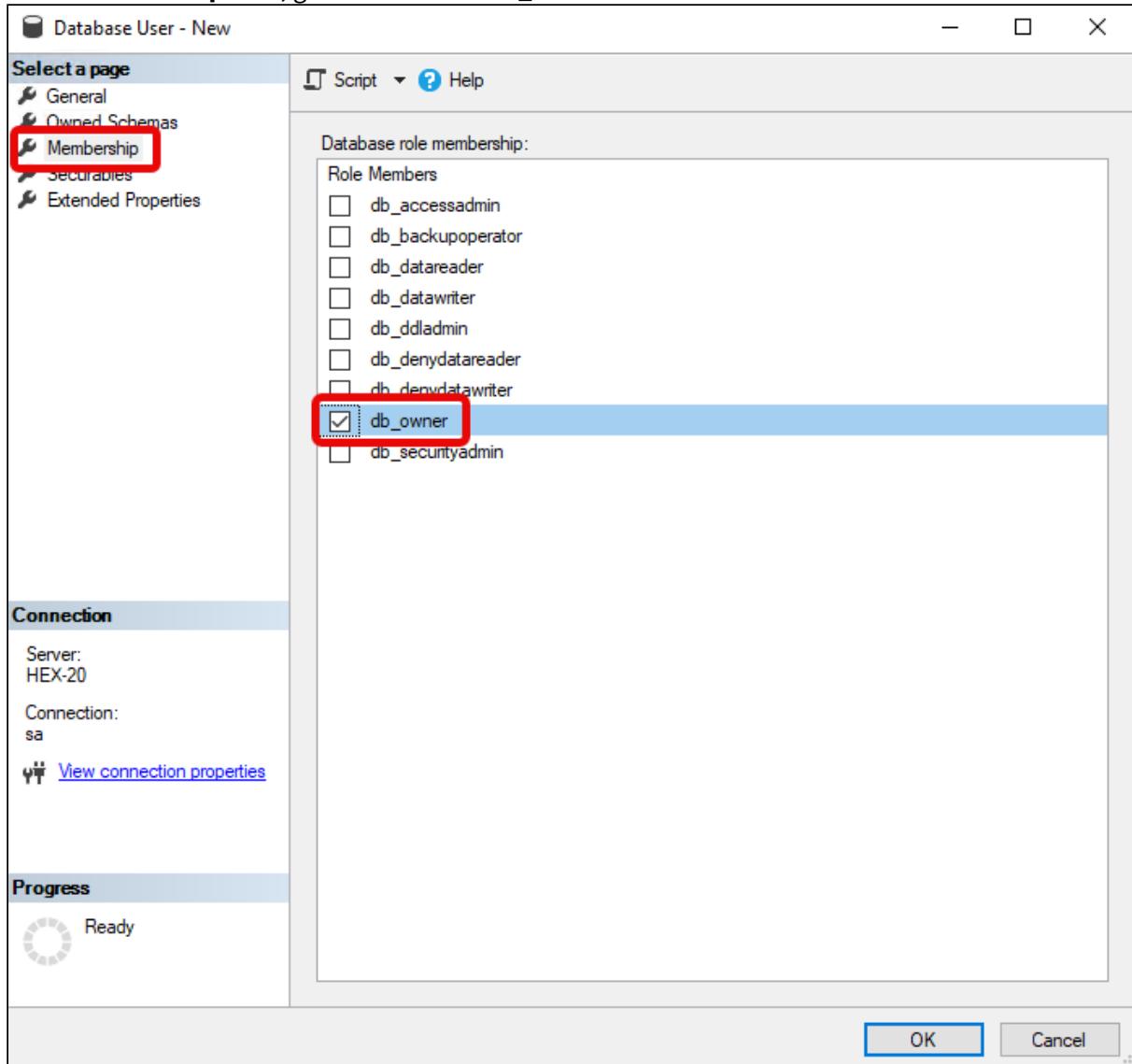
Using the GUI

- In SQL Server Management Studio, open the database that was created in [Creating the UMS Database \(see page 101\)](#).
- Under **Security > Users**, right-click **New User**.

3. Under **General**, search for your login name (<sql_user>) and give the user a name.

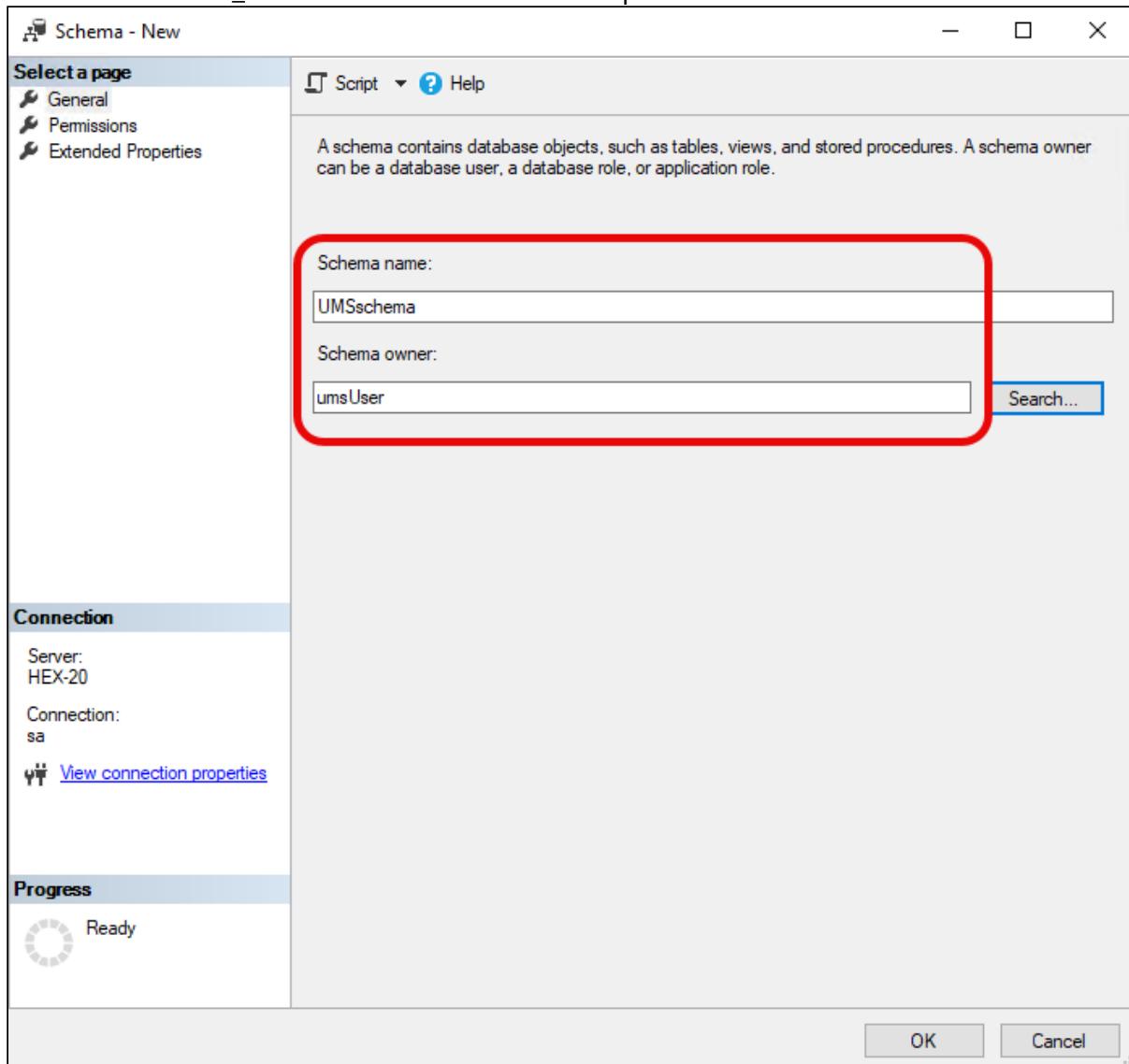


4. In the **Membership** area, give the user the **db_owner** role.



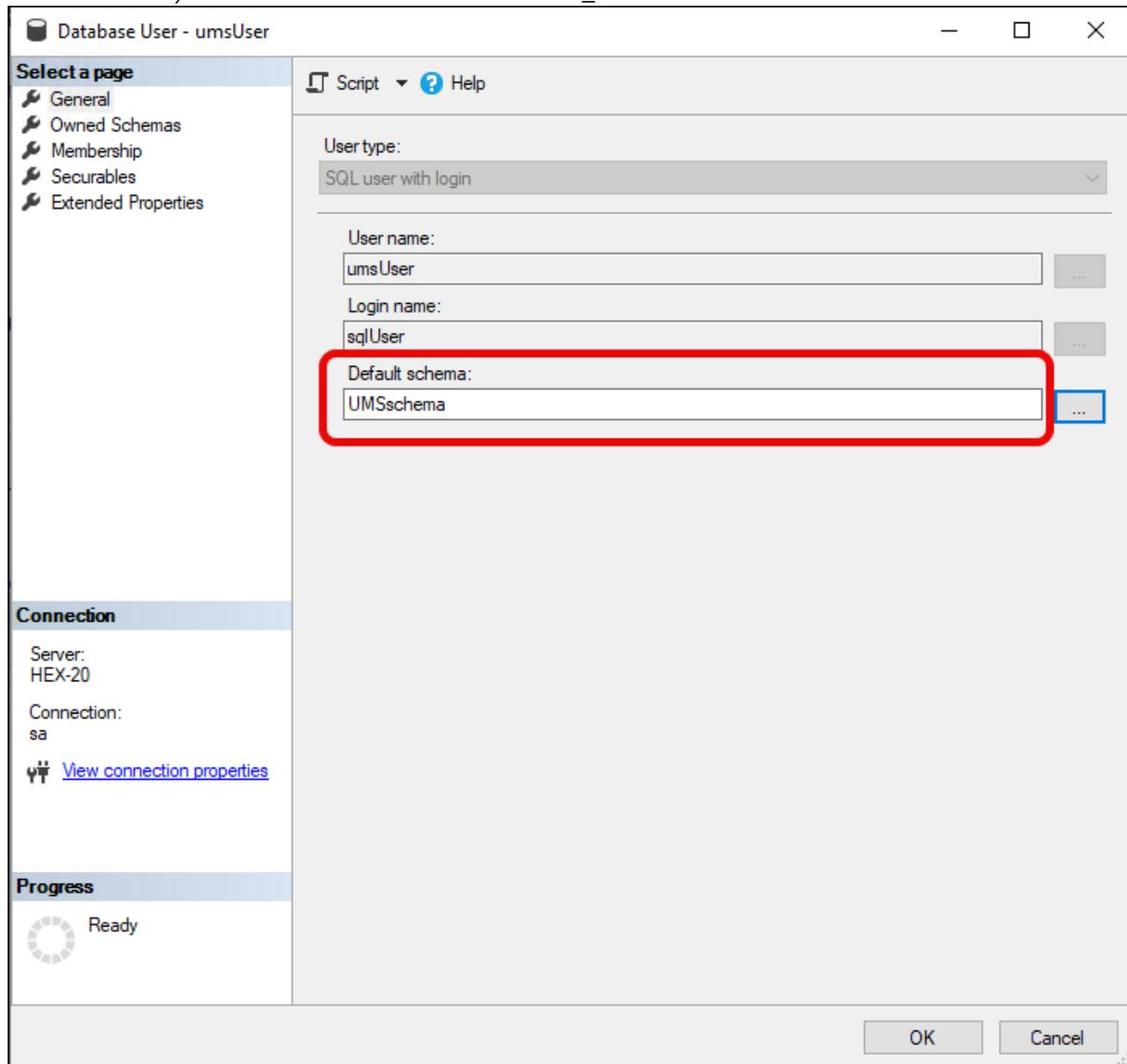
5. Go to **Security > Schemas** and right-click on **New Schema**.

6. Search for the <ums_user> as the **Schema owner** and provide a **Schema name**.



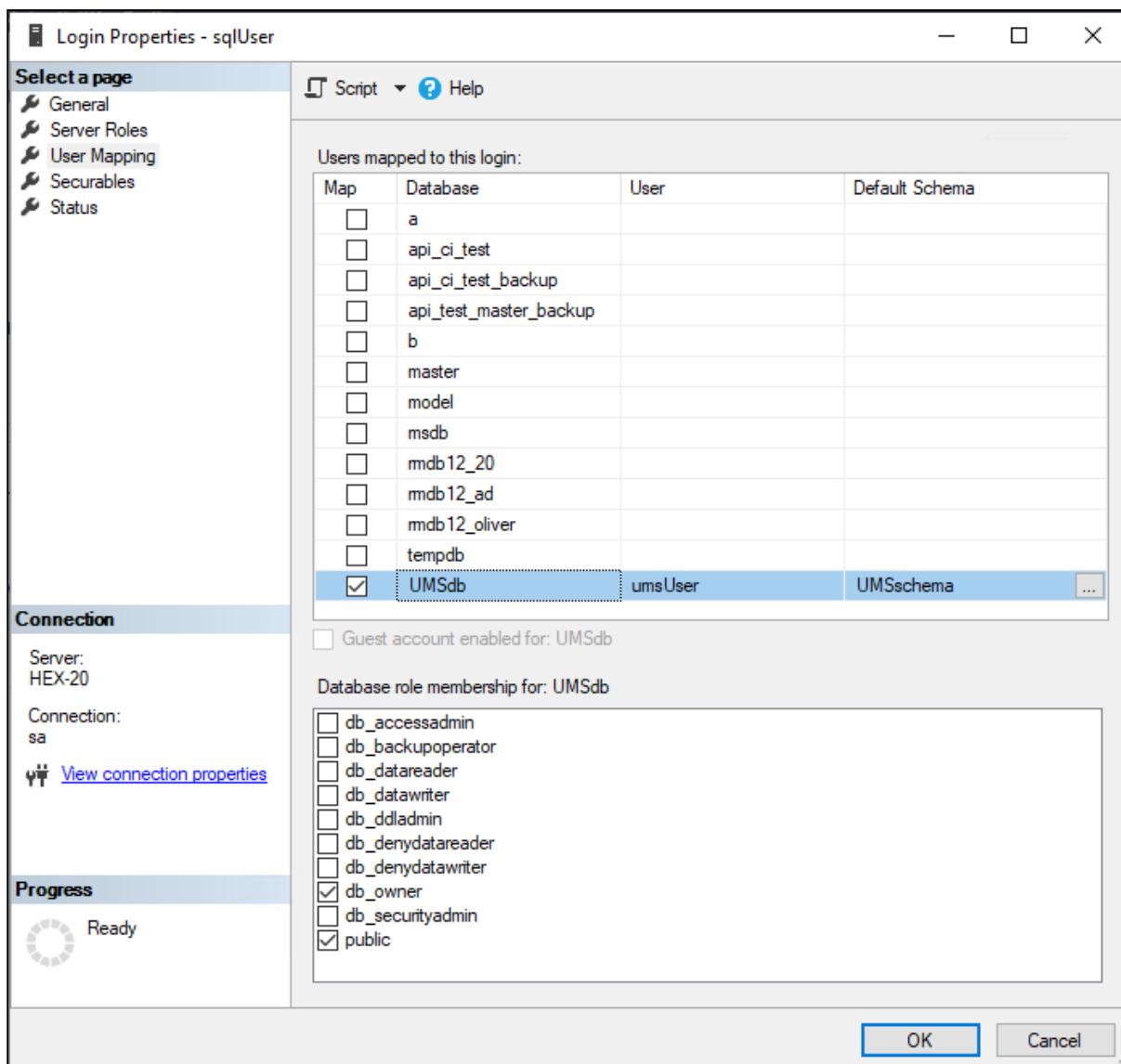
7. Under **Security > Users** in your UMS database, double-click on the <ums_user>.

8. Under **General**, set the default schema to <schema_name>.



9. Under **Security > Logins > Users**, double-click on the <sql_user>.

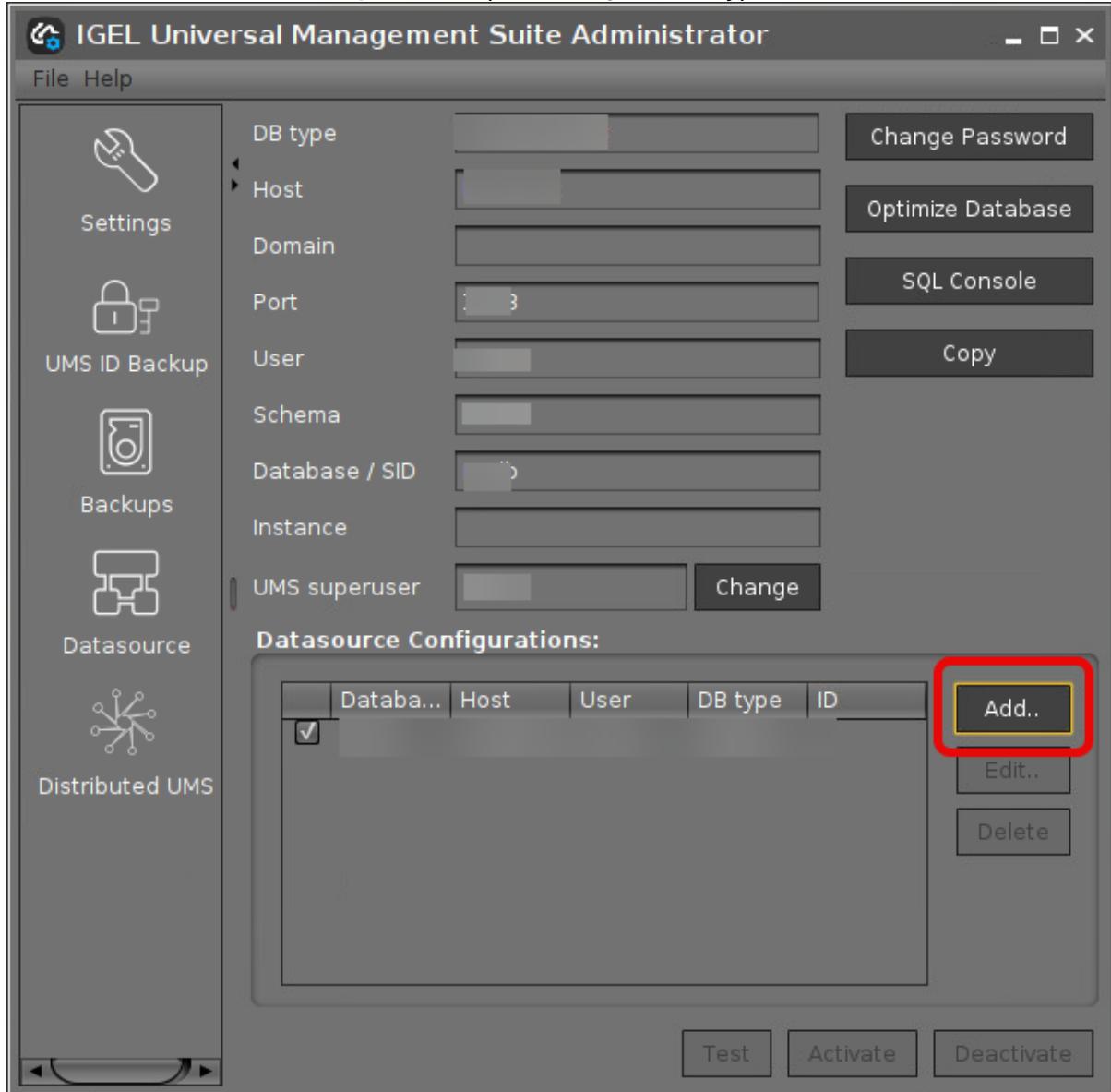
10. In the **User Mapping** area, check the mapping of the UMS database, the user, and the default schema.

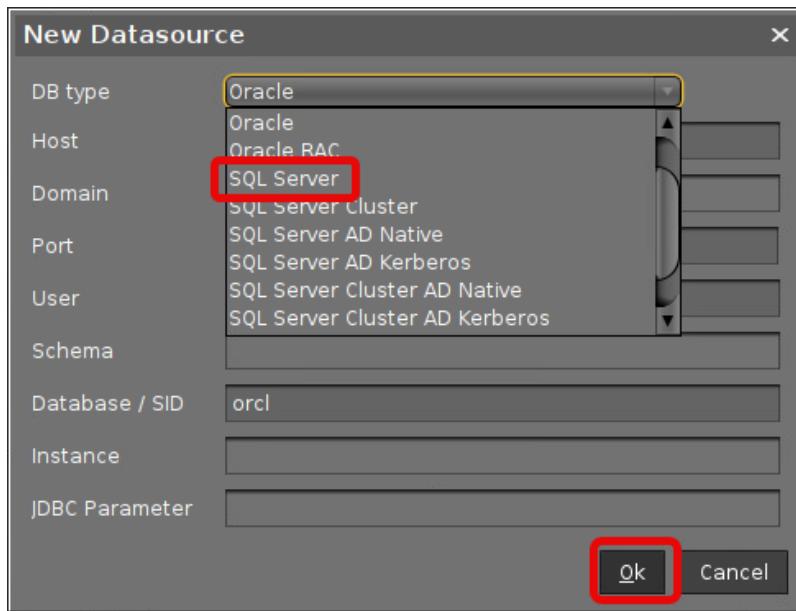


11. Depending on whether you are using a single server or a cluster for your Microsoft SQL database, continue with [Connecting the UMS to the Database \(Single Server Instance\)](#) (see page 109) or [Connecting the UMS to the Database \(Cluster\)](#) (see page 113),

Connecting the UMS to the Database (Single Server Instance)

1. In the [UMS Administrator](#) (see page 550), set up a new **SQL Server** type data source.

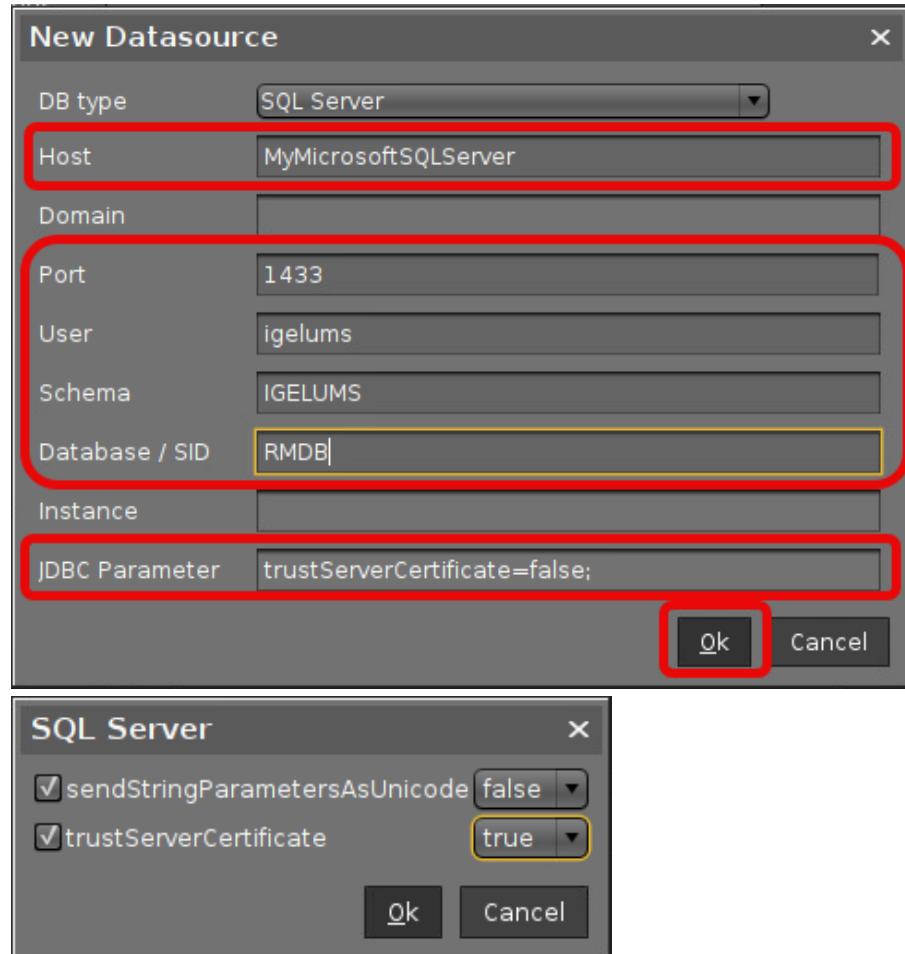


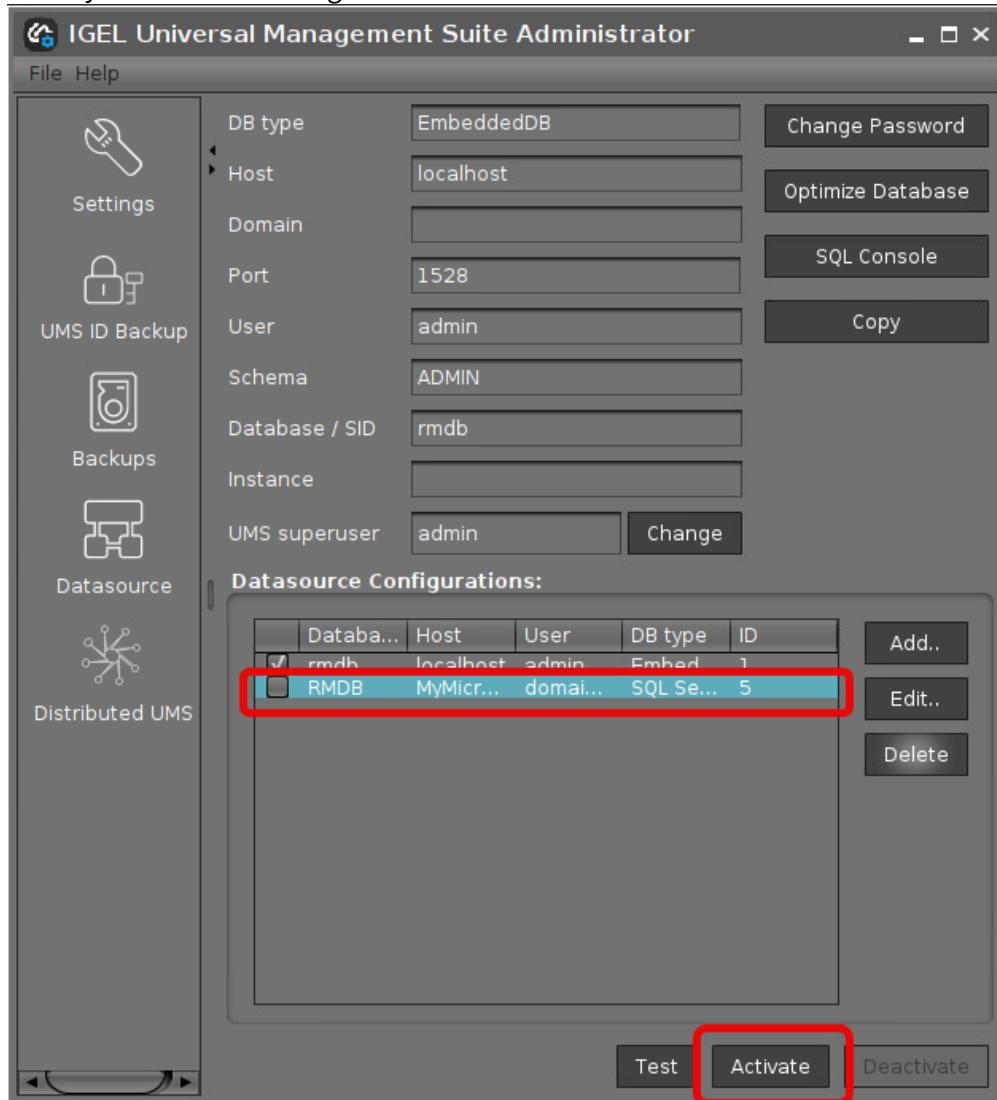


2. Edit the data as follows:

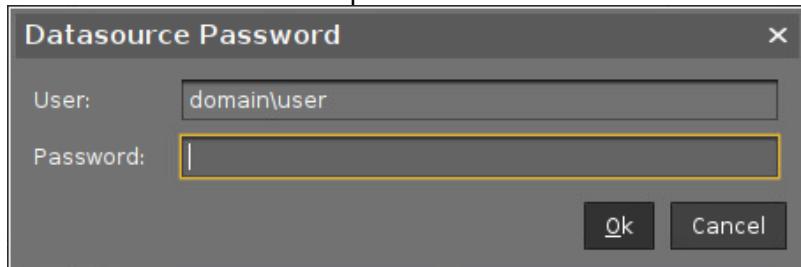
- **Host:** The hostname or IP address of the Microsoft SQL server; if you deploy MS SQL Server Always On Availability Groups, enter the domain name of the Always On Availability Group listener.
- **Port:** The port on which the Microsoft SQL Server listens for requests. (Default: 1433)
- **User:** The login name for connecting to the database
- **Schema:** The database schema
- **Database / SID:** The database name
- **JDBC Parameter** (double-click):
 - **sendStringParametersAsUnicode: false**

- **trustServerCertificate: true**



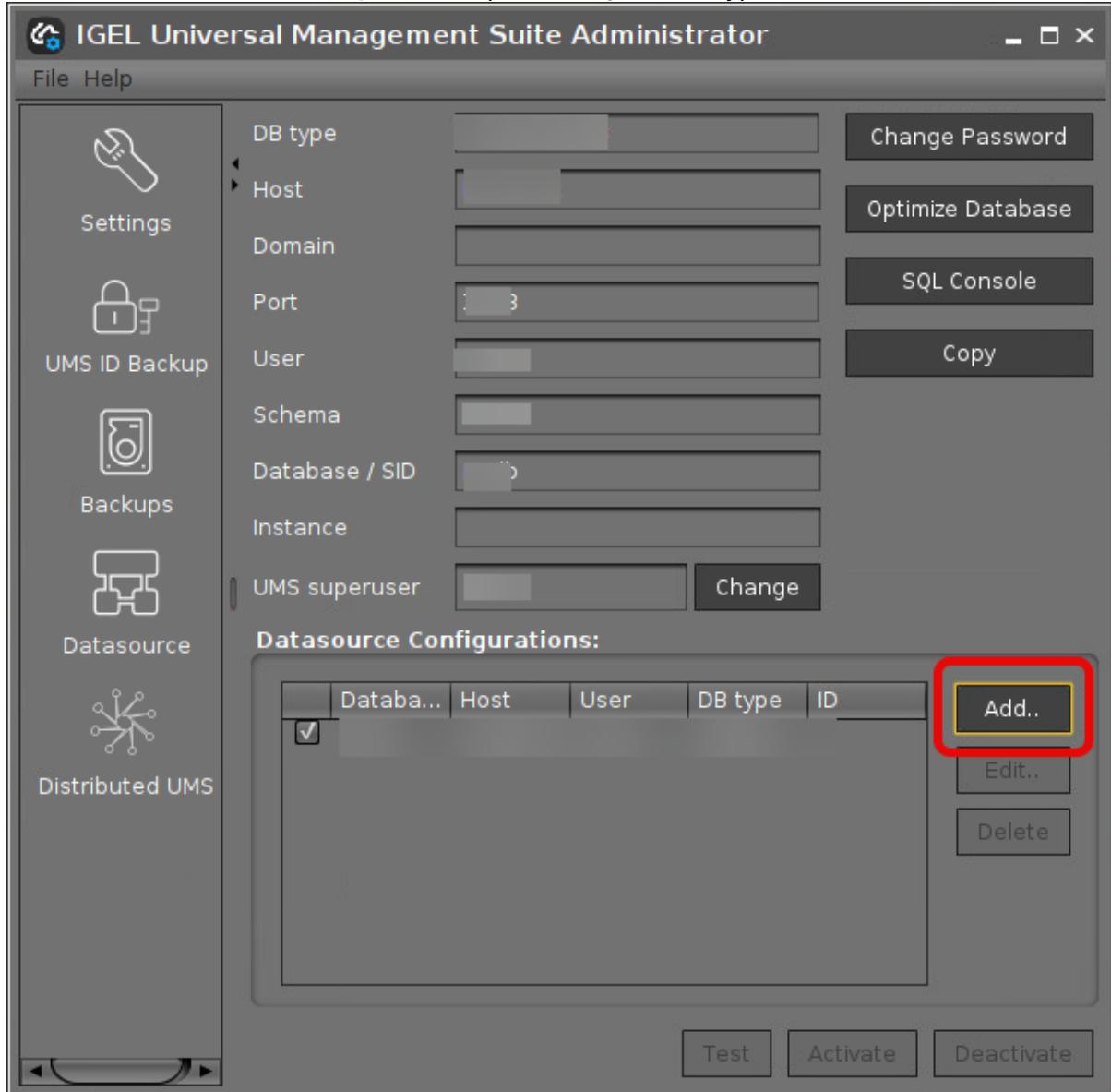
3. Select your database configuration and click **Activate**.

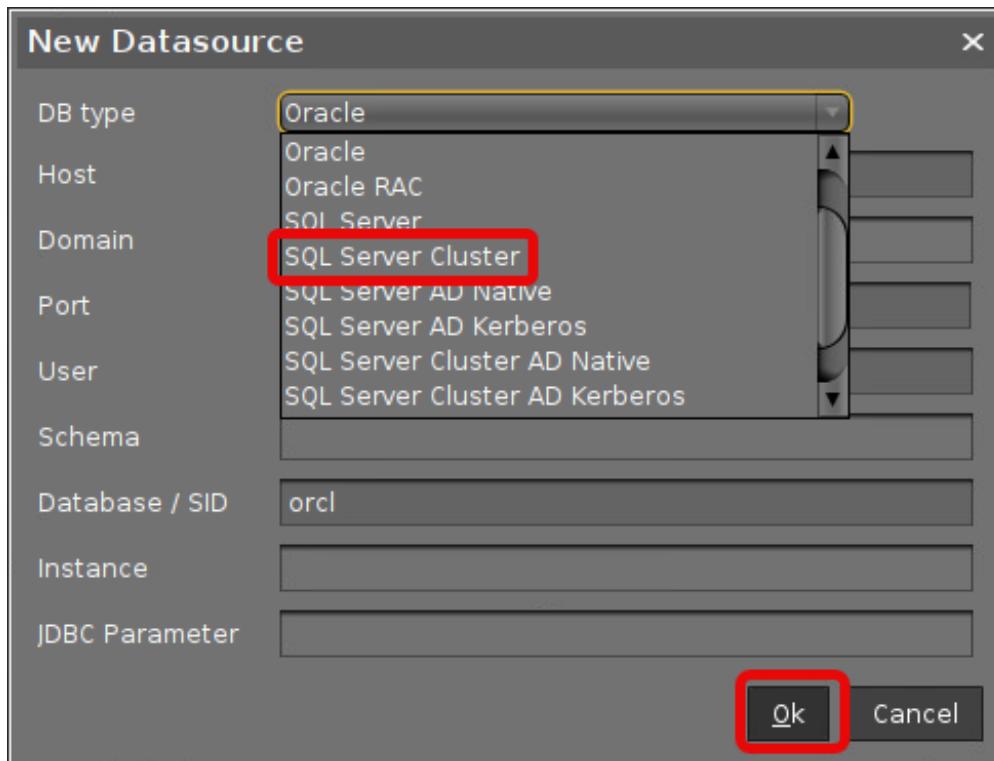
4. Enter the username and the password for the connection.



Connecting the UMS to the Database (Cluster)

1. In the [UMS Administrator](#) (see page 550), set up a new **SQL Server** type data source.

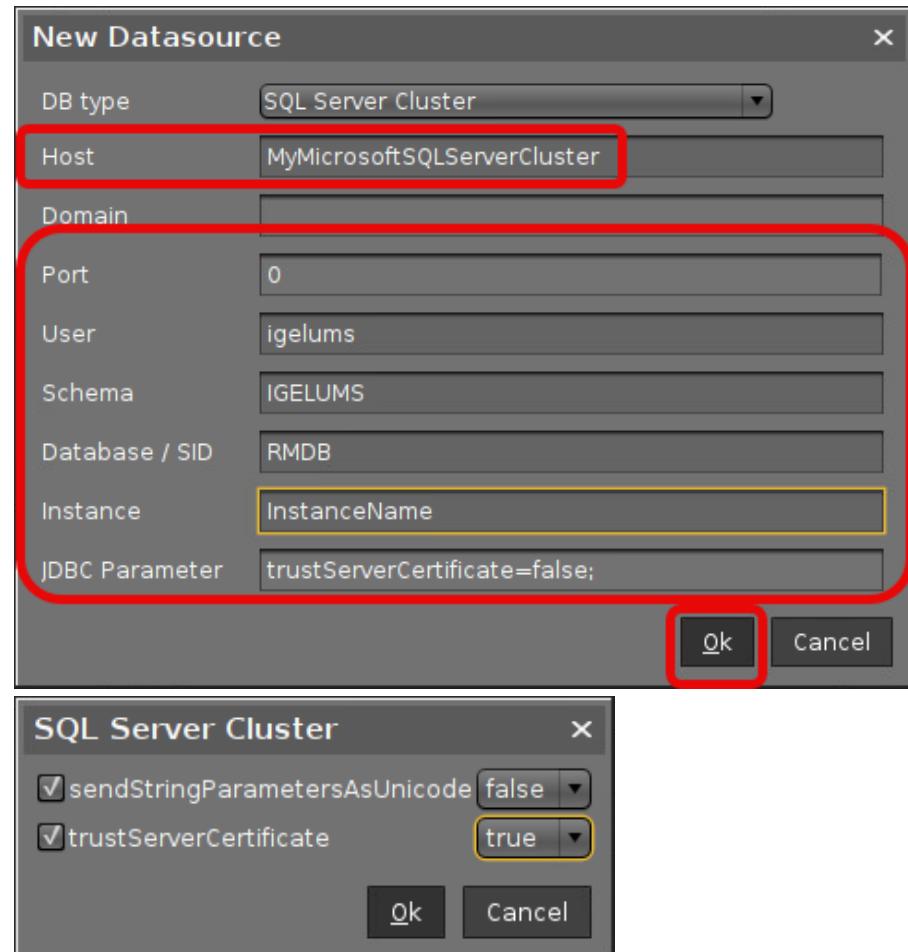




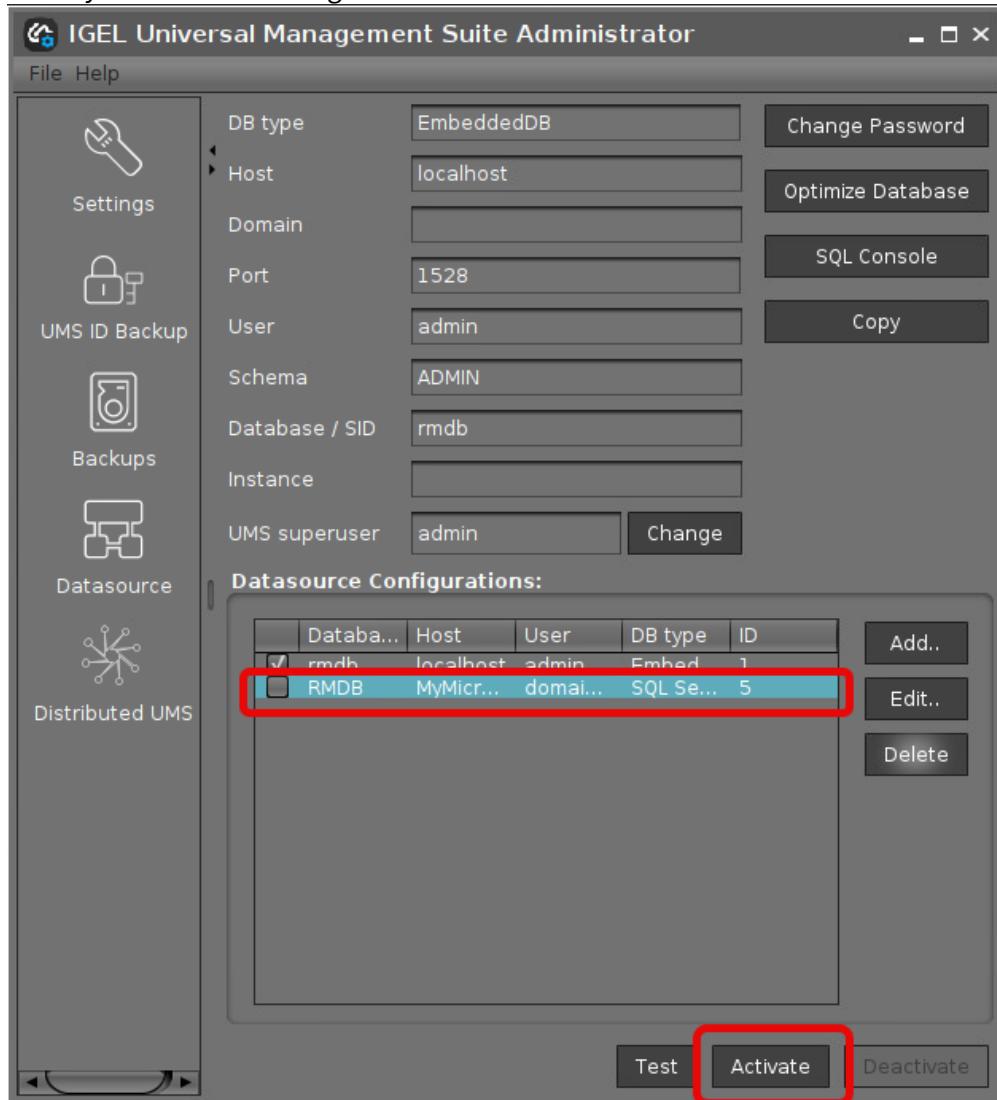
2. Edit the data as follows:

- **Host:** The hostname or IP address of the Microsoft SQL server; if you deploy MS SQL Server Always On Availability Groups, enter the domain name of the Always On Availability Group listener.
- **Port:** The port on which the Microsoft SQL Server listens for requests. (Default: 1433)
- **User:** The login name for connecting to the database
- **Schema:** The database schema
- **Database / SID:** The database name
- **Instance:** The instance for your Microsoft SQL Server Cluster
- **JDBC Parameter** (double-click):
 - **sendStringParametersAsUnicode: false**

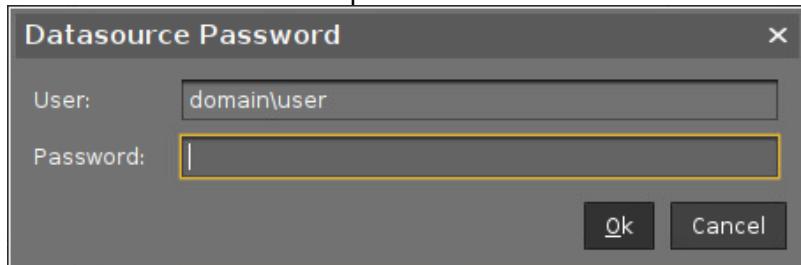
- **trustServerCertificate: true**



3. Select your database configuration and click **Activate**.



4. Enter the username and the password for the connection.



Microsoft SQL Server/Cluster with Native Active Directory (AD) Authentication

This article describes the setup of a UMS database using a Microsoft SQL server, the configuration of the database login, and the connection of the IGEL Universal Management Suite (UMS) to the database using native Active Directory (AD) authentication.

⚠ Using Microsoft Active Directory (AD) to connect your UMS to a Microsoft SQL server requires a deep understanding of your environment. For most environments, it is recommended to use native SQL authentication.

Prerequisites

For connecting the UMS Server to your UMS database with Microsoft Active Directory (AD) native authentication, the following components must be available:

- A Windows domain server
- The Microsoft SQL server on which the UMS database is running is located in the Windows domain
- The UMS Server and the UMS Administrator are located in the Windows domain
- The SQL service account has local administration rights to the UMS Server

Creating the UMS Database

It is recommended to create a separate database with a specific schema for the UMS.

⚠ Configuration Hints

The UMS Server application runs several services in parallel to provide the required functionality. These services establish separate connections to the database. The database must therefore allow a certain number of connections. The expected maximum number of connections is $128 * [\text{number of UMS Servers}]$. Please make sure that your database can handle these connections.

Using the SQL Management Console

- In the SQL Management Console, select **New Query** and enter the script below; replace the placeholders accordingly.

⚠ Do NOT use the schema **dbo** for the UMS database tables!

- <database_name> : The name for the UMS database
- <schema_name> : The name of the schema for the UMS database

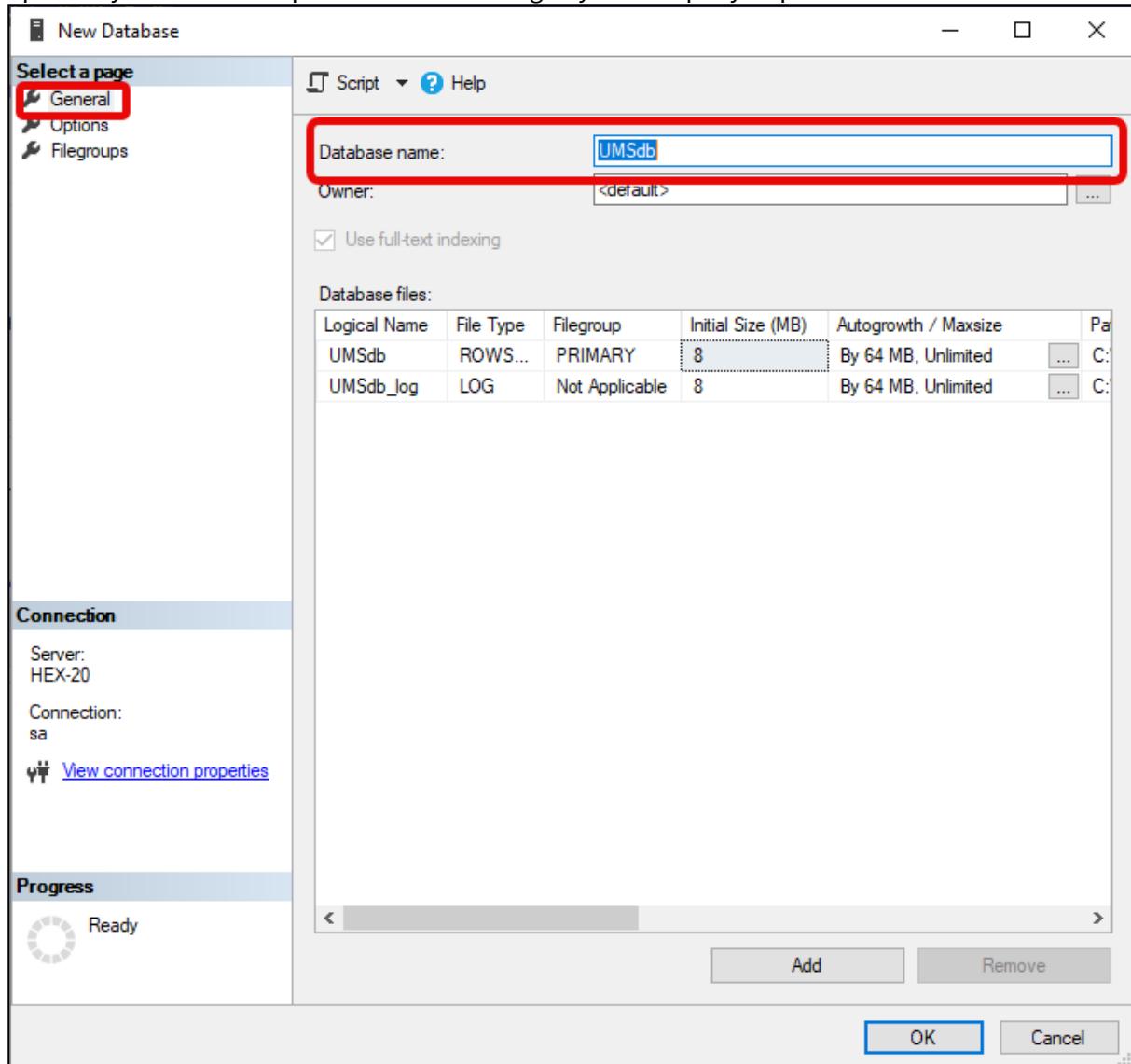
```
USE [master]
GO
```

```
CREATE DATABASE [<database_name>];  
GO  
USE [<database_name>];  
GO  
CREATE SCHEMA [<schema_name>];  
GO
```

Using the GUI

1. In SQL Server Management Studio, right-click **Databases** and select **New Database**.
2. Under **General**, give the database a name.

3. Optionally set additional parameters according to your company requirements.



Adding Users and a Group to the Windows Domain

- ▶ Make sure that your Windows domain contains users who have the following permissions:
 - Log in to the database server
 - Log in to the database that is connected to the UMS
 - Log in to the server with the UMS components
 - Run the UMS Server as a Windows service

- i** It is recommended to create a group in the domain that will contain the users for the database and put the users for the UMS into this group. This group will become the owner of the UMS database, allowing all users in the group to work with the database.

Adding the User or Group to Microsoft SQL Server

- i** Note: If the AD user you are going to use to connect to the Microsoft SQL Server already has an SQL login entry, or is in a group with login access, you can skip this step and continue with [Configuring the UMS User, Schema, and Database Permissions](#) (see page 122).

Using the SQL Management Console

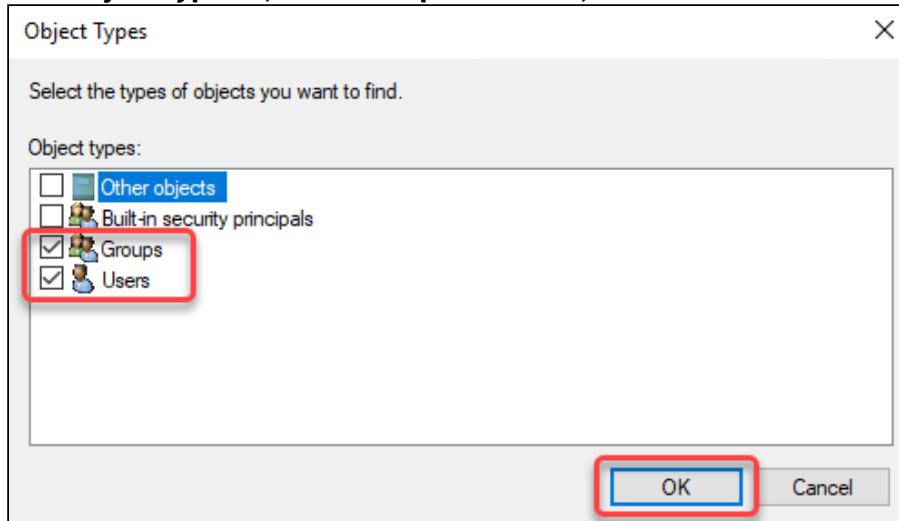
1. In SQL Server Management Studio, select **New Query**.
2. Use the following script to create the database login; replace <ad_user> with the AD user you want to use for connecting.

```
USE [master]
GO
CREATE LOGIN [[<ad_user>]] FROM WINDOWS;
GO
```

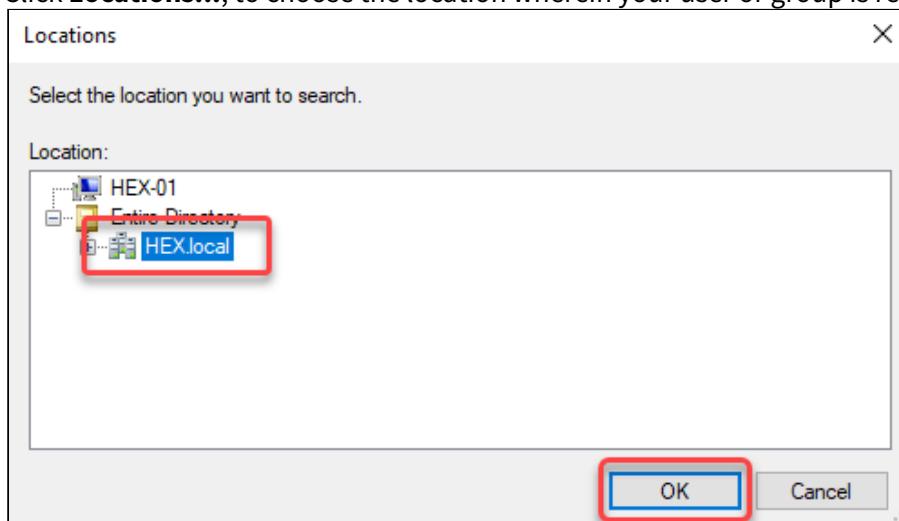
Using the SQL Server Management Studio (GUI Mode)

1. Connect to the database with the SQL Server Management Studio.
2. Open the **Security** branch, right-click on **Logins**, and select **New Login**.
3. Choose **Windows Authentication** for the login, and click **Search**.

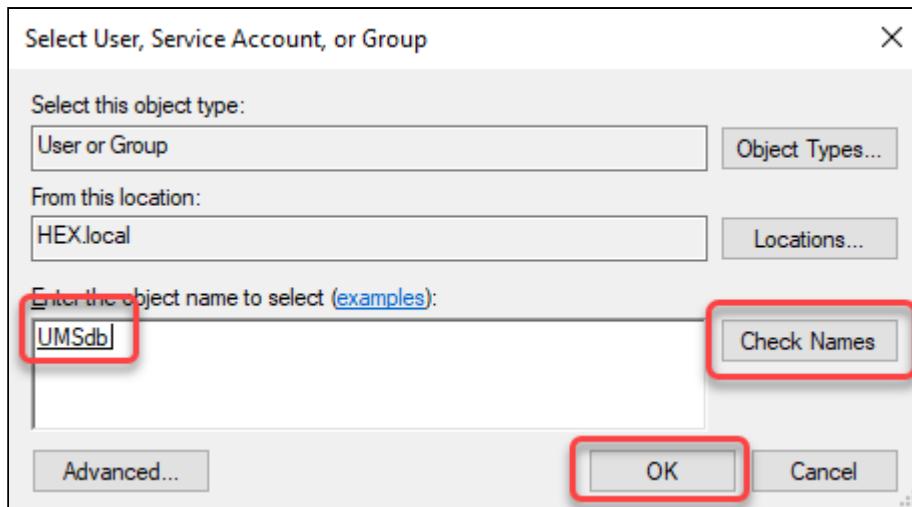
4. Click **Object Types...**, select **Groups** and **Users**, and click **OK**.



5. Click **Locations...**, to choose the location wherein your user or group is residing, and click **OK**.



6. Enter the name of the group or user, click **Check Names**, select the name of your user or group, and click **OK**.



If you have selected a group, all users in this group will be able to access the databases where this group is defined as the database owner. Also, if you selected a group, you should add at least one user who will become the main database owner.

Configuring the UMS User, Schema, and Database Permissions

Using the SQL Management Console

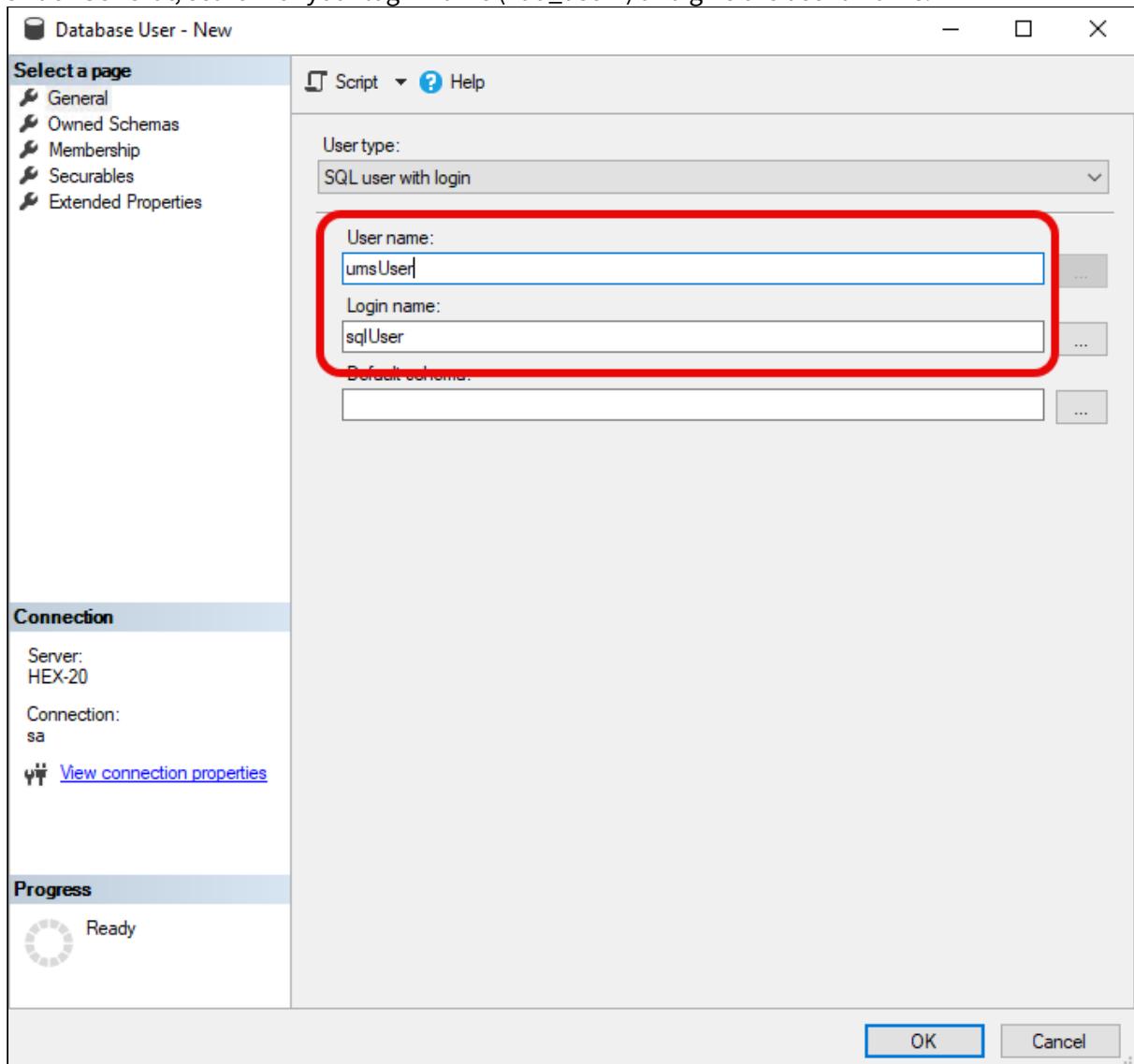
- ▶ In the SQL Management Console, select **New Query** and enter the script below; please note the following.
 - <ums_user> : The local alias in the database <database_name> of the real user <ad_user>
 - According to the Microsoft SQL Server documentation, the <ums_user> must be db_owner to create and alter tables.

```
USE [<database_name>]
GO
CREATE USER [<ums_user>] FOR LOGIN [<ad_user>];
GO
ALTER ROLE [db_owner] ADD MEMBER [<ums_user>];
GO
ALTER USER [<ums_user>] WITH DEFAULT_SCHEMA = [<schema_name>];
GO
ALTER AUTHORIZATION ON SCHEMA::[<schema_name>] TO [<ums_user>]
GO
```

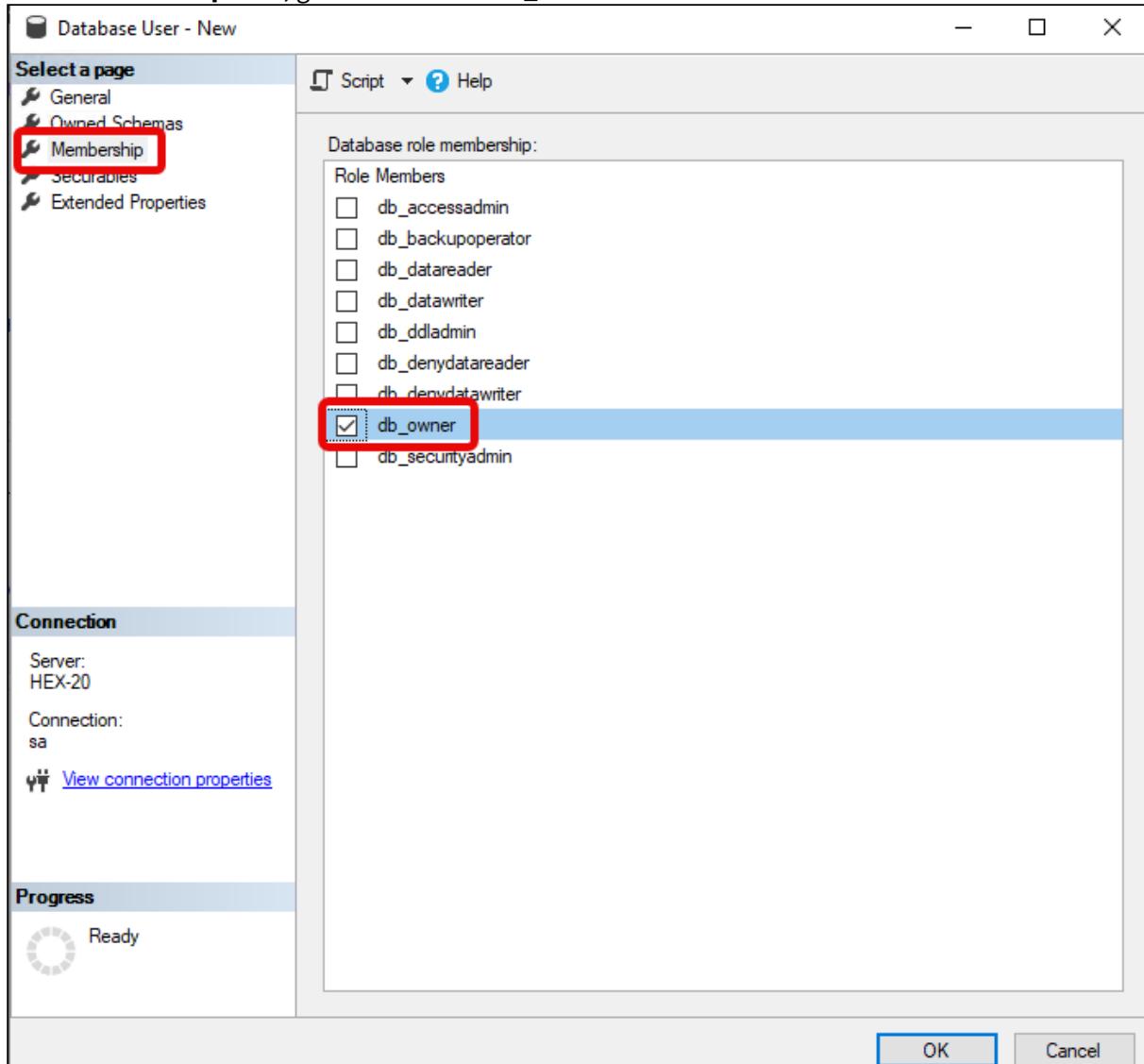
Using the GUI

1. In SQL Server Management Studio, open the database that was created in [Creating the UMS Database](#) (see page 117).

2. Under **Security > Users**, right-click **New User**.
3. Under **General**, search for your login name (<ad_user>) and give the user a name.

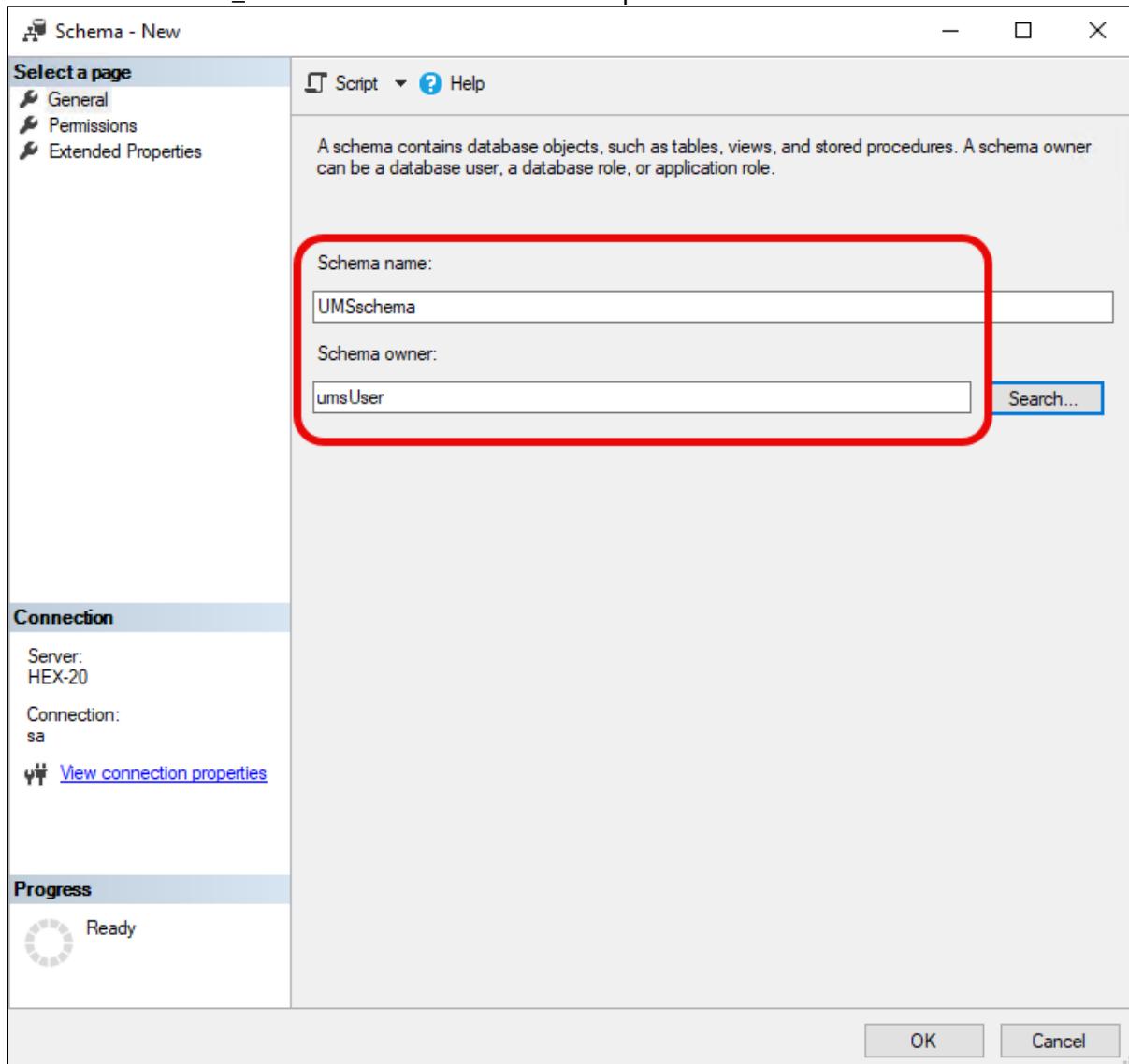


4. In the **Membership** area, give the user the **db_owner** role.



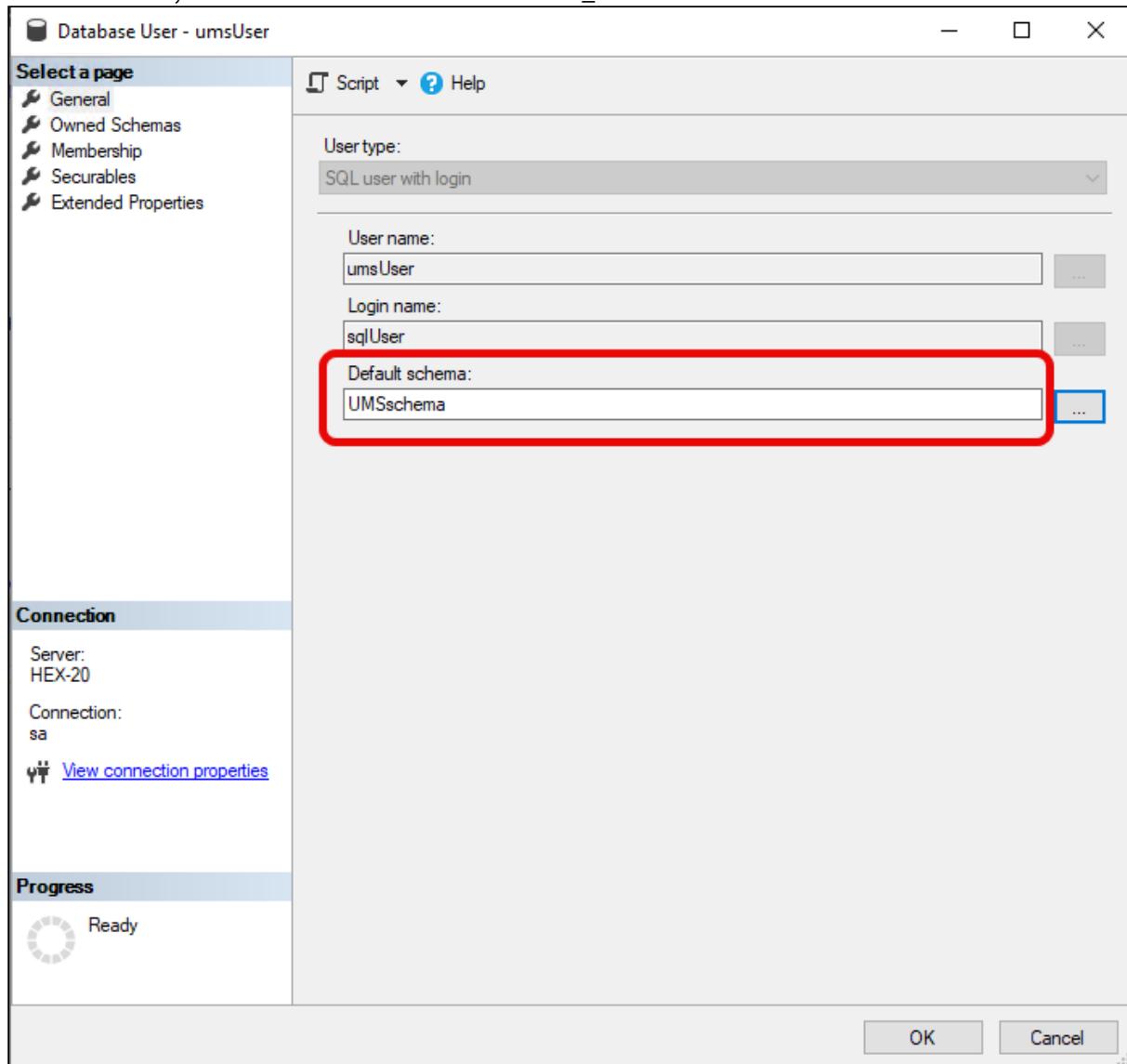
5. Go to **Security > Schemas** and right-click on **New Schema**.

6. Search for the <ums_user> as the **Schema owner** and provide a **Schema name**.



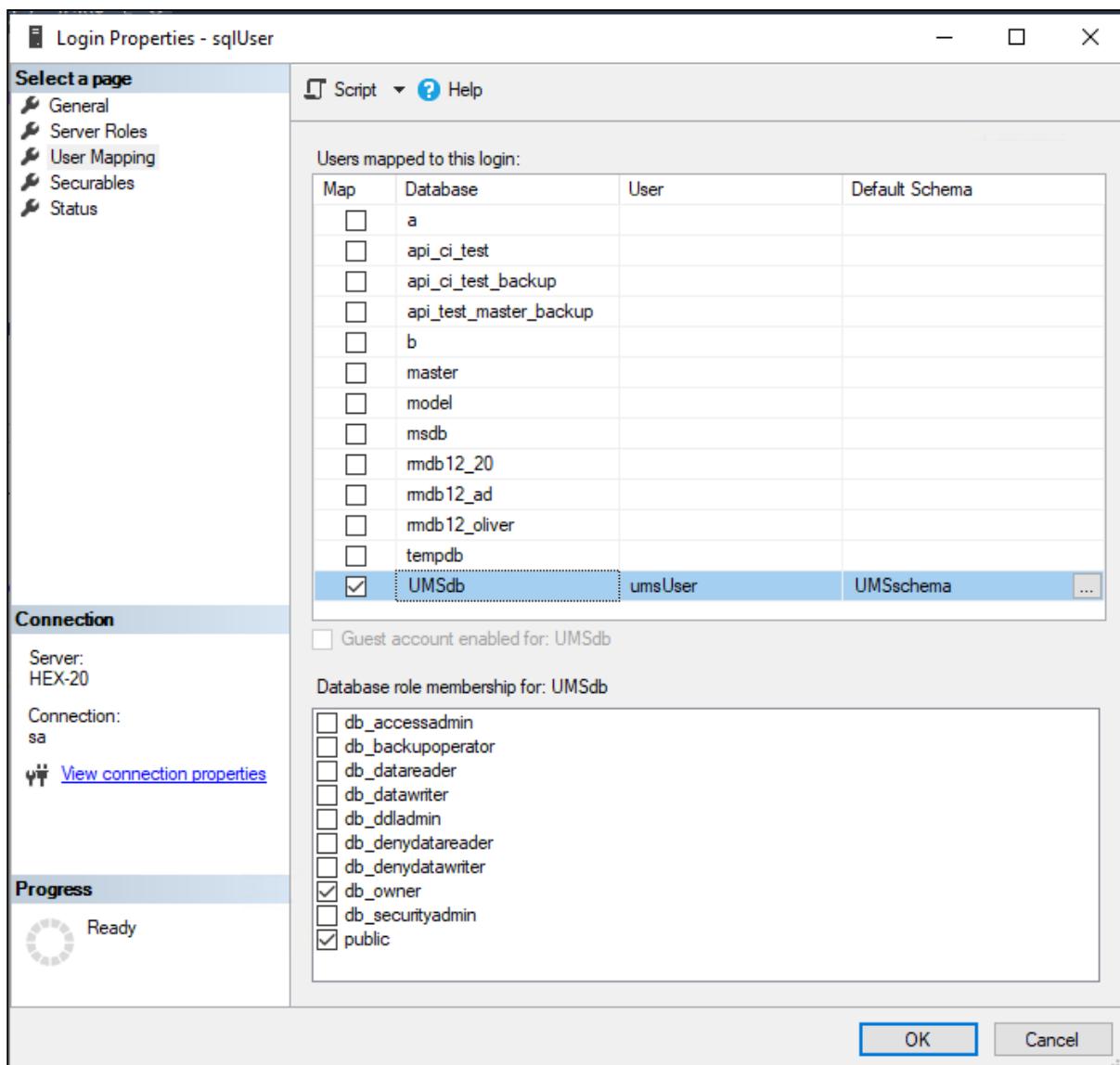
7. Under **Security > Users** in your UMS database, double-click on the <ums_user>.

8. Under **General**, set the default schema to <schema_name>.



9. Under **Security > Logins > Users**, double-click on the <ad_user>.

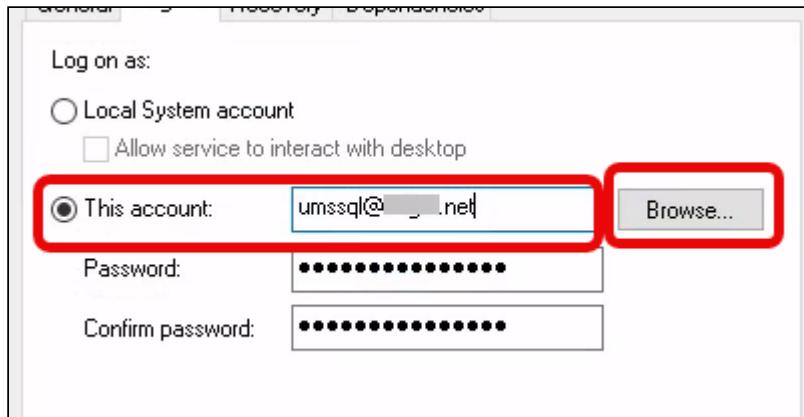
10. In the **User Mapping** area, check the mapping of the UMS database, the user, and the default schema.



Configuring the UMS Services

1. Log into the UMS Server with the credentials configured for connecting to the UMS database on the Microsoft SQL Server.
2. Open **services.msc** and right-click the **IGEL Remote Manager Server** service.
3. Select **Properties** and navigate to the **Log On** tab.

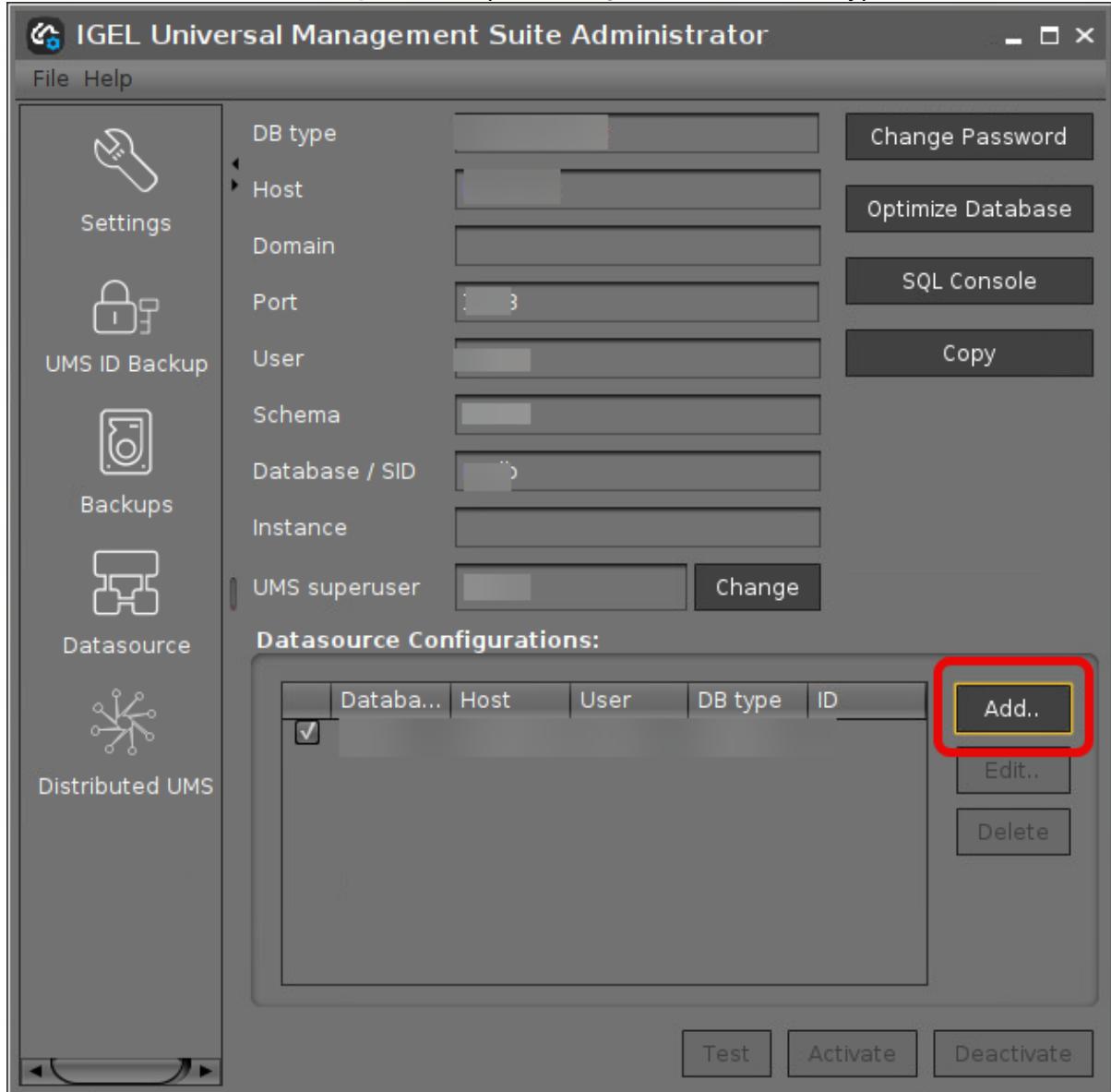
4. Select **This Account** and use the **Browse** button to find the one that owns the SQL database.

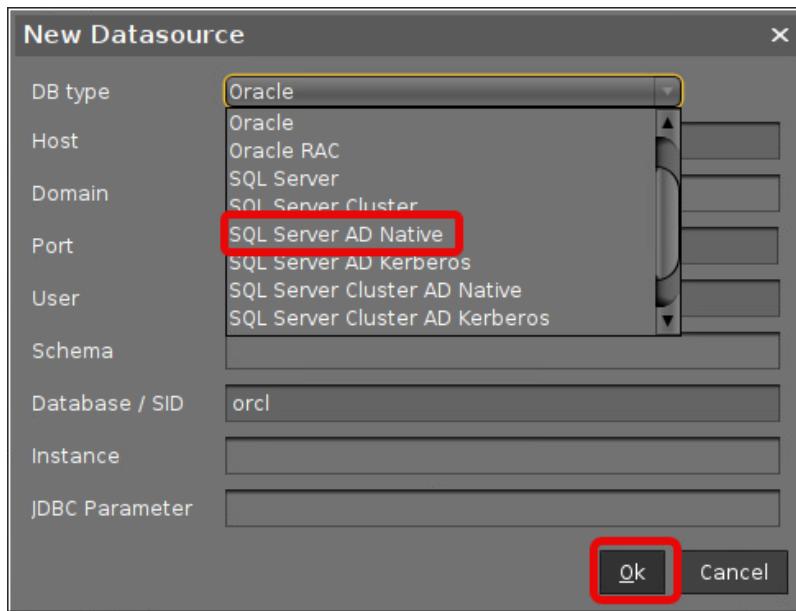


5. Depending on whether you are using a single server or a cluster for your Microsoft SQL database, continue with [Connecting the UMS to the Database \(Single Server Instance\)](#) (see page 129) or [Connecting the UMS to the Database \(Cluster\)](#) (see page 132),

Connecting the UMS to the Database (Single Instance)

1. In the [UMS Administrator](#) (see page 550), set up a new **SQL Server AD Native** type data source.

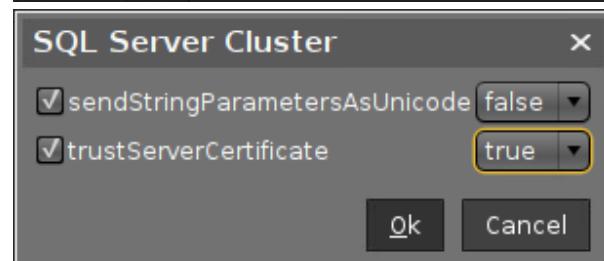
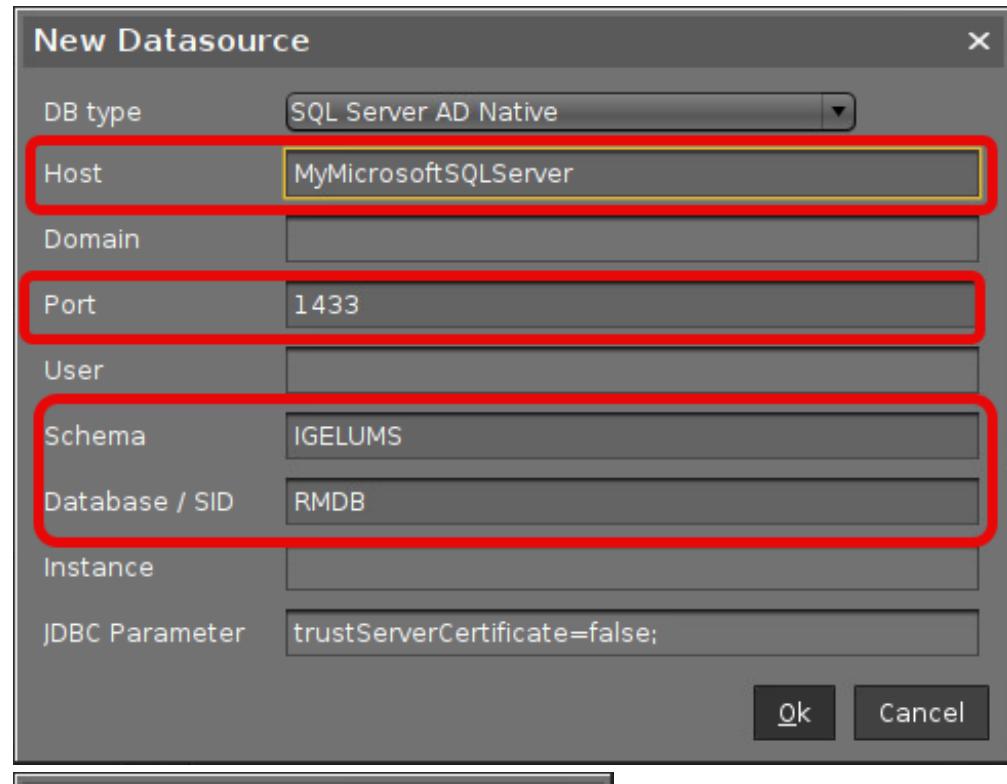




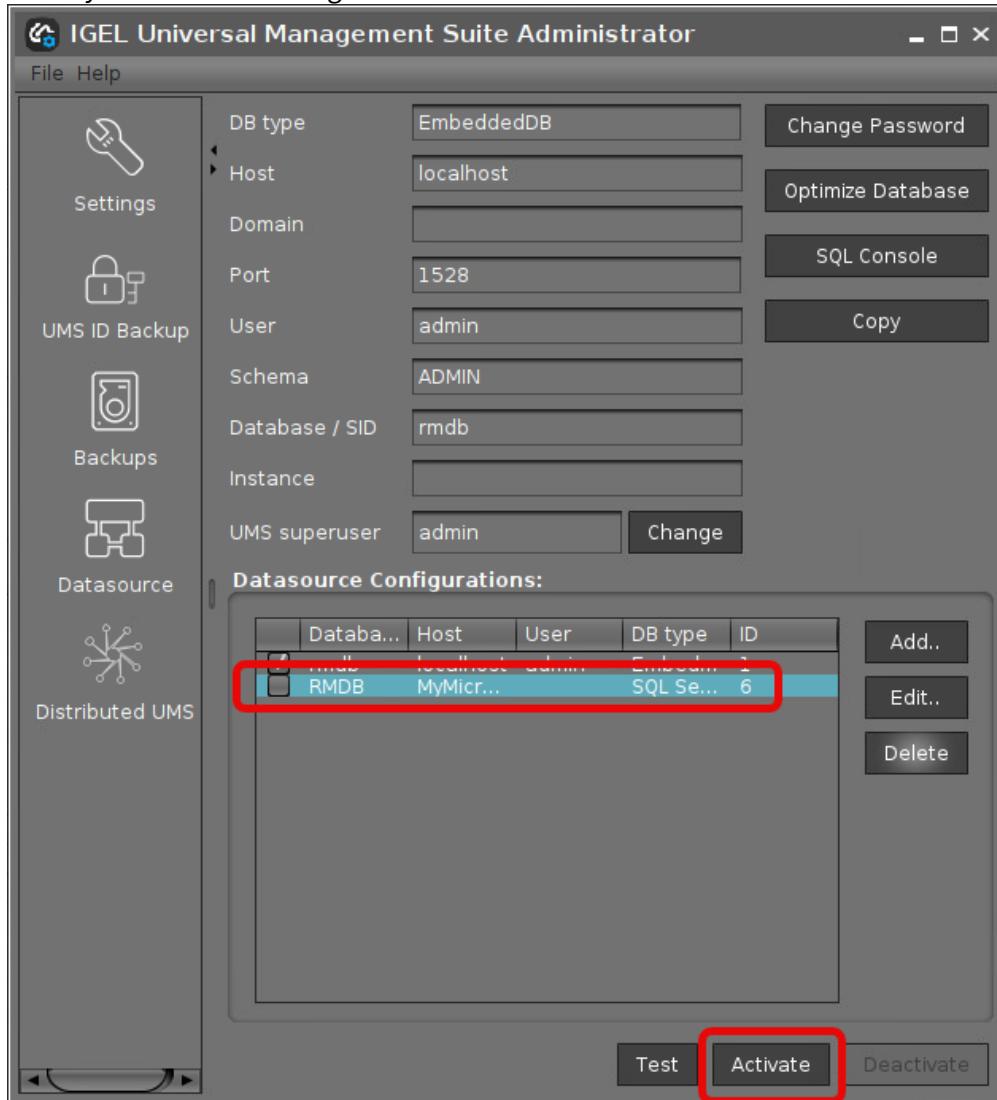
2. Edit the data as follows:

- **Host:** The Fully Qualified Host Name (FQDN) of the Microsoft SQL server. If you deploy MS SQL Server Always On Availability Groups, enter the domain name of the Always On Availability Group listener.
- **Port:** The port on which the Microsoft SQL Server listens for requests. (Default: 1433)
- **Schema:** The database schema
- **Database / SID:** The database name
- **JDBC Parameter** (double-click):
 - **sendStringParametersAsUnicode: false**

- **trustServerCertificate: true**

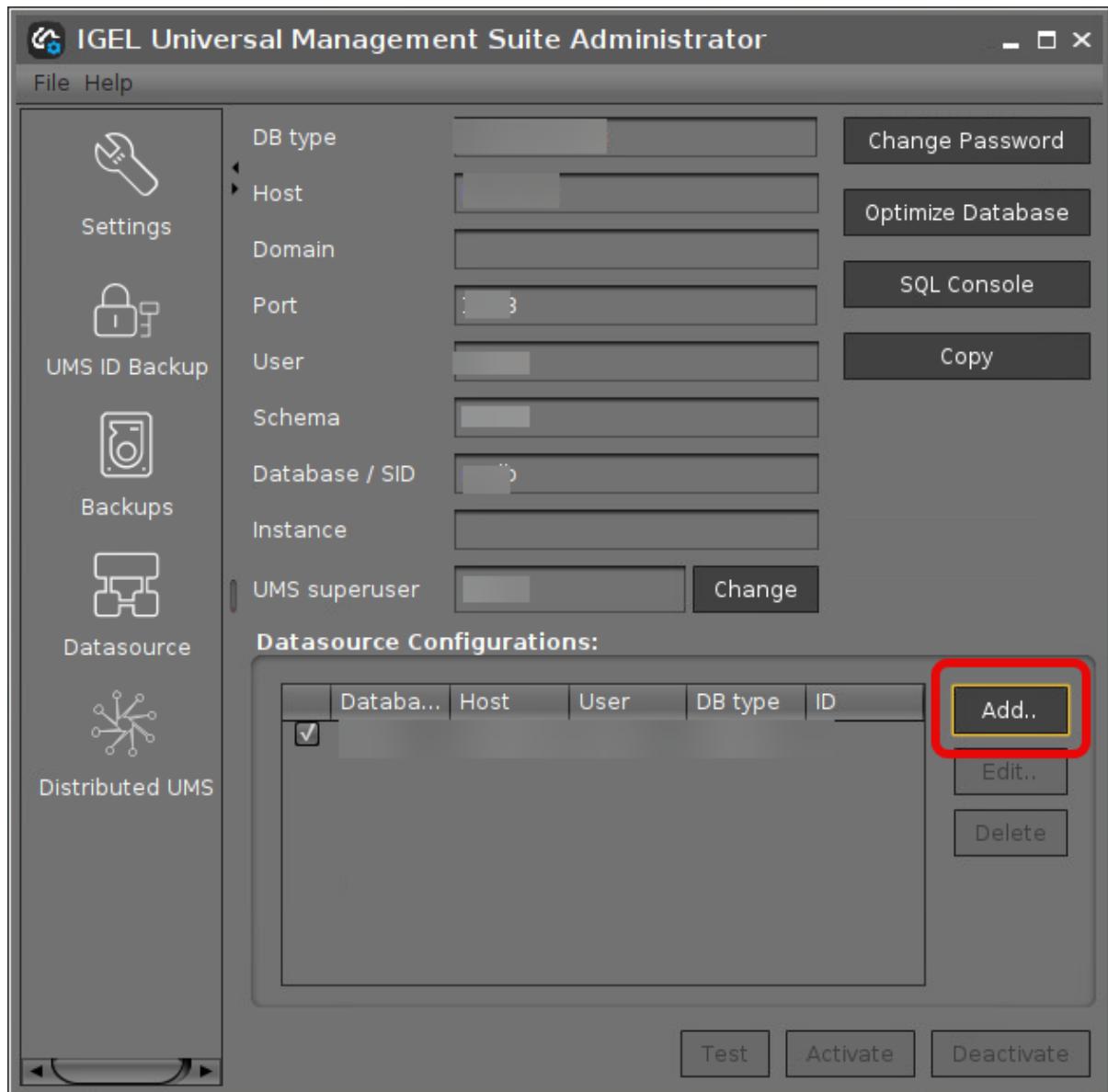


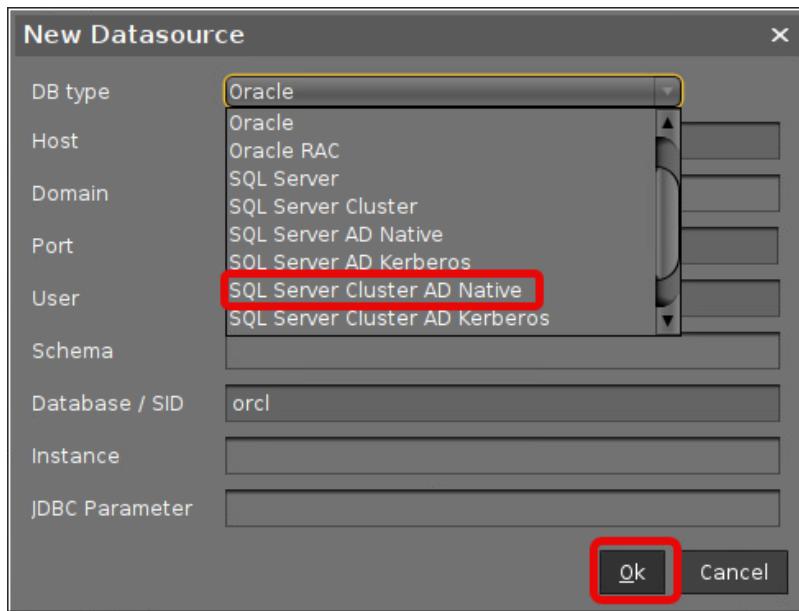
3. Select your database configuration and click **Activate**.



Connecting the UMS to the Database (Cluster)

1. In the [UMS Administrator](#) (see page 550), set up a new **SQL Server Cluster AD Native** type data source.

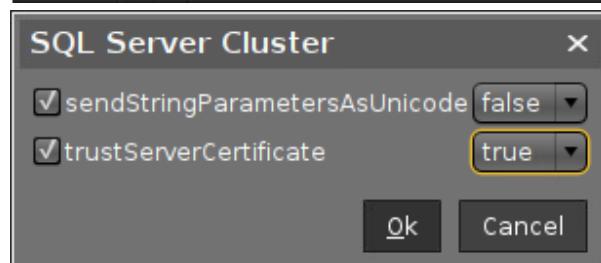
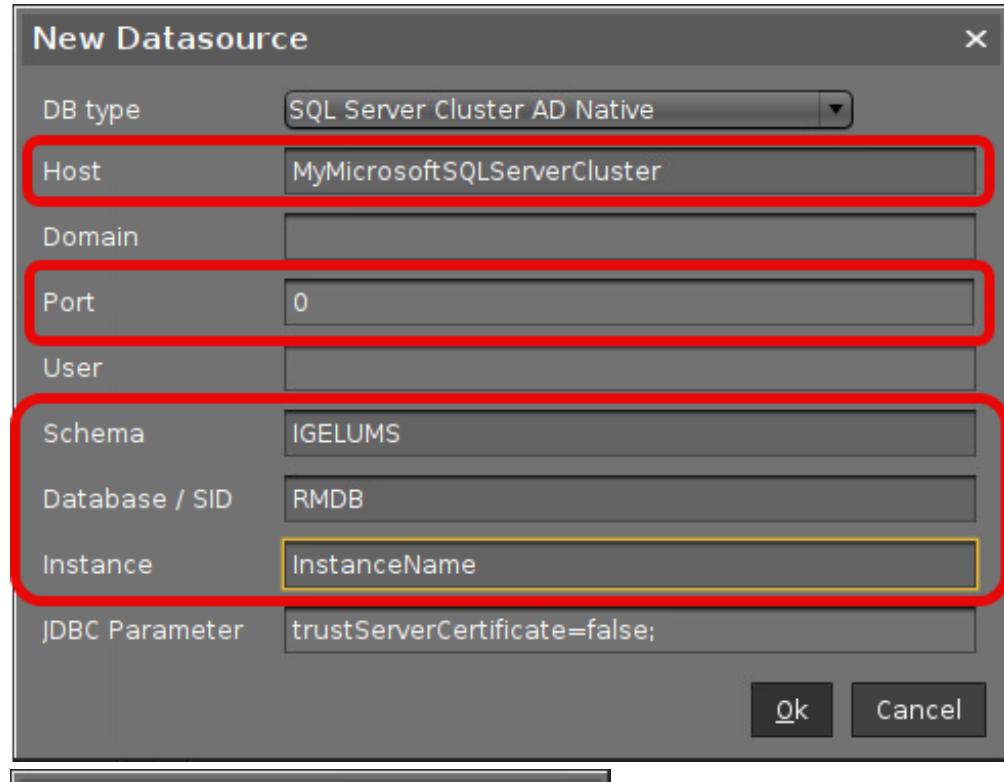




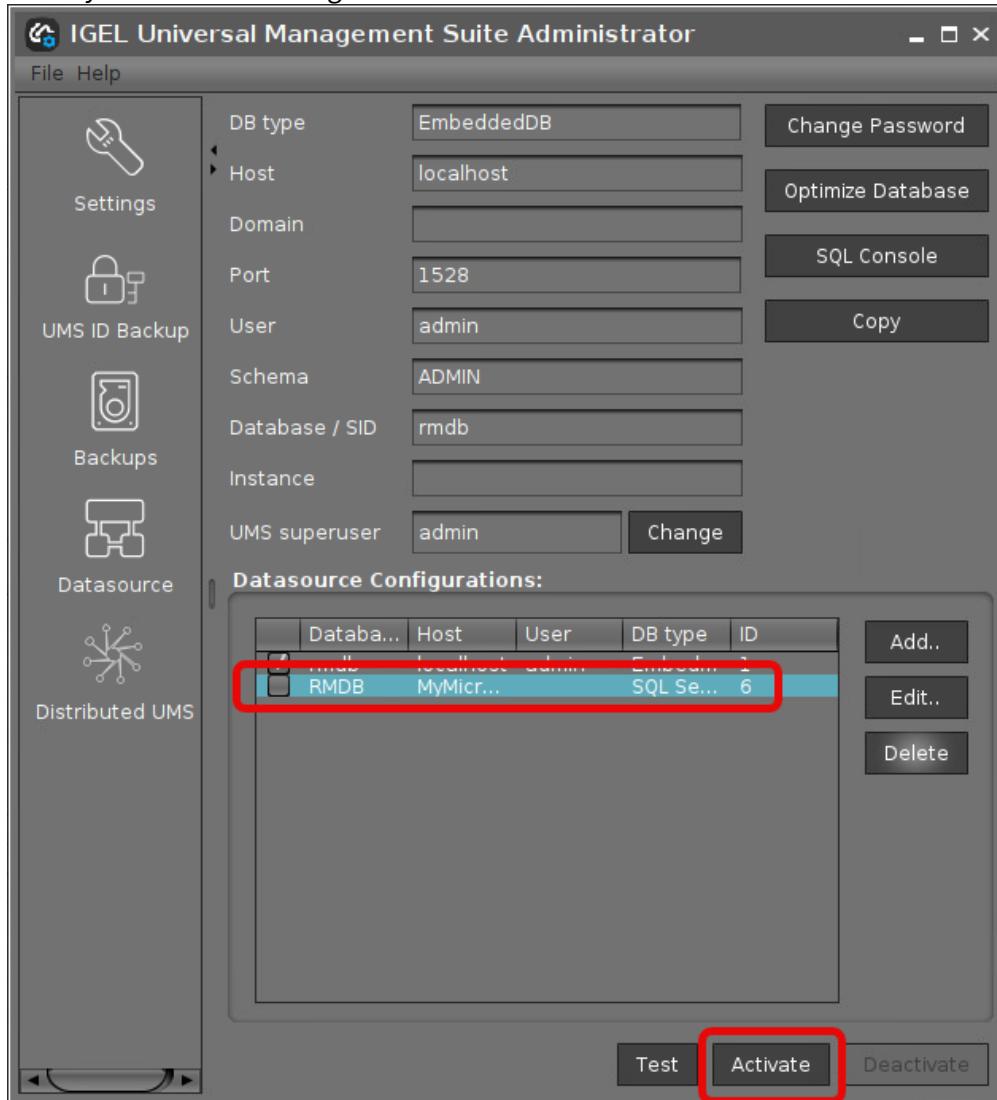
2. Edit the data as follows:

- **Host:** The Fully Qualified Host Name (FQDN) of the Microsoft SQL server
- **Port:** The port on which the Microsoft SQL Server listens for requests. (Default: 1433)
- **Schema:** The database schema
- **Database / SID:** The database name
- **Instance:** The instance for your Microsoft SQL Server Cluster
- **JDBC Parameter** (double-click):
 - `sendStringParametersAsUnicode: false`

- **trustServerCertificate: true**



3. Select your database configuration and click **Activate**.



Microsoft SQL Server/Cluster with Active Directory (AD) Authentication via Kerberos

This article describes the setup of a UMS database using a Microsoft SQL server, the configuration of the database login, and the connection of the IGEL Universal Management Suite (UMS) to the database using Active Directory (AD) authentication via Kerberos.

⚠ Using Microsoft Active Directory (AD) to connect your UMS to a Microsoft SQL server requires a deep understanding of your environment. For most environments, it is recommended to use native SQL authentication.

Prerequisites

For connecting the UMS Server to your UMS database with Microsoft Active Directory (AD) Kerberos authentication, the following components must be available:

- A Windows domain server
- The Microsoft SQL server on which the UMS database is running is located in the Windows domain
- The UMS Server and the UMS Administrator have access to the Windows domain
- The SQL service account has local administration rights to the UMS Server

Creating the UMS Database

It is recommended to create a separate database with a specific schema for the UMS.

⚠ Configuration Hints

The UMS Server application runs several services in parallel to provide the required functionality. These services establish separate connections to the database. The database must therefore allow a certain number of connections. The expected maximum number of connections is $128 * [\text{number of UMS Servers}]$. Please make sure that your database can handle these connections.

Using the SQL Management Console ►

- In the SQL Management Console, select **New Query** and enter the script below; replace the placeholders accordingly.

⚠ Do NOT use the schema **dbo** for the UMS database tables!

- <database_name> : The name for the UMS database
- <schema_name> : The name of the schema for the UMS database

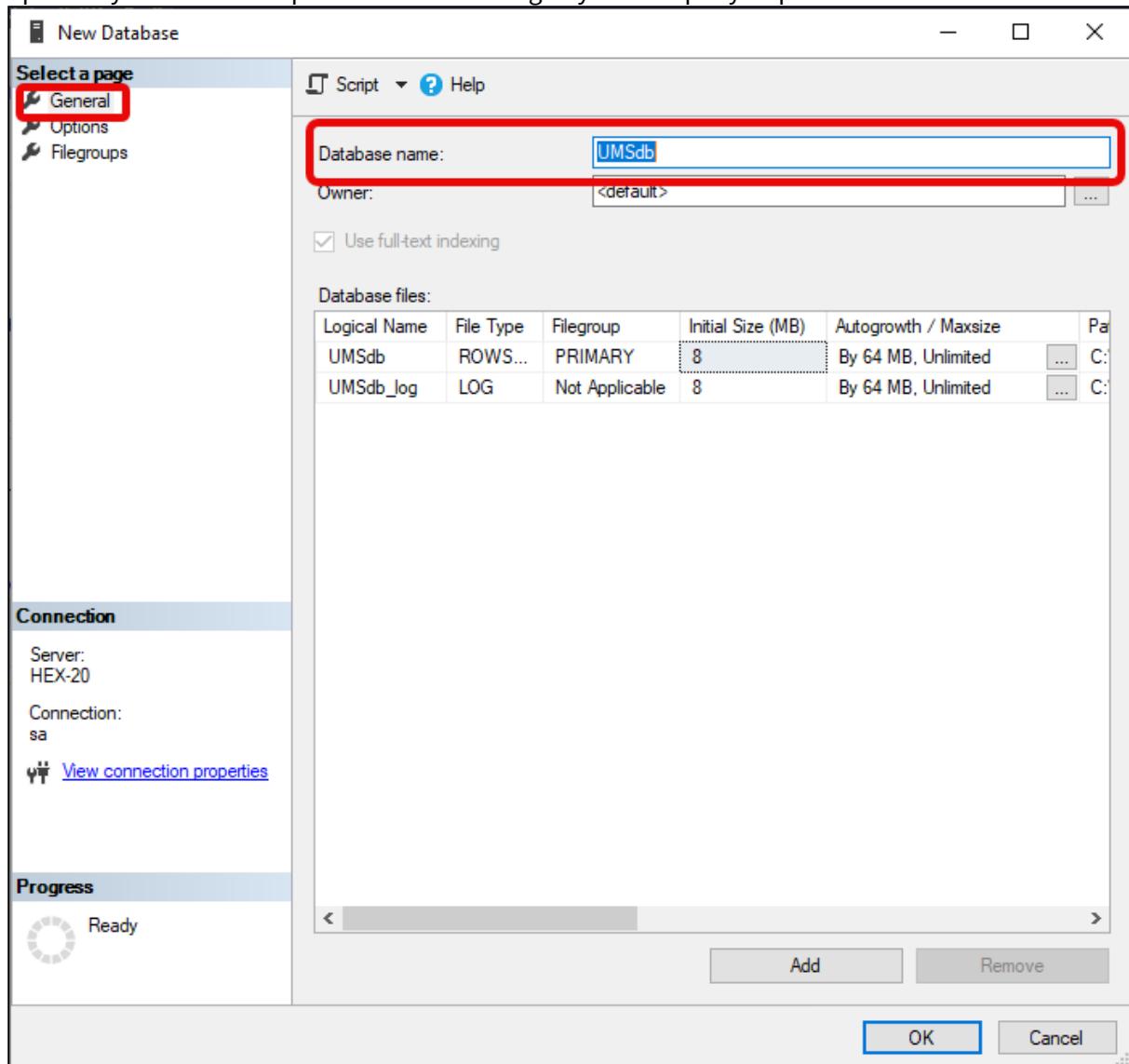
```
USE [master]
GO
```

```
CREATE DATABASE [<database_name>];  
GO  
USE [<database_name>];  
GO  
CREATE SCHEMA [<schema_name>];  
GO
```

Using the GUI

1. In SQL Server Management Studio, right-click **Databases** and select **New Database**.
2. Under **General**, give the database a name.

3. Optionally set additional parameters according to your company requirements.



Adding Users and a Group to the Windows Domain

- ▶ Make sure that your Windows domain contains users who have the following permissions:
 - Log in to the database server
 - Log in to the database that is connected to the UMS
 - Log in to the server with the UMS components

- ⓘ It is recommended to create a group in the Windos domain that will contain the users for the database and put the users for the UMS into this group. This group will become the owner of the UMS database, allowing all users in the group to work with the database.

Adding the User or Group to SQL

- ⓘ Note: If the AD user you are going to use to connect to the Microsoft SQL Server already has an SQL login entry, or is in a group with login access, you can skip this step and continue with [Configuring the UMS User, Schema, and Database Permissions](#) (see page 142).

Using the SQL Management Console

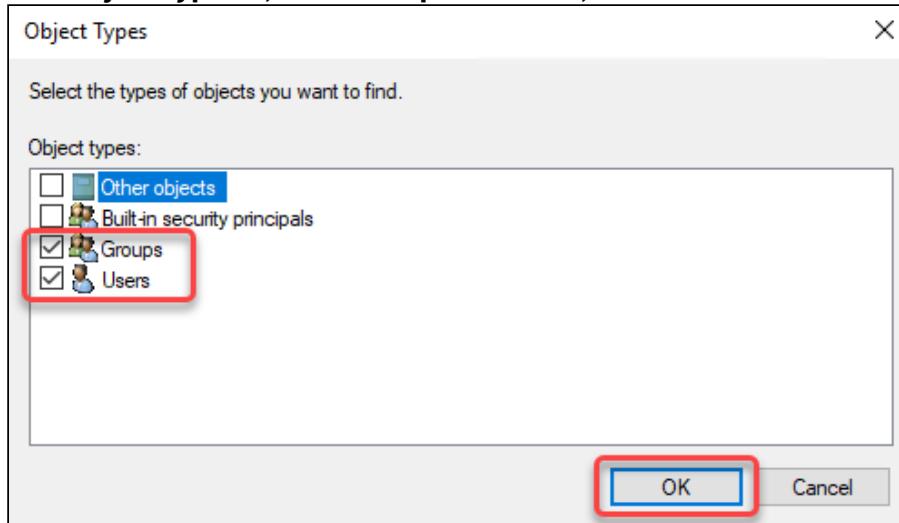
1. In SQL Server Management Studio, select **New Query**.
2. Use the following script to create the database login; replace <ad_user> with the AD user you want to use for connecting.

```
USE [master]
GO
CREATE LOGIN [[<ad_user>]] FROM WINDOWS;
GO
```

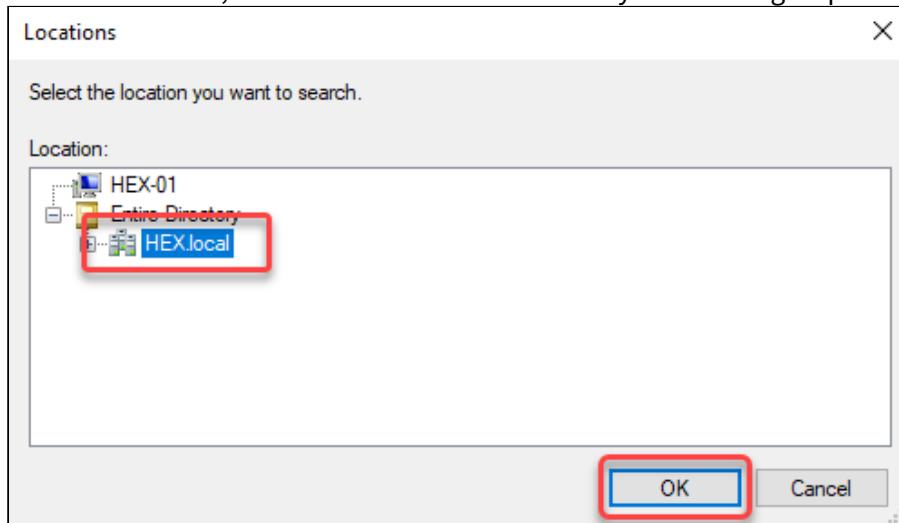
Using the SQL Server Management Studio (GUI Mode)

1. Connect to the database with the SQL Server Management Studio.
2. Open the **Security** branch, right-click on **Logins** and select **New Login**.
3. Choose **Windows Authentication** for the login, and click **Search**.

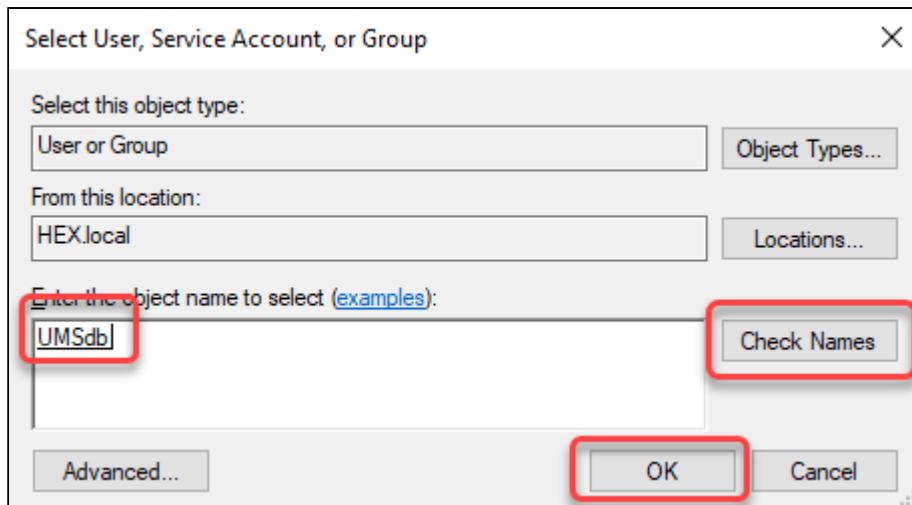
4. Click **Object Types...**, select **Groups** and **Users**, and click **OK**.



5. Click **Locations...**, to choose the location wherein your user or group is residing, and click **OK**.



6. Enter the name of the group or user, click **Check Names**, select the name of your user or group, and click **OK**.



If you have selected a group, all users in this group will be able to access the databases where this group is defined as the database owner. Also, if you selected a group, you should add at least one user who will become the main database owner.

Configuring the UMS User, Schema, and Database Permissions

Using the SQL Management Console

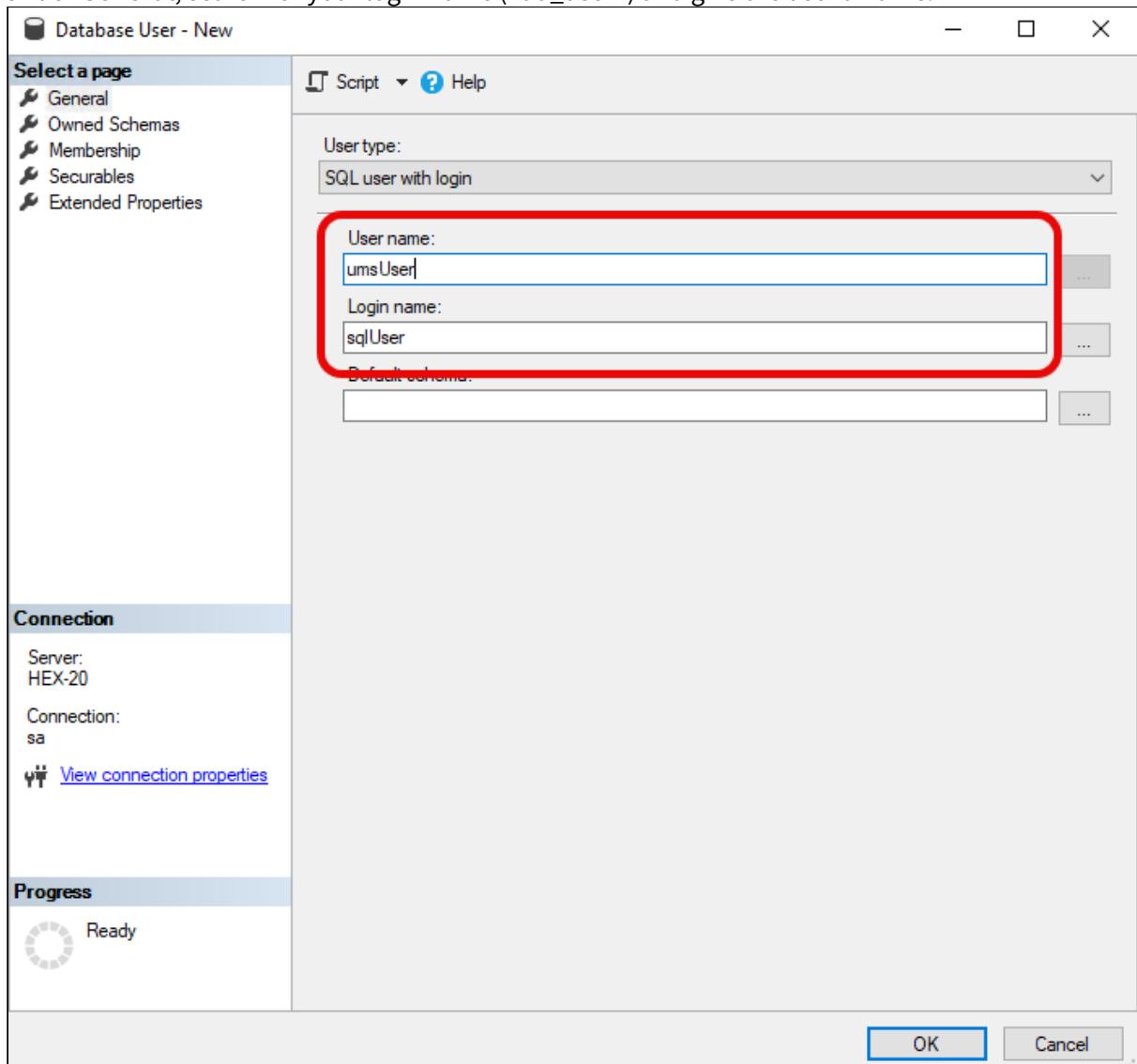
- ▶ In the SQL Management Console, select **New Query** and enter the script below; please note the following.
 - <ums_user> : The local alias in the database <database_name> of the real user <ad_user>
 - According to the Microsoft SQL Server documentation, the <ums_user> must be db_owner to create and alter tables.

```
USE [<database_name>]
GO
CREATE USER [<ums_user>] FOR LOGIN [<ad_user>];
GO
ALTER ROLE [db_owner] ADD MEMBER [<ums_user>];
GO
ALTER USER [<ums_user>] WITH DEFAULT_SCHEMA = [<schema_name>];
GO
ALTER AUTHORIZATION ON SCHEMA::[<schema_name>] TO [<ums_user>]
GO
```

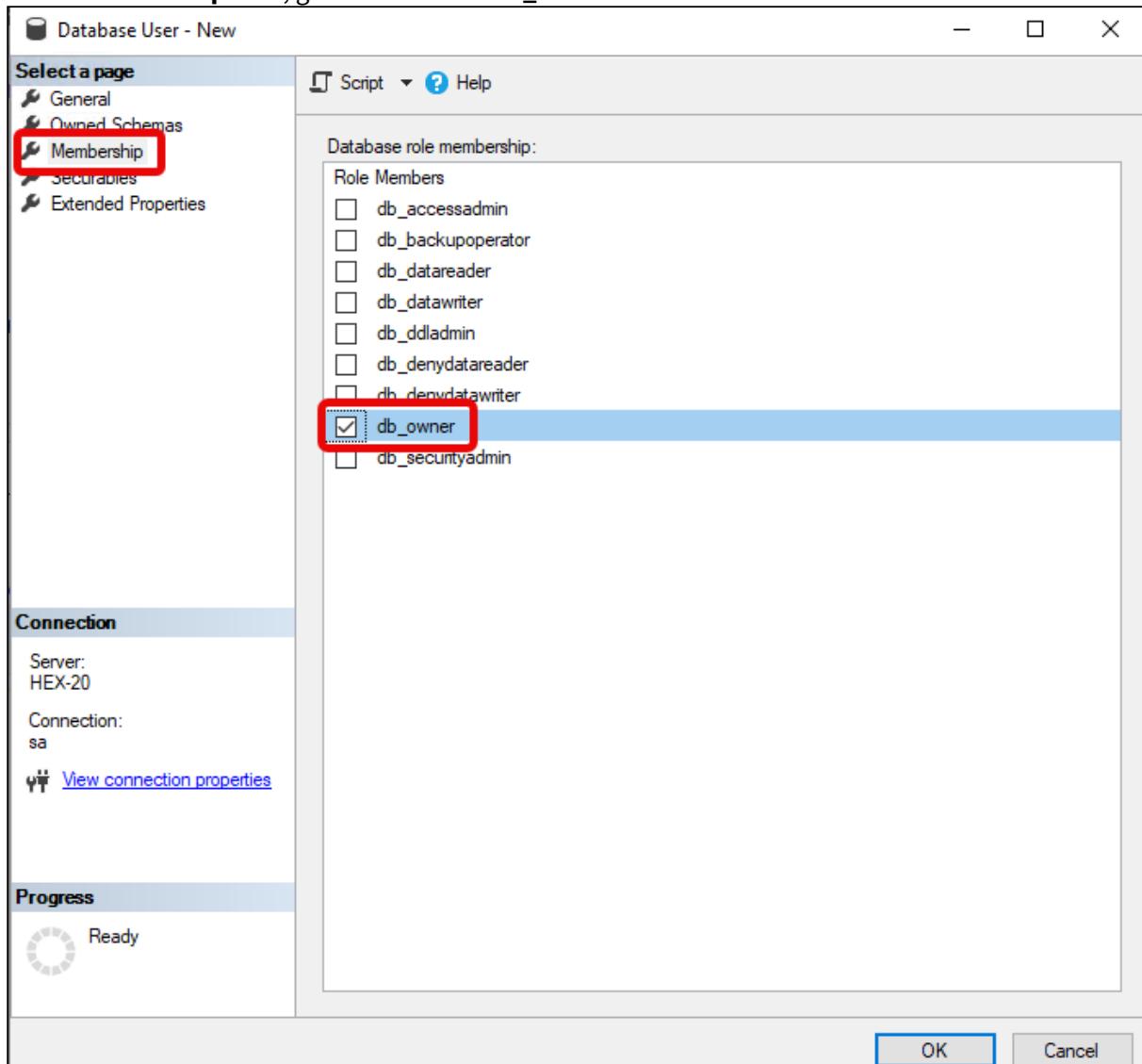
Using the GUI

1. In SQL Server Management Studio, open the database that was created in [Creating the UMS Database](#) (see page 137).

2. Under **Security > Users**, right-click **New User**.
3. Under **General**, search for your login name (<ad_user>) and give the user a name.

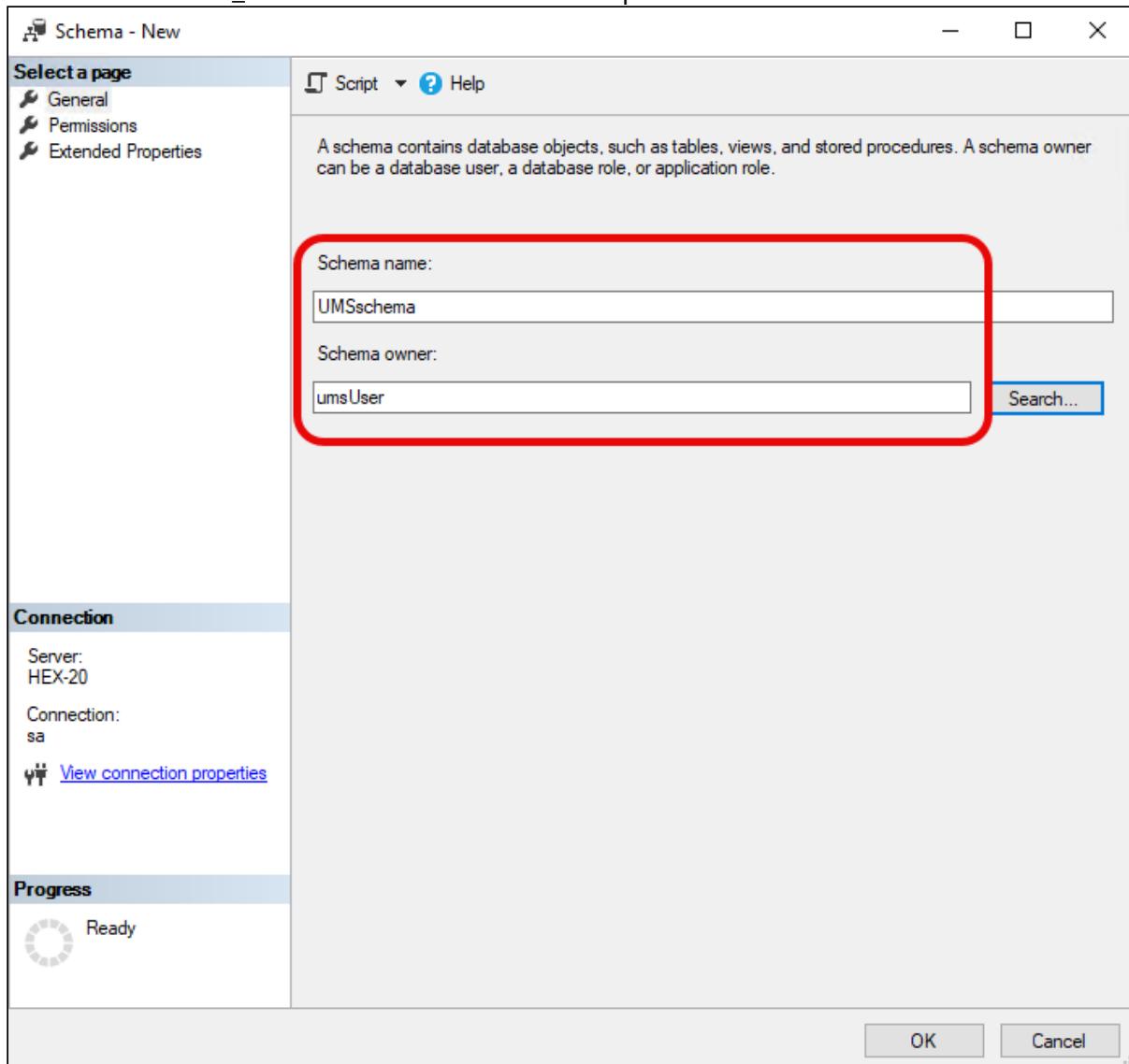


4. In the **Membership** area, give the user the **db_owner** role.



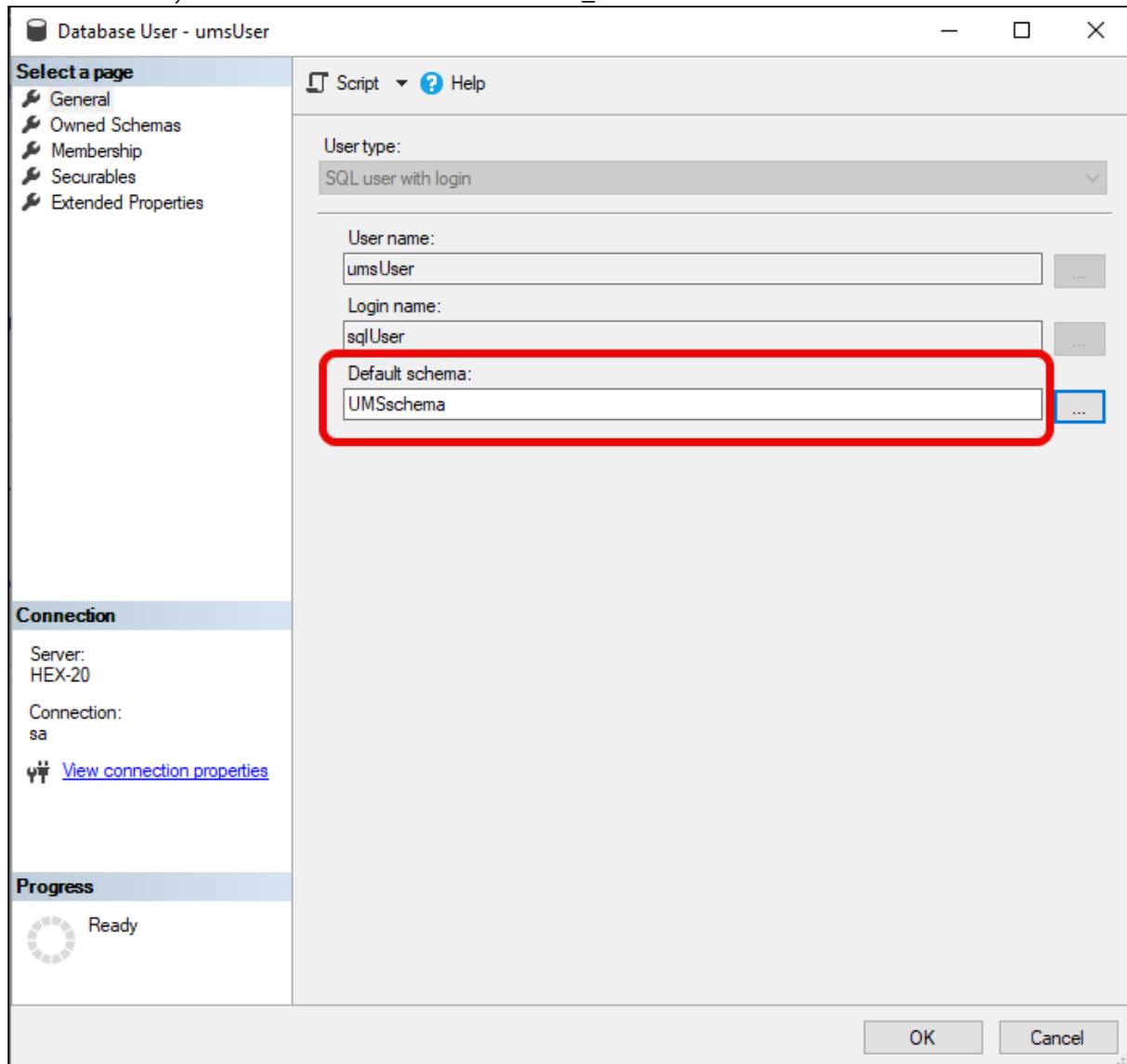
5. Go to **Security > Schemas** and right-click on **New Schema**.

6. Search for the <ums_user> as the **Schema owner** and provide a **Schema name**.



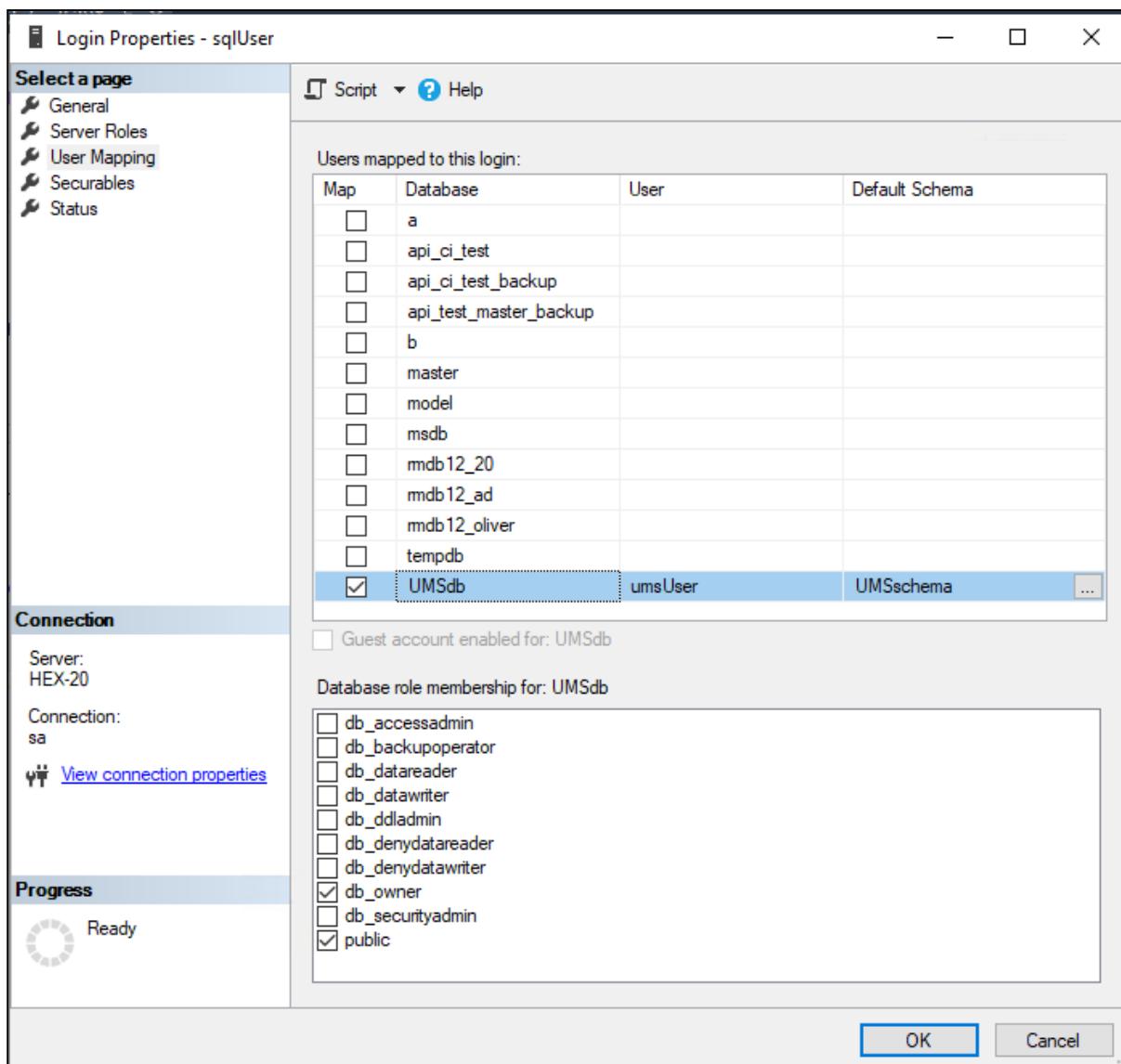
7. Under **Security > Users** in your UMS database, double-click on the <ums_user>.

8. Under **General**, set the default schema to <schema_name>.



9. Under **Security > Logins > Users**, double-click on the <ad_user>.

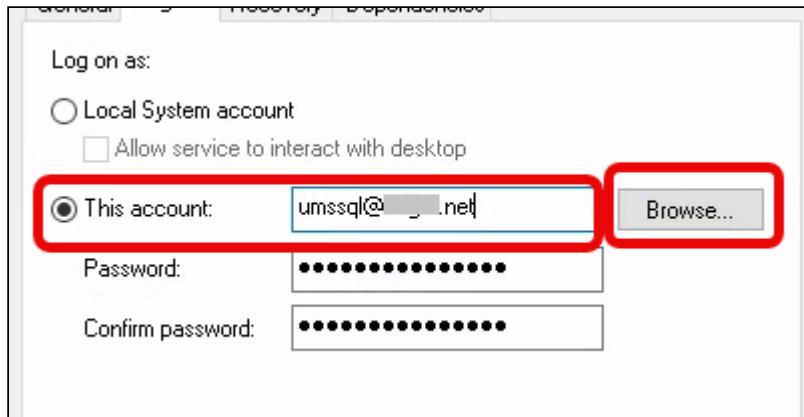
10. In the **User Mapping** area, check the mapping of the UMS database, the user, and the default schema.



Configuring the UMS Services

1. Log into the UMS Server with the credentials configured for connecting to the UMS database on the Microsoft SQL Server.
2. Open **services.msc** and right-click the **IGEL Remote Manager Server** service.
3. Select **Properties** and navigate to the **Log On** tab.

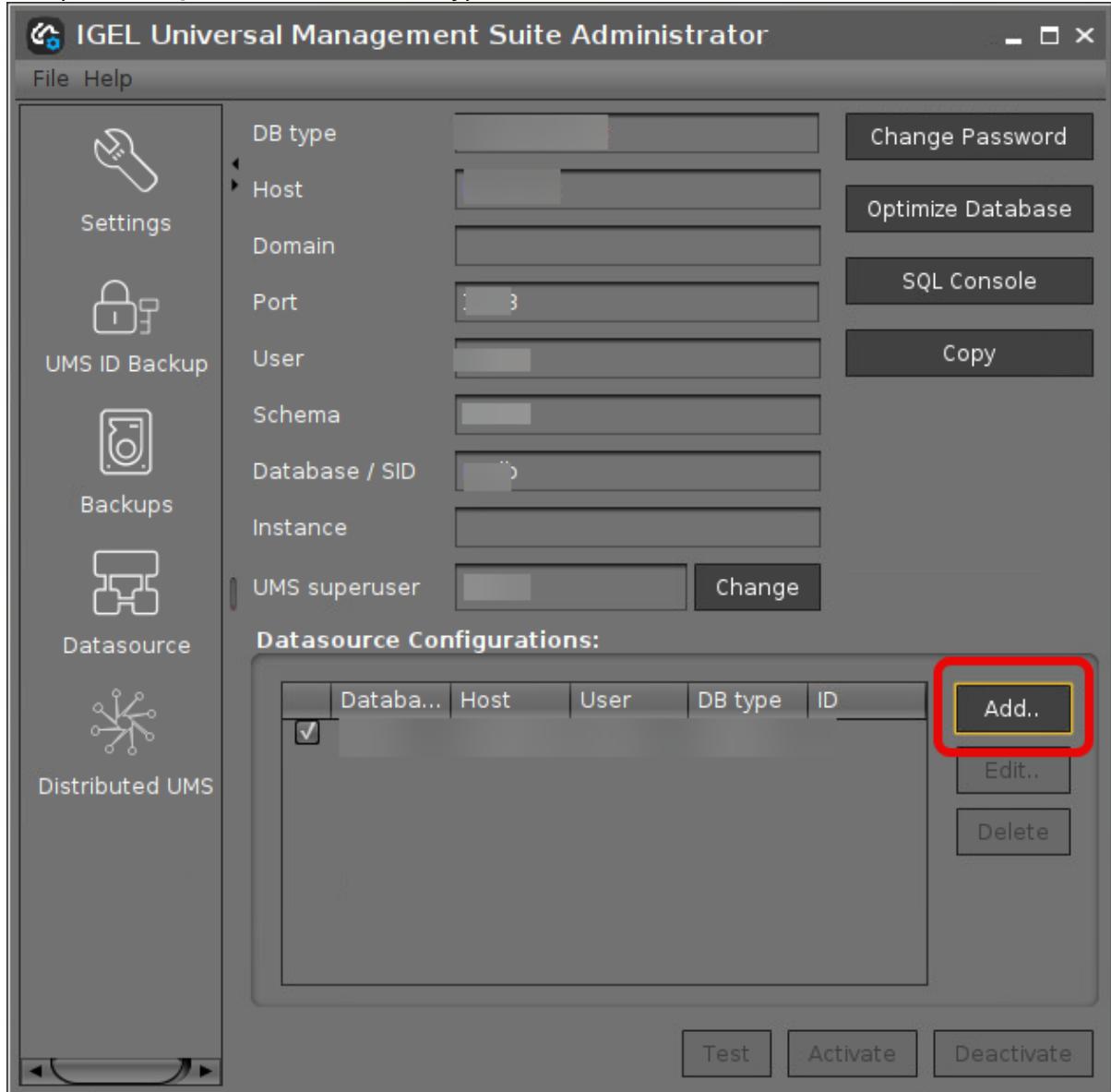
4. Select **This Account** and use the **Browse** button to find the one that owns the SQL database.

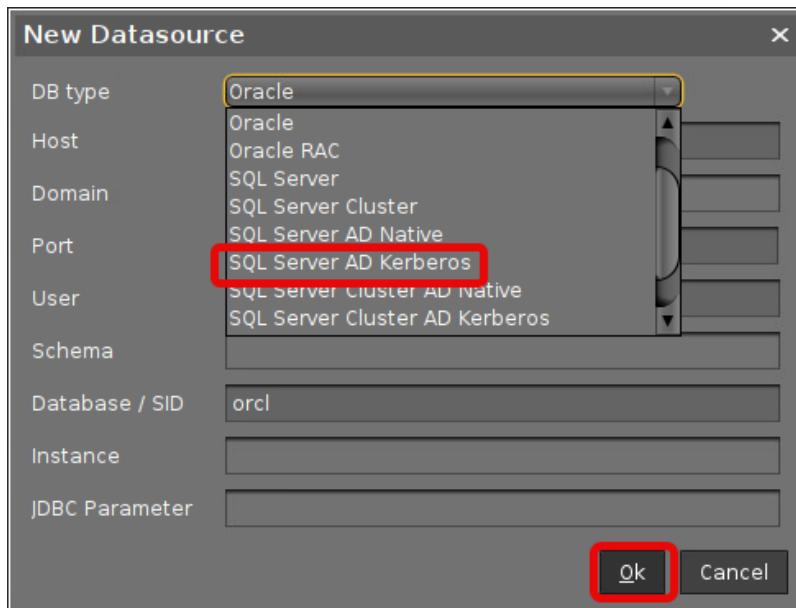


5. Depending on whether you are using a single server or a cluster for your Microsoft SQL database, continue with [Connecting the UMS to the Database \(Single Server Instance\)](#) (see page 149) or [Connecting the UMS to the Database \(Cluster\)](#) (see page 153),

Connecting the UMS to the Database (Single Instance)

1. Set up a new **SQL Server AD Kerberos** type data source.

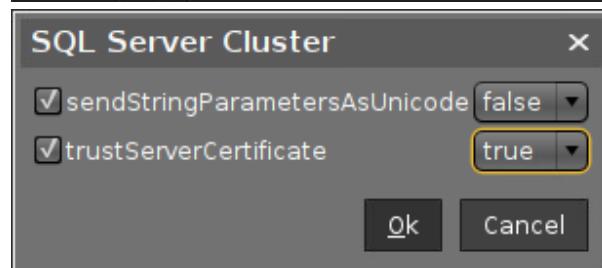
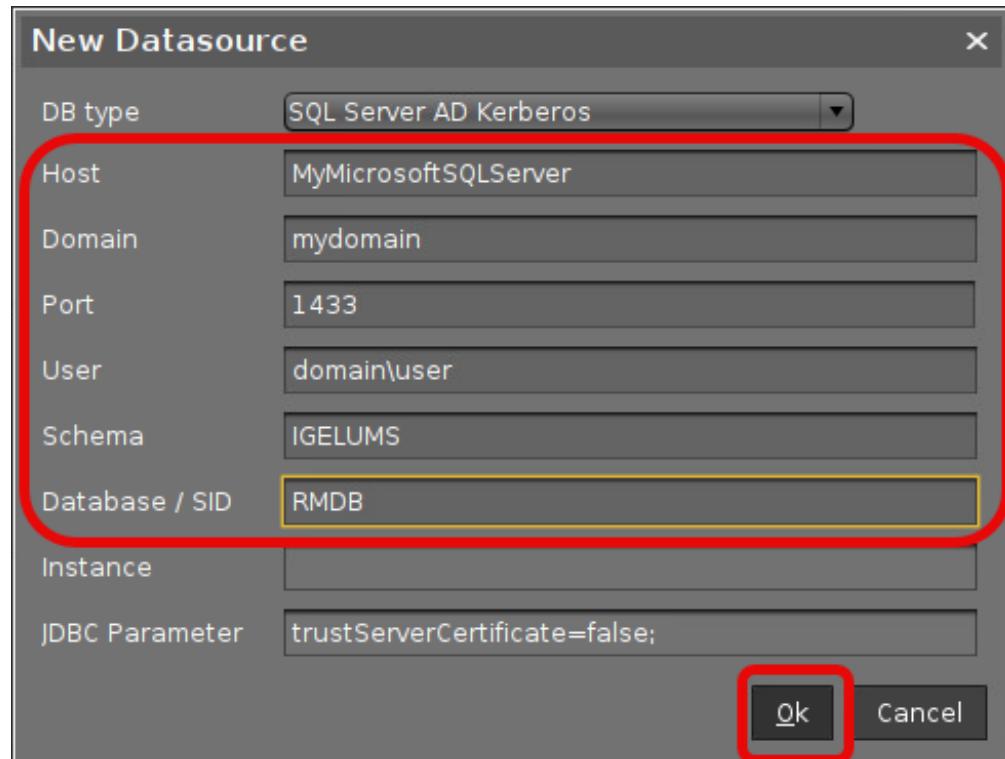




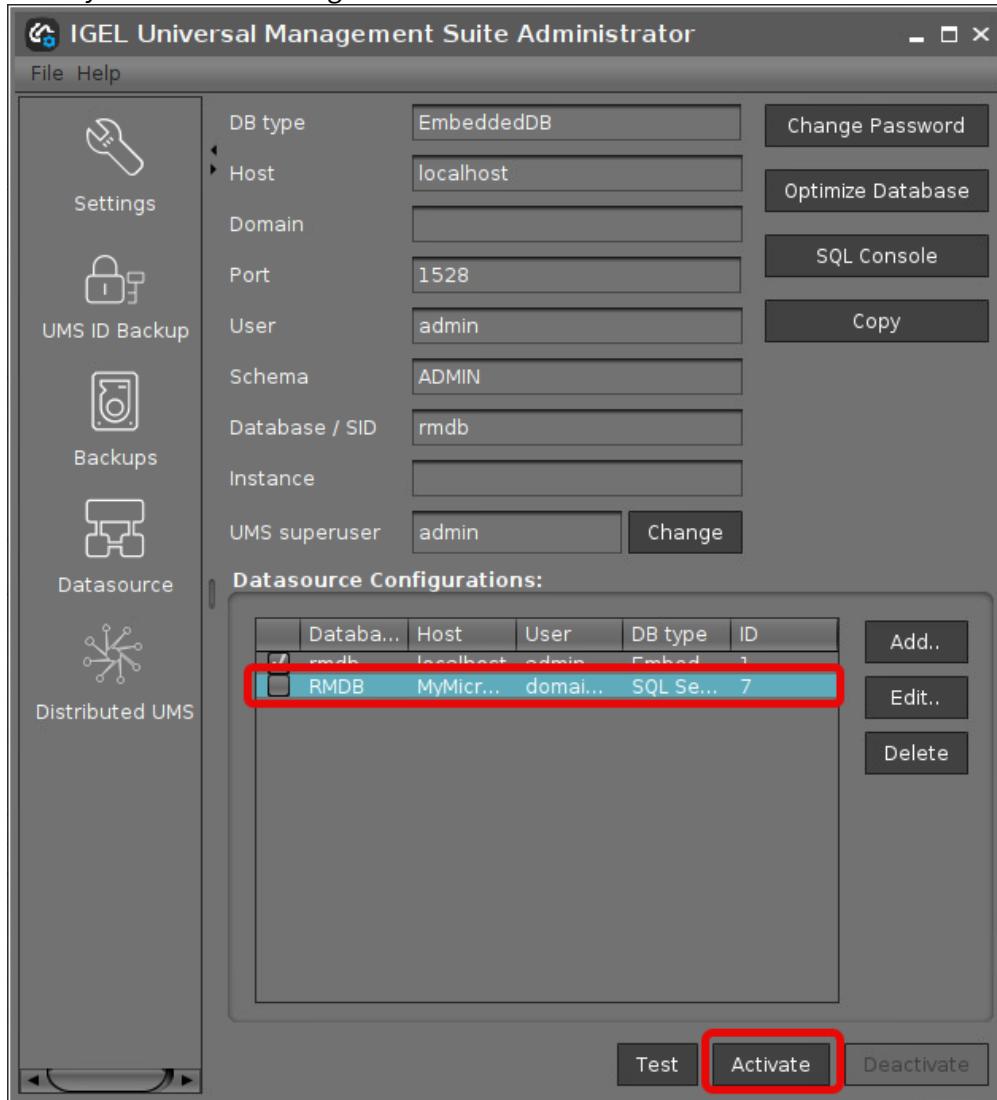
2. Edit the data as follows:

- **Host:** The Fully Qualified Host Name (FQDN) of the Microsoft SQL server. If you deploy MS SQL Server Always On Availability Groups, enter the domain name of the Always On Availability Group listener.
- **Domain:** The domain in which the <ad_user> is residing
- **Port:** The port on which the Microsoft SQL Server listens for requests. (Default: 1433)
- **User:** The <ad_user>; format: <domain_name>\<ad_user>
- **Schema:** The database schema
- **Database / SID:** The database name
- **JDBC Parameter** (double-click):
 - **sendStringParametersAsUnicode: false**

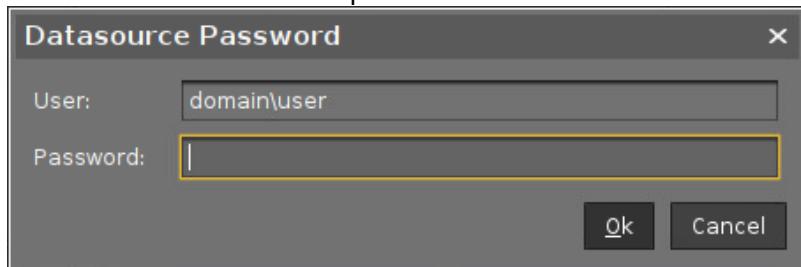
- **trustServerCertificate: true**



3. Select your database configuration and click **Activate**.

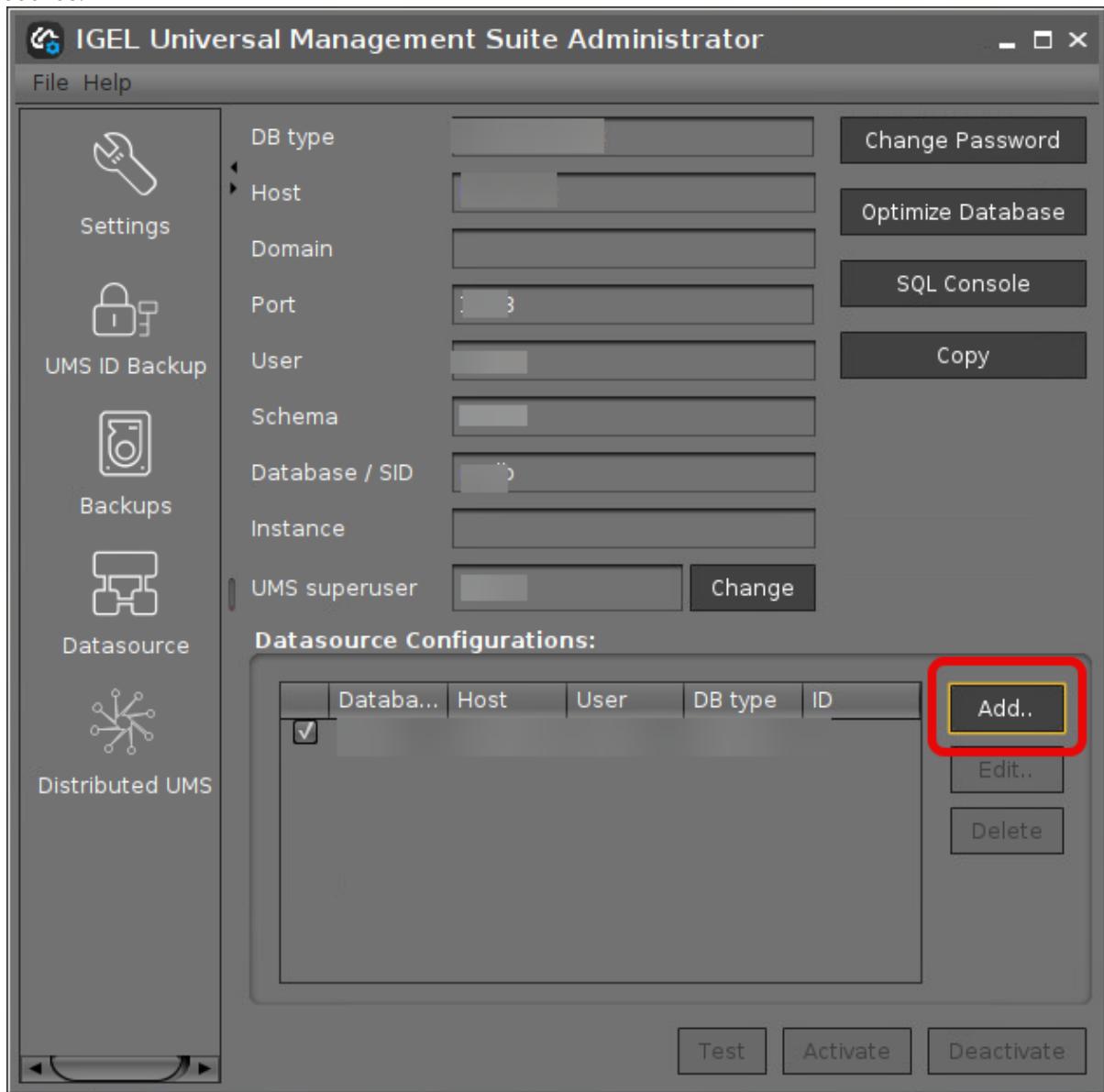


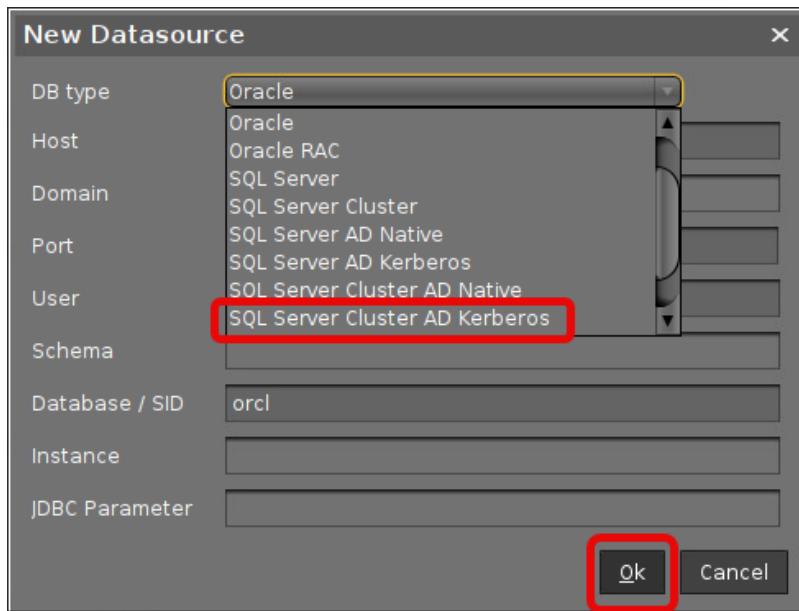
4. Enter the username and the password for the connection.



Connecting the UMS to the Database (Cluster)

1. In the [UMS Administrator](#) (see page 550), set up a new **SQL Server Cluster AD Kerberos** type data source.

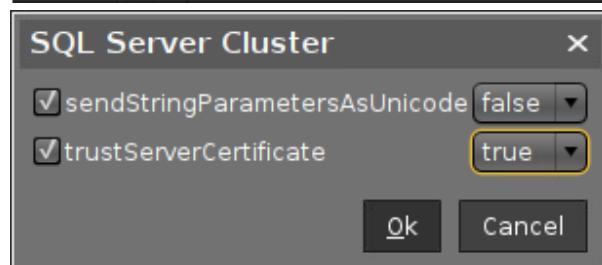
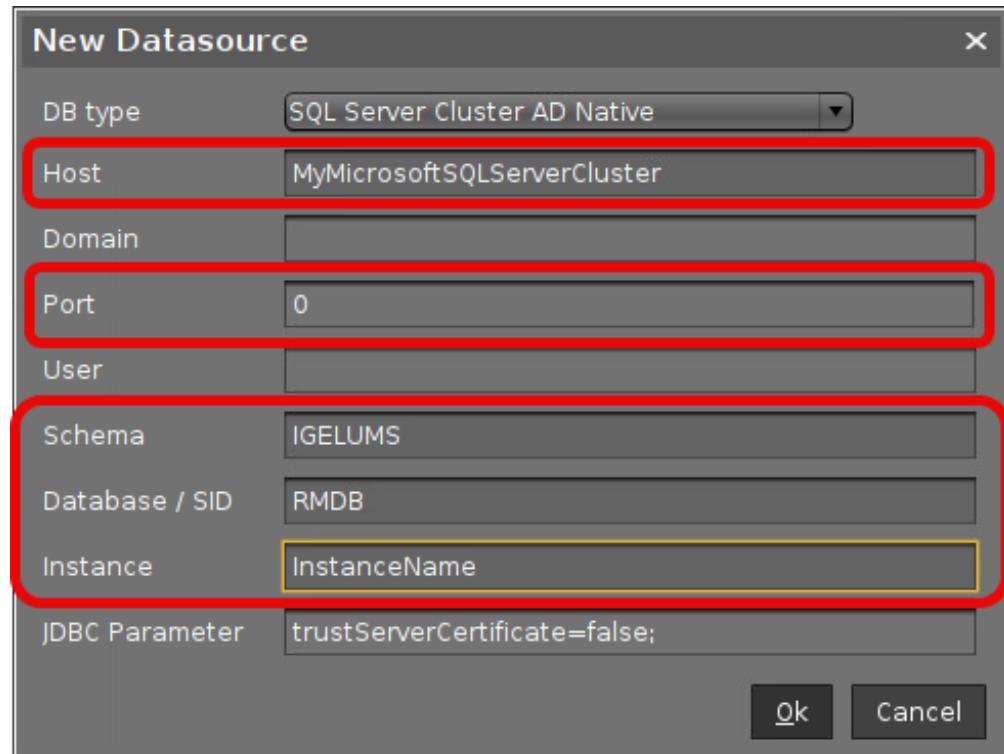




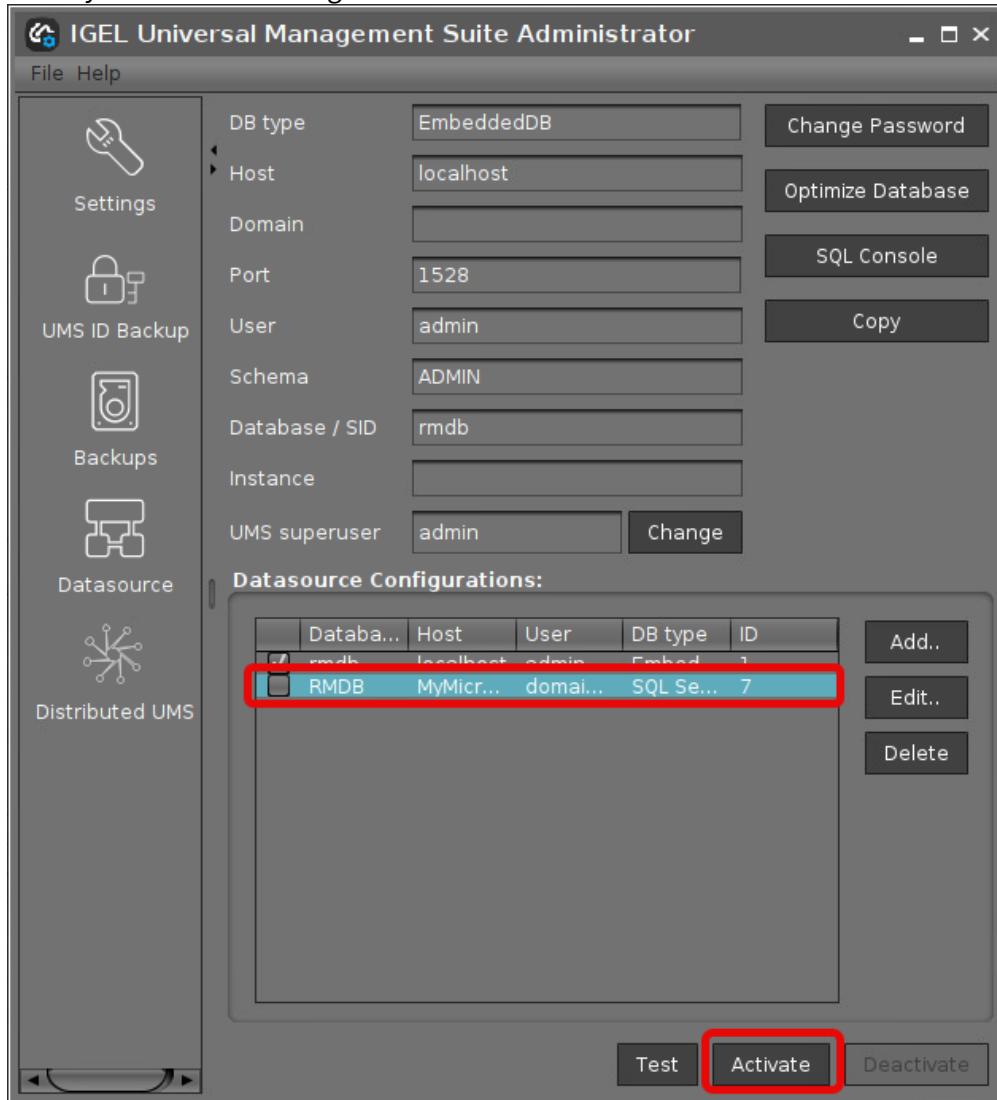
2. Edit the data as follows:

- **Host:** The Fully Qualified Host Name (FQDN) of the Microsoft SQL server
- **Port:** The port on which the Microsoft SQL Server listens for requests. (Default: 1433)
- **Schema:** The database schema
- **Database / SID:** The database name
- **Instance:** The instance for your Microsoft SQL Server Cluster
- **JDBC Parameter** (double-click):
 - `sendStringParametersAsUnicode: false`

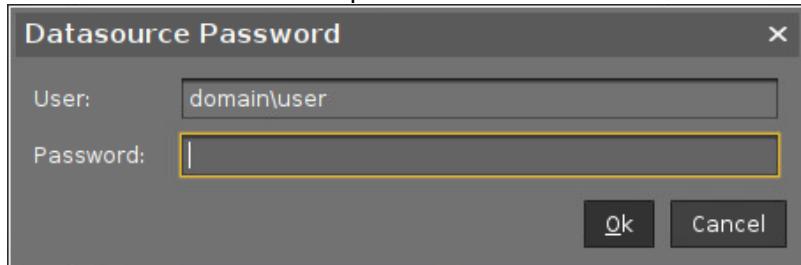
- **trustServerCertificate: true**



3. Select your database configuration and click **Activate**.



4. Enter the username and the password for the connection.



PostgreSQL

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

⚠ Configuration Hints

The UMS Server runs several services in parallel to provide the functionality. These services establish connections to the database. The database must therefore allow a certain number of connections. The recommendation is to set the maximum number of connections and the shared buffer size to the following values:

```
max_connections = 128 * [number of UMS Servers]
```

```
shared_buffers = 128MB * [number of UMS Servers]
```

These values are set in the configuration file for the PostgreSQL database (see the PostgreSQL documentation).

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>⁹.

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.

- i** 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`

⁹ <http://www.postgresql.org/>

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 550), 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)

User: rmlogin

Database / SID: rmdb

Apache Derby as a Data Source for the IGEL UMS

The following article explains how you can connect an Apache Derby external database as a data source for your IGEL Universal Management Suite (UMS) installation.

-  For details on the supported database systems, see the "Supported Environment" section of the release notes. 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 inside the Derby Database Administration, then define this 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 database instance `rmdb`, 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 > Datasource**, 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 general information on creating a data source in the UMS Administrator, see [How to Set Up a Data Source in the IGEL UMS Administrator](#) (see page 572).

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

Using an AWS Aurora PostgreSQL Database with IGEL Universal Management Suite (UMS)

This article describes how to connect an Amazon Web Services (AWS) Aurora PostgreSQL database to the IGEL Universal Management Suite (UMS).

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

Creating Your AWS Aurora PostgreSQL Database

- ▶ Follow the steps described in the AWS document [Creating a DB cluster and connecting to a database on an Aurora PostgreSQL DB cluster¹⁰](#). Important: Make sure to allow public access to your database; see step 11, last paragraph.

Connecting Your AWS Aurora PostgreSQL Database to Your UMS

- ▶ In the [UMS Administrator](#) (see page 550), create a new data source with the following parameters:
- **DB type:** PostgreSQL
 - **Host:** Fully Qualified Domain Name (FQDN) of the AWS database endpoint instance. This is the **Endpoint name** in AWS; see the [AWS document¹¹](#), section “Connect to an instance in an Aurora PostgreSQL DB cluster”, step 3.
 - **Port:** Port of the AWS Aurora server (default: 5432)
 - **User:** Username you have defined in AWS as **Master username**; see the [AWS document¹²](#), section “Create an Aurora PostgreSQL DB cluster”, step 9.
 - **Database / SID:** The specific database name. This is the **DB cluster identifier** as described in the [AWS document¹³](#), section “Create an Aurora PostgreSQL DB cluster”, step 8. If you have kept the default value of **DB cluster identifier** in AWS, keep the default value `postgres` here. You can find the value in AWS under **Additional configuration**.

¹⁰ https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP_GettingStartedAurora.CreatingConnecting.AuroraPostgreSQL.html

¹¹ https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP_GettingStartedAurora.CreatingConnecting.AuroraPostgreSQL.html

¹² https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP_GettingStartedAurora.CreatingConnecting.AuroraPostgreSQL.html

¹³ https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP_GettingStartedAurora.CreatingConnecting.AuroraPostgreSQL.html

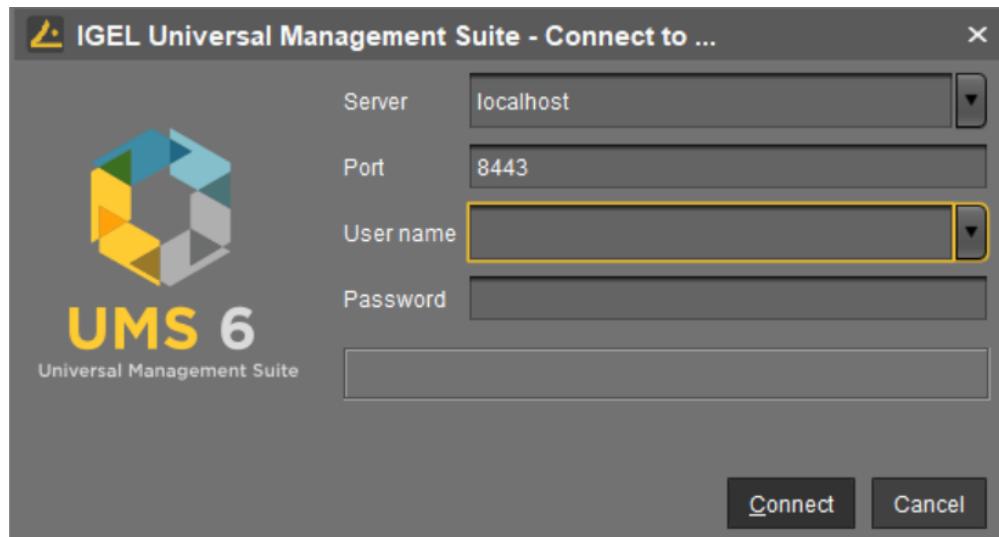
Connecting the UMS Console to the IGEL UMS Server

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

- ⓘ If you need to start the UMS Console under Linux from the terminal emulator, use the command / [IGEL installation directory] / RemoteManager.sh (if the default installation directory is used: / opt/IGEL/RemoteManager/RemoteManager.sh)
It is generally NOT recommended to execute RemoteManager.sh with sudo . On Red Hat Enterprise Linux 8, RemoteManager.sh can be executed only without sudo .

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 - Change Server Settings in the IGEL UMS Administrator](#) (see page 552).
 - **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**.

- i** After several failed login attempts via the UMS Console, IMI REST API, or WebDAV (e.g. `https://<server>:8443/ums_filetransfer/`), the brute-force protection will temporarily lock the user accounts for 10 minutes. The UMS Console will show a corresponding message when the user account is locked.

Registering the IGEL UMS

For the communication of your IGEL Universal Management Suite (UMS) with the IGEL Cloud Services, you must register your UMS.

Only, an authorized user can register the UMS, see Managing Users and Roles in the IGEL Customer Portal. For detailed instructions, see Registering the UMS.

Note that if the UMS is not registered, you will see the following error message when trying to import apps for IGEL OS 12 devices from the IGEL App Portal:

Authentication Error

No valid token provided.

Please contact your system administrator to register your UMS.

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

- i** It is not necessary to register the device in the UMS since this process is performed
- when you onboard the device using the IGEL Onboarding Service or One-Time Password Method in the IGEL Setup Assistant, see [Onboarding IGEL OS 12 Devices \(IGEL OS 12 devices\)](#)
 - when you set up the ICG connection on the device in the IGEL Setup Assistant or the ICG Agent Setup (IGEL OS 11 devices)

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

- [Scanning the network for devices and registering the found devices \(see page 167\)](#)
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 \(see page 179\)](#)
If you enable automatic registration and configure the DHCP tag and/or the DNS alias `igelrmsrv` with the IP or FQDN of the UMS Server, all devices on the server's network will be automatically registered at startup.

- i** IGEL recommends automatic registration when registering new IGEL OS 11 devices for the first time during the rollout. You can use automatic registration also for IGEL OS 12 devices that are inside the company network; for IGEL OS 12 devices outside the company network, it is preferable to use IGEL Onboarding Service, see [Initial Configuration of the IGEL Onboarding Service \(OBS\)](#) and [Onboarding IGEL OS 12 Devices](#).
Disable automatic registration as soon as all devices have been registered, so that no unknown devices can obtain sensitive settings.

- [Importing devices \(see page 173\)](#)
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 181)

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 \(IGEL OS 11 and earlier\)](#)

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. This function is described for the UMS Console as well as for the UMS Web App.

For an overview of device registration methods, see [Registering IGEL OS Devices on the UMS Server \(see page 165\)](#).

-  The scan and register feature can only be used when an endpoint device can open a direct connection to the UMS. Thus, when an external load balancer / reverse proxy is configured, this feature might not be usable; see NGINX: Example Configuration for as Reverse Proxy in IGEL OS with SSL Offloading.

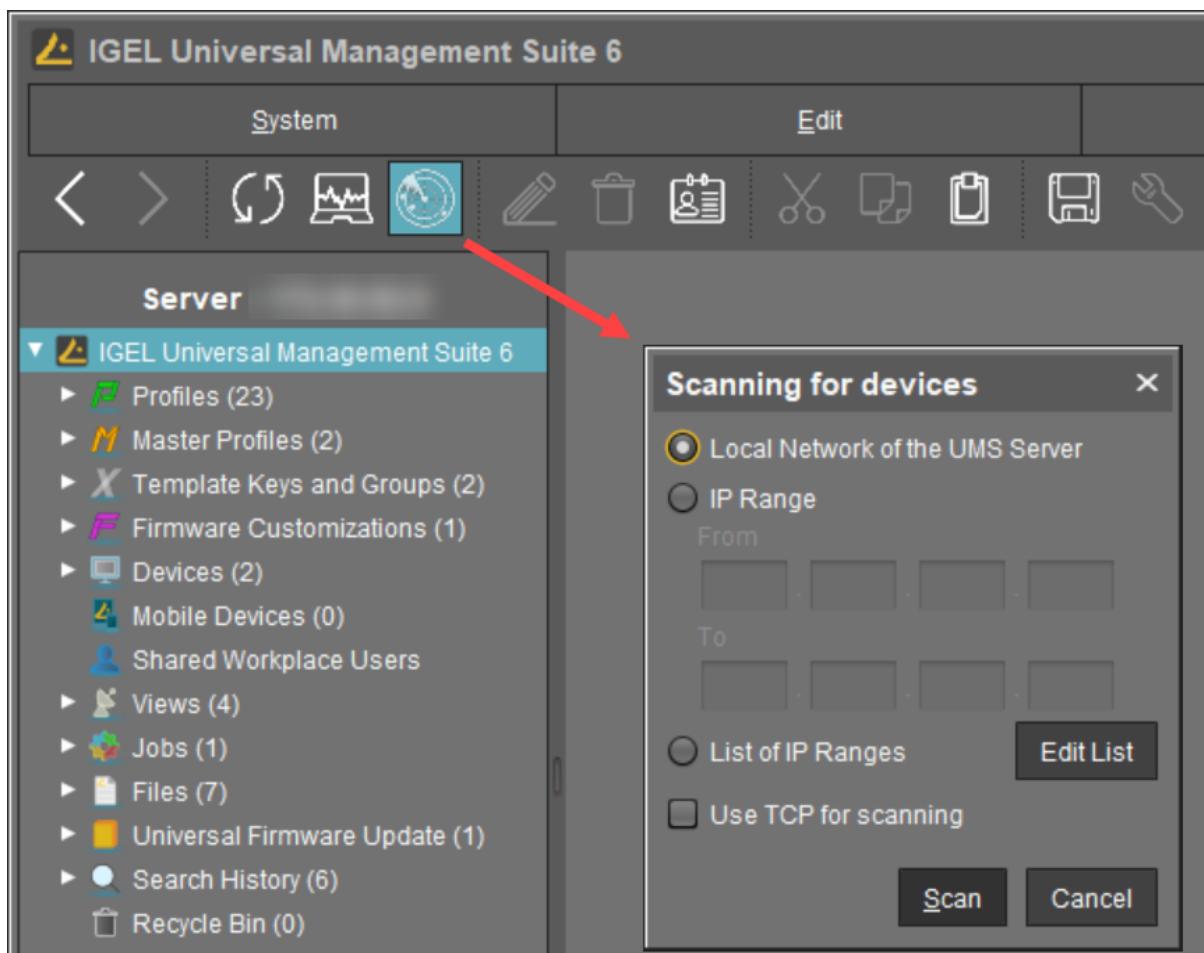
In order to find devices in the network, the following requirements must be met:

- 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 3 (UDC3)

Scan and Register Function in the UMS Console

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.

i 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.

i If TCP is used for searching, the search procedure will take longer; the scan results can be more reliable, however.

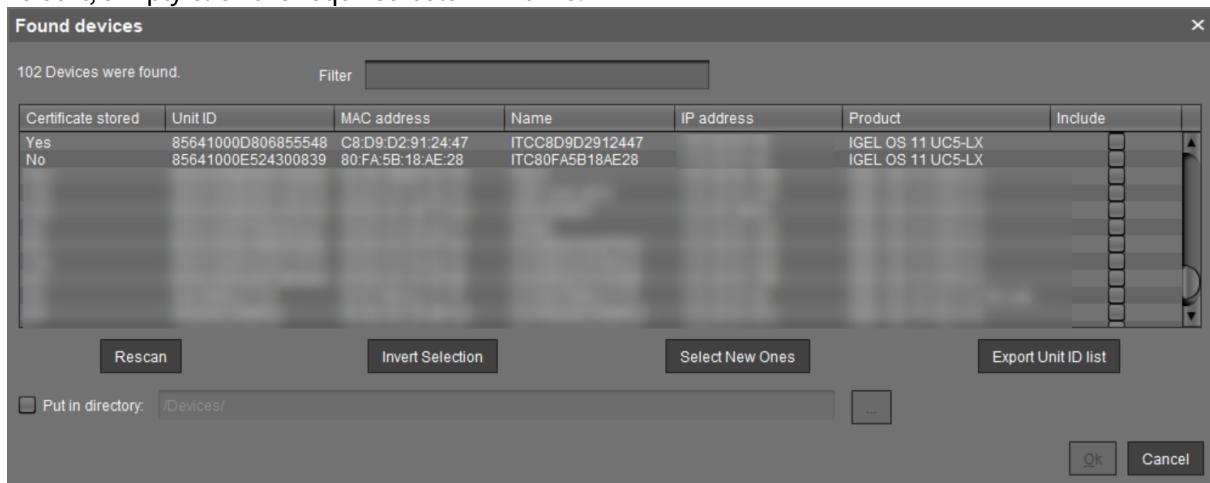
4. Click **Scan**.

The search results will be shown in the **Found devices** window. The devices can now be registered.

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.



i 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 \(see page 205\)](#).
OR
- the device has already been registered on some other UMS. In this case, see [Troubleshooting: Registration of a Device via Scanning for Devices Fails](#).

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.

- i** 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.

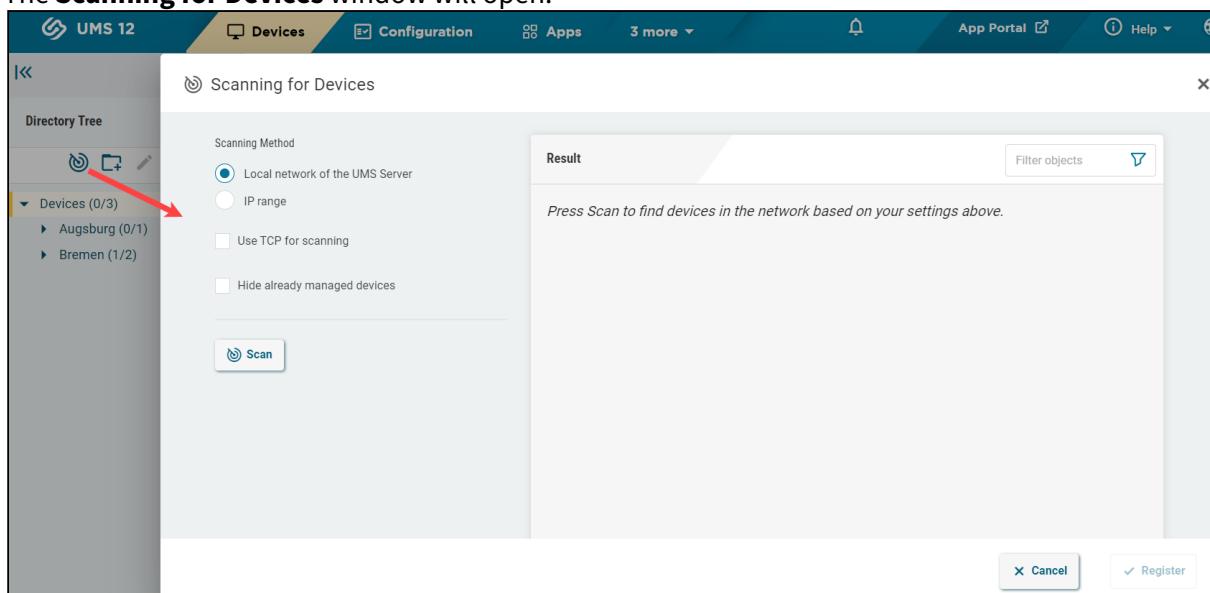
The devices will be placed in the **Devices** directory in the structure tree if no other directory was specified under **Put in directory**.

Scan and Register Function in the UMS Web App

To search for devices in the network and register them in the UMS, proceed as follows:

1. Open the UMS Web App and go to **Devices**.
2. If you want the devices to be placed in a specific directory during the registration, highlight the required directory in the structure tree. If no specific directory is selected, the devices will be placed in the **Devices** directory.
3. Click **Scan for devices** .

The **Scanning for Devices** window will open.



4. Specify the search area:
 - **Local network of the UMS Server:** The UMS Server will send a broadcast message to the network.

i 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. To specify the IP range, use the format [IP-Start] – [IP-End], e.g. 192.168.0.0 – 192.168.178.210. To specify several IP ranges, press [Enter].

- **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.

i If TCP is used for searching, the search procedure will take longer; the scan results can be more reliable, however.

- **Hide already managed devices:** Devices that have already been registered, i.e. that have already a server certificate from some UMS, will not be shown in the search results.

5. Click **Scan**.

The search results will be shown. The devices can now be registered.

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 **Name, Unit ID, MAC Address, IP Address, or Product** column, enter the corresponding character string in the **Filter** field.
To filter the results in the **Already Managed** column, enable or disable **Hide already managed devices**.

42 Devices						
	Name	Unit ID	MAC Address	IP Address	Product	Already Managed
<input type="checkbox"/>	ITC00505693000D	00505693000D	00505693000D		IGEL OS 11 UC1-LX	Yes
<input checked="" type="checkbox"/>	ITC00505693020B	00505693020B	00505693020B		IGEL OS 12 UC1-LX Starter	No
<input checked="" type="checkbox"/>	ITC005056934D76	0050569305B3	005056934D76		IGEL OS 12 UC1-LX Starter	No
<input type="checkbox"/>						Yes
<input type="checkbox"/>						Yes
<input type="checkbox"/>						Yes
<input type="checkbox"/>						No
<input type="checkbox"/>						Yes

- i** A device with **Already Managed** = "Yes" will not be registered unless the UMS has the same certificate.
"Yes" for **Already Managed** 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 or check the [recycle bin](#) (see [page 383](#)) if you want to verify that it is registered on this UMS.
OR
 - the device has already been registered on some other UMS. In this case, see [Troubleshooting: Registration of a Device via Scanning for Devices Fails](#).

2. Select the devices that are to be registered. You have the following options:
 - Manual selection: Select the individual devices that are to be registered.
 - Selecting all devices: This will highlight all devices, but only the devices that have not yet received a server certificate from the UMS will be registered:

42 Devices				
<input checked="" type="checkbox"/>	Name	Unit ID	MAC Address	IP Address

3. Check if the correct directory is selected under **Add devices to directory**.

4. Click **Register**.

The devices will now be registered in the UMS database. This may take some time.

- i** 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.

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.

- i** 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 308).

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 179), 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 174)
 - **Long Format:** See [Import with Long Format](#) (see page 175)
 - **IGEL Serial Number Format:** See [Import with IGEL Serial Number](#) (see page 177)
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. The import file should be UTF-8 encoded.

- **Unit ID:** If the device is an IGEL device or a device converted with UDC3 or IGEL OS Creator (OSC), the unit ID is identical to the MAC address of the device. If the device is a UD Pocket, the unit ID is hard-wired into the UD Pocket's USB flash drive.
- **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 for the IGEL Universal Management Suite \(UMS\)](#) (see page 415).

- **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

The long format provides detailed data as described in the following. The import file should be UTF-8 encoded.

- **Directory:** Storage directory in the UMS structure tree. This directory must exist before the devices are imported.
- **Unit ID:** If the device is an IGEL device or a device converted with UDC3 or IGEL OS Creator (OSC), the unit ID is identical to the MAC address of the device. If the device is a UD Pocket, the unit ID is hard-wired into the UD Pocket's USB flash drive.
- **Product and Version:** Product name and firmware version of the device (separated with a semicolon)
- **Name:** Name of the device



- 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 for the IGEL Universal Management Suite \(UMS\)](#) (see page 415).

- **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 for the IGEL Universal Management Suite \(UMS\)](#) (see page 415).

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.

For a general overview of device registration methods, see [Registering IGEL OS Devices on the UMS Server \(see page 165\)](#).

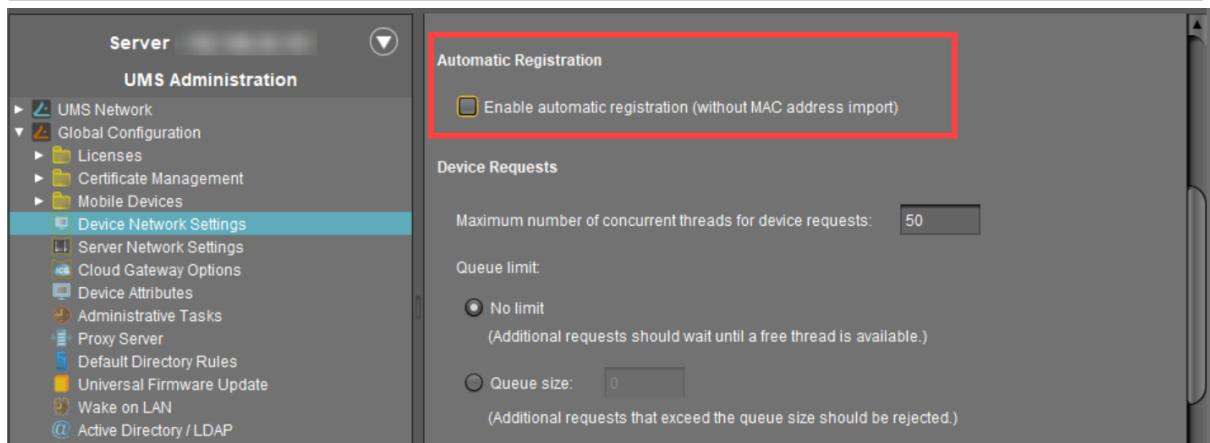
You can configure the UMS Server so that all IGEL OS devices on the server's network are automatically registered at startup. To do this, the devices must be given the address of the UMS Server via **DHCP or DNS**.

- ⓘ IGEL recommends automatic registration when registering new IGEL OS 11 devices for the first time during the rollout. You can use automatic registration also for IGEL OS 12 devices that are inside the company network; for IGEL OS 12 devices outside the company network, it is preferable to use IGEL Onboarding Service, see Initial Configuration of the IGEL Onboarding Service (OBS) and Onboarding IGEL OS 12 Devices.
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.

- i** 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

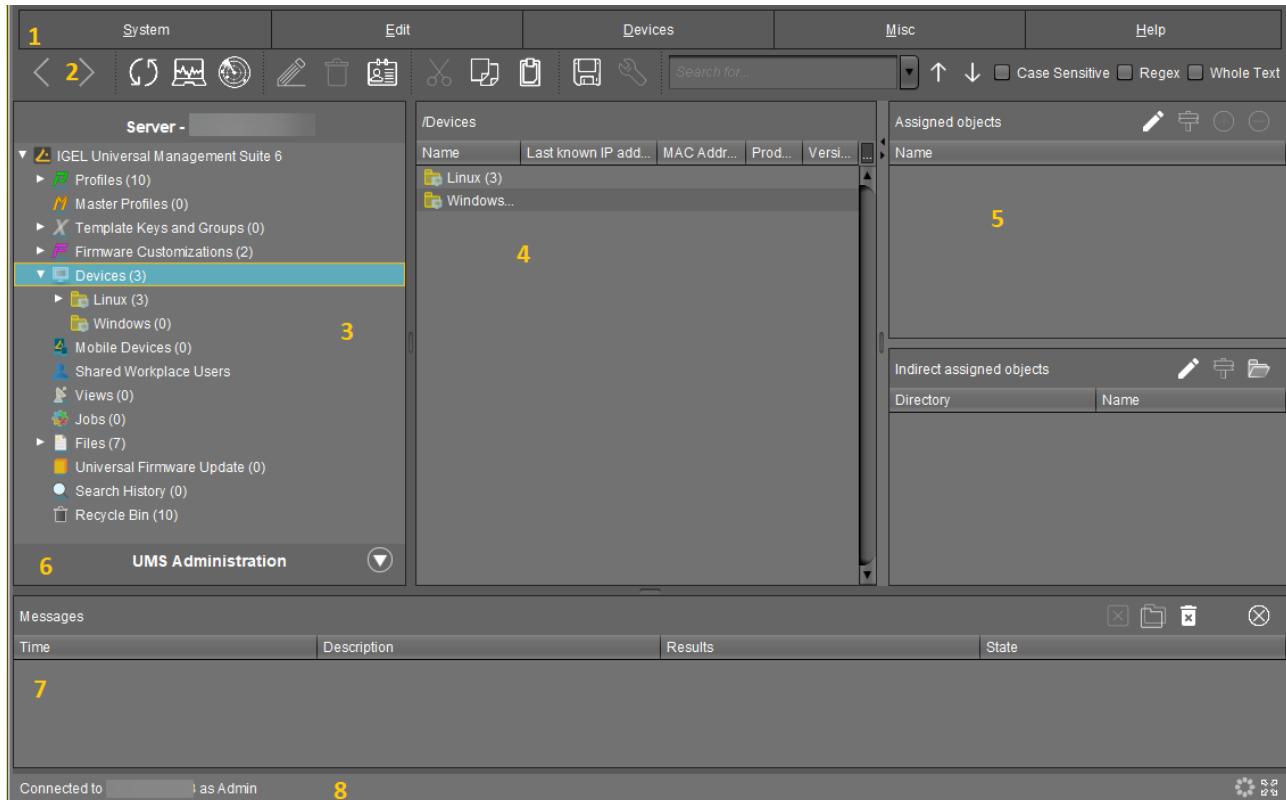
UMS Console User Interface

The program's graphical user interface and the tools available are described in detail below.

- [The Console Window \(see page 183\)](#)
- [Menu Bar of the IGEL UMS Console \(see page 185\)](#)
- [Structure Tree of the IGEL UMS Console \(see page 196\)](#)
- [Symbol Bar \(see page 197\)](#)
- [Content Panel of the IGEL UMS Console \(see page 199\)](#)
- [Messages \(see page 201\)](#)
- [Status Bar \(see page 202\)](#)
- [Assigned Objects \(see page 203\)](#)
- [Context Menu \(see page 204\)](#)
- [Search for Objects in the UMS \(see page 205\)](#)

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. See Menu Bar of the IGEL UMS Console (see page 185) .
2	Symbol bar	Frequently used commands relating to objects in the structure tree. See Symbol Bar (see page 197) .
3	Structure tree	Provides access to all UMS objects such as devices registered on the UMS Server, directories, profiles, views, scheduled tasks, etc. See Structure Tree of the IGEL UMS Console (see page 196) .
4	Content panel	Information regarding the selected object. Many entry fields can be edited directly. See Content Panel of the IGEL UMS Console (see page 199) .

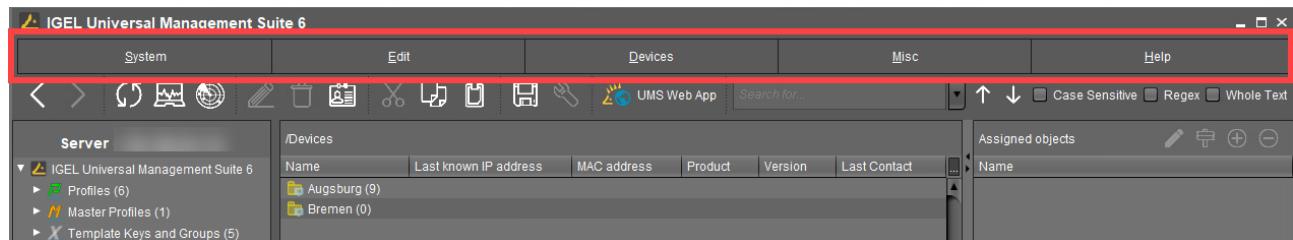
5	Assigned objects	Objects assigned to the devices or folders. See Assigned Objects (see page 203) .
6	UMS Administration	Administrative tasks, e. g. configuring domains, Universal Firmware Updates, and the scheduled backup of the UMS database (only Embedded DB) See UMS Administration (see page 386) .
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. See Messages (see page 201) .
8	Status row	Status messages from the console, e. g. the server currently connected and the user name. See Status Bar (see page 202) .

-  You can change the vertical and horizontal limits between the structure 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 of the IGEL UMS Console

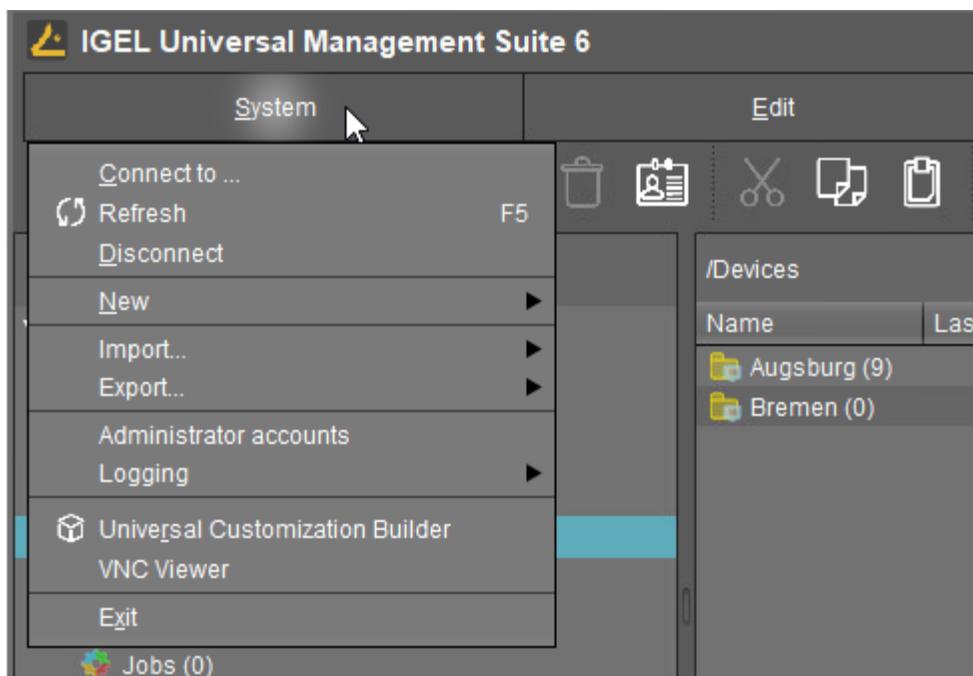
In the following article, you will learn about settings which you can configure in the menu bar of the IGEL Universal Management Suite (UMS) Console.

The menu bar of the UMS Console comprises the following menus:



System

In this menu, you will find options for actions relating to the UMS:



Connect to: Allows you to establish the UMS Server connection; the existing connection will be closed and the new one will be displayed in the same UMS Console window. For detailed information, see [Connecting the UMS Console to the IGEL UMS Server](#) (see page 162).

- **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. For detailed information, see [Exporting and Importing Data](#) (see page 306), [Exporting and Importing Profiles](#) (see page 231), and [Importing Devices](#) (see page 173).

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. For detailed information, see [Create Administrator Accounts](#) (see page 519).

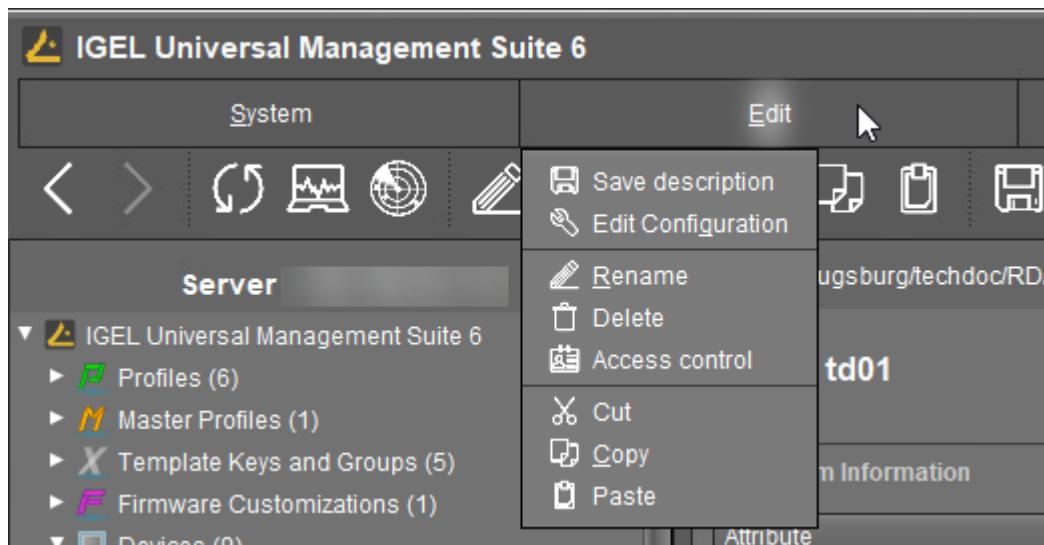
Logging: Allows you to display and export recordings of messages, events, and VNC log entries. For more information on logging, see [Logging](#) (see page 501) and [User Logs](#) (see page 537).

VNC viewer: Allows you to shadow a device. For more details on shadowing, see [Shadowing - Observe IGEL OS Desktop via VNC](#) (see page 320).

Exit: Allows you to close the UMS Console application.

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 structure tree.

Delete: Allows you to delete an object in the structure tree.

Access control: Allows you to manage user and group rights for the selected object. For detailed information, see [Create Administrator Accounts \(see page 519\)](#).

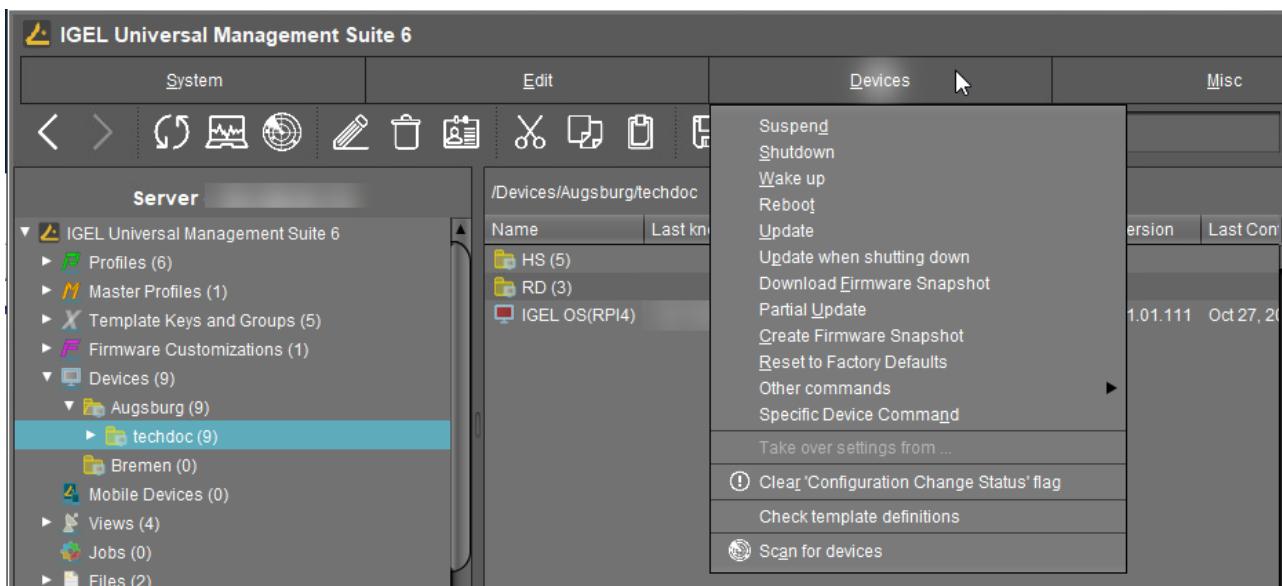
Cut: Allows you to cut a data object and copy it to the clipboard.

Copy: Allows you to copy data objects to the clipboard.

Paste: Allows you to paste data objects from the clipboard.

Devices

In this menu, you will find all commands that can be sent to the selected devices:



- ⓘ Most of these commands can also be accessed from the context menu, i.e. by right-clicking on a single device or a device directory.

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.

i See also Reset to Factory Defaults (IGEL OS) or Reset to Factory Defaults (Windows).

Other commands:

- **Send message:** Sends a message to the highlighted devices.
- **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.
- **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. See also How to Remove a UMS Certificate from an OS 11 Device.
- **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).
- **Start Login Enterprise Launcher:** Starts Login Enterprise Launcher if it has been configured, see Login Enterprise Launcher in IGEL OS.

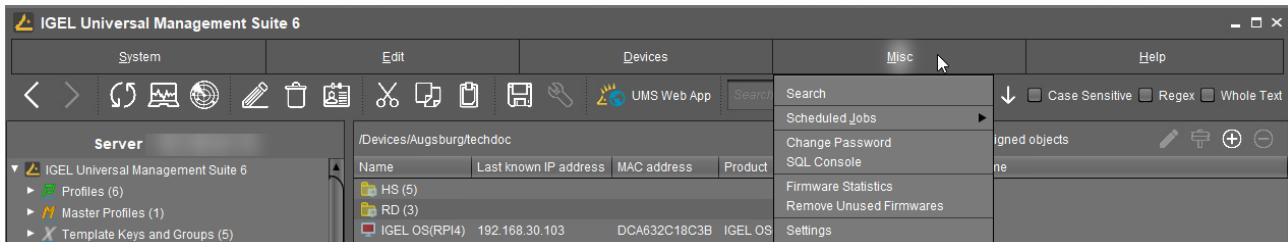
Take over settings from....: Sends profile settings to the device on a one-off basis.

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. See [Assigning Template Profiles and Values to the Devices](#) (see page 268). For general information on template profiles, see [Template Profiles in the IGEL UMS](#) (see page 256).

Scan for devices: Searches for devices in the network of the UMS Server.

Misc



Search: Allows you to search for objects - the search is listed in the structure tree under [Search History](#) (see page 381) 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 devices 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.

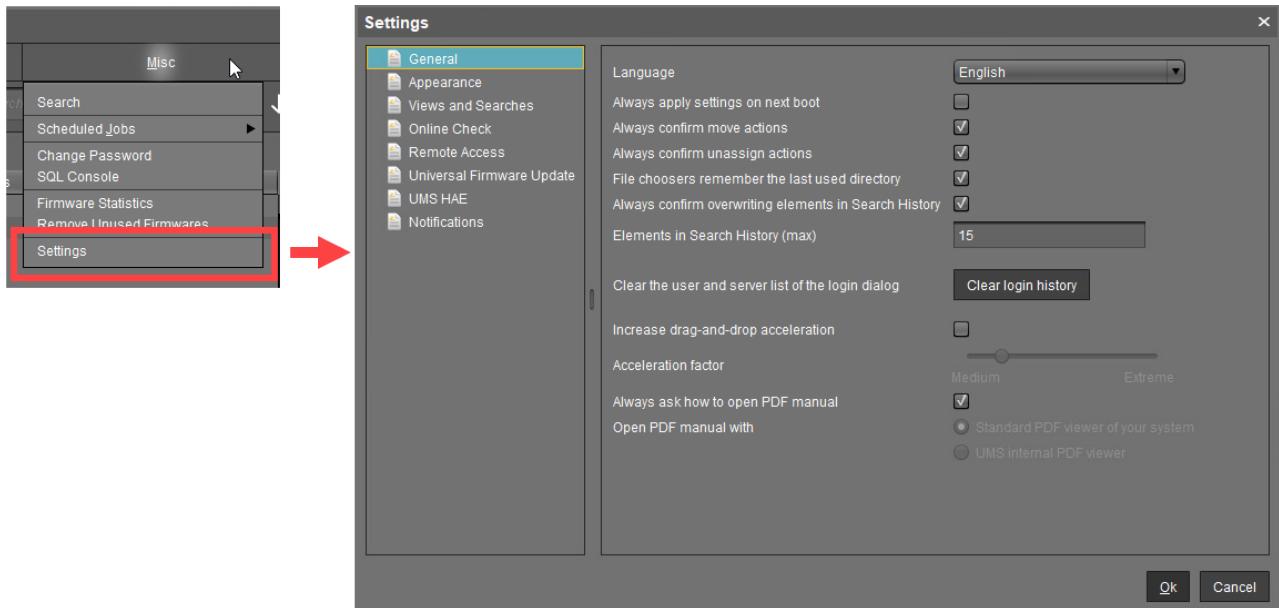
Firmware Statistics: A list of firmware versions registered in the database with filter function.

Remove Unused Firmwares: Opens a dialog which lists unused firmware and allows you to delete it from the database individually or collectively.

 **Remove Unused Firmwares** feature does NOT remove the downloaded firmware from **UMS Console > Universal Firmware Update** (see page 377).

Settings: Allows you to change configuration parameters such as language and appearance of the UMS Console, types of notifications, etc. For more details, see "Settings" below.

Settings



Here you can change the following parameters:

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.

- Always ask how to open PDF manual** (Default)

Open PDF manual with: If the checkbox above has been disabled, you can select the way the PDF manual must be opened:

- **Standard PDF viewer of your system**
- **UMS internal PDF viewer**

Appearance

Skin: Selection of possible themes/color combinations in which the GUI is displayed.

Possible options:

- **Workspace** (Default)
- **Smart contrast**
- **Pewter**
- **Cinder grey**
- **Ocean**

Device commands always in background

- In the background. (Default)

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)

Show content amount of directories

- Will be shown. (Default)

Load collapsed/uncollapsed tree status at login

- The structure tree will be restored to how it was at the last login. (Default)

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 \(see page 286\)](#). (Default)

- The status icons will not be shown.

Directory tooltip contains directory tree path

- Will be shown. (Default)

Directory tooltip contains directory and content amount

- The number of directories and the objects in the directory will be shown in the tooltip. (Default)

Views and Searches

You can configure the display of view and search results.

Lifetime for views: Defines how long the results of views are cached.

Possible options:

- **Details are never stored:** The view results are not cached. Thus, they must be loaded anew each time the view is selected in the structure tree under **Views**. (Default)
- **Details are kept for [time span]:** The view results are cached for the selected time span. When the time span has expired, the view results must be loaded anew when the view is selected in the structure tree under **Views**. The option "Details are kept for 30 minutes" is recommended for most cases.

Lifetime for searches: Defines how long the results of searches are cached.

- **Details are never stored:** The search results are not cached. Thus, they must be loaded anew each time the search is selected in the structure tree under **Search History**. (Default)
- **Details are kept for [time span]:** The search results are cached for the selected time span. When the time span has expired, the search results must be loaded anew when the search is selected in the structure tree under **Search History**. The option "Details are kept for 30 minutes" is recommended for most cases.

When opening a view result...

Possible options:

- **Automatically load amount and items:** The devices are loaded immediately when a view is selected in the structure tree under **Views**. With large amounts of devices, this may result in high loading times. You can refresh the display by clicking **Refresh**. (Default)
- **Automatically load amount:** The amount of devices is loaded immediately when you select a view in the structure tree under **Views**. You can load the devices by clicking **Load devices**.
- **Show parameters only:** Nothing is loaded immediately when a view is selected in the structure tree under **Views**. You can load the devices by clicking **Search for hits > Load devices**.

When opening a search result...

- **Automatically load amount and items:** The devices / profiles / views are loaded immediately when a search is selected in the structure tree under **Search History**. With large amounts of devices / profiles / views, this may result in high loading times. You can refresh the display by clicking **Refresh**. (Default)
- **Automatically load amount:** The amount of devices / profiles / views is loaded immediately when a search is selected in the structure tree under **Search History**. You can load the devices / profiles / views by clicking **Search for hits > Load device / Load profile / Load view**.
- **Show parameters only:** Nothing is loaded immediately when a search is selected in the structure tree under **Search History**. You can load the devices / profiles / views by clicking **Search for hits > Load device / Load profile / Load view**.

Show amount of views in tree

- The amount of devices is shown in the structure tree, provided that the amount has been loaded at least once. (Default)
- The amount of devices is not shown.

Show amount of hidden devices in view

- The amount of hidden devices is shown in the structure tree.
- The amount of hidden devices is not shown. (Default)

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)
For icons indicating the online status, see [Devices](#) (see page 286).

Never: No check is executed.

Check now: The online check is executed when this button is clicked.

Remote Access

External VNC viewer: Allows you to configure an external VNC viewer by entering or selecting the path to the executable file. This applies only to the UMS Console, not the IGEL UMS Web App.

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

Activate automatic status refresh

The registration status of the firmware update will be refreshed automatically. (Default)

Automatic status refresh interval: Interval in seconds. (Default: 3)

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

Show notifications on startup

The notification will pop up automatically on each connection to the UMS Console. (Default)

The notification will not pop up automatically. To see the notification, go to **Help > Notifications**.

Show following notifications for the current user or group

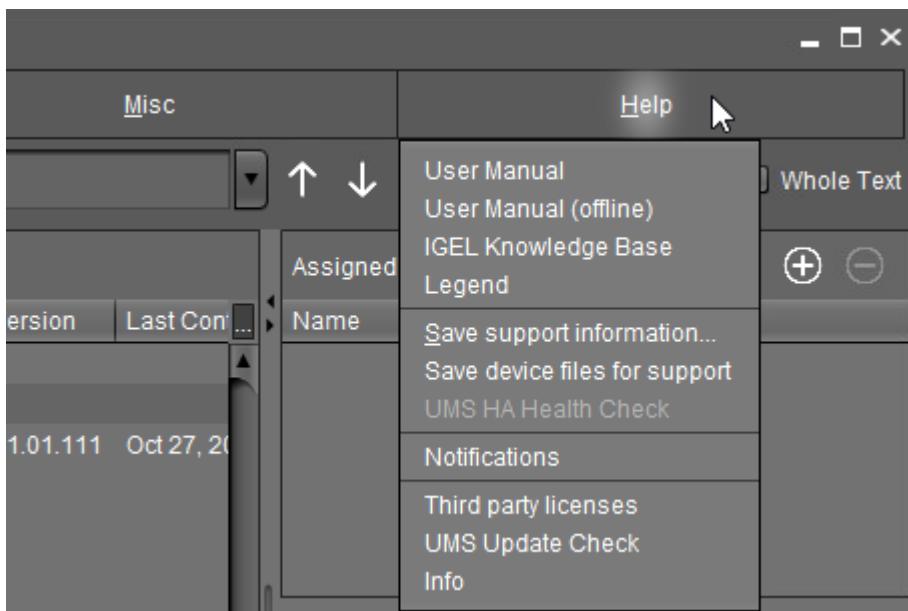
Possible options:

- **Show all:** Notifications of all types will be displayed.
- **Show nothing:** No notifications will be shown.
- **Show custom:** You can select which notification types are to be displayed.

For details on various notification types, see How to Configure Notifications in the IGEL UMS.

Help

In this area, you will find information that may help you when using the UMS.



User Manual: Link to the manual on kb.igel.com¹⁴

User Manual (offline): Opens the user manual in PDF format.

IGEL Knowledge Base: Link to further online documentation on kb.igel.com¹⁵.

Legend: Icons used in the UMS and their meanings.

Save support information....: 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 and also stores log files from the connected ICGs. 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 in the IGEL UMS](#) (see page 545).

Save device files for support: Saves log and configuration files for a device, for example `setup.ini` and `group.ini`, in a ZIP file.

¹⁴ <http://kb.igel.com>

¹⁵ <http://kb.igel.com>

UMS HA Health Check: Checks whether the interaction between the components of the High Availability system is working properly, in particular, whether the components can exchange messages and data. Further information can be found under UMS HA Health Check - Analyse Your IGEL UMS High Availability and Distributed UMS Systems.

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 of the IGEL UMS Console

You can highlight or select objects in the structure tree of the IGEL Universal Management Suite (UMS) Console by clicking on them. Multiple selections are possible using the [Shift] or [Ctrl] key.

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**.

You can also 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 **Misc > 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 \(see page 207\)](#): Create and organize standard profiles.
- [Priority Profiles \(see page 253\)](#): Create and organize priority profiles.
- [Template Keys and Groups \(see page 256\)](#): Keys and values for use in template profiles.
- [Firmware Customizations \(see page 274\)](#): Customize the user interface to suit your corporate design.
- [Devices \(see page 286\)](#): Organize managed devices.
- [Shared Workplace users \(see page 327\)](#): Assign specific profiles to AD users.
- [Views \(see page 328\)](#): Create configurable list views for devices.
- [Jobs - Sending Automated Commands to Devices in the IGEL UMS \(see page 355\)](#): Define scheduled tasks, e.g. firmware updates.
- [Files \(see page 366\)](#): Registering files for transfer to devices.
- [Universal Firmware Update \(see page 377\)](#): Allows you to download the current firmware versions for distribution to devices.
- [Search History \(see page 381\)](#): Saved search queries.
- [Recycle Bin \(see page 383\)](#): 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
UMS Web App	Open the IGEL UMS Web App.
	Find 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 of the IGEL UMS Console

The content panel of the IGEL Universal Management Suite (UMS) Console 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.

Illustrative List of Details Shown in the Content Panel for Some Objects from the UMS Structure Tree

Server - [IP Address]

- **Profiles:** Name, description, profile ID, etc. See [Profiles in the IGEL UMS \(see page 207\)](#).
- **Priority Profiles:** Name, description, profile ID, etc. See [Priority Profiles in the IGEL UMS \(see page 253\)](#).
- **Template Profiles:** Name and description of template keys and value groups. See [Template Profiles in the IGEL UMS \(see page 256\)](#).
- **Firmware Customizations:** Name, use case, and configuration parameters of a firmware customization. See [Firmware Customizations in the IGEL UMS \(see page 274\)](#).
- **Devices:** System information, license and monitor information, features, etc. See [Devices \(see page 286\)](#) and [View Device Information in the IGEL UMS \(see page 288\)](#).

 With a **Copy to Clipboard (ASCII)** button at the bottom of the content panel, you can copy the device information in ASCII format.

- **Shared Workplace Users:** Name, email addresses of the users from Active Directory, etc. See [Shared Workplace Users \(see page 327\)](#).
- **Views:** Name, rule, matching devices, etc. See [Views \(see page 328\)](#).
- **Jobs:** Job info, schedule, execution results, etc. See [Jobs - Sending Automated Commands to Devices in the IGEL UMS \(see page 355\)](#).
- **Files:** Source URL, classification, device file location, access rights, etc. See [Files - Registering Files on the IGEL UMS Server and Transferring Them to Devices \(see page 366\)](#).
- **Universal Firmware Update:** Firmware update settings and version, download status, etc. See [Universal Firmware Update \(see page 377\)](#).
- **Search History:** Name, rule, matching devices, etc. See [Search History \(see page 381\)](#).
- **Recycle Bin:** Name and type of the deleted object, its deletion date, etc. See [Recycle Bin - Deleting Objects in the IGEL UMS \(see page 383\)](#).

UMS Administration

- **Server:** Information regarding the service executed, requests, failed and waiting requests. See [Server - View Your IGEL UMS Server Information \(see page 388\)](#).
- **Load Balancer:** Information regarding the service executed, requests, failed and waiting requests. See [Load Balancer - View Your IGEL UMS Load Balancer Information \(see page 391\)](#).

- **Licenses:** License summary, registered licenses. See [Licenses \(see page 397\)](#).
- **Certificate Management:** Signature algorithm, key, status of the certificates, etc. See [Certificate Management \(see page 407\)](#).
- **Device Attributes:** Device attributes such as name, type, etc. See [Managing Device Attributes for IGEL OS Devices \(see page 432\)](#).
- **Administrative Tasks:** List with tasks, execution history. See [Administrative Tasks - Configure Scheduled Actions for the IGEL UMS \(see page 436\)](#).
- **Proxy Server:** Name, host, port, etc. See [Proxy Server \(see page 479\)](#).
- **Universal Firmware Update:** Settings for the Universal Firmware Update, settings for the FTP servers to which the files are copied (optional). See [Universal Firmware Update \(see page 492\)](#).
- **Wake-on-LAN:** Wake-on-LAN configuration parameters. See [Wake on LAN \(see page 494\)](#).
- **Active Directory / LDAP:** Active Directory / LDAP domains. See [Active Directory / LDAP \(see page 497\)](#).
- **Remote Access:** Secure VNC connection, graphics settings, etc. See [Remote Access \(see page 499\)](#).
- **Logging:** Log message settings, logging event settings. See [Logging \(see page 501\)](#).
- **Mail Settings:** Mail settings, recipient for administrative task result and service emails. See [Mail Settings \(see page 507\)](#).
- **UMS Features:** Activating recycle bin, template profiles, priority profiles, etc. See [UMS Features \(see page 512\)](#).

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.

Messages			
Time	Description	Results	State
1/21/20 12:30 PM	Wake up devices	The action ended successfully.	 Finished
1/21/20 12:29 PM	Reboot devices	 The action failed.	 Failed

- ▶ 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

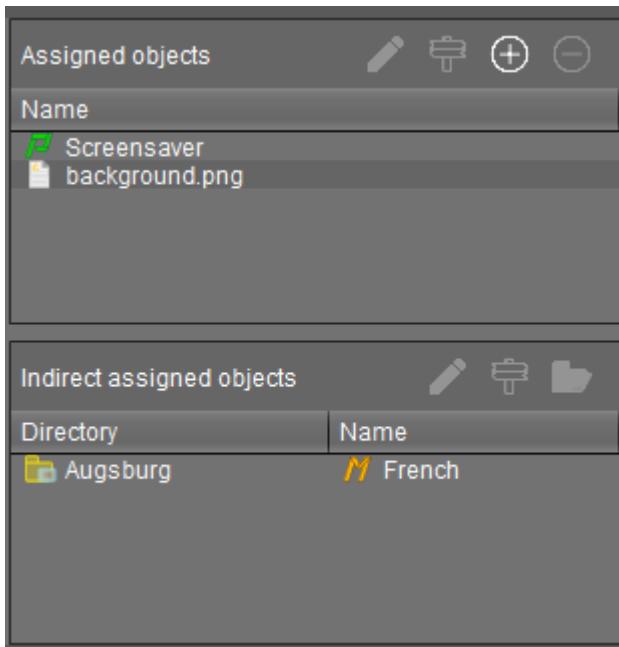
The **status bar** shows the name of the UMS Server currently connected and the user who is logged in to the UMS Console. The symbol at the bottom right indicates the status of the message window. For example, it signals when new warning messages are present. These can be seen here even if the message 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.

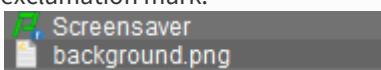


The screenshot shows the 'Assigned objects' interface divided into two main sections:

- Assigned objects:** This section contains a table with a single row. The first column is labeled 'Name' and contains two items: 'Screensaver' (with a green icon) and 'background.png' (with a white icon). The second column contains edit, delete, and add buttons.
- Indirect assigned objects:** This section contains a table with two columns: 'Directory' and 'Name'. It shows one entry: 'Augsburg' in the 'Directory' column and 'French' in the 'Name' column. The second column contains edit, delete, and add buttons.

- 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 185](#)).

Search for Objects in the UMS

Objects within the UMS structure tree can be found using the following functions:

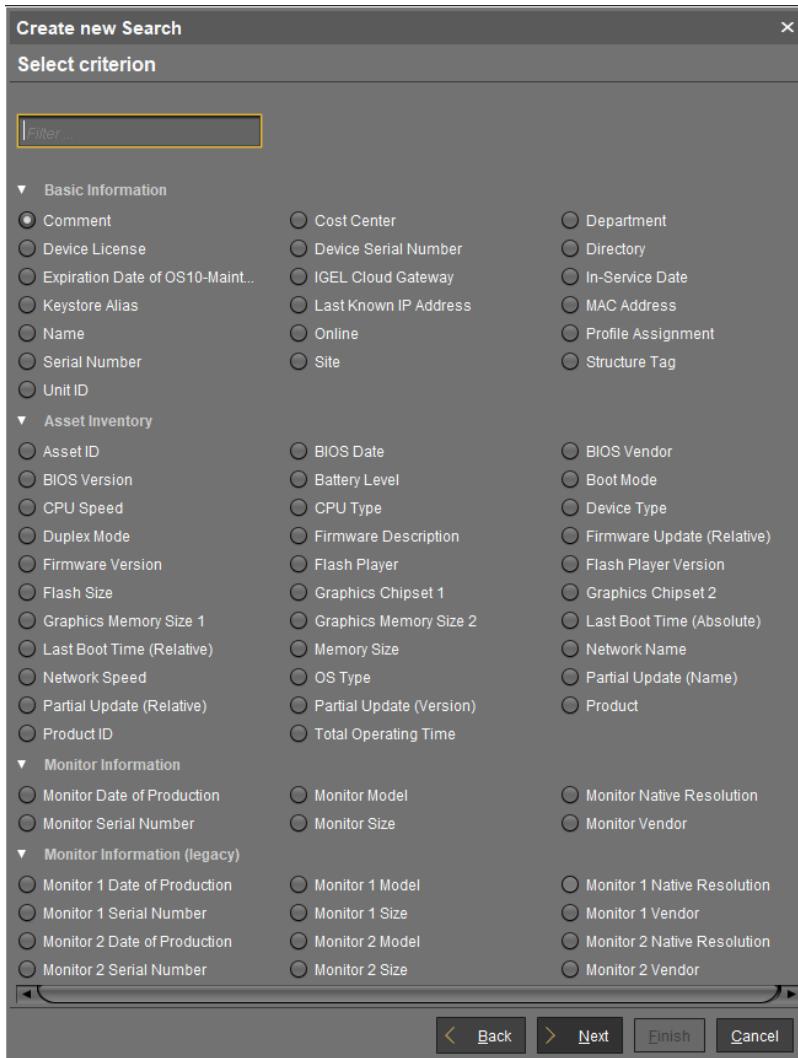
- **Quick Search**
- **Search function**
- **View**

Quick Search

The **Quick Search**  in the [symbol bar](#) (see page 197) 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 381) in the structure tree and can therefore be processed or reused easily.



Views

Views (see page 328) 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 355).

From UMS Version 5.02.100, both search results and views can be assigned to profiles. See also [Assigning Objects to a View \(see page 354\)](#) and [Assign Objects to the Devices of Views or Device Searches \(see page 466\)](#).

Profiles in the IGEL UMS

In the IGEL Universal Management Suite (UMS), you can create and manage profiles. **Profiles** are predefined configurations that can be assigned globally to managed devices via the UMS.

Menu path: **UMS Console > Profiles**

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.

Name	Language
Description	
Based on	IGEL OS 11 11.08.230.rc7.01
Profile ID	107
► Expert mode	

i 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.

Profile Types

The following profile types exist:

	<p>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 212).</p> <p>If you use Shared Workplace, 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 IGEL Shared Workplace (see page 243) and Prioritization of Profiles in the IGEL UMS (see page 239).</p>
	<p>Template profiles are profiles where one or more settings are set via variables. These values are determined dynamically. Standard and priority profiles can thus be used and combined even more flexibly. See the Template Profiles in the IGEL UMS (see page 256) chapter.</p> <p>If you deploy Shared Workplace, notice that template profiles cannot be used.</p>
	<p>Priority profiles can overwrite the settings of standard profiles and have their own authorizations, see Priority Profiles in the IGEL UMS (see page 253). The order of effectiveness is exactly the opposite of what it is for the standard profiles. See Order of Effectiveness of Priority Profiles (see page 244).</p>

Profiles for IGEL OS 12 and IGEL OS 11 Devices

- The procedure for creating profiles for IGEL OS 12 and IGEL OS 11 devices is different. If you want to configure, for example, Chromium browser settings for your IGEL OS 12 and IGEL OS 11 devices, you have to create two profiles – one for OS 12 devices and another for OS 11 devices.
- Profiles for IGEL OS 12 devices can only be created and changed in the UMS Web App. It is not possible to create/edit them in the UMS Console.
- Profiles for IGEL OS 11 devices can be created and edited in the UMS Console and the UMS Web App.
- The direct assignment of OS 12 profiles to OS 11 devices is not possible, and vice versa. If you assign an OS 12 profile to an OS 11 device indirectly, i.e. via a directory structure, the settings from the OS 12 profile are ignored for the OS 11 device (and vice versa).

This chapter explains what profiles are and how they work and describes how to create and manage profiles in the UMS Console. For details on profiles in the UMS Web App, see Configuration - Centralized Management of Device Settings in the IGEL UMS Web App.

- [Choosing the Right Profile \(see page 210\)](#)
- [Configuration Levels \(see page 211\)](#)
- [Effectiveness of Settings \(see page 212\)](#)
- [Using Profiles \(see page 213\)](#)
- [Prioritization of Profiles in the IGEL UMS \(see page 239\)](#)

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=Sc38mRv5Z1s&t=2s>

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 \(see page 213\)](#) chapter, you can find out how to set up and assign profiles.

In the [Template profiles \(see page 256\)](#) chapter, you can also find out how to create profiles with variable values.

In the [Prioritization of Profiles in the IGEL UMS \(see page 239\)](#) chapter, the priority rule is explained.

Priority Profiles

The use of one or two **priority profiles** can be helpful in a hierarchical structure with various administrators and complex rights management. With a priority profile, a higher-ranking administrator can influence other administrators' profile settings without withdrawing their management rights.

Read the chapter [Priority Profiles in the IGEL UMS \(see page 253\)](#) very carefully before you use this profile type.

- ! Use **priority 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 and Parameters Configurable in the User Profile](#).

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 239](#)) apply.

Free Instances

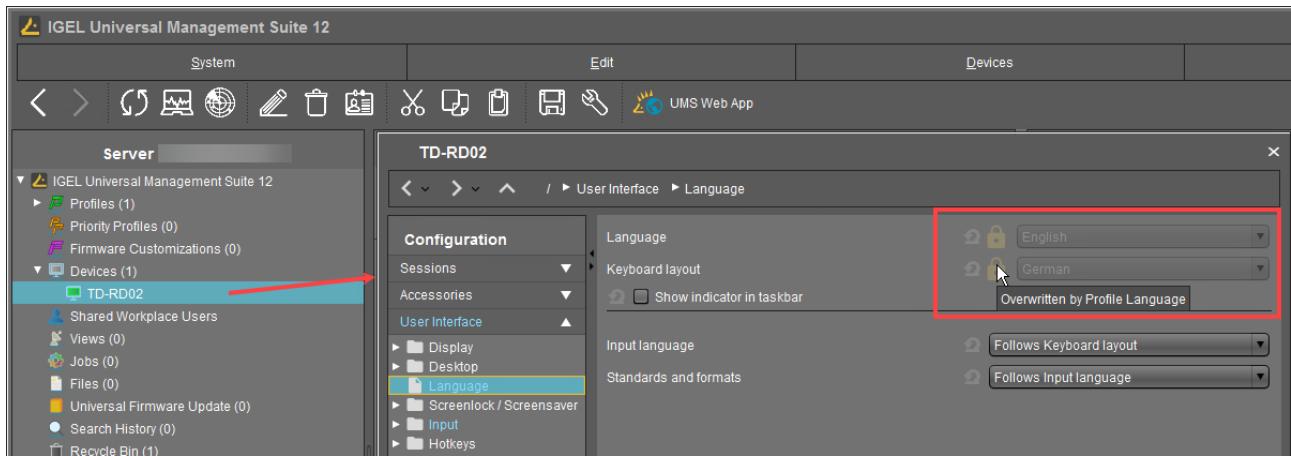
These are the instances that the user can add or delete via . These include sessions, USB devices, printers, accessories, VPN connections, and everything that can be selected in device lists.

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 in the IGEL UMS](#) (see [page 214](#)).

Effectiveness of Settings

Parameters set via a profile are blocked in the configuration dialog in the UMS as well as in the IGEL Setup and indicated by a lock symbol.



These blocked settings 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.

- i** 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 in the IGEL UMS \(see page 214\)](#)
- [How to Allocate IGEL UMS Profiles \(see page 220\)](#)
- [Checking Profiles in the IGEL UMS \(see page 223\)](#)
- [Editing Profiles in the IGEL UMS \(see page 226\)](#)
- [Removing Assigned Profiles from a Device \(see page 229\)](#)
- [Deleting Profiles \(see page 230\)](#)
- [Exporting and Importing Profiles \(see page 231\)](#)
- [Copy Profiles in the IGEL UMS \(see page 235\)](#)
- [Copy Profile Directories in the IGEL UMS \(see page 236\)](#)
- [Comparing Profiles in the IGEL UMS \(see page 237\)](#)

Creating Profiles in the IGEL UMS

In the following article, you will learn how to create profiles in the UMS Console. You will also find here the information on **Overwrite sessions** and other expert mode settings for profiles.

For how to create profiles in the UMS Web App, see How to Create and Assign Profiles in the IGEL UMS Web App.

Menu path: **UMS Console > Profiles**

Profiles for IGEL OS 12 and IGEL OS 11 Devices

- The procedure for creating profiles for IGEL OS 12 and IGEL OS 11 devices is different. If you want to configure, for example, Chromium browser settings for your IGEL OS 12 and IGEL OS 11 devices, you have to create two profiles – one for OS 12 devices and another for OS 11 devices.
- Profiles for IGEL OS 12 devices can only be created and changed in the UMS Web App. It is not possible to create/edit them in the UMS Console.
- Profiles for IGEL OS 11 devices can be created and edited in the UMS Console and the UMS Web App.
- The direct assignment of OS 12 profiles to OS 11 devices is not possible, and vice versa. If you assign an OS 12 profile to an OS 11 device indirectly, i.e. via a directory structure, the settings from the OS 12 profile are ignored for the OS 11 device (and vice versa).

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

- ▶ Update your UMS to the current version.
- ▶ For all relevant [OS 11 profiles](#) (see page 214), set **Based on** to the appropriate firmware version.
- ▶ For OS 12 profiles, note the following: An OS 12 profile configures ALL versions of an app, unless a specific version is set under **Show Versions**.

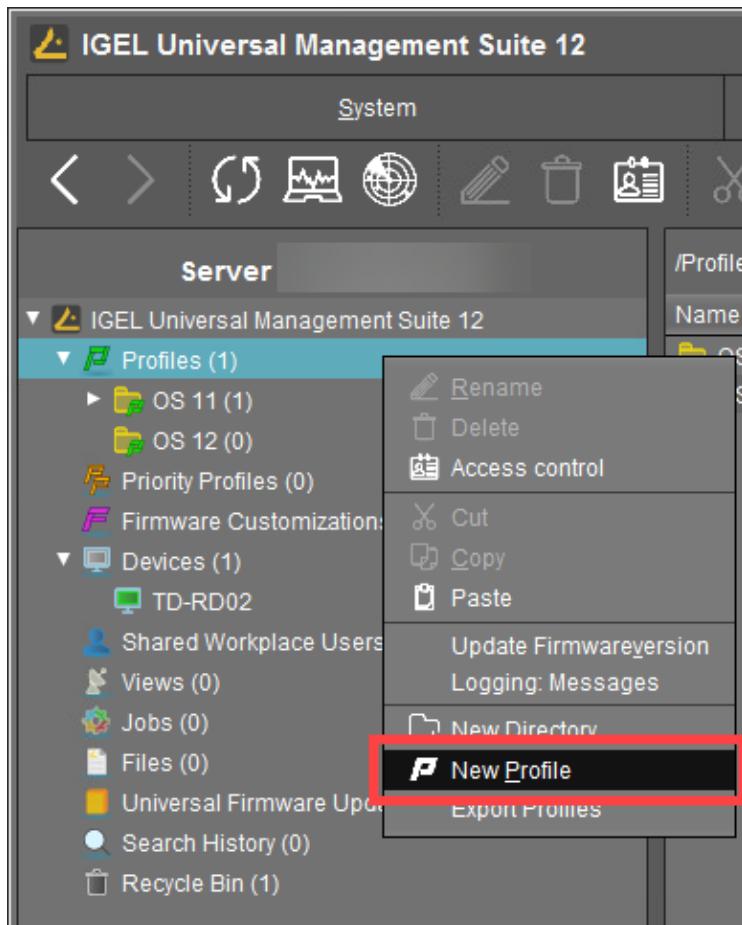
 For a better overview, it is recommended to organize profiles using subdirectories.

How to Create a Profile

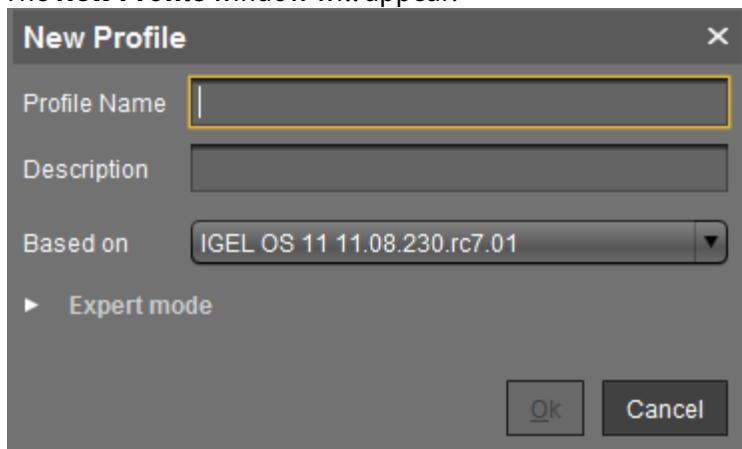
To create a new profile, proceed as follows:

1. In the UMS Console, click **Profiles > [context menu] > New Profile** or **System > New > New Profile**.

Alternatively, you can import a previously created profile. See [Exporting and Importing Profiles](#) (see page 231).

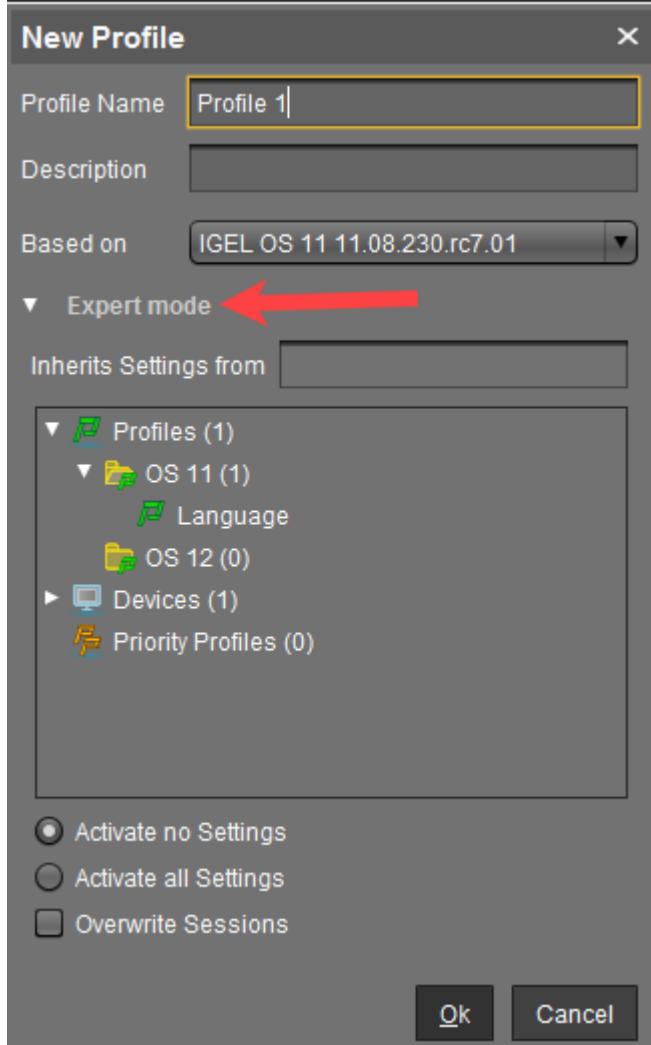


The **New Profile** window will appear.



2. Enter a **Name** and a **Description** for the profile.
3. Under **Based on**, select a firmware version for the new profile.

4. Optional (usually not required): Click **Expert mode** to define the following settings:



- **Inherits Settings from:** You can specify here whether the new profile should use settings from an existing profile or device. If yes, select the required profile / device from the list.
- **Activate no settings:** Initially, there are no active parameters. (Default)
- **Activate all settings:** All available parameters of the profile will be active.
- **Overwrite sessions:** All free instances will be overwritten by the profile.

⚠️ IMPORTANT! Before changing the default settings here, inform yourself about the possible consequences, see "New Profile: Expert Mode" below. **Activate 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.

5. Click **OK** to set up and save the profile.

i 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**.

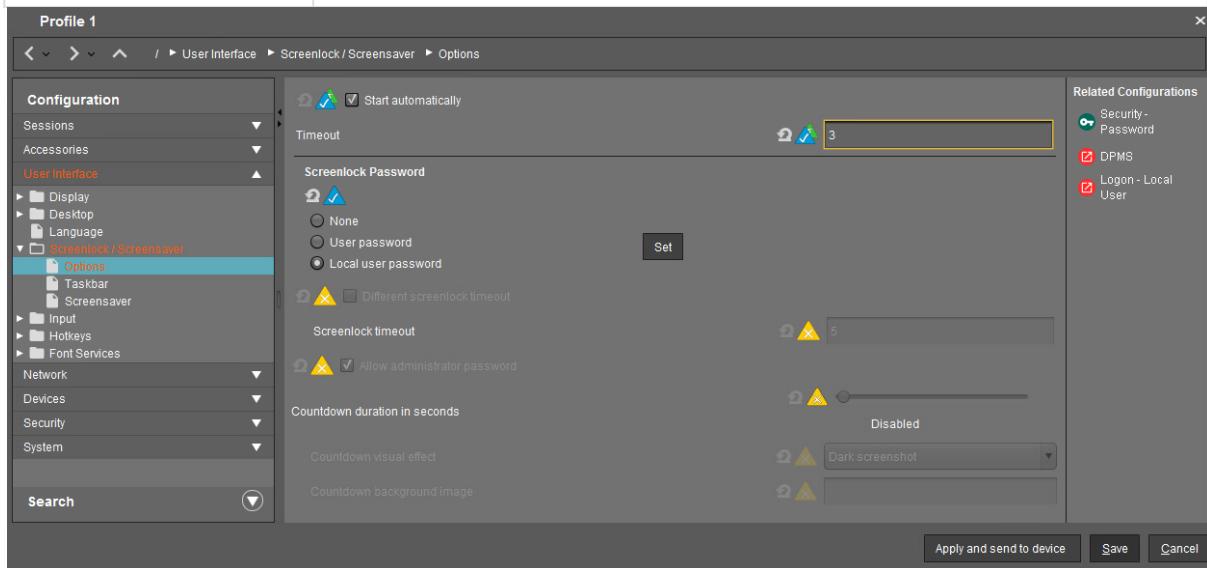
6. Configure the desired settings.

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.
	Reset to the default value.

The following activation symbols are only displayed if template profiles are activated (see [Template Profiles in the IGEL UMS \(see page 256\)](#)):

	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.



7. Save the settings:

- Click **Apply and send to device** to save the settings without quitting the profile.
- Click **Save** to save the settings and quit the profile.

8. Assign the profile to the required devices / device directories. See [How to Allocate IGEL UMS Profiles](#) (see page 220).

New Profile: Expert Mode

⚠ Expert mode for profiles is usually NOT required and should only be used in exceptional cases.

The options in the window **New Profile > Expert mode** have the following meaning:

Inherits Settings from

Defines if the new profile inherits settings from an existing profile or device.

Activate no settings

No parameters are initially active.

Activate all settings

All available parameters for the profile are enabled. Note that all settings are locked on the device with a lock symbol. A profile with **Activate all settings** option enabled prevents settings from 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. Therefore, you should use this option only if it is really 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

ⓘ Here, "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 [Configuration Levels](#) (see page 211).

- Overwrites the free instances defined on the device or assigned via 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. (Default)

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 priority profile (see page 253) 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 priority profile. Sessions in priority profiles can only be overwritten by a priority profile.

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=MI522x3qqn0>



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:
https://www.youtube.com/watch?v=zeHiW4_uG0s&t=4s



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:
<https://www.youtube.com/watch?v=h8EpnPNUmkg>

How to Allocate IGEL UMS Profiles

In the IGEL Universal Management Suite (UMS) Console, you can assign a profile to a device or a device directory. 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.

Direct and Indirect Assignment of Objects in the IGEL UMS

Objects in the IGEL UMS can be assigned directly or indirectly:

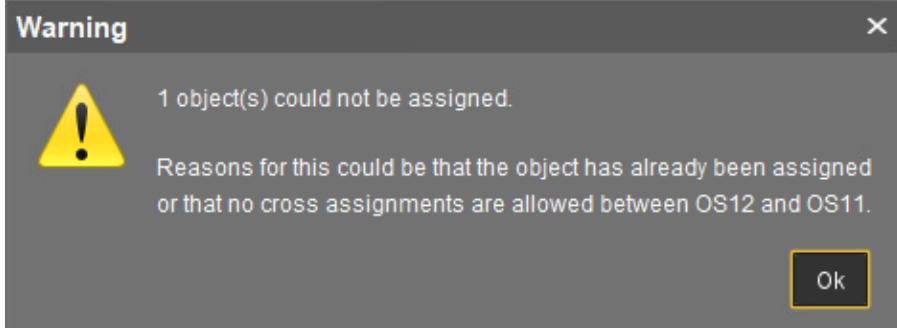
- Directly assigned objects have been assigned to an individual device or directory.
- Indirectly assigned objects have been "inherited" via the directory structure.

Whether a profile is assigned directly or indirectly influences the priority of a profile, see [Order of Effectiveness of Profiles](#) (see page 240).

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.

The direct assignment of OS 12 profiles to OS 11 devices is not possible, and vice versa:



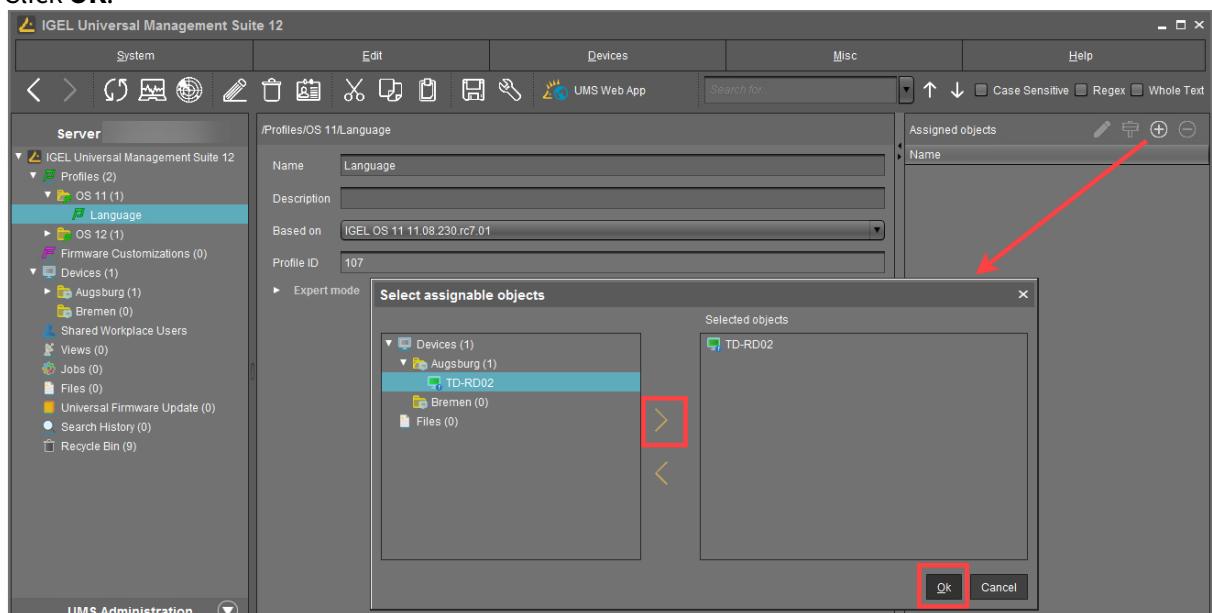
If you assign an OS 12 profile to an OS 11 device indirectly, i.e. via a directory structure, the OS 12 profile is NOT regarded for the OS 11 device (and vice versa).

How to Assign a Profile: Starting from the Profile

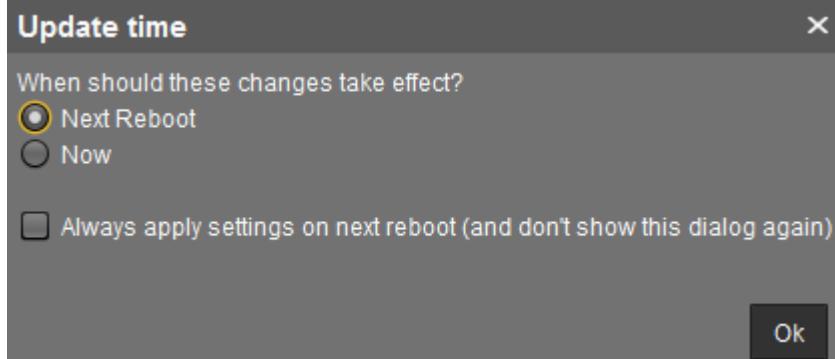
1. In the UMS Console, go to **Profiles** and select the required profile.
 2. Under **Assigned objects**, click .
- The **Select assignable objects** window will open.

3. Highlight the required device or device directory and click .

4. Click **OK**.



5. Decide whether the new settings are to take effect immediately or at the next reboot of the device.



Bear in mind that users who are working may be disturbed if changes take effect immediately.

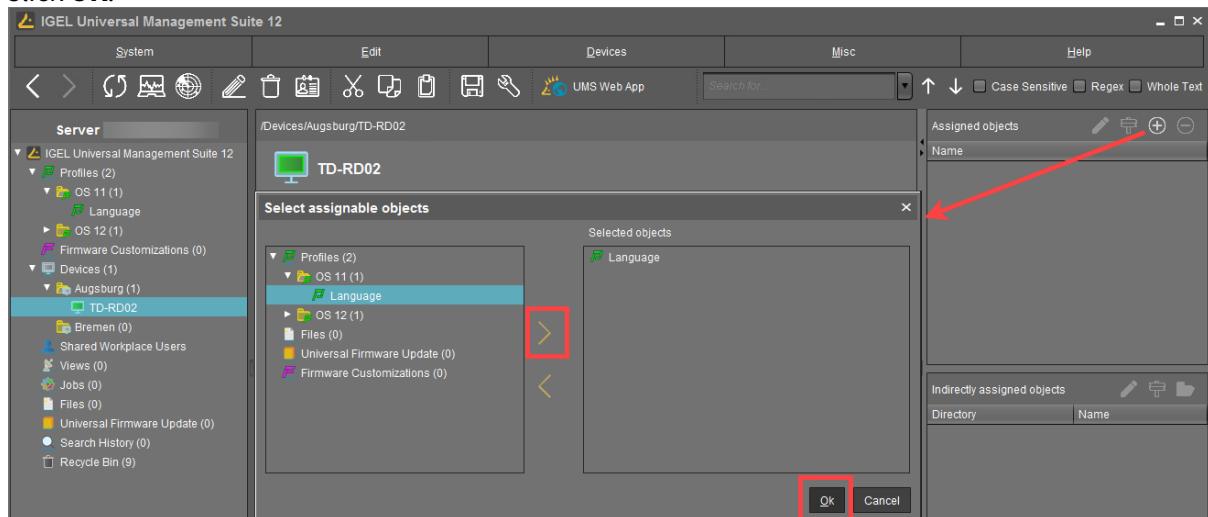
- Devices that have not yet received the configuration changes are flagged with an exclamation mark .

How to Assign a Profile: Starting from the Device / Device Directory

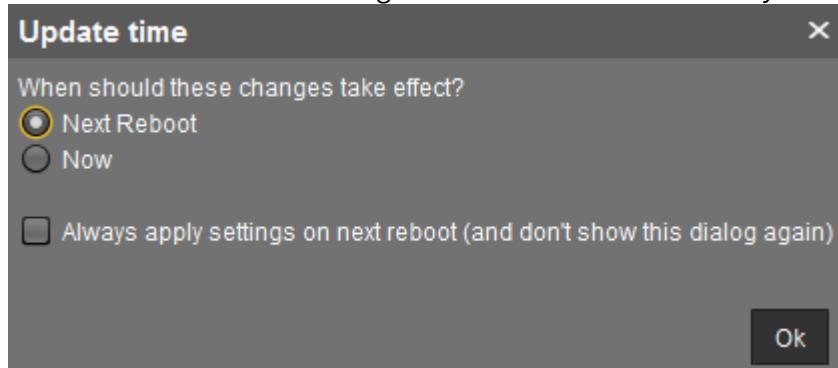
1. In the UMS Console, go to **Devices** and select the required device or device directory.
2. Under **Assigned objects**, click . The **Select assignable objects** window will open.

3. Highlight the required profile and click .

4. Click **OK**.



5. Decide whether the new settings are to take effect immediately or at the next reboot of the device.



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**.

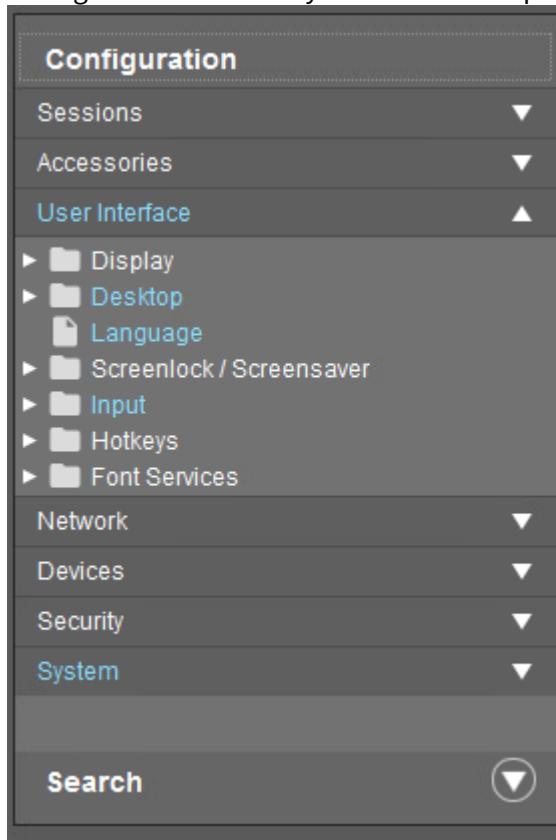
Name
Background
Language

Checking Profiles in the IGEL UMS

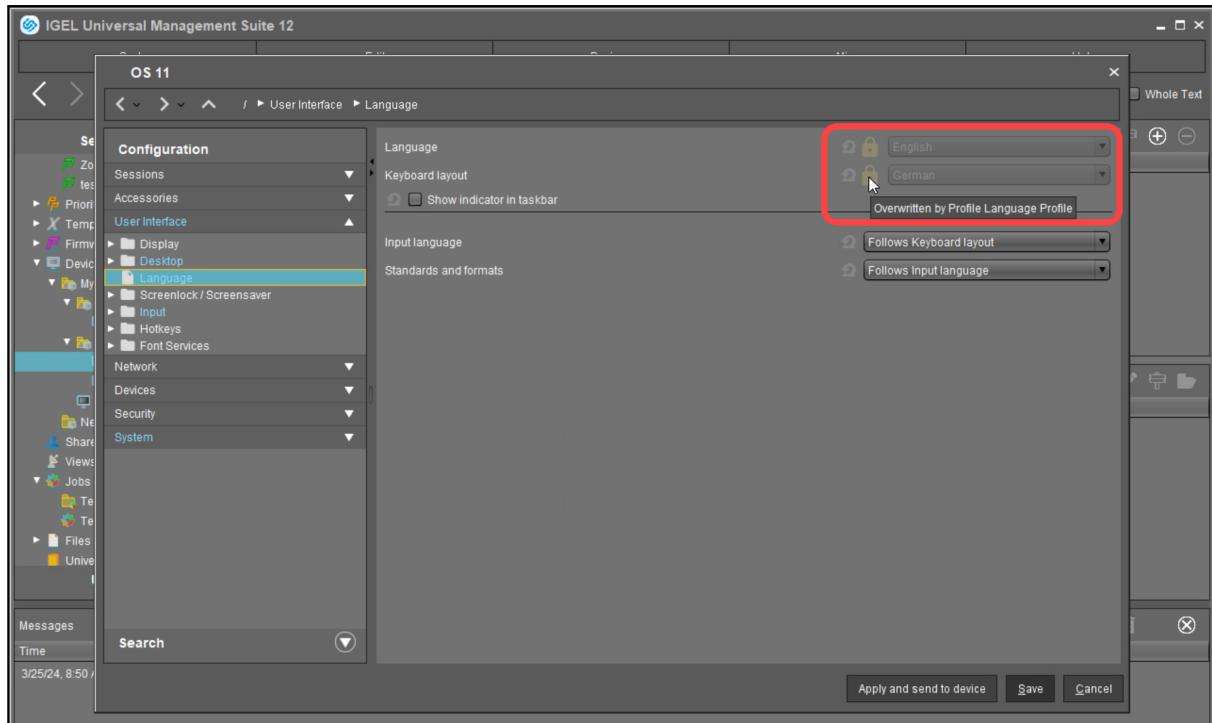
If you have assigned a profile to a device in the IGEL Universal Management Suite (UMS), you can check the results as follows. In the IGEL UMS Web App, you can do it as described in [How to Check which Profiles Define Parameters in the IGEL UMS Web App](#).

1. In the **UMS Console**, go to **Devices** and select the required device.
2. Click [**device's context menu**] > **Edit Configuration** or **Edit** > **Edit Configuration**.
Or you can simply double-click the device.

The current configuration for the device will be displayed. Paths highlighted in blue lead to settings that have already been set via the profiles.



A lock symbol will be shown in front of each setting configured via an assigned profile. The value that you have specified in the profile will be shown. You cannot change the setting here.



3. 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 object or edit its configuration.

Name
Background
Language

- ▶ Select an object and click to edit the object.
- ▶ Select an object and click to navigate to this object in the structure tree.
- ▶ Double-click an assigned object to jump straight to it.

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=h8EpnPNUmkg>

Editing Profiles in the IGEL UMS

In the IGEL Universal Management Suite (UMS), you can edit the existing profiles. You can edit the **description data** of a profile as well as the **profile configuration**.

Menu path: **UMS Console > Profiles**

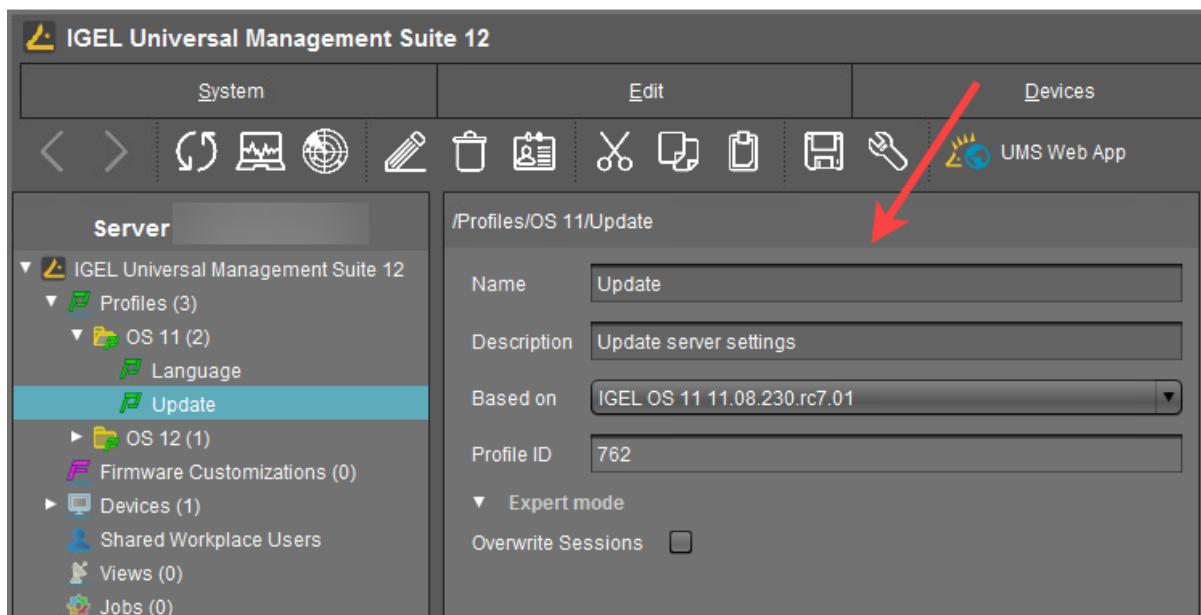
How to Edit Description Data of a Profile

Description data consist of the name of the profile, a descriptive text, the firmware version this profile is based on, and the overwrite flag for sessions.

To edit these settings:

1. Under **Profiles**, select the required profile.
2. Change the settings according to your needs.

i When changing the firmware version under **Based on**, remember that profile settings will be lost if they are not supported in the new firmware.



3. To save the changes, click or **Edit > Save description**.

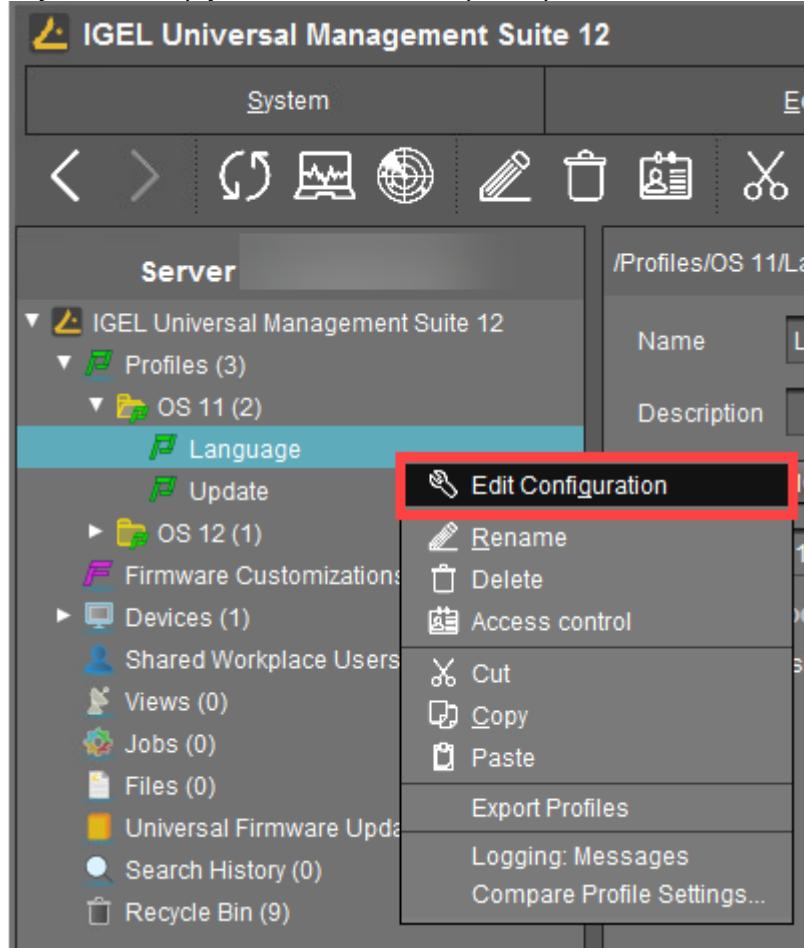
The data are now updated in the database.

How to Edit the Profile Configuration

To edit the profile configuration, proceed as follows:

- Under **Profiles**, select the required profile and click [**context menu**] > **Edit Configuration** or **Edit** > **Edit Configuration**.

Or you can simply double-click the required profile.



The configuration dialog 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 is used.
- 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.
	Reset to the default value.
The following activation symbols are only displayed if template profiles are activated (see Template Profiles in the IGEL UMS (see page 256)):	
	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.

3. Save the changes.

4. Determine when the changes should take effect – immediately or at the next reboot of the device.

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.

- i** 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

In the IGEL Universal Management Suite (UMS), 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 \(see page 312\)](#).

- ⓘ In the UMS Console, only OS 11 profiles can be exported or imported. If you need to export / import OS 12 profiles, see Exporting and Importing Profiles in the IGEL UMS Web App.

- [Exporting a Profile and Firmware \(see page 232\)](#)
- [Importing a Profile and Firmware \(see page 233\)](#)

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.

i 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 \(see page 234\)](#)

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 Profiles in the IGEL UMS

In the IGEL Universal Management Suite (UMS), you can copy a profile and paste it into any profile directory.

- ⓘ Copying and pasting are also possible between standard profile directories and priority profile directories. If you copy a standard profile and paste it into a priority profile directory, the copy of the standard profile will be defined as a priority profile. If you copy a priority profile and paste it into a standard profile directory, the copy will be defined as a standard profile. Information regarding priority profiles can be found under [Priority Profiles in the IGEL UMS](#) (see page 253).

Menu path: **UMS Console > Profiles**

- ⓘ It is currently not possible to copy IGEL OS 12 profiles.

To copy a profile, proceed as follows:

1. In the **UMS Console > Profiles**, 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 into 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 Directories in the IGEL UMS

In the IGEL Universal Management Suite (UMS), you can copy a profile directory and paste it into any directory.

- i** Copying and pasting are also possible between standard profile directories and priority profile directories. If you copy a standard profile directory and paste it into a priority profile directory, the copies of the standard profiles will be defined as priority profiles. If you copy a priority profile directory and paste it into a standard profile directory, the copies of the priority profiles will be defined as standard profiles. Information regarding priority profiles can be found under [Priority Profiles in the IGEL UMS \(see page 253\)](#).

Menu path: **UMS Console > Profiles**

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.

Name	Session Name "Bootlogo"	Value "Bootlogo"	Status	Session Name "Wallpaper"	Value "Wallpaper"
system.customization....		true	only in profile "Bootlogo"		
system.customization....		Admin	only in profile "Bootlogo"		
system.customization....		false	only in profile "Bootlogo"		
userinterface.languag...		English	equal		English
system.customization....		ums_filetransfer/MyPic...	only in profile "Bootlogo"		
system.customization....		igelstart.jpg	only in profile "Bootlogo"		
system.customization....		0007433305240b2101	only in profile "Bootlogo"		
system.customization....		9080	only in profile "Bootlogo"		
system.customization....		172.30.91.90	only in profile "Bootlogo"		
system.customization....		HTTP	only in profile "Bootlogo"		
userinterface.keyboar...		English(US)	changed		French
windowmanager.cust...			only in profile "Wallpaper"		Admin
windowmanager.cust...			only in profile "Wallpaper"		ums_filetransfer/MyPic...
windowmanager.cust...			only in profile "Wallpaper"		172.30.91.90
windowmanager.cust...			only in profile "Wallpaper"		true
windowmanager.cust...			only in profile "Wallpaper"		9080
windowmanager.cust...			only in profile "Wallpaper"		HTTP
windowmanager.cust...			only in profile "Wallpaper"		0007433305240b2101
windowmanager.cust...			only in profile "Wallpaper"		Wallpaper

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 in the IGEL UMS

In the IGEL Universal Management Suite (UMS), 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 IGEL 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 \(see page 243\)](#).

The procedure for setting up and configuring profiles is described in [Use profiles \(see page 213\)](#). 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.



Lowest Priority



Highest Priority

- [Order of Effectiveness of Profiles \(see page 240\)](#)
- [Order of Effectiveness of Profiles in IGEL Shared Workplace \(see page 243\)](#)
- [Order of Effectiveness of Priority Profiles \(see page 244\)](#)
- [Order of Effectiveness of All Profiles \(see page 250\)](#)
- [Summary - Prioritization of IGEL UMS Profiles \(see page 251\)](#)

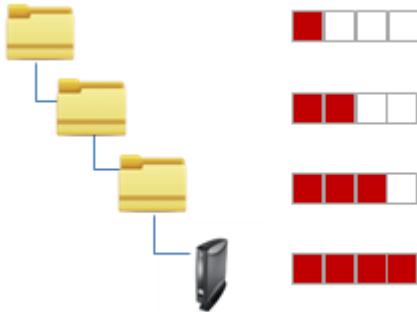
Order of Effectiveness of Profiles

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?

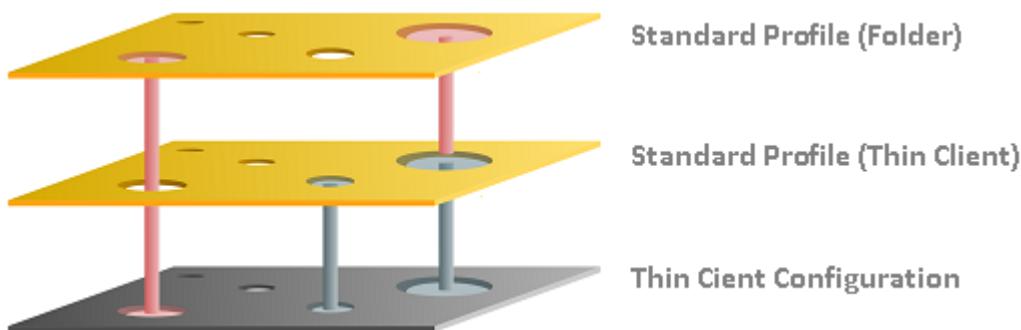
- ❗ Avoid competing settings in a number of profiles. If possible, set up one profile per setting, e.g. a profile for language settings, one for a left-handed mouse, etc.

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 242).

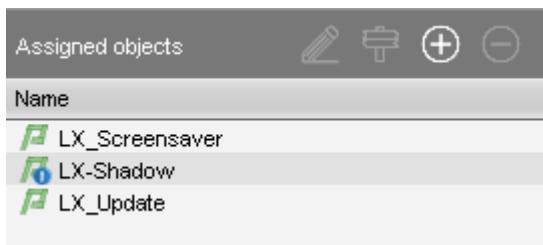
Rule: If several profiles are assigned on an equal basis, the newer profile with the higher profile ID has priority.

-  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.

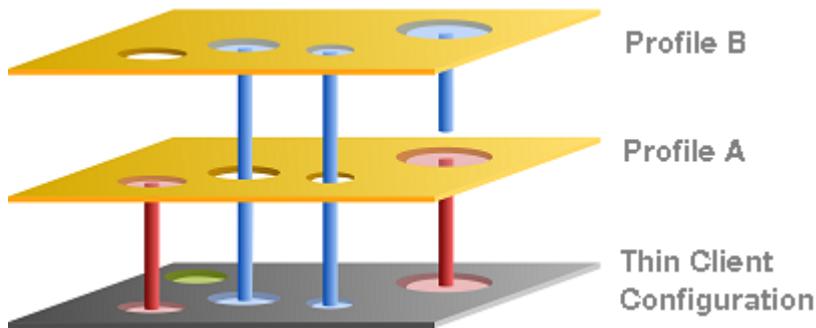
In this example, the "screen saver" profile has the highest priority.



Name
LX_Screensaver
LX_Shadow
LX_Update

Example – Standard Profiles

In the IGEL Universal Management Suite (UMS), 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 IGEL Shared Workplace

In IGEL Shared Workplace, you can use profiles to configure user settings. For further information, see the guide [IGEL Shared Workplace - Assigning a User Profile](#).

Template profiles and template keys (see page 256) 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 priority 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

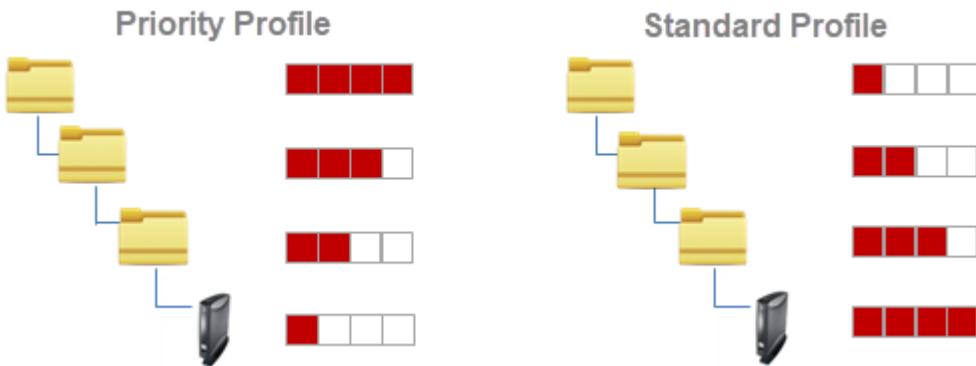
Rule: Profiles that are assigned to an object are prioritized in descending order according to profile ID (highest ID = highest priority).

Rule: Groups within a level are prioritized in alphabetical order.

Order of Effectiveness of Priority Profiles

Priority profiles allow more flexible access rights within the IGEL Universal Management Suite (UMS) as they can override the settings for standard profiles and have their own authorizations.

Priority 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:

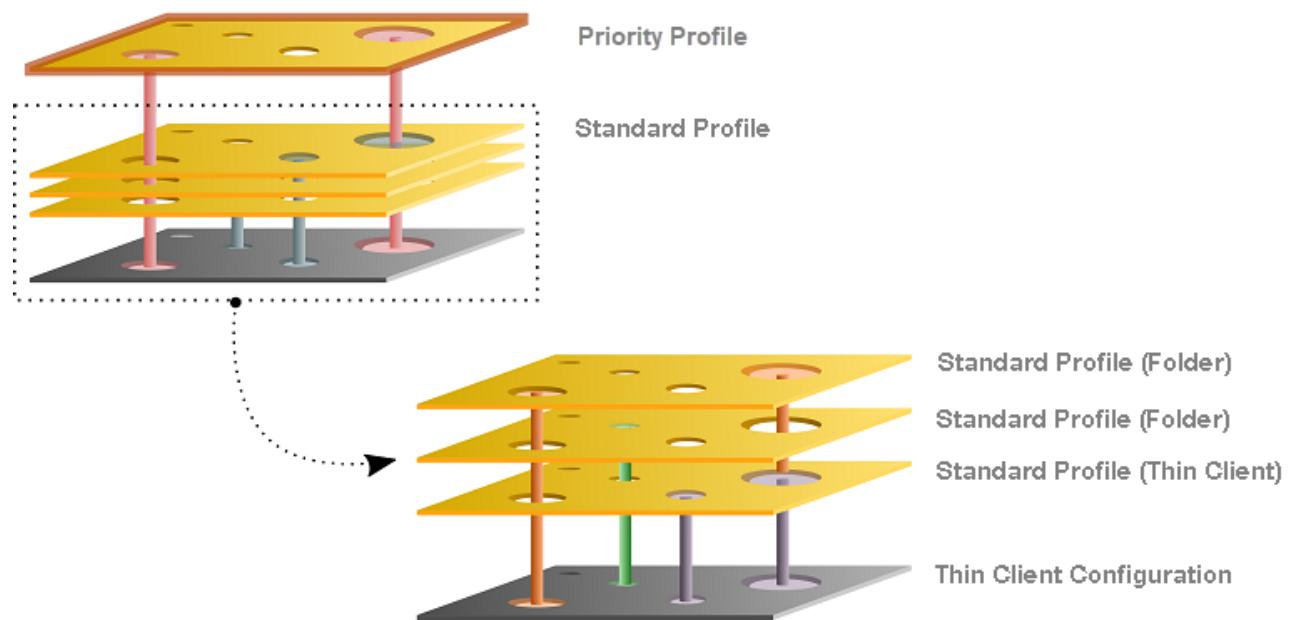


The following applies to priority profiles:

Higher priority	than...
further away from the device	closer to the device
higher-level directory	sub-directory

Rule: Priority profiles override all standard profiles.

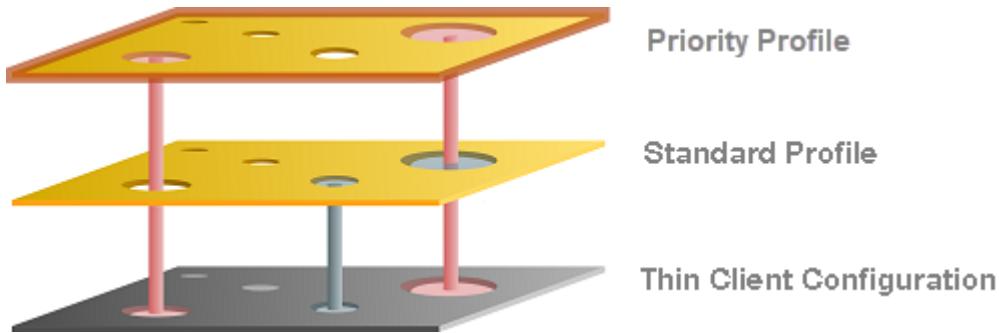
The following graphic shows that the priority profile setting overrides that of the standard profiles if the same parameter is pre-populated. Settings that are not double-populated are effective without restriction.



- Example – Priority Profiles (see page 246)
- Example – Priority and Various Standard Profiles (see page 247)
- Priority Profiles in IGEL Shared Workplace (see page 248)

Example – Priority Profiles

In the IGEL Universal Management Suite (UMS), we will create a standard profile and a priority profile which we assign to a device.



- **Standard profile:** You assign to the device a standard profile in which (gray) the language and the keyboard layout are set to German.
- **Priority profile:** You assign to a higher-level directory a priority profile. This specifies the background image and the language is set to English (red).

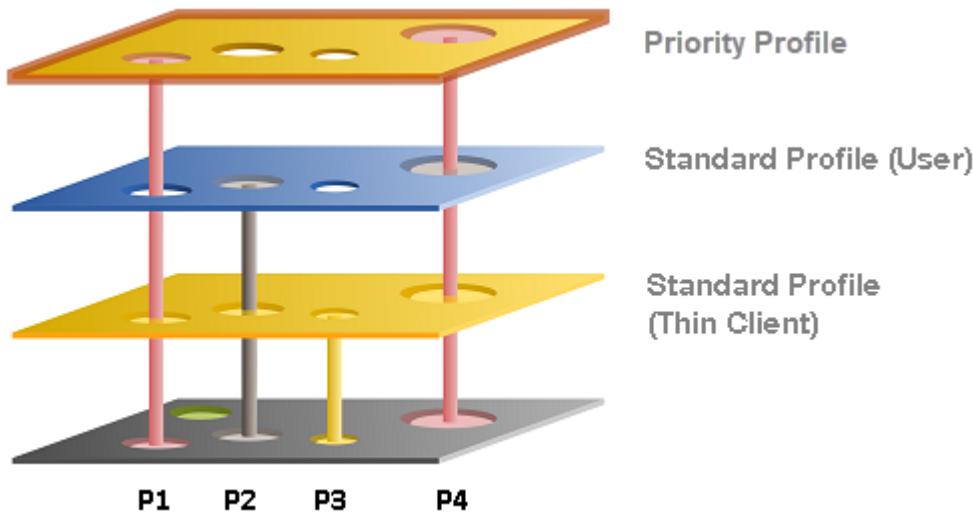
The settings that arrive at the device are:

- Gray: Keyboard German (standard profile)
- Red: Background image and language setting English (priority profile)

The "German" language setting from the standard profile has no effect on the device because the priority profile has set the language parameter to English. If the parameter settings are the same, the priority profile overwrites the values of standard profiles.

Example – Priority and Various Standard Profiles

In the IGEL Universal Management Suite (UMS), we will create a priority 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.
- **Priority profile:** You assign to a higher-level directory a priority 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 device are:

- Yellow: (**P3**) Keyboard layout German (standard profile device)
- Grey: (**P2**) Right-handed mouse (standard profile user)
- Red: (**P4, P1**) Medium mouse speed and double-click interval (priority profile)

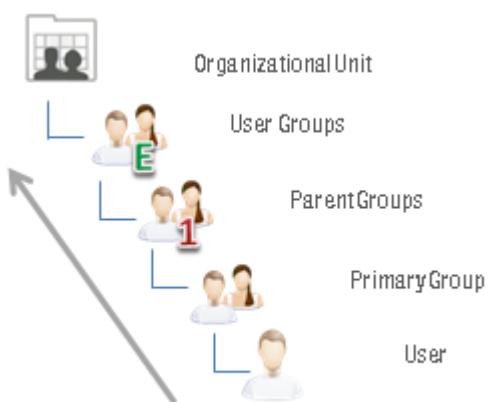
Priority Profiles in IGEL Shared Workplace

Profiles assigned to users have a higher priority than profiles assigned to devices. In the case of the priority profiles, the relevant group rather than the individual device or user is prioritized. This means:

Rule: Priority profiles assigned to user groups have a higher priority than those assigned to individual users. These have higher priority than priority profiles assigned to device directories. Priority profiles assigned to an individual device have the lowest priority.

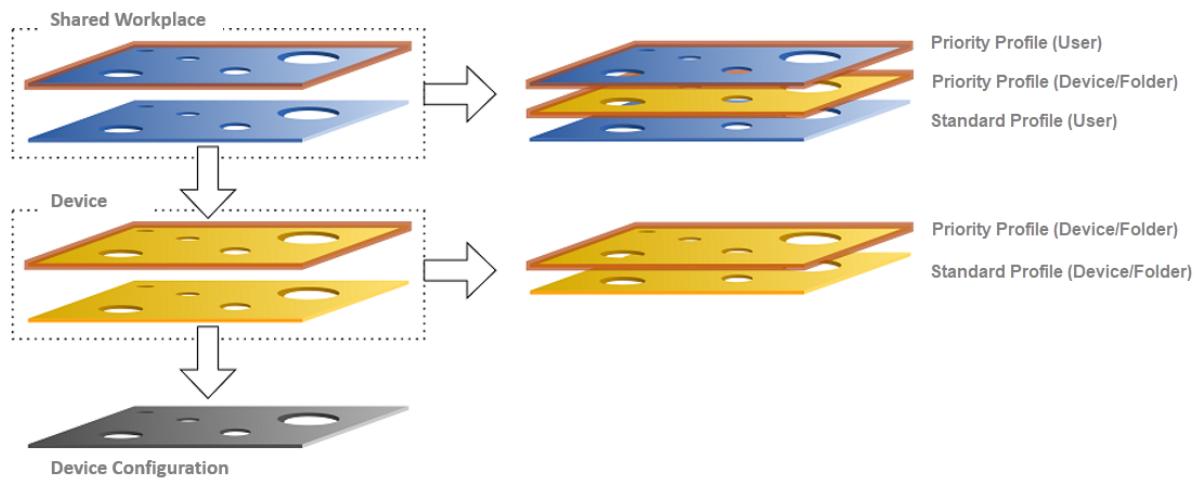


Higher priority	than...
user-specific profiles	device-specific profiles
further away from the user/device	closer to the user/device



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 priority 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 - Prioritization of IGEL UMS Profiles

The following overview summarizes all rules relating to the priority of profiles in the IGEL Universal Management Suite (UMS):

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 \(see page 242\)](#).
- 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 \(see page 211\)](#) 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

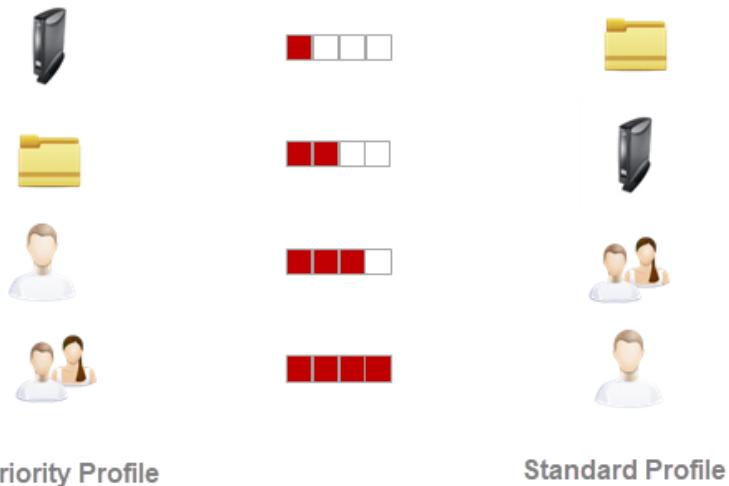
- The closer the standard profile is to the device, the higher its priority.

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 - Priority profiles

- Priority profiles override all standard profiles.
- Settings in priority profiles can only be overwritten by priority profiles.
- Priority profiles are prioritized the other way around compared to the standard profiles.
- Priority profiles which are closer to the object have lower priority.
- Priority profiles assigned to user groups have a higher priority than those assigned to individual users. These have higher priority than priority profiles assigned to device directories. Priority profiles assigned to an individual device have the lowest priority.



For information on the prioritization of firmware customizations, see [Firmware Customizations in the IGEL UMS \(see page 274\)](#).

For information on the prioritization of Universal Firmware Updates, see [Precedence of IGEL UMS Profiles and Universal Firmware Updates](#).

Priority Profiles in the IGEL UMS

In the IGEL Universal Management Suite (UMS), you can create priority profiles (formerly called "master profiles").

The aim of priority 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 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.

Menu path: **UMS Console > Priority Profiles**

Most Important Features of Priority Profiles

- Priority profiles are identical to standard profiles in terms of their effects but are prioritized differently. For more information, see [Order of Effectiveness of priority Profiles](#) (see page 244).
- Priority profiles are profiles whose settings override all standard profiles.
- Priority profiles cannot be overwritten by standard profiles.
- Priority profiles have their own section in the UMS structure tree. However, they have to be first enabled; see the instructions below.

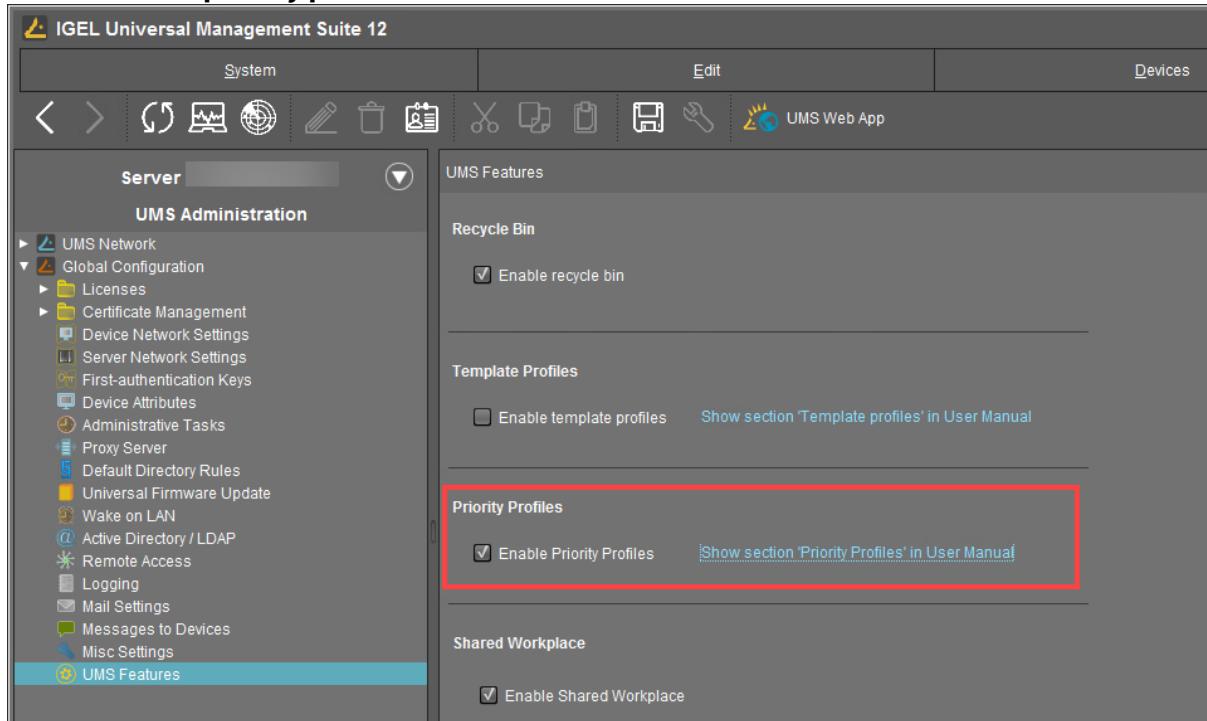
How to Enable Priority Profiles

By default, the **priority profiles** function is disabled. If you want to use priority profiles, proceed as follows.

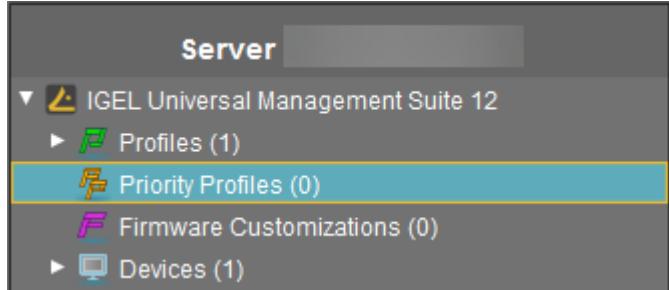
Through the UMS Console

1. In the UMS Console, select **UMS Administration > Global Configuration > UMS Features**.

2. Activate **Enable priority profiles**.



The node **Priority Profiles** appears in the structure tree. You can now create priority profiles: the procedure is identical to the creation of standard profiles, see [Creating Profiles in the IGEL UMS \(see page 214\)](#).



Through the UMS Web App

1. In the UMS Web App, go to the **Network > Settings** area.
2. Go to the **UMS Features** tab.
3. Activate **Enable priority profiles**.

For more information, see Network Settings in the IGEL UMS Web App.

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=FZFPpdSe0lM>

Template Profiles in the IGEL UMS

In the IGEL Universal Management Suite (UMS), you can use template profiles. Template profiles have to be first enabled under **UMS Administration > Global Configuration > UMS Features**, see [Activating Template Profiles in the IGEL UMS](#) (see page 258).

Menu path: **UMS Console > Template Profiles**

A **template profile** allows you to add variables for individual parameters in the profile and to assign their values to objects.

- i Both **standard profiles** and **priority 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 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

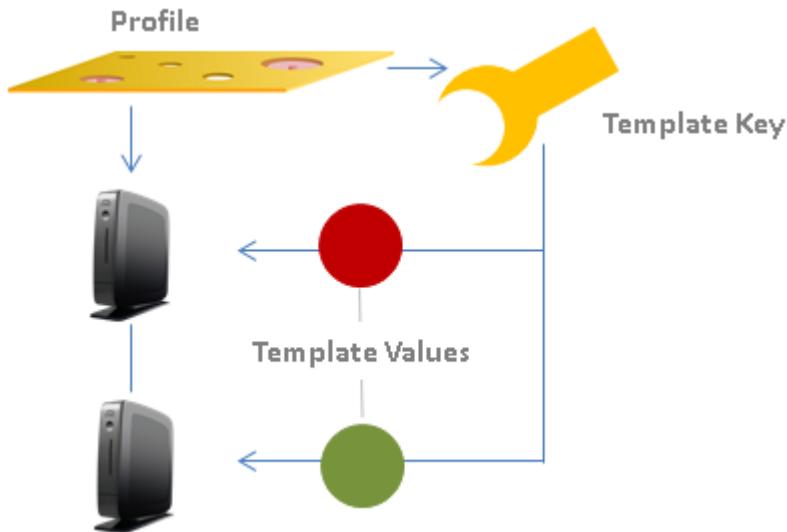
In many cases, the desired settings cannot be combined via various profiles, see [free instances](#) (see page 211). The unnecessarily large number of profiles is also difficult to manage in the long term.

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 260). 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 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=uJnIK5u688c>

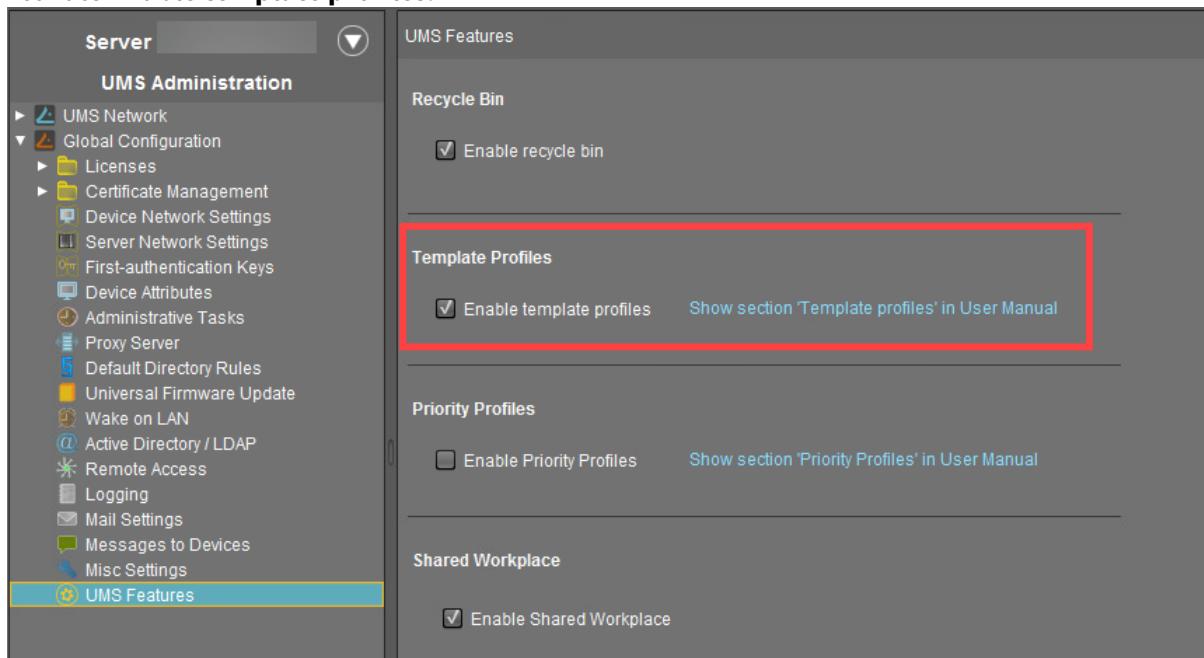
- Activating Template Profiles in the IGEL UMS (see page 258)
- Creating Template Keys and Values (see page 260)
- Using Template Keys in Profiles (see page 266)
- Assigning Template Profiles and Values to the Devices (see page 268)
- Value Groups (see page 270)
- Export Template Keys and Value Groups (see page 272)
- Import Template Keys and Value Groups (see page 273)

Activating Template Profiles in the IGEL UMS

If you would like to use the template profiles function in the IGEL Universal Management Suite (UMS), you must enable it first through the UMS Console or the IGEL UMS Web App.

Activating Template Profiles through UMS Console

1. In the UMS Console, go to **UMS Administration > Global Configuration > UMS Features**.
2. Activate **Enable template profiles**.



The **Template Keys and Groups** node appears in the UMS structure tree.



Activating Template Profiles through UMS Web App

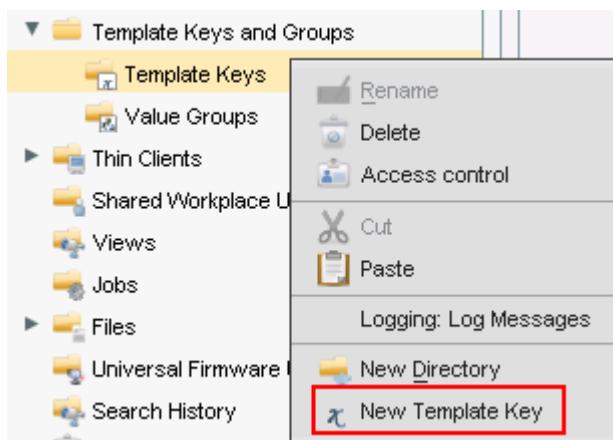
1. In the UMS Web App, go to the **Network > Settings** area.
2. Go to the **UMS Features** tab.
3. Activate **Enable template profiles**.

For more information, see Network Settings in the IGEL UMS Web App.

Creating Template Keys and Values

To create template keys and values, proceed as follows:

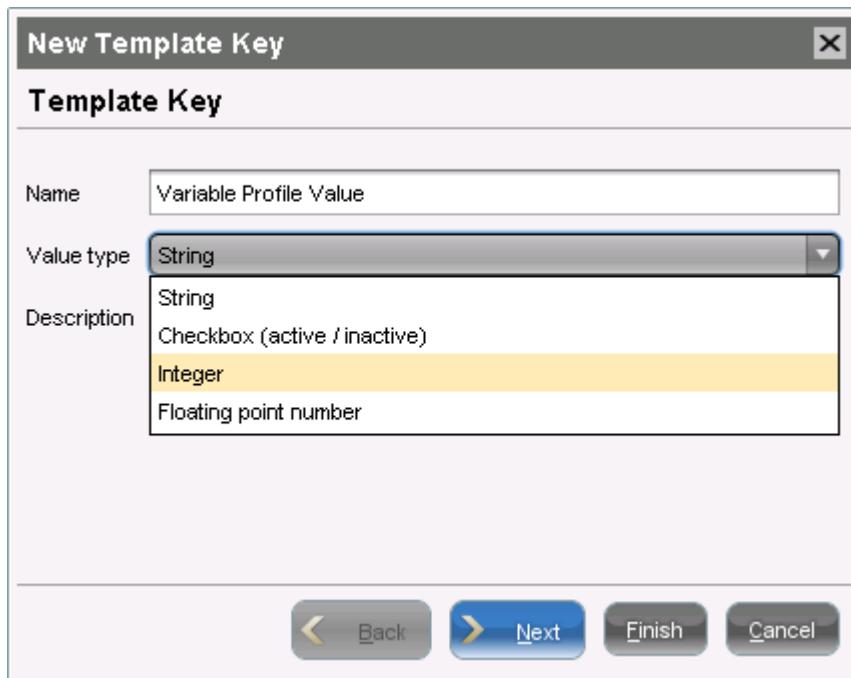
1. Open the context menu for the **Template Keys** folder.
2. Click on **New Template Key**.



 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**.

New Template Key

Create Values

Template Key Name Variable Profile Value

Specified Values

Value	Description

New Value

Value Value-1

Description First value of the key

Create Value

Back Next Finish Cancel



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.

New Template Key

Create Values

Template Key Name	Variable Profile Value
-------------------	------------------------

Specified Values

Value	Description
↳ Value-1	First value of the key
↳ Value-2	Second value of the key
↳ Value-3	Third value of the key

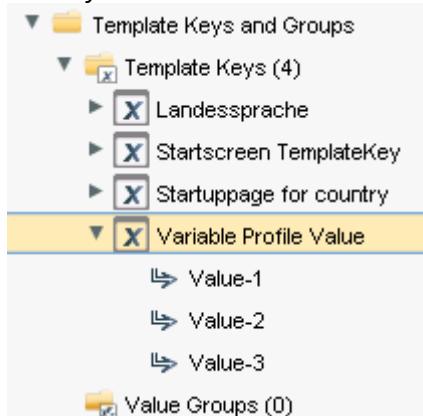
New Value

Value	Value-3
Description	Third value of the key

Create Value

Back Next Finish Cancel

The key with its values will be shown in the tree:



- i** The recommended workflow is to create template keys and values from the [profile configuration](#) (see page 264).

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.

- i** 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**
6. Click on **Add**
- An assistant will guide you through the steps for creating a new template key:
7. Give a **name** for the key.

- i** The **value type** for the key is stipulated by the parameter.

8. Optionally, give a **description** of the key.

Template Key	
Name	New Key
Value type	String
Description	optional

9. Click on **Next**.

To enter the first value of the key, proceed as follows:

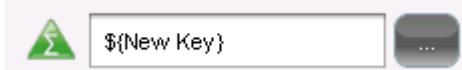
1. Define the desired parameter value in the **Value** field.
2. Optionally, add a **description** of the value.
3. Click on **Create Value**.

i 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.

New Value	
Value	<input type="text"/>
Description	<input type="text"/> Create Value
<input type="button" value="Back"/> <input type="button" value="Next"/> <input type="button" value="Finish"/> <input type="button" value="Cancel"/>	

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: .

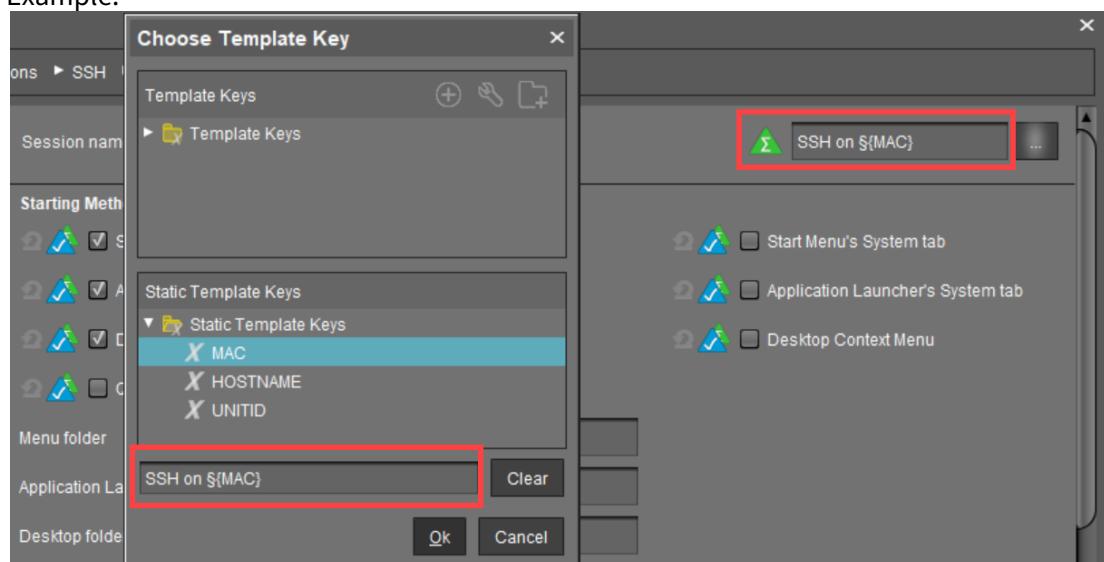
Using Template Keys in Profiles

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.

- i** These and other icons and their meanings can be found under **UMS Console > Help > Legend**.

- i** 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 264).
7. Click on **OK**.
8. **Save** the template profile.
9. You can also combine template keys:

Global home page 

`www.${Domain}${Country}`



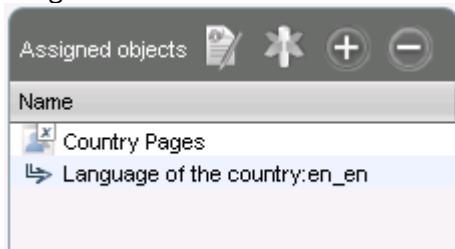
Profiles which use at least one template key in the configuration are labeled with a special symbol in the structure tree: .

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).

i 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:

Check the template definitions				
Thin Client	Profile	Template Expression	Description	
Doku-1-LX (00E0C53627...)	Template Profile	\$(New key)	Missing value for template key "New key"	
Prod-1 (00E0C5111111)	Template Profile	\$(New key)	Missing value for template key "New key"	
Prod-2 (00E0C5222222)	Template Profile	\$(New key)	Missing value for template key "New key"	
Prod-0 (00E0C5000000)	Template Profile	\$(New key)	Missing value for template key "New key"	

Or click on a device and the results of the check will be shown immediately:

A blue computer monitor icon with an orange exclamation mark inside a circle.

Missing Template Values

▶ **System Information**

▼ **Template Definition Check Results**

Severity	Profile	Template Expression	Description
Error	Browser	www.\${Domain}\${(C...	Missing value for te...
Information	Browser	www.\${Domain}\${(C...	value for template ke...

▶ **Monitor Information**

▶ **Features**

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.

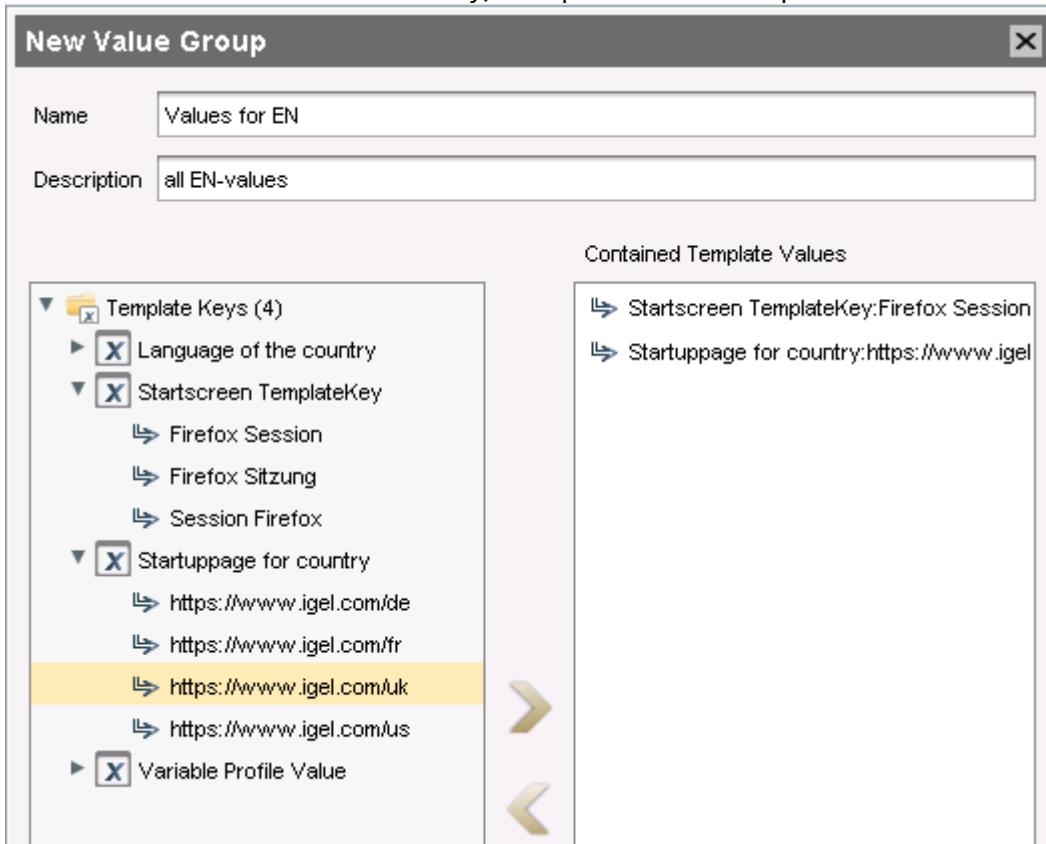
Value Groups

In value groups, logically associated values from various template keys can be brought together and assigned together to devices.

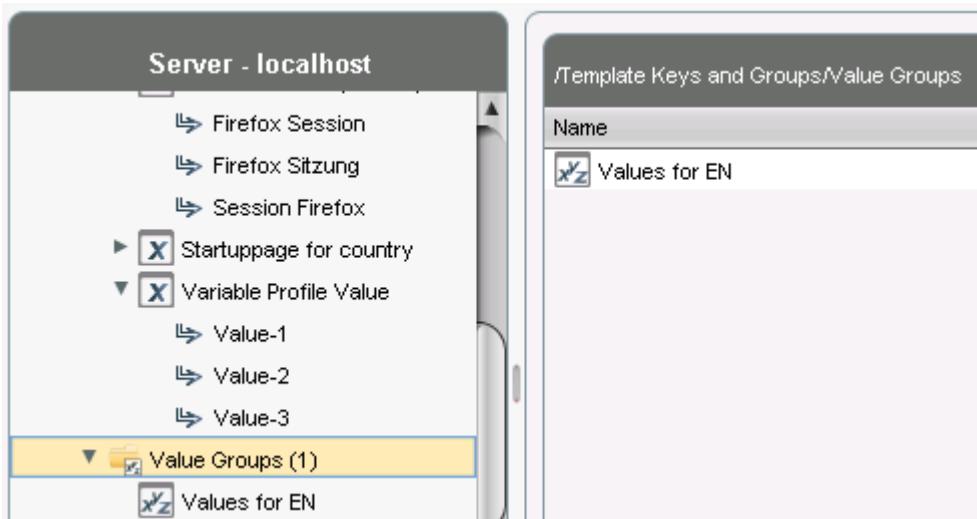
If for example you have various profiles which are to receive country-specific settings via template keys and value assignments, all values for a country / a language can be grouped in a value group. When such a group is assigned, a device also receives all values for its country / its language contained 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.

- i** 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.

i 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 rousp.**
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.

Firmware Customizations in the IGEL UMS

You can customize the user interface of your IGEL OS devices to suit your corporate design using the firmware customization function in the IGEL Universal Management Suite (UMS). The configuration takes place in a dedicated wizard; for a minimal configuration, only a name and a file object need to be specified.

Menu path: **UMS Console > Firmware Customizations**

Mode of Action

A firmware customization can be assigned to a device or a directory.

Firmware customizations override standard profiles but in turn can be overridden by priority profiles. They are therefore between priority profiles and standard profiles in terms of their priority. Further information regarding the prioritization of profiles can be found under [Prioritization of Profiles in the IGEL UMS \(see page 239\)](#).

If several use 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 device directory. 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 \(see page 275\)](#)
- [Export Firmware Customizations \(see page 284\)](#)
- [Import Firmware Customizations \(see page 285\)](#)

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 276)
 - [Start Menu](#) (see page 277)
 - [Taskbar Background](#) (see page 278)
 - [Screensaver](#) (see page 279)
 - [Screensaver \(Custom Partition\)](#) (see page 280)
 - [Bootsplash](#) (see page 282)
 - [Background Image](#) (see page 283)
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 you 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 you 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 you 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 you 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 you 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.
 - **Remove file:** 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 you 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 you 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 endpoint 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 converted with the IGEL UDC/OSC, and devices with the IGEL UMA, the unit ID is set to 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 OS Device

The following icons in the structure tree show the status of an IGEL OS 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).

To enable the following status displays, the **Devices send updates** option under **UMS Administration > Global Configuration > Device Network Settings > Advanced Device's Status Updates** must be enabled (default).



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.

These and more icons and their meanings can be found under **UMS Console > Help > Legend**.

For status displays used in the IGEL UMS Web App, see Devices - View and Manage Your Endpoint Devices in the IGEL UMS Web App.

Device Commands

You can send a command to a device via the context menu (i.e. by right-clicking on a single device or a device directory) or via **Menu bar > Devices** (see page 185).

- [View Device Information in the IGEL UMS](#) (see page 288)
- [Managing Devices](#) (see page 295)
- [Configuring Devices](#) (see page 303)
- [Exporting and Importing Data](#) (see page 306)
- [Send Message](#) (see page 313)
- [Secure Terminal \(Secure Shell\)](#) (see page 316)
- [Shadowing - Observe IGEL OS Desktop via VNC](#) (see page 320)

View Device Information in the IGEL UMS

By selecting the corresponding endpoint device in the **Devices** area of the IGEL Universal Management Suite (UMS), you can view the up-to-date device information, e.g. the Unit ID, MAC address of the device, details on the available licenses, information on connected monitors, user login history, etc.

For information on device management in the IGEL UMS Web App, see [Devices - View and Manage Your Endpoint Devices in the IGEL UMS Web App](#).

Menu path: **Devices > [Directories] > [Name of the device]**

The screenshot shows the IGEL UMS interface. On the left, there is a navigation tree under the heading "Server". The tree includes categories like "IGEL Universal Management Suite 6", "Profiles (20)", "Master Profiles (2)", "Template Keys and Groups (2)", "Firmware Customizations (1)", and "Devices (2)". Under "Devices", there are "Augsburg (2)" and "techdoc (2)", which contains "RD (2)" and "TD-RD01". The node "TD-RD01" is expanded, showing its sub-node "TD-RD03". On the right, the main pane displays the path "/Devices/Augsburg/techdoc/RD/TD-RD03" and the device name "TD-RD03" with a monitor icon. Below the device name is a list of detailed information items: "Template Definition Check Results", "Monitor Information", "Asset Inventory", "Features", "Windows Updates and Hotfixes", "Partial updates", "File Transfer status", and "User Login History". At the bottom right of the main pane, there is a button labeled "Copy to Clipboard (ASCII)".

For details on icons for an IGEL OS device, see [Devices](#) (see page 286).

- ▶ Click on the triangle symbols to expand or collapse hierarchy levels.
- ▶ Click **Copy to Clipboard (ASCII)** to copy the device information in ASCII format.

The following details regarding the selected device are shown:

System Information

- **Name**
- **Site**
- **Comment**
- **Department**
- **Cost center**
- **Asset ID**
- **In-service date**
- **Serial number**
- **[custom attributes]**: The attributes added under **UMS Administration > Global Configuration > Device Attributes** are shown. For details, see [Managing Device Attributes for IGEL OS Devices](#) (see page 432).

Advanced System Information

- **Unit ID**
- **MAC address**
- **Last IP**
- **Product**
- **Product ID**
- **Version**: Version of the operating system
- **Firmware description**
- **Connected to**: Shows for an IGEL OS 12 device to which device connector it is connected.
- **IGEL Cloud Gateway**
- **Expiration date of OS 10 maintenance subscription**
- **Last contact**: The time of the last contact between the device and the UMS. See here also Monitoring Device Health and Searching for Lost Devices.
- **Last boot time**
- **Network name (at boot time)**
- **Runtime since last boot**
- **Total operating time**
- **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**
- **Flash size (MB)**: Size of the flash memory (MB)
- **Memory size (MB)**
- **Network speed**
- **Duplex mode**
- **Graphic chipset 1**
- **Graphics memory 1 (MB)**
- **Graphic chipset 2**

- **Graphics memory 2 (MB)**
- **Device type**
- **OS type:** Operating system type
- **BIOS vendor**
- **BIOS version**
- **BIOS date**
- **Boot mode**
- **Device serial number**
- **Structure tag.** For details on structure tags, see Using Structure Tags with IGEL OS 11 Devices.

Network Adapters

In this area, all available network adapters of a device are listed. This information is provided as of IGEL OS 11.07.100.

The following information regarding network adapters is shown:

- **Type:** Type of the network adapter
- **MAC:** MAC address of the network adapter
- **Name:** Name of the corresponding network interface
- **State:** State of the network adapter as sent by the endpoint device, for example: **down, up** (the network adapter is connected to a network, not necessarily the same network as the UMS).

▼ Network Adapters			
Type	MAC	Name	State
Ian	00E0C520986A	enp1s0	up
wlan	147590F9731F	wlan0	down

ⓘ Read Out Network Adapter Data via API

You can read out network adapter information via a REST interface. For details, see Device in the IMI API V3 Reference.

License Information

In this area, the licenses available for the device are listed.

▼ License Information	
License Information	
Workspace Edition Maintenance	Licensed until Apr 15, 2023
Enterprise Management Pack	Licensed until Apr 15, 2023
Workspace Edition Add-on 90meter	Unlicensed
Workspace Edition Add-on Ericom PowerTerm	Unlicensed

Template Definition Check Results

In this area, you see the results of the check if template profiles and values have been assigned correctly, see [Assigning Template Profiles and Values to the Devices](#) (see page 268). For general information on template profiles, see [Template Profiles in the IGEL UMS](#) (see page 256).

The following information is shown.

- **Severity**
- **Profile**
- **Template expression**
- **Description**

▼ Template Definition Check Results			
Severity	Profile	Template Expression	Description
● Error	Browser	https://www.igel.\${Language}	Missing value for template key ...
● Error	Browser	https:\\igel.\${Language}	Missing value for template key ...

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...

Asset Inventory

(i) 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 licenses 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.

The Asset Inventory Tracker can be activated or deactivated under **UMS Administration > Global Configuration > UMS Features > Enable inventory tracking**.

- ▼ Asset Inventory
 - ▶ Keyboard
 - ▶ Mouse
 - ▼ other
 - ▼ MT7610U ("Archer T2U" 2.4G+5G WLAN Adapter

Attribute	Value
Name	MT7610U ("Archer T2U" 2.4G+5...
Connector	usb
Vendor	Ralink Technology, Corp.
Device id	761a
custom_productName	WiFi
custom_vendorName	MediaTek
revision	0100
serialID	MediaTek_WiFi_1.0
usbPort	3-2

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.

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 applies only for Windows devices, not IGEL OS devices, and is available from IGEL Universal Desktop W7 Version 3.12.100.

The following information regarding partial updates is shown.

- **Name**
- **Version**
- **Date**
- **Description**

File Transfer Status

As of 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 firmware customizations).

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.

File Transfer status					
Filename	File ID	Classification	Status	Status Message	Assigned via
background.png	13287	Start menu Image	Ok		Wallpaper

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 (see page 510) > Enable user logon history** checkbox

If logging is enabled, the following information is saved and displayed:

- **User name**
Name of the user who logged in to the device
- **Login time**
Time at which the user logged in
- **Logout time**
Time at which the user logged off

- **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.

- [Creating a Directory in the IGEL UMS](#) (see page 296)
- [Copying a Device Directory](#) (see page 298)
- [Importing a Directory](#) (see page 299)
- [Deleting a Directory](#) (see page 300)
- [Moving Devices](#) (see page 301)
- [Assigning Updates](#) (see page 302)

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 207) 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](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.

- (i) 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.

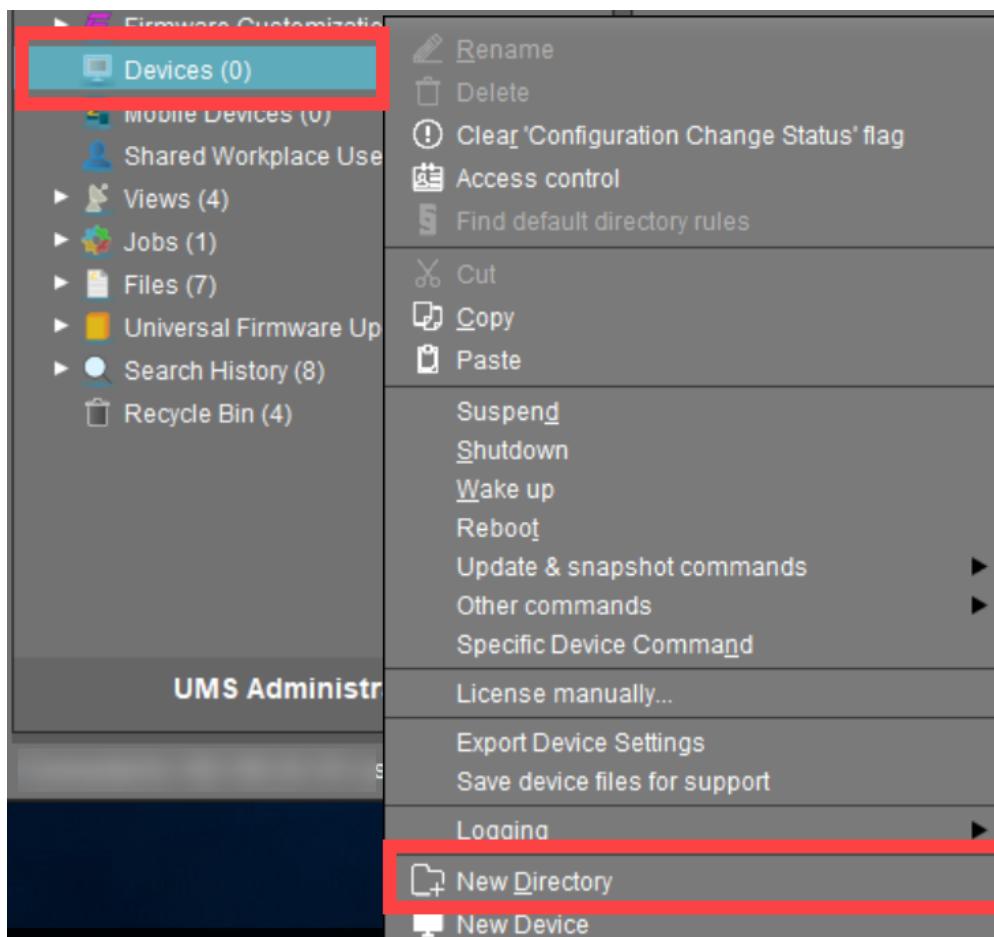
Alternatively, you can import a directory structure, see [Importing a Directory \(see page 299\)](#).

For details on how to create a directory in the IGEL UMS Web App, see [Creating a Directory Structure in the IGEL UMS Web App](#).

Menu path: **UMS Console > Devices**

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.

For the created directory, you can also define default directory rules, see [Default Directory Rules](#) (see page 481).

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.

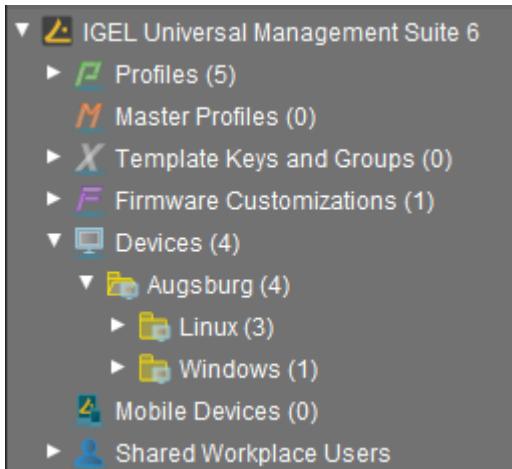
To copy a device directory, proceed as follows:

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.

For details on how to copy a directory in the IGEL UMS Web App, see [Copying a Device Directory in the IGEL UMS Web App](#).

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.

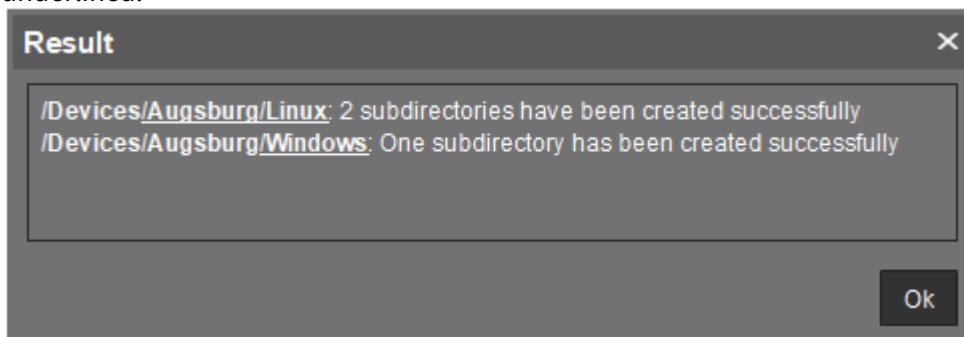


The tree structure shown above is based on the following file:

```
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.



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**.

For details about directory deletion in the IGEL UMS Web App, see Deleting a Directory in the IGEL UMS Web App.

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**.

For details on how to move devices in the IGEL UMS Web App, see Moving Devices in the IGEL UMS Web App.

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

i 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 [Job Configurations and Execution Results \(see page 359\)](#).
 - f. Assign the job to devices or directories, see [Assigning Objects to a Job \(see page 364\)](#).

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 \(see page 307\)](#)
- [Import Firmwares \(see page 308\)](#)
- [Export Device Settings in the IGEL UMS \(see page 309\)](#)
- [Import Devices as Profiles \(see page 312\)](#)

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 in the IGEL UMS

In the IGEL Universal Management Suite (UMS), you can export device settings. All changed settings are saved in the exported file, i.e. all settings which deviate from the default values, no matter if they are set via the UMS profiles or locally on the device.

Exporting device settings can be necessary for support purposes (see Exporting the Local Configuration of the IGEL OS Device) or if you want, for example, to import them later as a profile (see [Import Devices as Profiles \(see page 312\)](#)) and, by using the [compare profile settings \(see page 237\)](#) function, compare the existing configurations of one device with configurations of another device in order to find out the differences in settings.

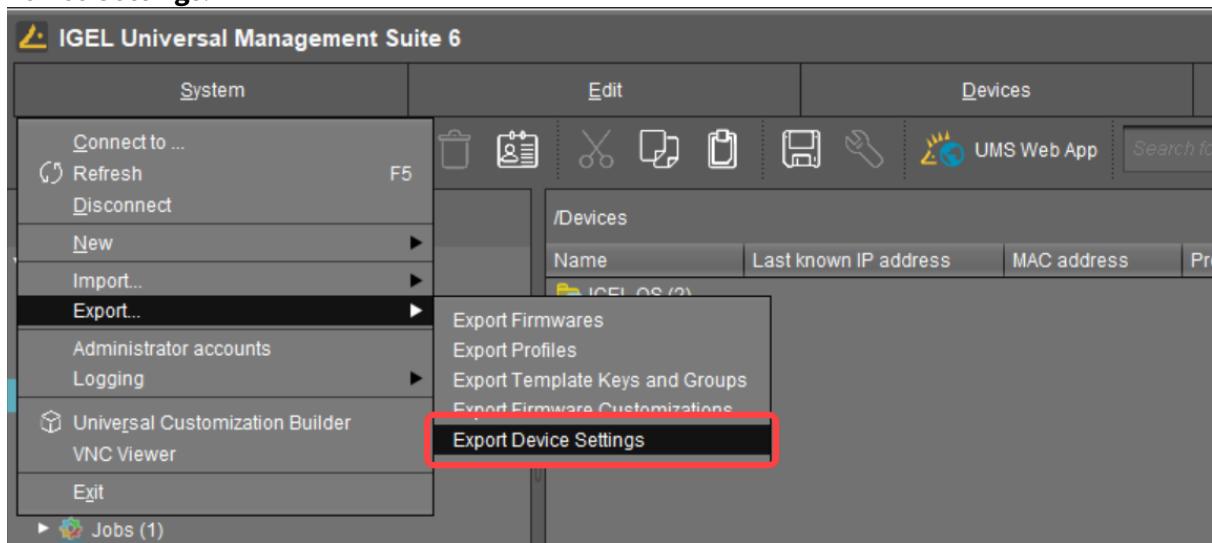
- ⓘ In the UMS Console, you can export the device settings for IGEL OS 11 devices only. If you need to export the settings of IGEL OS 12 devices, see [Exporting Device Settings as a Profile in the IGEL UMS Web App](#).

If you want to export / import purely profiles, see [Exporting and Importing Profiles \(see page 231\)](#).

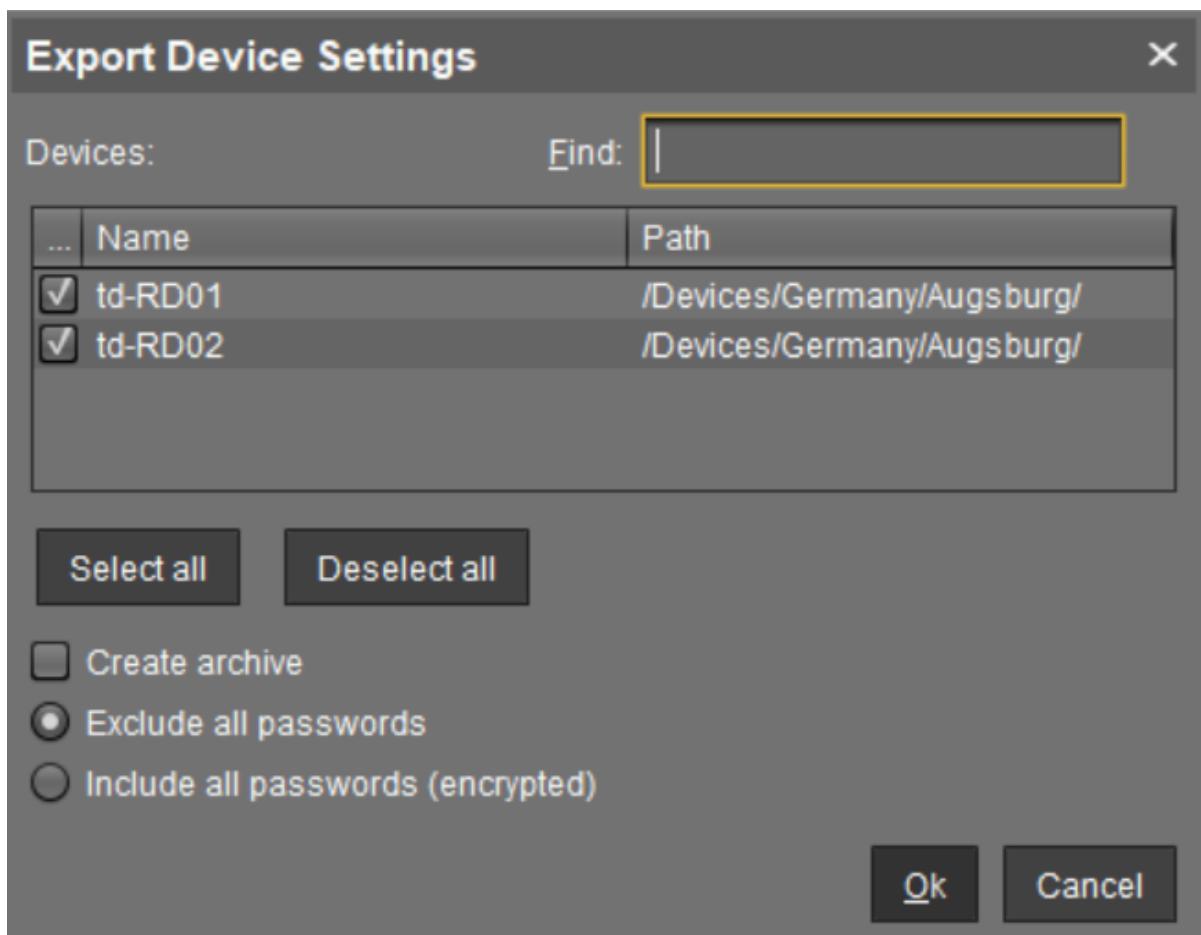
Menu path: **System > Export > Export Device Settings**

To export device settings, proceed as follows:

1. If you would like to preselect devices, highlight the desired devices or directories in the **UMS Console > Devices**.
2. Go to **System > Export > Export Device Settings** or **Devices > [device's context menu] > Export Device Settings**.



In the **Export Device Settings** window, the previously selected devices or all available devices will be displayed.



3. 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. In UMS 6.10.130 or higher, you can specify whether passwords should be exported:
 - **Exclude all passwords:** All passwords will be excluded, i.e. replaced with a placeholder in the exported file. (Default)
If you import the exported device settings later as a profile (see [Import Devices as Profiles \(see page 312\)](#)), no passwords will be included. You will have to set the passwords anew.
 - **Include all passwords (encrypted):** All passwords will be included in the exported file and encrypted.
If you import the exported device settings later as a profile, all passwords will be imported too and can further be used.

6. Click **OK** and select a save location.
7. Click **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 in the IGEL UMS](#) (see page 309).

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 Message

In the IGEL Universal Management Suite (UMS), you can send a message to any device. The message will be displayed to the user immediately. Messages to devices are enabled and configured under **UMS Administration > Global Configuration > Messages to Devices**; see [Messages to Devices \(see page 509\)](#).

Messages to IGEL OS 12 devices can also be sent via the UMS Web App, see [Sending a Message to Devices via the IGEL UMS Web App](#).

Menu path: **UMS Console > Devices > [Name of the device / device directory] > Other Commands > Send Message**

You can launch the editor via the context menu in the **Device** node or via the main menu under **Devices > Other Commands > Send Message**.

- i** Formatted messages are displayed on IGEL OS 11 devices. On IGEL OS 12 devices, messages will be automatically displayed without formatting since only plain text messages are currently supported.

Under **Select Template**, you can choose from various format templates. These include preset templates and those that you created under **UMS Administration > Global Configuration > Messages to Devices** (see page 509):

- {01 template: Info}: For informative texts, with an information symbol
- {02 template: Warning}: For warning texts, with an attention symbol
- {03 template: Error}: For error messages, with an error symbol
- {04 template: Custom Icon}: Freely configurable message with its own symbol (see below)
- {05 template: Alert}: Red alarm message, with an information symbol and a table with a moving bell symbol
- {06 template: Blue}: Blue message window, with an 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.

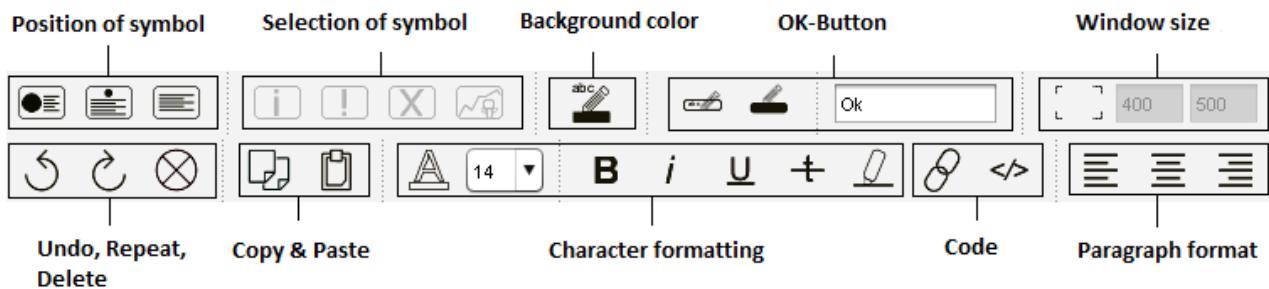
- i** In order to save templates, the user will need to write rights on the [Messages to Devices \(see page 509\)](#) node.

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.

- i 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**



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.

i 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](#)¹⁶.

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.

¹⁶ <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 - Observe IGEL OS Desktop via 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**.

- [Launching a VNC Session](#) (see page 321)
- [IGEL VNC Viewer](#) (see page 322)
- [External VNC Viewer](#) (see page 324)
- [Secure Shadowing \(VNC with SSL/TLS\)](#) (see page 325)

 For shadowing, **remote access** rights are required. See [Object-Related Access Rights](#) (see page 530).

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
- UMS user interface: The UMS Console and the UMS Web App have different VNC viewers.

For shadowing in the IGEL UMS Web App, see [Remote Access to Devices via Shadowing](#) in the IGEL UMS Web App.

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=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
- UMS user interface: The UMS Console and the UMS Web App have different VNC viewers.

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 <i>IGEL</i> 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: <ul style="list-style-type: none"> • 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
- UMS user interface: The UMS Console and the UMS Web App have different VNC viewers.

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)

In the IGEL Universal Management Suite (UMS), you can activate secure VNC for specific devices or globally for all devices.

Additional information on secure shadowing can be found under Secure Shadowing (VNC with TLS/SSL).

Menu path: **Setup > System > Remote Access > Shadow > Secure mode**

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.

How to Activate Secure Shadowing

To enable secure shadowing for specific devices:

1. In the configuration dialog or IGEL Setup, go under **System > Remote Access > Shadow** and activate **Allow remote shadowing**.
2. Enable **Secure mode** and save the settings.

To enable secure shadowing globally for all devices:

1. In the configuration dialog or IGEL Setup, go under **System > Remote Access > Shadow** and activate **Allow remote shadowing**.
2. In the UMS Console, go under **UMS Administration > Global Configuration > Remote Access** and activate **Enable secure VNC globally**. See [Remote Access](#) (see page 499).

 **Secure Shadowing and IGEL OS 12**

Shadowing of IGEL OS 12 devices through the UMS is always via Unified Protocol and therefore secure, i.e. communication is always encrypted. By default, shadowing over plain VNC protocol is denied. However, you can deactivate the **Deny shadowing via external VNC tool** option under **System > Remote Access > Shadow** if you want that the devices could be shadowed by the [external VNC viewer](#) (see page 324) via plain VNC protocol.

 **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
- UMS user interface: The UMS Console and the UMS Web App have different VNC viewers.

Shared Workplace Users

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.

- ❖ If you deactivate **Enable Shared Workplace** under **UMS Administration > Global Configuration > UMS Features**, the structure tree node **Shared Workplace Users** will be hidden and Shared Workplace users will NOT be able to log in!

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.

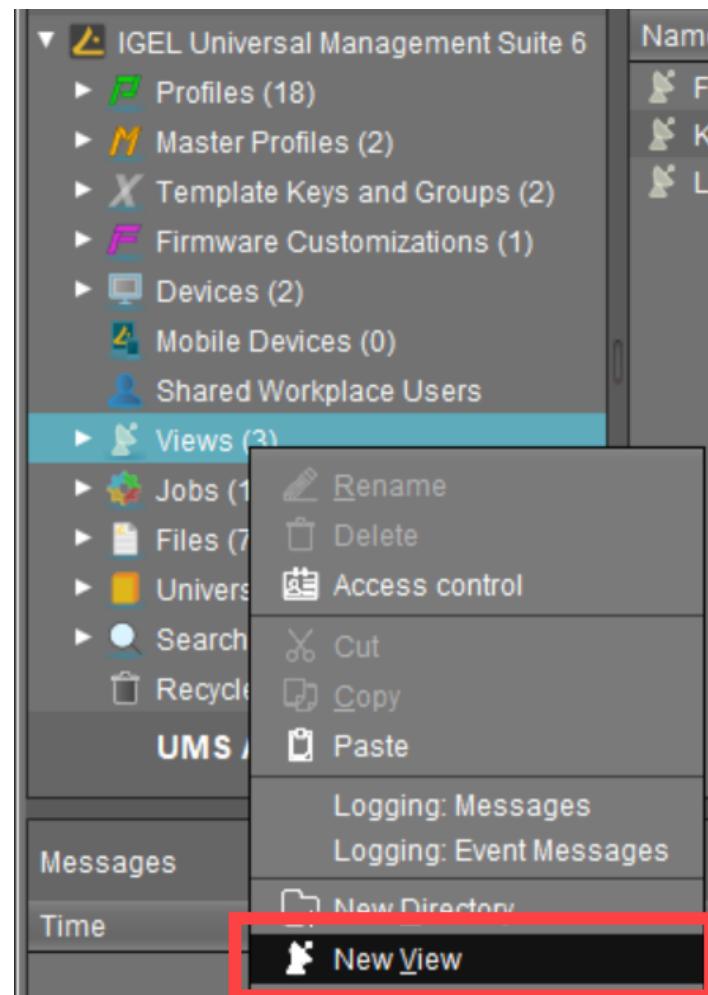
-
- How to Create a New View in the IGEL UMS (see page 329)
 - Copying a View (see page 350)
 - Copying a View Directory (see page 351)
 - Saving the View Results List (see page 352)
 - Sending a View as Mail (see page 353)
 - Assigning Objects to a View (see page 354)

How to Create a New View in the IGEL UMS

The following article details how to create a view in the IGEL Universal Management Suite (UMS). A view is a selection of devices according to definable criteria which are logically linked one after another, see [Views \(see page 328\)](#). You can create a view using a standard procedure or graphical / text expert mode.

For information on how you can configure the display of view results, see [Views and Searches \(see page 191\)](#).

Menu path: **Views > [Context Menu] > New View**

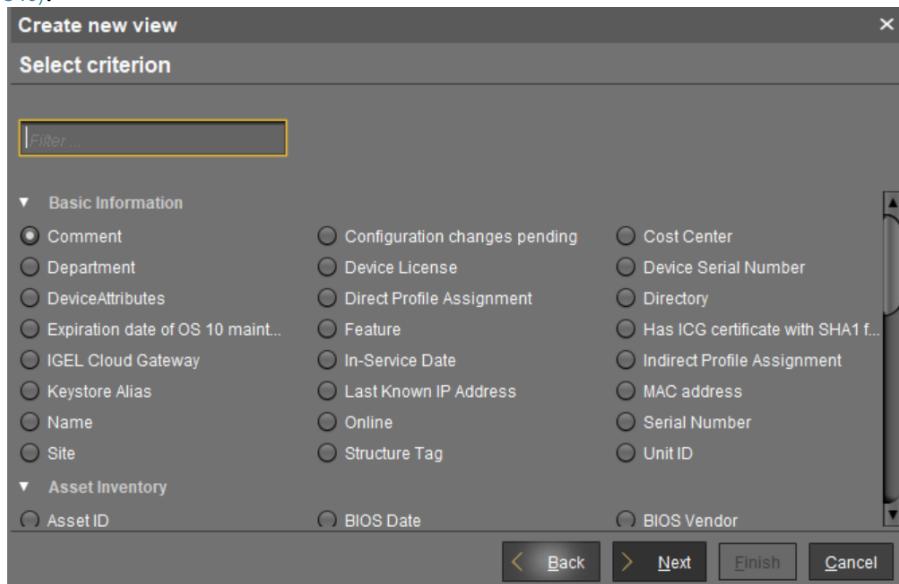


- ⓘ View editing is possible only in expert mode. In order to change the created view, e.g. for adding further criteria, select **Views > [name of the view] > [context menu] > Edit view**.

How to Create a View: Standard Procedure

Typically, you create a view as follows:

1. In the UMS Console, go to **Views > [context menu] > New View** or **System > New > New View**. The **Create new view** window will open.
2. Give a **Name** and a **Description**.
3. Click **Next**.
4. In the **Select criterion** window, select a parameter.
You will find a list of all available search parameters under [Possible Search Parameters](#) (see page 340).



5. Click **Next**.
6. 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`.
General information on regular expressions can be found e.g. under [Class Pattern¹⁷](#) in the Oracle documentation.
- 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 pattern entered.
- The parameter value must match the pattern 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.
- **Not like:** The parameter value must differ from the value entered.

7. Click **Next**.

8. In the **Finish view creation** window, select one of the following options:

- **Create view:** The view will be generated when you click **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.

9. Depending on the option selected, click **Finish** or **Next**. You can add as many criteria with AND/OR links as you want.

For an example, see [Example: Creating a View \(see page 343\)](#).

How to Create a View: Expert Mode

You can also create a new view using expert mode – either in graphical form or in text mode. It is possible to switch back and forth between graphical and text mode as long as the entered data in either mode is complete and valid.

How to Create a View Using Graphical Mode

To create a view using graphical mode, proceed as follows:

1. In the UMS Console, go to **Views > [context menu] > New View** or **System > New > New View**. The **Create new view** window will open.

¹⁷ <https://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html>

2. Click **Expert mode.**

The **New View** window will open.

3. Select **Graphical mode.**

The screenshot shows the 'New View' dialog box. At the top, there are fields for 'Name' and 'Description'. Below these, the 'Rule' tab is selected, showing two rows of search criteria. The first row is linked by 'AND' and contains 'Device License' as the criterion, 'equal to' as the operator, and 'WORKSPACE_EDITION' as the value. The second row is also linked by 'AND' and contains 'Device License' as the criterion, 'equal to' as the operator, and 'EXPIRED' as the value. There are 'Add column' and 'Add row' buttons at the bottom right of the rule editor. The 'Graphical mode' tab is highlighted with a red box.

4. Give a **Name and a **Description**.**

5. Under **Criterion, select a parameter.**

You will find a list of all available search parameters under [Possible Search Parameters](#) (see page 340).

6. Select an **Operator and define the **Value**.** The list of operators can vary depending on the selected criterion.

- **equal to:** The parameter value must match the value entered.
- **like:** The parameter value must match the pattern entered.
- **not like:** The parameter value must differ from the pattern/value entered.
- **less than:** The parameter value must be less than the value entered.
- **greater than:** The parameter value must be greater than the value entered.

7. Click **Add column / Add row to define further criteria / values.**

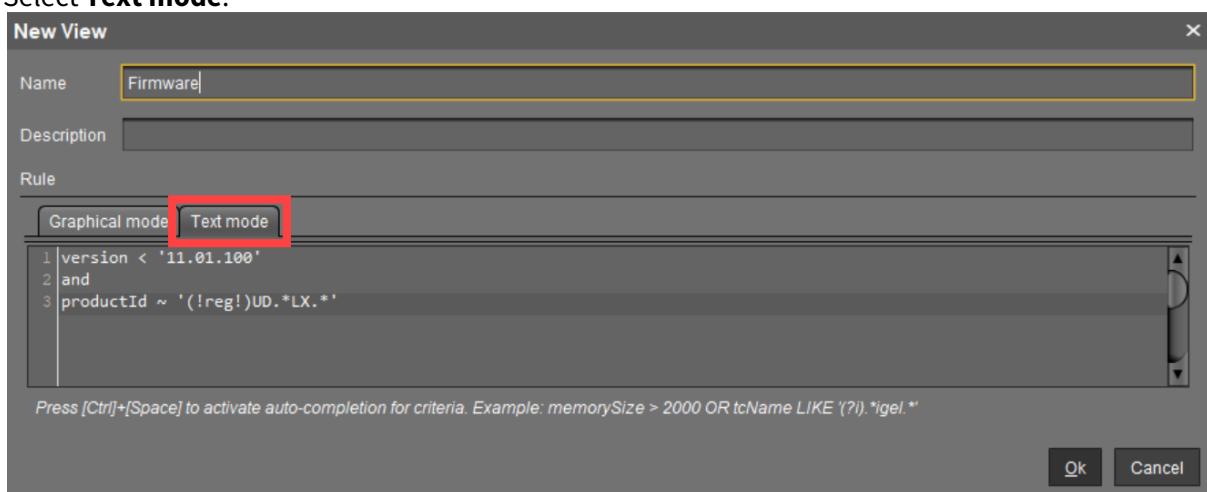
- Criteria / values in the same row are linked with a logical AND.
- Criteria / values in different rows are linked with a logical OR.

8. Click **OK.**

How to Create a View Using Text Mode

To create a view using text mode, proceed as follows:

1. In the UMS Console, go to **Views > [context menu] > New View** or **System > New > New View**.
The **Create new view** window will open.
2. Click **Expert mode**.
The **New View** window will open.
3. Select **Text mode**.



4. Give a **Name** and a **Description**.

5. Under **Rule**, enter your query.

Text mode allows entering a rule in an SQL-like query, consisting of one or more expressions, see [Queries in Text Mode of Views: Expression Parts](#) (see page 333) below.

You can press [Enter] to type from the new line. Line breaks can be entered at any time for convenience, but they are not preserved as the query is generated dynamically whenever a switch to text mode occurs.

6. Click **OK**.

Queries in Text Mode of Views: Expression Parts

- An expression consists of three parts: CRITERION OPERATOR VALUE

Example: `memorySize > 1000`

This query will find all devices with a system memory greater than 1000 MB.

- Multiple expressions can be combined with logical operators AND and OR. Note that AND takes precedence over OR and binds its surrounding expressions stronger.

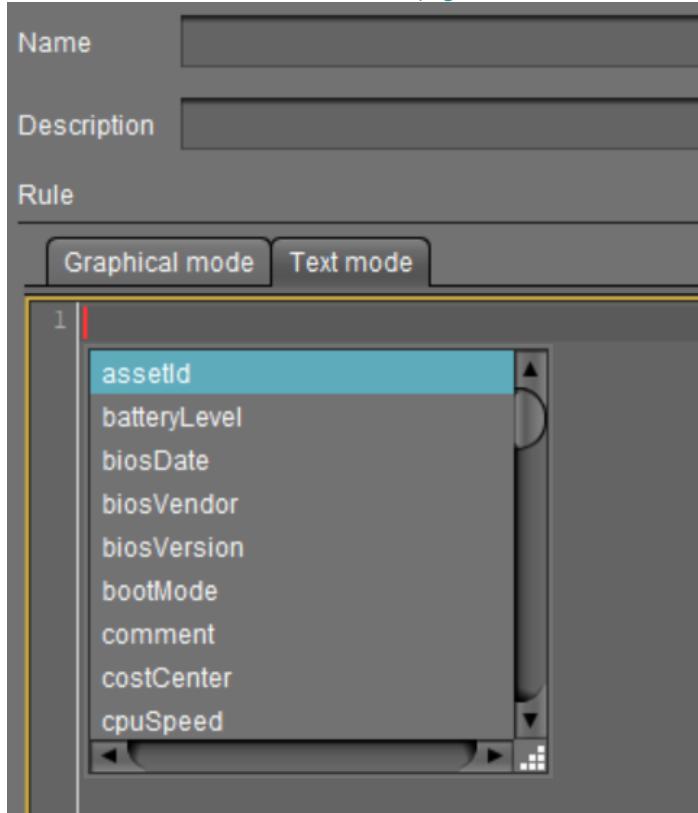
Example: `memorySize > 1000 and department = '(?i)sales' or tcName ~`

'Dev.*'

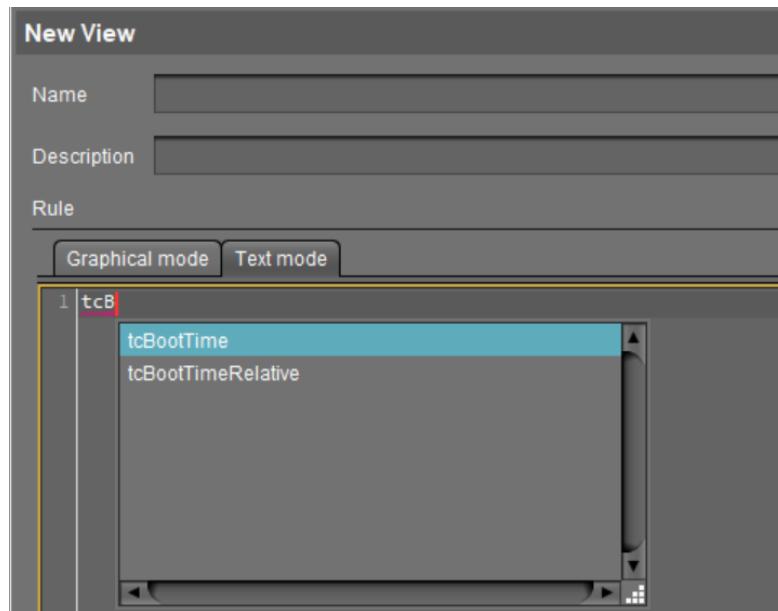
The search result of this query will contain all devices that fulfill the memory and department constraints simultaneously and additionally all devices whose name starts with 'Dev'.

Criterion

- Possible criteria and their internal identifiers can be found under [Text Mode of Views: Matrix of Possible Criteria and Operators](#) (see page 344).
- [Ctrl] + [Space] for auto-completion:
 - At any time when a criterion is expected, you can press [Ctrl] + [Space] to activate auto-completion.
A popup window listing all possible criteria opens. Device attributes are also listed here via their internal identifier if such an identifier has been specified under **UMS Administration > Global Configuration > Device Attributes > UMS internal identifier**, see [Managing Device Attributes for IGEL OS Devices](#) (see page 432).

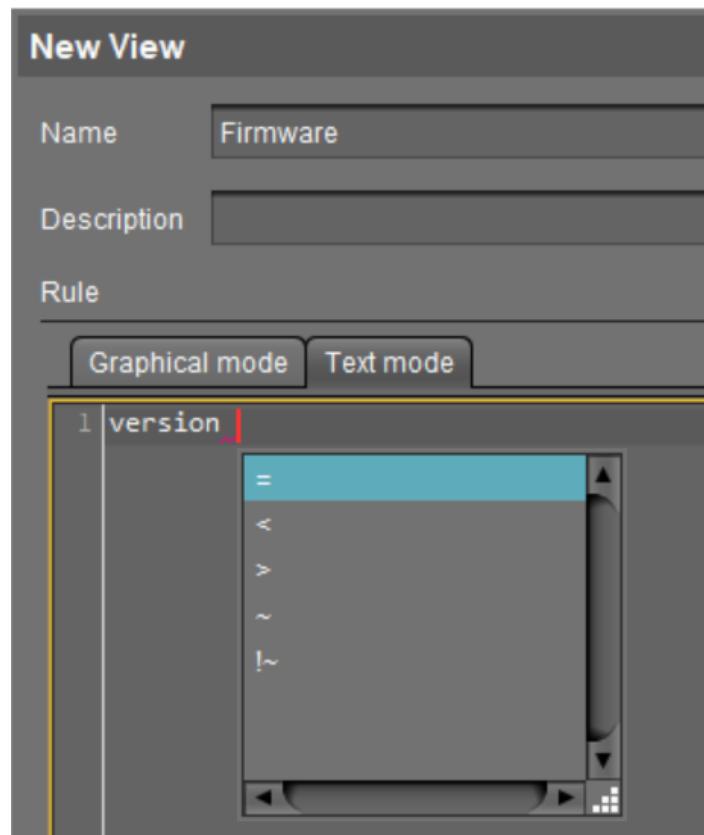


- Auto-completion also works when a criterion is entered only partially. It will then show only criteria matching the already entered fragment. If only one criterion matches the fragment, it will be completed without showing the popup window.

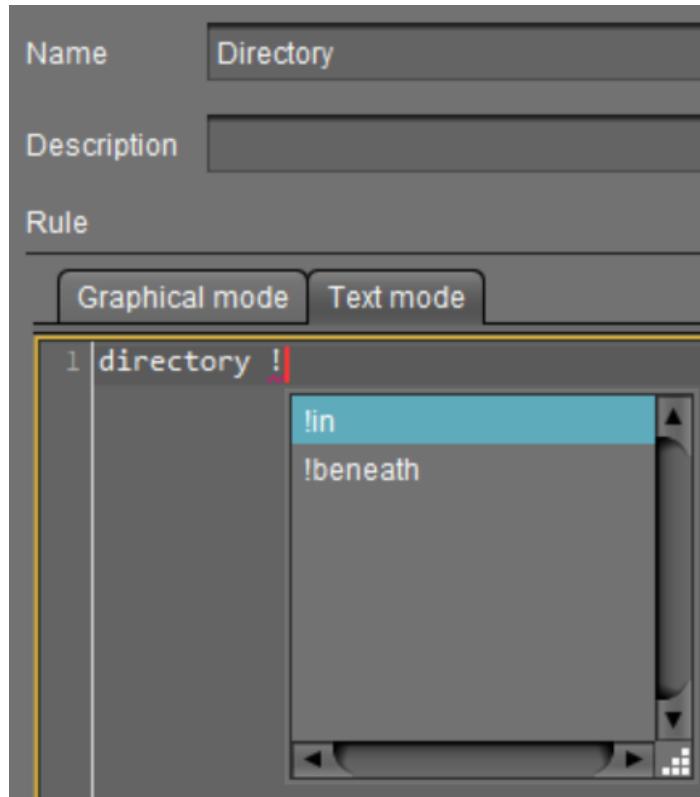


Operator

- For the list of operators possible for the criterion entered, see [Text Mode of Views: Matrix of Possible Criteria and Operators](#) (see page 344).
- [Ctrl] + [Space] for auto-completion:
 - At any time when an operator is expected, i.e. after a criterion and an entered space, you can press [Ctrl] + [Space] to activate auto-completion. A popup window listing all operators which are possible for the entered criterion opens.



- Auto-completion also works when an operator is entered only partially. It will then show only operators matching the already entered fragment. If only one operator matches the fragment, it will be completed without showing the popup window.



- The available operators are listed in the following table. The "Operator" column shows the operator names as they are provided in the selection lists of graphical mode. Multiple variations of operators are recognized for convenience or readability. Therefore, "LIKE" can also be written, for example, as "~".

Operator	Pattern(s)				
equal to	=				
less than	<				
greater than	>				
like	~	like	Like	LIKE	
not like	!~	!like	!Like	!LIKE	
in	in	In	IN		
not in	!in	!In	!IN		
beneath	beneath	Beneath	BENEATH		
not beneath	!beneath	!Beneath	!BENEATH		
is true	= true				

Operator	Pattern(s)			
is false	= false			

Value

- Text- and date-based values have to be enclosed in double ("") or single ('') quotation marks.
- Numeric values (integer, decimal values) do not require quotation marks.

Examples of Queries in the Text Expert Mode of Views

Device's **Name** contains "igel", where (?i) is a flag expression for case-insensitive matching:

```
tcName LIKE '(?i).*igel.*'
```

Consider case:

```
tcName LIKE '.*IGEL.*'
```

Compare whole text:

```
tcName LIKE '(?i)td-IGEL01'
```

Devices with a specific **Monitor Size**:

```
monitorSize = 24.1
```

Devices with a specific **Last Boot Time (Absolute)**:

```
tcBootTime > '2021-05-01' and tcBootTime < '2021-06-25'
```

Devices with device attribute values "KB" or "KM", where `deviceAttributeSubdepartments` is an identifier specified under **Device Attributes > UMS internal identifier**, see [Managing Device Attributes for IGEL OS Devices](#) (see page 432):

```
deviceAttributeSubdepartments ~ 'KB' or deviceAttributeSubdepartments ~ 'KM'
```

Examples of Regular Expressions in the Text Expert Mode of Views

Regular expressions are introduced by `(!reg!)`. For general information on regular expressions, see e.g. [Class Pattern¹⁸](#) in the Oracle documentation. Note that not all regular expression constructs described there are supported by the UMS, or their behavior in the UMS may be different.

- Any character zero or more times: `.*`

All devices whose product ID contains "UD-LX", e.g. `UD3-LX51`

```
productId LIKE '(!reg!)UD.*LX.*'
```

- Any character one or more times: `.+`

All devices whose name contains any character one or more times after "igel", e.g. `igel1`, `igel203`

```
tcName ~ '(!reg!)igel.+'
```

- Any character one time or not at all: `.?`

All devices whose name contains any character one time or not at all after "igel", e.g. `igel` and `igel1`

```
tcName like '(!reg!)igel.?'
```

- A digit [0-9]: `\d`

All devices whose name contains a digit after "igel", after which any character follows one or more times, e.g. `igel20`, `igel00E0C520986A`, `igel3DE`

```
tcName ~ '(!reg!)igel\d.+'
```

- Range: `[a-zA-Z]`

All devices whose name contains a hexadecimal number (e.g. for MAC addresses) one or more times after "igel", e.g. `igel00E0C520986A`

```
tcName ~ '(!reg!)igel[0-9A-F]+'
```

¹⁸ <https://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html>

Possible Search Criteria in the IGEL UMS

In the IGEL Universal Management Suite (UMS), the following parameters can be used as search parameters for a view. For more information on views, see [How to Create a New View in the IGEL UMS](#) (see page 329).

Basic Information

- **Comment**
- **Configuration changes pending**
- **Cost Center**
- **Department**
- **Device License**
- **Device Serial Number**
- **Direct Profile Assignment**
- **Directory**
- **Expiration date of OS 10 maintenance subscription**
- **Feature**
- **Has ICG certificate with SHA1 fingerprint**
- **IGEL Cloud Gateway**
- **In-Service Date**
- **Indirect Profile Assignment**
- **Keystore Alias**
- **LAN:** The endpoint device has at least one LAN network adapter. See the section "Network Adapters" under [View Device Information in the IGEL UMS](#) (see page 288).
- **LAN active:** The endpoint device is connected to the UMS via a LAN network adapter. See the section "Network Adapters" under [View Device Information in the IGEL UMS](#) (see page 288).
- **Last Known IP Address**
- **MAC address**
- **Name**
- **Online**
- **Serial Number**
- **Site**
- **Structure Tag**
- **Unit ID**
- **WLAN:** The endpoint device has at least one WLAN network adapter. See the section "Network Adapters" under [View Device Information in the IGEL UMS](#) (see page 288).
- **WLAN active:** The endpoint device is connected to the UMS via a WLAN network adapter. See the section "Network Adapters" under [View Device Information in the IGEL UMS](#) (see page 288).
- **[Name of the Device Attribute].** For details on device attributes, see [Managing Device Attributes for IGEL OS Devices](#) (see page 432).

Advanced System Information

- **Asset ID**
- **BIOS Date**

- **BIOS Vendor**
- **BIOS Version**
- **Battery Level**
- **Boot Mode**
- **CPU Speed**
- **CPU Type**
- **Device Type**
- **Duplex Mode**
- **Firmware Description**
- **Firmware Update (Relative)**
- **Firmware Version**
- **Flash Player**
- **Flash Player Version**
- **Flash Size**
- **Graphics Chipset 1**
- **Graphics Chipset 2**
- **Graphics Memory Size 1**
- **Graphics Memory Size 2**
- **Installed Apps:** Finds IGEL OS 12 devices that have a certain app / app version installed.
- **Last Boot Time (Absolute)**
- **Last Boot Time (Relative)**
- **Last contact time (absolute)** (see Monitoring Device Health and Searching for Lost Devices)
- **Last contact time (relative)** (see Monitoring Device Health and Searching for Lost Devices)
- **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 criterion** 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 creation** 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. See also see [Views and Searches \(see page 191\)](#) to learn about the options for displaying the view results.

Text Mode of Views: Matrix of Possible Criteria and Operators

Criterion name	Internal identifier	equal to	less than	greater than	like	not like	in	not in	beneath	not beneath	is true	is false
Asset ID	assetId	x	x	x	x	x						
BIOS Date	biosDate	x	x	x								
BIOS Vendor	biosVendor	x	x	x	x	x						
BIOS Version	biosVersion	x	x	x	x	x						
Battery Level	batteryLevel		x	x								
Boot Mode	bootMode	x	x	x	x	x	x					
CPU Speed	cpuSpeed		x	x								
CPU Type	cpuType	x	x	x	x	x	x					
Comment	comment	x	x	x	x	x	x					
Configuration changes pending	tcConfigChange									x	x	
Cost Center	costCenter	x	x	x	x	x	x					
Department	department	x	x	x	x	x	x					
Device License	licenseInfo	x										
Device Serial Number	deviceSerialNumber	x	x	x	x	x	x					
Device Type	deviceType	x	x	x	x	x	x					
Direct Profile Assignment	profile2TCAAssignment	x					x					
Directory	directory						x	x	x	x		
Duplex Mode	duplexMode	x										

Criterion name	Internal identifier	equal to	less than	greater than	like	not like	in	notin	beneath	not beneath	is true	is false
Expiration date of OS 10 maintenance subscription	subscriptionxExpirationDate	x	x									
Feature	tcFeature	x				x						
Firmware Description	customFirmwarename	x	x	x	x	x						
Firmware Update (Relative)	tcFwupdateTimeRelative		x	x								
Firmware Version	version	x	x	x	x	x	x					
Flash Player parameter					x	x						
Flash Player Version	flashPlayerVersion	x		x	x	x	x					
Flash Size	flashSize		x	x								
Graphics Chipset 1	graphicsChipset1	x	x	x	x	x	x					
Graphics Chipset 2	graphicsChipset2	x	x	x	x	x	x					
Graphics Memory Size 1	graphicsMemorySize1		x	x								
Graphics Memory Size 2	graphicsMemorySize2		x	x								
Has ICG certificate with SHA1 fingerprint	usgCertFingerprint	x				x						

Criterion name	Internal identifier	equal to	less than	greater than	like	not like	in	not in	beneath	not beneath	is true	is false
IGEL Cloud Gateway	usg									x	x	
IGEL Cloud Gateway, last boot via ICG	usgLastBoot									x	x	
In-Service Date	inServiceDate	x	x	x	x	x						
Indirect Profile Assignment	indProfile2TCAssignment	x					x					
Keystore Alias	keystoreAliases	x	x	x	x	x						
Last Boot Time (Absolute)	tcBootTime	x	x	x								
Last Boot Time (Relative)	tcBootTimeRelative		x	x								
Last Known IP Address	ipAddress	x	x	x	x	x						
Last contact time (absolute)	tcLastContact	x	x	x								
Last contact time (relative)	tcLastContactRelative		x	x								
License Id	licenseInfoLicenseId	x										
License expiration date	licenseInfoExpirationDate	x	x	x								
MAC address	macAddress	x	x	x	x	x						

Criterion name	Internal identifier	equal to	less than	greater than	like	not like	in	not in	beneath	not beneath	is true	is false
Memory Size	memorySize		x	x								
Monitor 1 Date of Production	monitor1DateOfProduction	x	x	x	x	x						
Monitor 1 Model	monitor1Model	x	x	x	x	x						
Monitor 1 Native Resolution	monitor1NativeResolution	x	x	x	x	x						
Monitor 1 Serial Number	monitor1SerialNumber	x	x	x	x	x						
Monitor 1 Size	monitor1Size	x	x	x		x						
Monitor 1 Vendor	monitor1Vendor	x	x	x	x	x						
Monitor 2 Date of Production	monitor2DateOfProduction	x	x	x	x	x						
Monitor 2 Model	monitor2Model	x	x	x	x	x						
Monitor 2 Native Resolution	monitor2NativeResolution	x	x	x	x	x						
Monitor 2 Serial Number	monitor2SerialNumber	x	x	x	x	x						
Monitor 2 Size	monitor2Size	x	x	x		x						
Monitor 2 Vendor	monitor2Vendor	x	x	x	x	x						

Criterion name	Internal identifier	equal to	less than	greater than	like	not like	in	not in	beneath	not beneath	is true	is false
Monitor Date of Production	monitorDateOfProduction	x	x	x	x	x						
Monitor Model	monitorModel	x	x	x	x	x						
Monitor Native Resolution	monitorNativeResolution	x	x	x	x	x						
Monitor Serial Number	monitorSerialNumber	x	x	x	x	x						
Monitor Size	monitorSize	x	x	x		x						
Monitor Vendor	monitorVendor	x	x	x	x	x						
Name	tcName	x	x	x	x	x						
Network Name	tcNetworkName	x	x	x	x	x						
Network Speed	networkSpeed		x	x								
OS Type	osType	x	x	x	x	x						
Online	online									x	x	
Partial Update (Name)	partialUpdateName	x			x	x						
Partial Update (Relative)	partialUpdateTimeRelative		x	x								
Partial Update (Version)	partialUpdateVersion	x			x	x						
Product	model	x	x	x	x	x						
Product ID	productId	x	x	x	x	x						

Criterion name	Internal identifier	equal to	less than	greater than	like	not like	in	not in	beneath	not beneath	is true	is false
Serial Number	serialNumber	x	x	x	x	x						
Site	site	x	x	x	x	x						
Structure Tag	umsStructureTag	x	x	x	x	x						
Total Operating Time	totalUsageTime		x	x								
Unit ID	unitId	x	x	x	x	x						
[Name of the Device Attribute]	Identifier specified under UMS Administration > Global Configuration > Device Attributes > UMS internal identifier (see page 432)	x	x	x	x	x						

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:

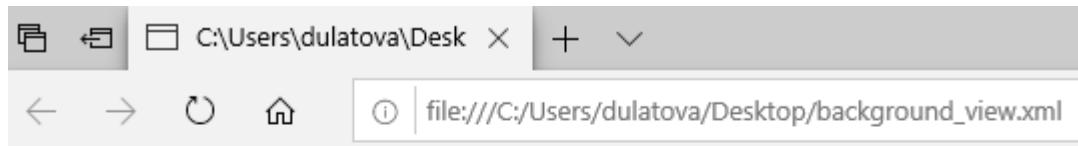
1. Click on the view directory that you want to copy.
2. Open the context menu for the directory and select **Copy**.
3. Click on the directory in which you would like to paste the copy of the view directory. This can also be the directory in which the original view directory is located.
4. Open the 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>
```

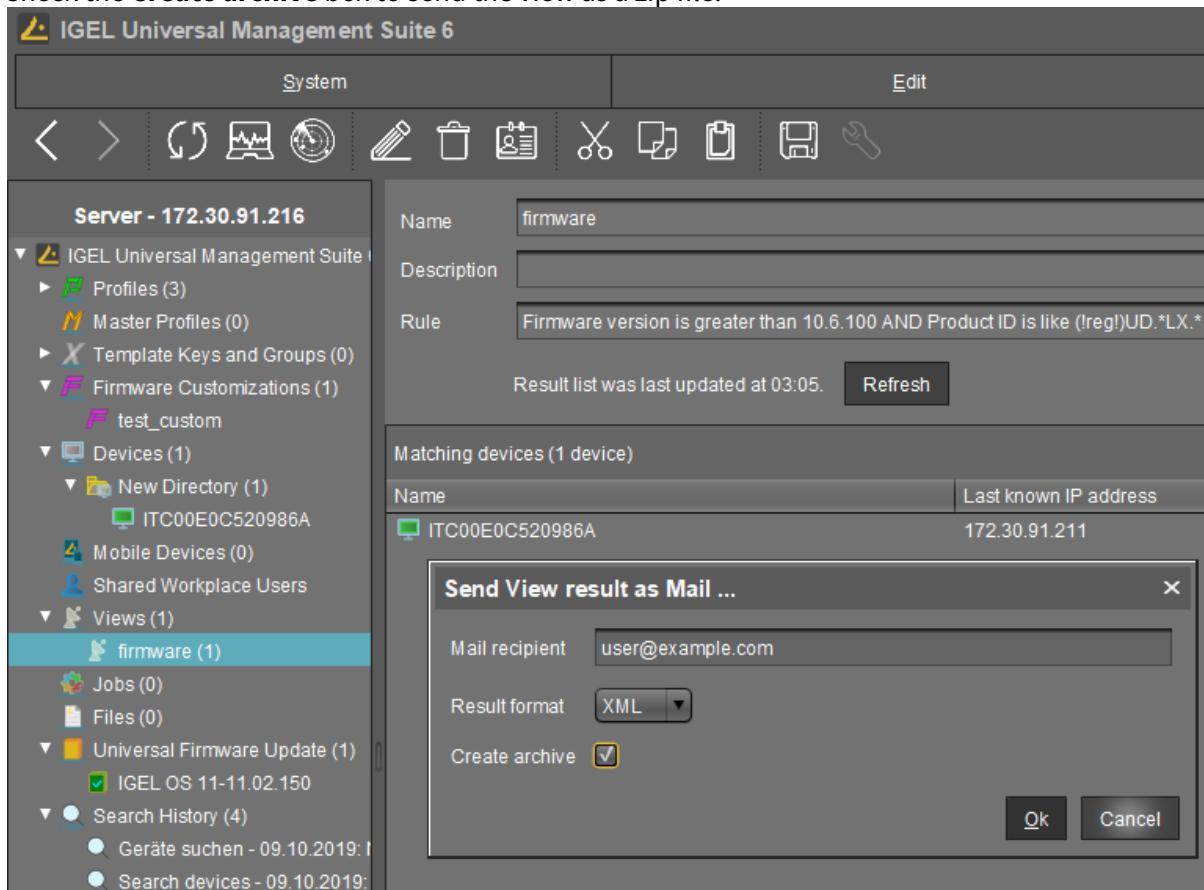
- ⓘ The **Save as...** option is always active in the context menu if **Automatically load amount and items** is selected under **Menu Bar > Misc > Settings > Views and Searches > Page Behavior > When opening a view result...**. If one of the other parameters is chosen, the **Save as...** option will only be active after clicking a button **Load devices** (or **Search for hits > Load devices**) in the content panel of the view. See also [Views and Searches](#) (see page 191).

Sending a View as Mail

- ⓘ** Emails can only be sent if you have configured appropriate [mail settings](#) (see page 507) under **UMS Administration > Global Configuration > Mail Settings**.

To send a view as mail, proceed as follows:

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 460).

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 466).

- ⓘ Using the same principle, you can assign objects to devices that you have filtered via a [search](#) (see page 381).

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.

- ⓘ Options **Assign objects to the devices of the view...** and **Detach objects from the devices of the view...** are always active in the context menu if **Automatically load amount and items** is selected under **Menu Bar > Misc > Settings > Views and Searches > Page Behavior > When opening a view result...**. If one of the other parameters is chosen, the above options will only be active after clicking a button **Load devices** (or **Search for hits > Load devices**) in the content panel of the view. See also [Views and Searches](#) (see page 191).

Jobs - Sending Automated Commands to Devices in the IGEL UMS

You can define jobs for the IGEL Universal Management Suite (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.

Menu path: **UMS Console > Jobs**

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 \(see page 530\)](#).
 - **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 \(see page 537\)](#).
 - **Execute Job:** Executes the job immediately.
-
- [How to Set Up a New Job \(see page 356\)](#)
 - [Commands for Jobs \(see page 357\)](#)
 - [Job Configurations and Execution Results \(see page 359\)](#)
 - [Assigning Objects to a Job \(see page 364\)](#)

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=F7NI4PDBUMM>

How to Set Up a New Job

You can set up jobs in the UMS Console to manage a selection of devices by sending scheduled commands to them.

Menu path: UMS Console structure tree > **Jobs**

To create a job:

1. Select **Jobs** > [context menu] > **New Scheduled Job** or **System** > **New** > **New Scheduled Job**.
The configuration dialog opens. The parameters configured in the dialog can later be changed by editing the Job.
2. Under **Details**, provide the basic information of your Job and the Command to perform. For more information on the parameters, see "Details" in [Job Configurations and Execution Results \(see page 359\)](#) and [Commands for Jobs \(see page 357\)](#).
3. Under **Schedule**, you can further adjust the execution time. For more information on the parameters, see "Schedule" in [Job Configurations and Execution Results \(see page 359\)](#).
4. Under **Select assignable objects**, you can assign your Job to Devices, Device folders, Views, Searches. You can also assign the object later. For more information, see [Assigning Objects to a Job \(see page 364\)](#).
You can also assign Advanced Searches created in the UMS Web App. For more information, see [Search for Devices in the IGEL UMS Web App](#).
5. Click **Finish** to save the Job.

Commands for Jobs

Here you find information on the commands that you can define for a job in the IGEL Universal Management Suite (UMS).

- **Update**
 - IGEL OS 12: Triggers the activation of the assigned app version for IGEL OS 12 devices.
The **Update** command is only needed if **System > Update > Activate app after the installation** is disabled; see How to Configure the Background App Update in the IGEL UMS Web App.
 - IGEL OS 11 or earlier: Executes the firmware update with the existing settings, see also [Universal Firmware Update](#) (see page 492).
- **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 (IGEL OS 11 or earlier).
- **Update when shutting down**: Executes the firmware update when the device shuts down (IGEL OS 11 or earlier).
- **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.
- **Remove Flashplayer**: Removes the Flash Player plugin for Firefox.
- **Download Firmware Snapshot**: Executes the firmware update with the existing settings (WES).
- **Send Message**: Sends a selected message template to the devices. You can create templates for messages under **UMS Administration > Global Configuration > Messages to Devices**. For more information on templates, see [Send Message](#) (see page 313).
- **Partial Update**: Executes the partial update with the existing settings (WES). See also Partial Update.
- **Update desktop customization**: Updates the desktop background and the boot logo.
- **BIOS - Get settings**: Gets the current BIOS settings from the device. This command is used by the BIOS Tools for Selected HP Devices.
- **BIOS - Set password**: Sets a password for the BIOS. This command is used by the BIOS Tools for Selected HP Devices.
- **BIOS - Set settings**: Deploys the changed BIOS settings to the device. This command is used by the BIOS Tools for Selected HP Devices.
- **BIOS - Trigger update**: Triggers a BIOS update. This command is used in the BIOS Update for Devices Supported by LVFS and by the BIOS Tools for Selected HP Devices.
- **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.

- **Start Login Enterprise launcher:** Starts Login Enterprise Launcher if it has been configured, see Login Enterprise Launcher in IGEL OS.
- **Update the firmware of an attached HP G5 Dock**
- **Upgrade to IGEL OS12**

Job Configurations and Execution Results

Here, you can find all the parameters defined for the Job under **Details** and **Schedule**. You can also check the **Execution Results** for a completed job.

Menu path: Structure tree > **Jobs** > [Specific Job]

/Jobs/Test Advanced Search

Details

Name	Test Advanced Search
Command	Update
Execution time	09:12
Start date	2025-03-23
Comment	

Options

<input checked="" type="checkbox"/> Log results	<input type="checkbox"/> Retry next boot
Max. Threads	99
Delay	0
Seconds	
Timeout	30

Job-Info

Job ID	26948
Next Execution	Mar 23, 2025, 9:12 AM
User	Admin

Schedule

Execution time	09:12	Start date	2025-03-23
<input type="checkbox"/> Expiration date		Time	11:19

Repeat Job

<input checked="" type="radio"/> Never	
<input type="radio"/> Every	0 day
<input type="radio"/> Weekdays	Mon Tue Wed Thu Fri Sat Sun
<input type="checkbox"/> Exclude public holidays	

Cancel job execution

<input checked="" type="radio"/> Never	
<input type="radio"/> Time	00:00
<input type="radio"/> Max. duration	00:00

Execution Results

Name	MAC address	Execution time	Status	Message

Details

Name

Name of the job.

Command

Command which is executed for all assigned devices. For more information, see [Commands for Jobs \(see page 357\)](#).

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 \(see page 448\)](#)", after the start of the UMS Console, the following notification pop-up will be shown:

Notifications					
<input type="checkbox"/> Don't show again	Info Type	Notification Type	Message	Message creation date	
<input type="checkbox"/>	Information	Admin Tasks	Care: you did not create an automatic backup task	May 22, 2019	
<input checked="" type="checkbox"/>	Information	Admin Tasks	Care: you did not create a cleanup task for Delete job execution data	May 22, 2019	
<input checked="" type="checkbox"/>	Information	Admin Tasks	Care: you did not create a cleanup task for Delete logging data	May 22, 2019	

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

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.

Execution Results

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:

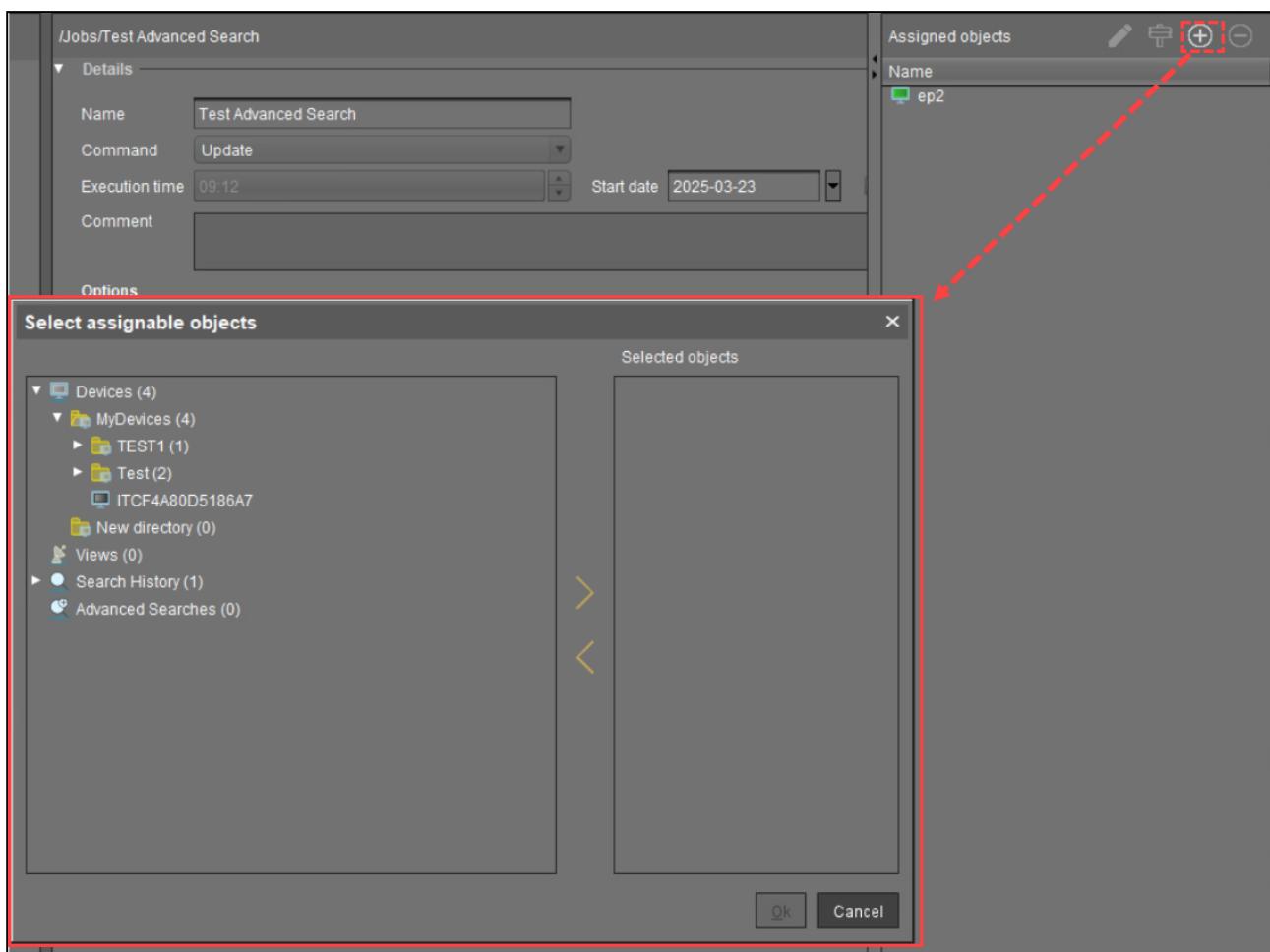
Being executed	The job is currently being executed.
OK	The job is complete, all assigned devices have been dealt with.
Out of time	The job was aborted before all assigned devices could be dealt with because the abort time or the maximum duration has been reached.
Canceled	The job was stopped for an unknown 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.

Assigning Objects to a Job

Jobs can be assigned to devices through object assignment.



By clicking **Add (+)**, you can use the following assignments:

- You can select specific devices.
- You can select a device directory. The job will then be assigned to all devices located in this directory at the point of execution.
- You can use dynamic device selection by selecting a View / Search / Advanced search. At the point of execution, the devices will first be ascertained on the basis of the selection conditions for the View / Search / Advanced search. 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.

Files - Registering Files on the IGEL UMS Server and Transferring Them to Devices

Through a **file transfer** functionality in the IGEL Universal Management Suite (UMS), you can save files in the device's local file system. A file must be registered on the 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. For information on file management in the IGEL UMS Web App, see Upload and Assign Files in the IGEL UMS Web App.

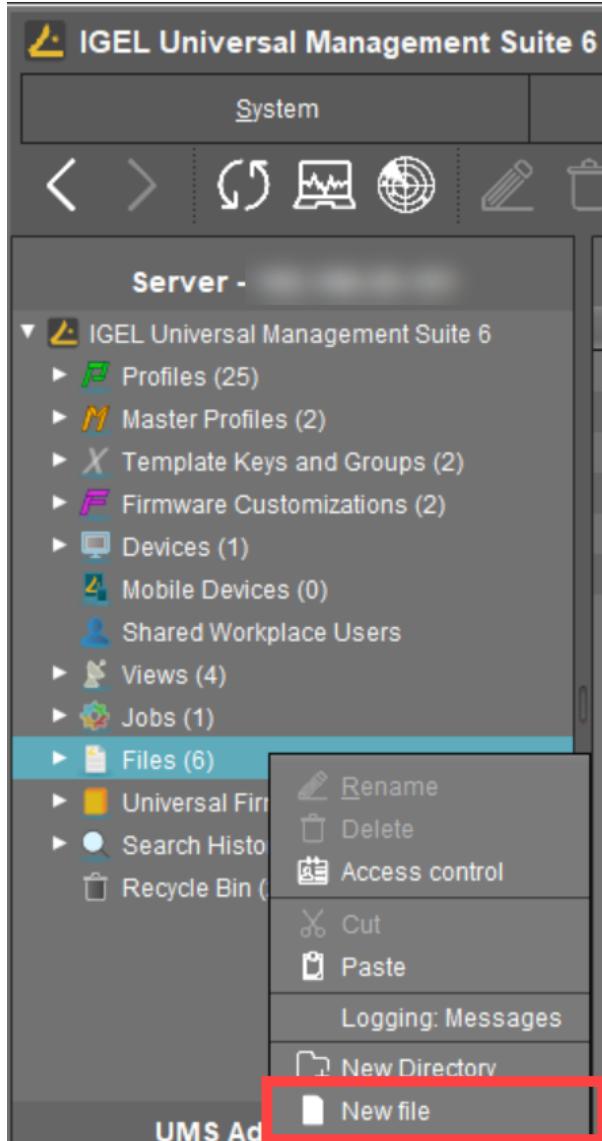
Menu path: **Files > [context menu] > New file**

How to Register a File on the UMS Server

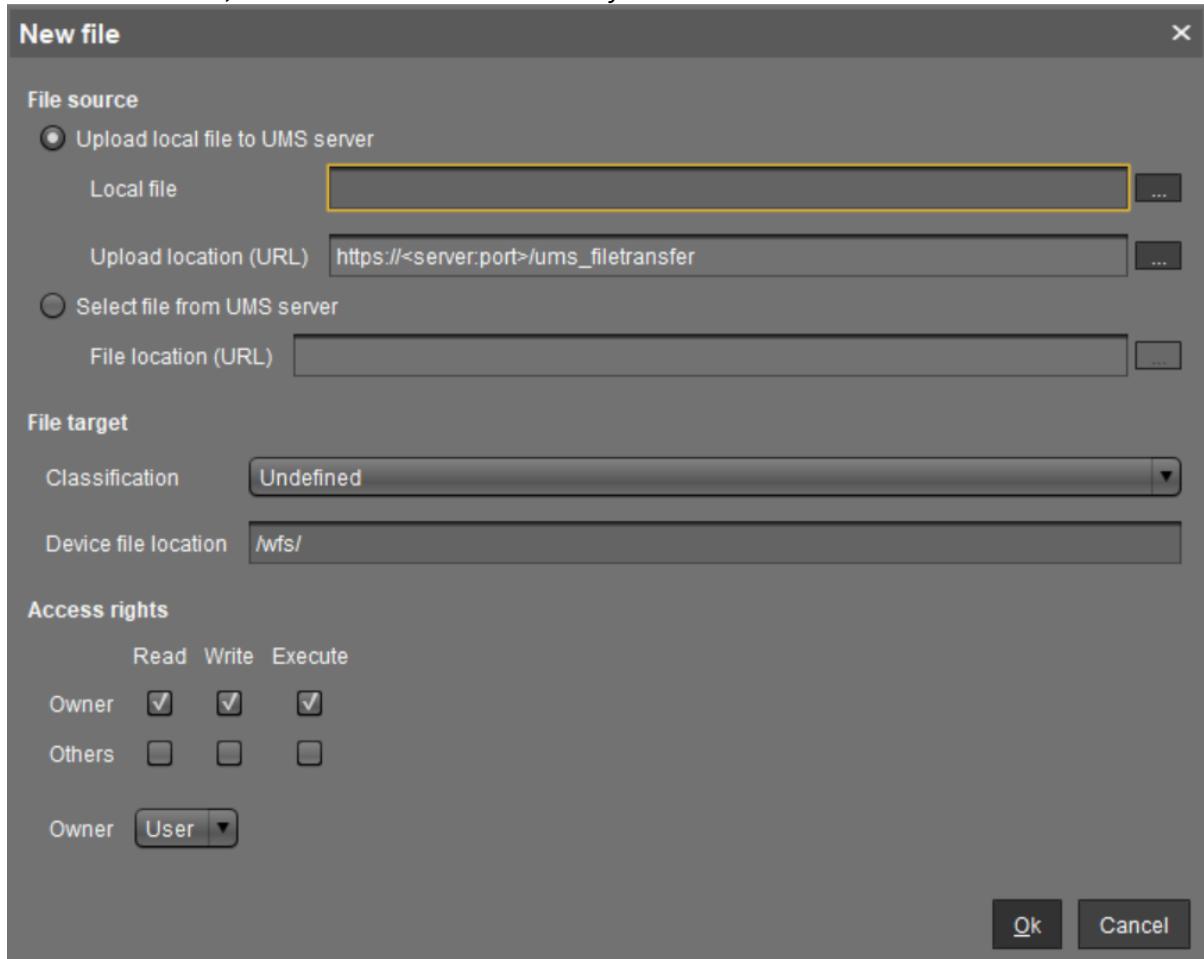
A file must be registered on the UMS Server before it can be loaded onto a device.

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**.



- Under **File source**, select a local file or one already on the server.



- Select the **upload location (URL)**. You can only use the directory `ums_filetransfer` or sub-directories created in it.
- 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**
 - App signing certificate**
 - Common certificate**

For information on certificate deployment, see Deploying Trusted Root Certificates in IGEL OS.

5. For the **Undefined** classification, specify the path in the device's local file system under **Device file location**.

If you enter a directory which does not yet exist, it will be created automatically.

 Note that paths must end with a path separator – a slash "/" or a backslash "\".

 Because of its space limit, the use of the `/wfs/` folder is NOT recommended for large files (>2 MB).

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. Click **OK** to confirm the settings.

The file will now be copied to the web resource and will be registered on the UMS Server.

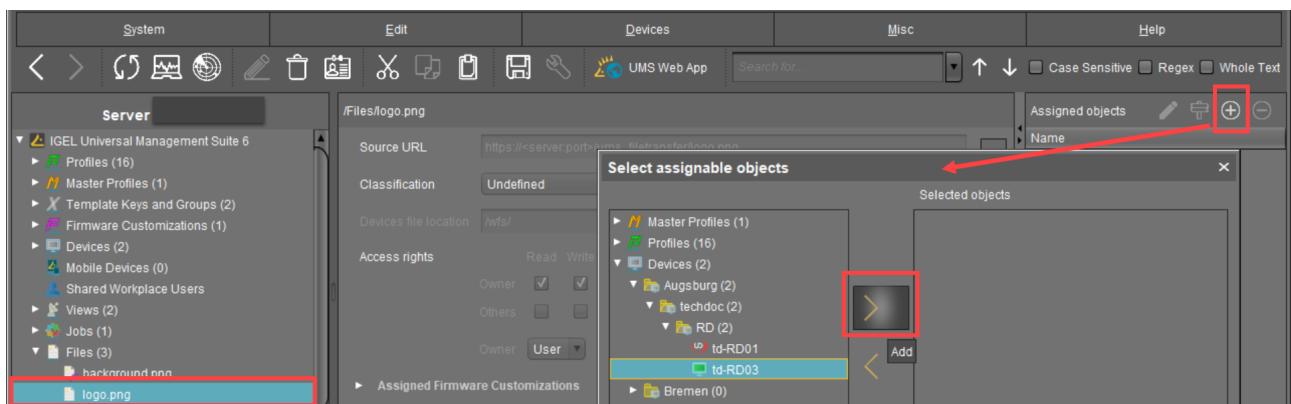
 Registered files are automatically synchronized between the UMS Servers. For more information, see [Which Files Are Automatically Synchronized between the IGEL UMS Servers?](#)

How to Transfer a File to a Device

In order to upload a registered file to a device, it must be assigned to the device either directly or indirectly via a device directory or profile. If a file has been assigned to a profile, it will be transferred to the devices along with the profile settings when you assign this profile to the devices.

► Via drag and drop, move the file to the required device / device directory or profile. Alternatively, click the  symbol in the **Assigned objects** area; you can use the **Assigned objects** area in the **Files**, **Devices**, or **Profiles** tree nodes.

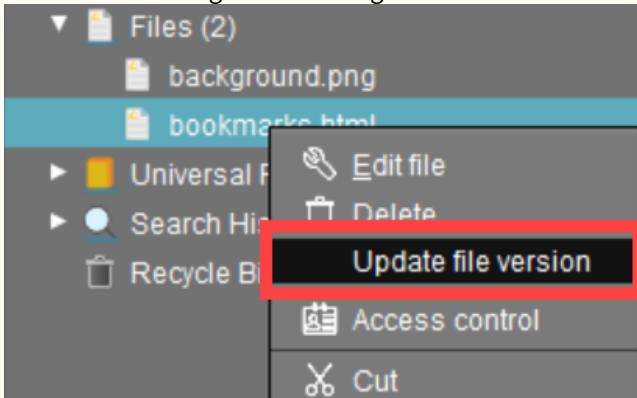
Example:



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.

⚠ Update File Version

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.



Afterwards, click **Other commands > Settings UMS->Device** from the device's context menu or in the menu bar under **Devices** to speed up the transfer of settings to the devices.

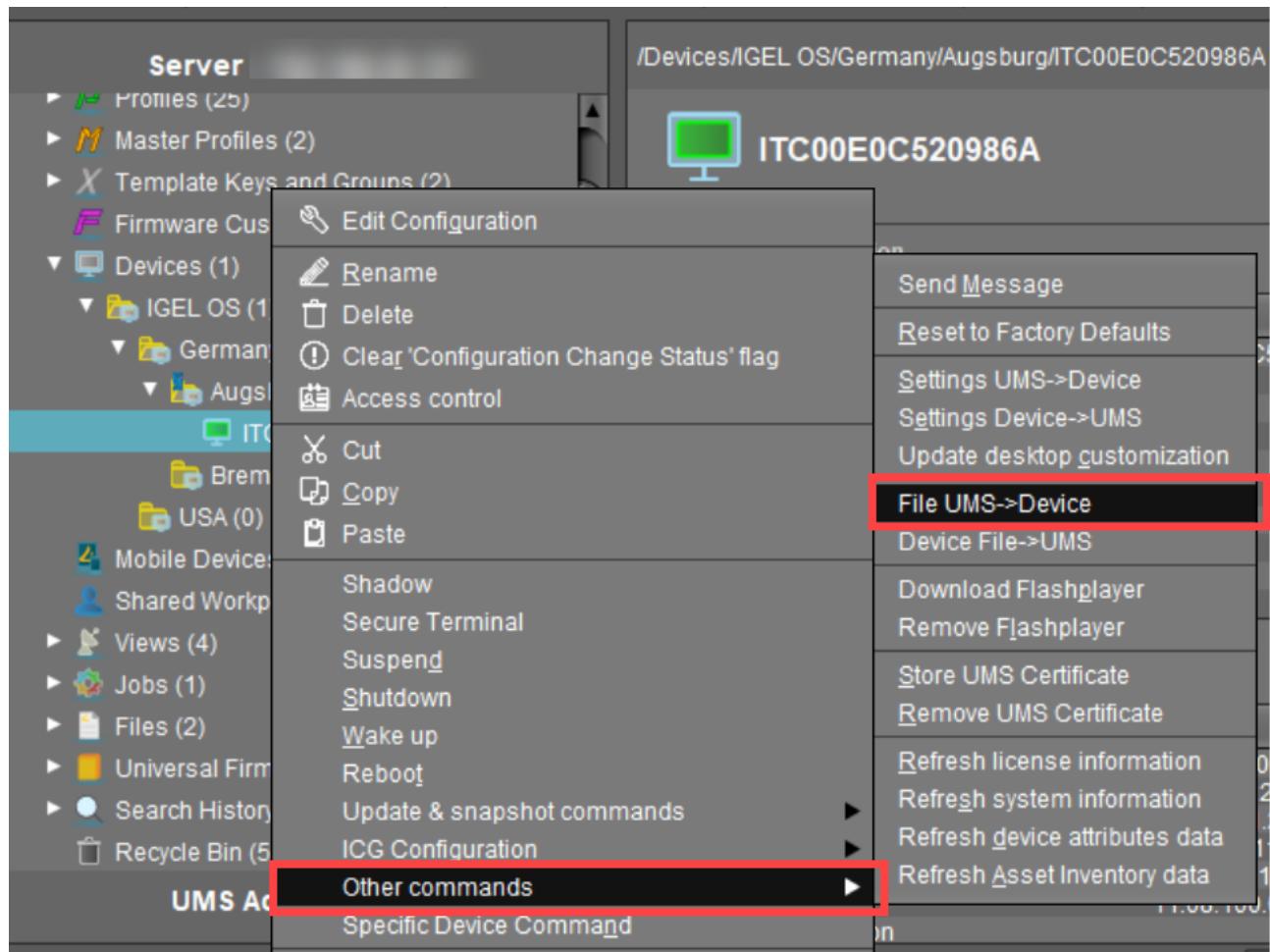
- ⓘ From UMS version 5.02.100, the IP address of the UMS is used when transferring the file. This ensures that the transfer works even in the event of DNS problems.

Transferring a File Without Assignment

A file registered on the UMS Server can also be transferred to the device without assignment:

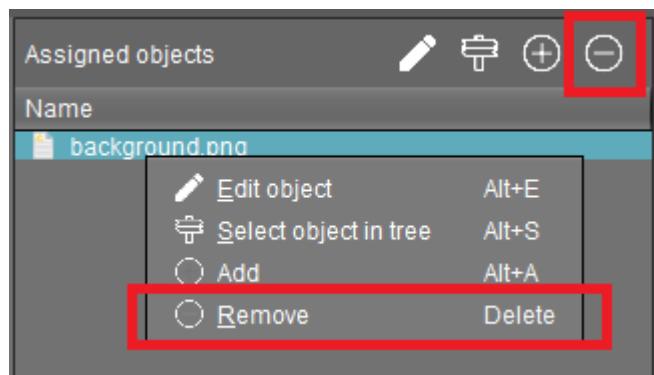
- ▶ Select **Other commands > File UMS->Device** from the device's context menu or under **Devices** in the menu bar.

- ⚠** This is a straightforward file copying operation. The file is NOT updated if the file version on the UMS Server changes.

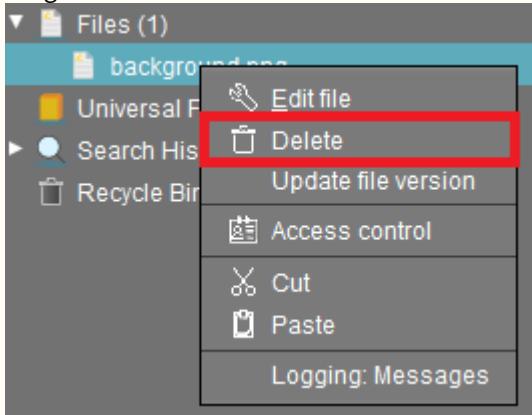


How to Remove a File from a Device

- To permanently remove a file from a device, select the device in the structure tree and delete the file assignment in the **Assigned objects** area.



- ⚠** If you delete a file in the structure tree under **Files**, it will be removed from ALL devices to which it was assigned.



IGEL Tech Video

See also IGEL Community Tech Video on how to transfer files to IGEL OS:



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:
<https://www.youtube.com/watch?v=7EFCiZvlNPM>

Transferring a File to the IGEL UMS Server

The following article explains how you can transfer a file from your endpoint device to the IGEL Universal Management Suite (UMS).

To download a file on a device to the web resources, proceed as follows:

- ▶ In the context menu of a device or under **Devices** in the menu bar, select **Other commands > Device File->UMS**.

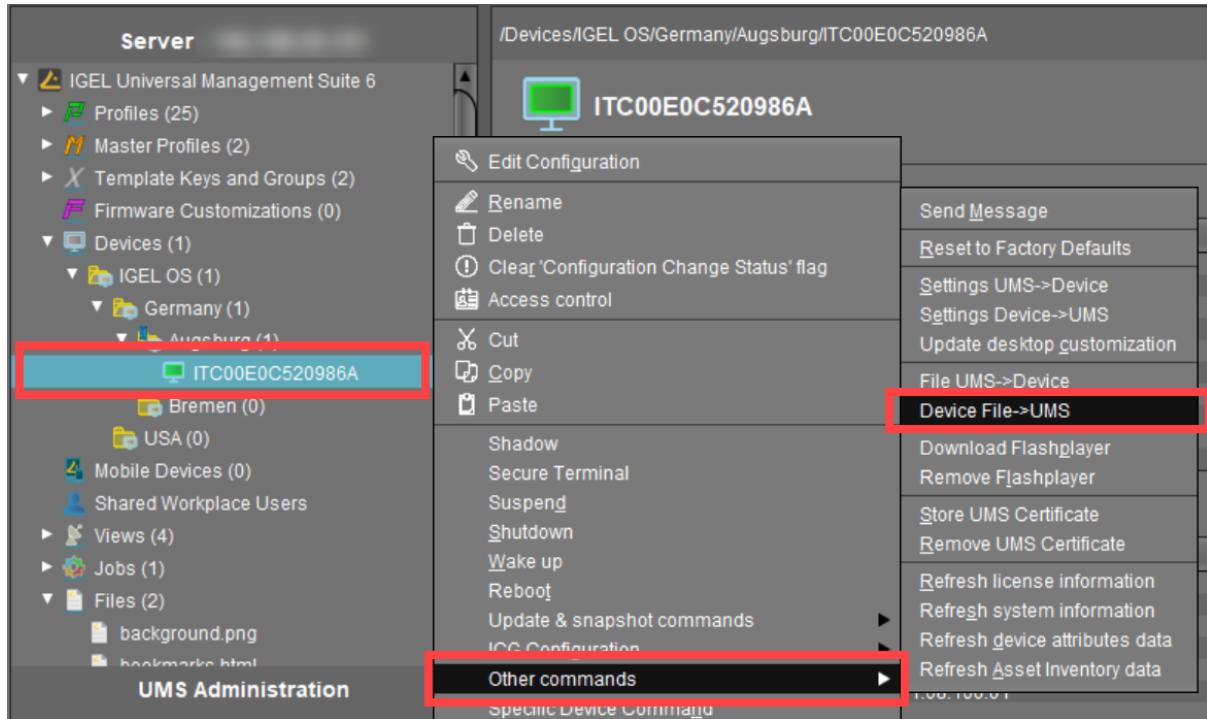
The UMS cannot search through the device's local file system. Therefore, you have to know the location and name of the file you would like to download to the web resource.

- ⓘ 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 **Files > New File**, see [Files - Registering Files on the IGEL UMS Server and Transferring Them to Devices](#) (see page 366).

Example for How to Use the Command "Device File->UMS"

The **Device File->UMS** command can be used, for example, 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.

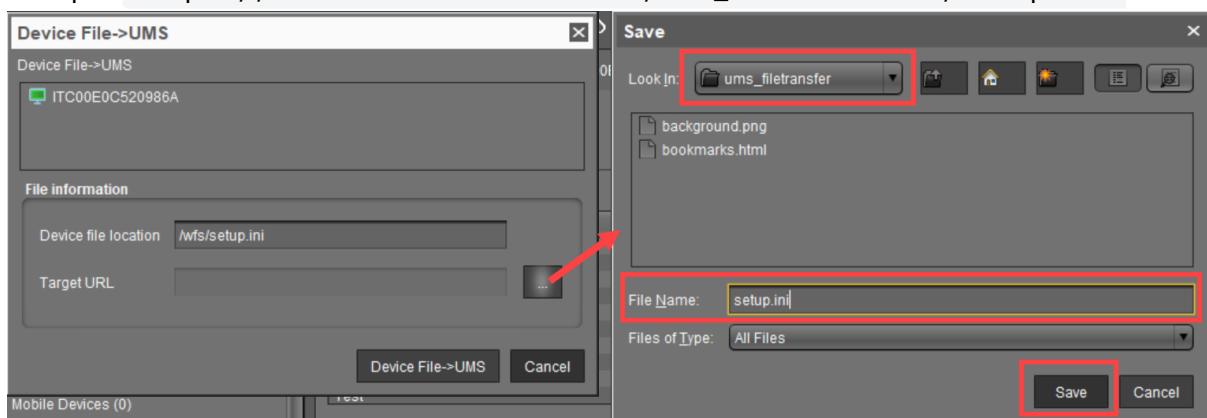


2. Under **Device file location**, specify `/wfs/` as the source.

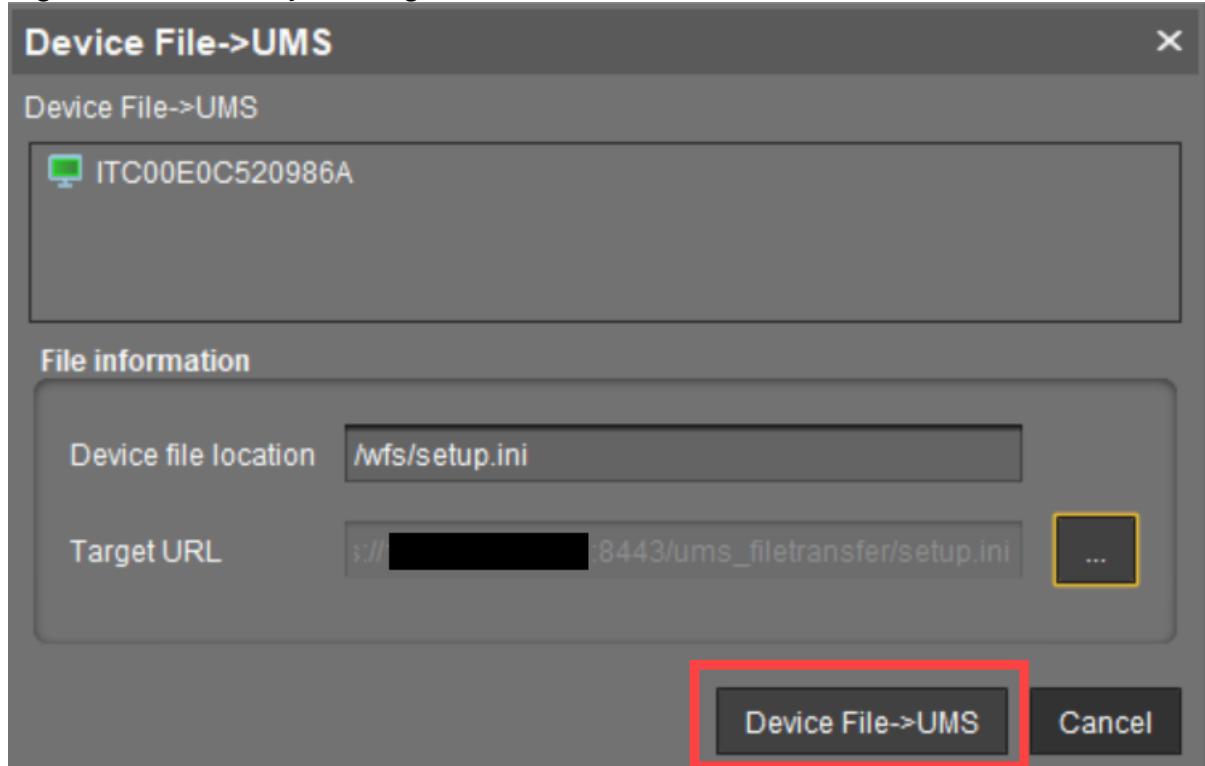
Example: `/wfs/setup.ini`

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**.



The file will be transferred to `/rmguiserver/webapps/ums_filetransfer`.

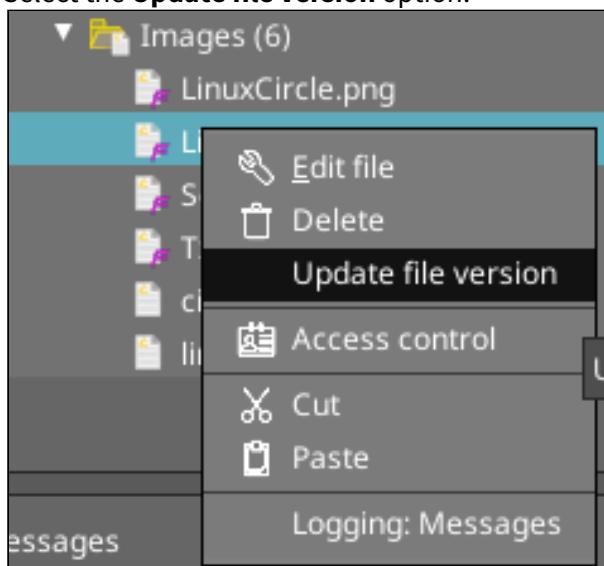
For more information on reading out the local device configuration, see also Exporting the Local Configuration of the IGEL OS Device.

Updating File Version in IGEL UMS

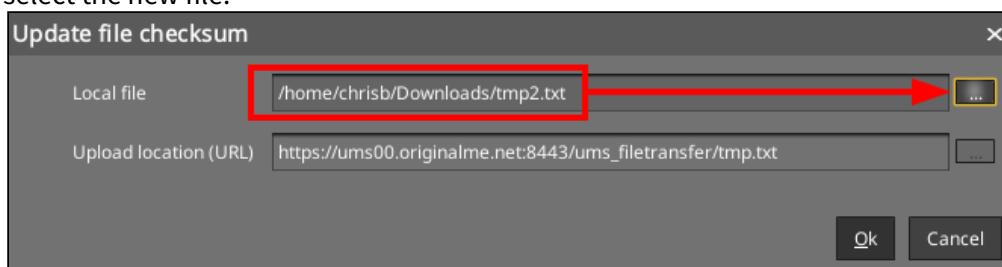
In order to update a file version once it is deployed to a device, you will want to utilize the **Update File Version** option in the IGEL Universal Management Suite (UMS).

To update the file version on your existing devices:

1. Right-click the file object in UMS.
2. Select the **Update file version** option.



3. In the **Update file checksum** dialog, click the "..." (three dots) button to launch a file browser, and select the new file.



4. Click **OK** to upload and replace the file in the ums_filetransfer directory.
5. Send updated device settings, or reboot devices to have the file sent to the devices and replace the original file on the device.

Universal Firmware Update

Menu path: **Server - [UMS Server address]** > **Universal Firmware Update**

In this area, you can search for new firmware updates for IGEL devices and devices converted by OSC, import the configuration data for specific firmware versions, and provide the firmware files for distribution.

The following options are available in the context menu:

- [Check for new firmware updates](#) (see page 378)
- **Snapshot -> Universal Firmware Update**
- **Firmware archive (zip file) -> Universal Firmware Update**
- **Access control.** See [Access Rights](#) (see page 521).

When you select **Snapshot -> Universal Firmware Update** or **Firmware Archive (zip file) -> Universal Firmware Update**, you can choose one of the following options:

- [Import Firmwares](#) (see page 308): Imports the configuration data for specific firmware versions from XML files that have been generated by a UMS instance.
- [Snapshot -> Universal Firmware Update](#) (see page 379): Registers a Windows Embedded Standard snapshot as a Universal Firmware Update.
- [Firmware archive \(zip file\) -> Universal Firmware Update](#) (see page 380): Registers the firmware files for IGEL OS as a Universal Firmware Update.

 Once you have provided the update files, you must assign them to the devices and launch the update process. See [Assigning Updates](#) (see page 302).

 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 492). If you have a High Availability environment and use the WebDAV for downloading the firmware updates, see [Which Files Are Automatically Synchronized between the IGEL UMS Servers?](#).

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=XfIN_BEyDZc

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: **Server - [UMS Server address]** > **Universal Firmware Update** > [context menu] > **Snapshot -> Universal Firmware Update**

In this area, you can register a snapshot of a Windows Embedded Standard device as a Universal Firmware Update. The snapshot file is stored in a WebDAV directory.

Snapshot file: Name of the snapshot file.

Select snapshot: Opens a dialog for the selection of the snapshot file. Only snapshot files with an SNP filename extension can be uploaded.

Name: Name of the modified snapshot.

Firmware Archive (Zip File) -> Universal Firmware Update

Menu path: **Server - [UMS Server address]** > **Universal Firmware Update** > [context menu] > **Firmware Archive (Zip File)** -> **Universal Firmware Update**

In this area, you can load firmware updates for IGEL OS from a local source. The firmware file is stored in a WebDAV directory.

- (i) 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 382)

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. Search editing is possible only in expert mode. For details on expert mode, see [Expert Mode \(see page 331\)](#). Text expert mode is possible for the search type **Devices** only.

The following options are always active if **Automatically load amount and items** is selected under **Menu Bar > Misc > Settings > Views and Searches > Page Behavior > When opening a search result...**. If one of the other parameters is chosen, the options below will only be active after clicking the button **Load device** (or **Load profile / Load view**) in the content panel of the search query.

- **Save as...:** Saves the search result in one of the following formats: XML, XSL-FO, HTML, or CSV.

The following options are only active if you have chosen **Devices** as a search type:

- **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 \(see page 354\)](#).
- **Detach objects from the devices from the search...:** Removes the assigned objects.

Recycle Bin - Deleting Objects in the IGEL UMS

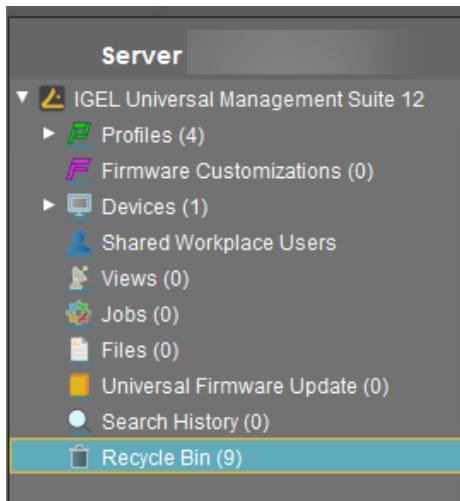
In the IGEL Universal Management Suite (UMS), you can move objects to the **Recycle Bin**. If the recycle bin is disabled, the objects are removed permanently straight away.

The recycle bin is enabled or disabled globally for all UMS users.

- i** You can enable / disable the recycle bin under **UMS Console > UMS Administration > Global Configuration > UMS Features**.

- ⚠** If you cannot register your endpoint device in the UMS, it is recommended to check if this device is in the recycle bin. If yes, restore the device from the recycle bin or delete it from the recycle bin and re-register. For further solutions, see Troubleshooting: Registration of a Device via Scanning for Devices Fails.

Menu path: **UMS Console > 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.

- i** 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. 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.

- i** 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.

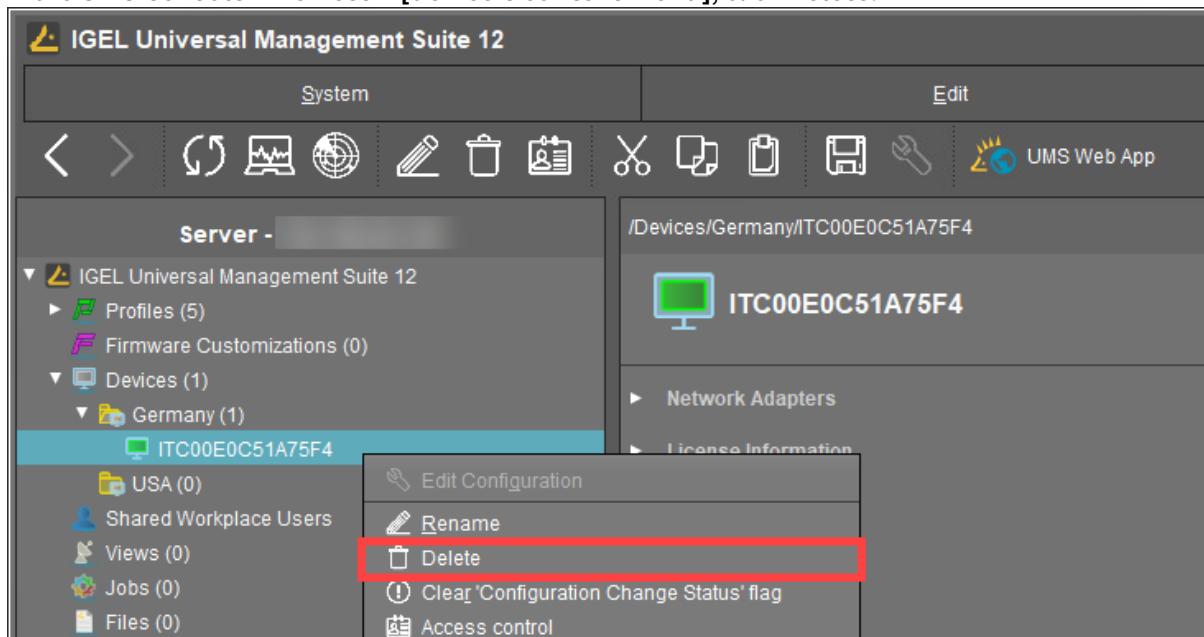
Virtually all elements from the UMS structure tree can be moved to the recycle bin: Devices, profiles, views, jobs, files and their directories. Shared Workplace users cannot be deleted, while administrator accounts (in account management) can only be deleted permanently. Search history elements can also be deleted only permanently (with [Shift-Del] or **Delete** function in the context menu). 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.

Removing Devices from the UMS

To delete devices in the UMS:

1. In the **UMS Console > Devices > [device's context menu]**, click **Delete**:

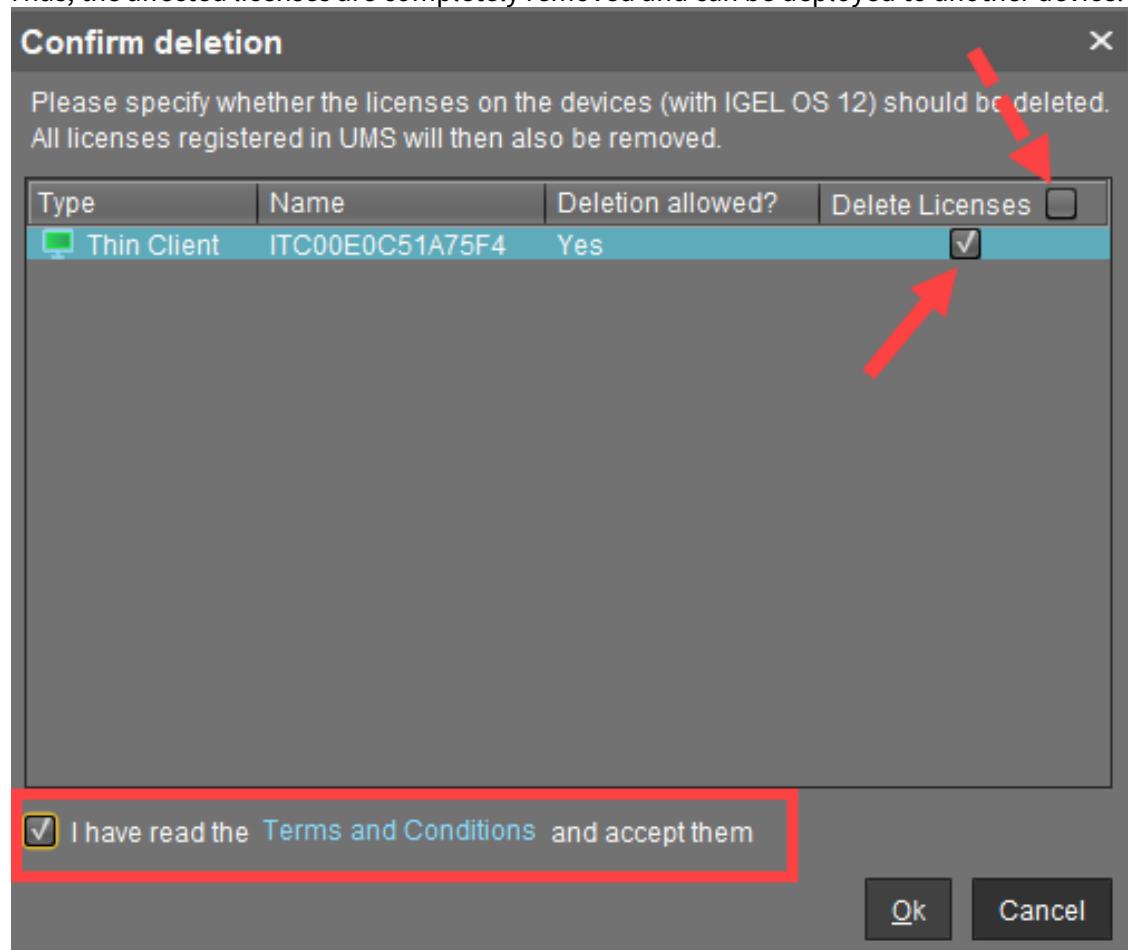


2. For IGEL OS 12 devices only: In the **Confirm deletion** dialog, specify whether the licenses should be deleted and accept the **Terms and Conditions**.

If you enable **Delete Licenses**:

- all licenses will be removed from the device if the device is online (Device level)
- all licenses registered in the UMS for the device will be removed from the UMS (UMS level)
- corresponding Unit IDs will be removed from all registered Product Packs if the IGEL License Portal (ILP) can be reached (ILP level)

Thus, the affected licenses are completely removed and can be deployed to another device.



ⓘ If the recycle bin is enabled, the **Confirm deletion** dialog will be shown when the devices are deleted from the recycle bin.

UMS Administration

- [UMS Network \(see page 387\)](#)
- [Global Configuration \(see page 396\)](#)

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 - View Your IGEL UMS Server Information](#) (see page 388)
- [Load Balancer - View Your IGEL UMS Load Balancer Information](#) (see page 391)
- [IGEL Cloud Gateway](#) (see page 393)

Server - View Your IGEL UMS Server Information

In the **Server** node of the IGEL Universal Management Suite (UMS) Console, you can find basic information on all servers that belong to your UMS installation. For an individual server, additional details such as process information, service status, statistical data, etc. are available. You can also define here the Public Address and Public Web Port for your UMS Server.

Menu path: **UMS Console > UMS Administration > UMS Network > Server**

"Server" Node in the IGEL UMS

The **Server** node lists all servers belonging to the UMS installation:

- With a standard installation, only one available server normally appears here.

Host	Device Communication Port	Version	IP address
td-ums-srv2019	30001	6.08.100.rc7	

- In a High Availability (HA) network, all installed servers are shown.

Process ID	Process Name	Timestamp	Service status	Mode
9c8ad658-d5e5-42e4-9747-87a45cc5ff3e	qajshasn02	14.07.2021 12:54	Service is running	Update Mode
2591491b-1144-4357-b00d-48aa056dfbc8	qajshasn03	14.07.2021 12:54	Service is running	Update Mode
e4eb53f3-703c-4798-87c9-b5039c262cc0	qajshasn01	14.07.2021 12:54	Service is running	Update Mode
dbd51173-6a77-4d06-a34e-a85d204c68f5	qajshawsrv03.qa.test	14.07.2021 12:41	Service is running	Normal Mode
39d52c12-5942-4563-a81c-31ffd1f124f11	qajshawsrv02.qa.test	14.07.2021 12:52	Service is running	Update Mode
b912ca44-ed69-455b-96f6-95478a62fe95	qajshawsrv01.qa.test	14.07.2021 12:42	Service is running	Update Mode

(i) Normal Mode and Update Mode (for HA Installations Only)

A server is in normal mode whenever it is NOT temporarily connected to the embedded update database created during the UMS HA update, see Updating HA Installation: Without Downtime of the Servers. Thus, **normal mode** means that the server is running with the normal "run configuration", but not with the database in update mode.

Individual Server

For an individual server, the following basic options are available.

Status Displays for the IGEL UMS Server

The status of the servers is shown by the following icons:

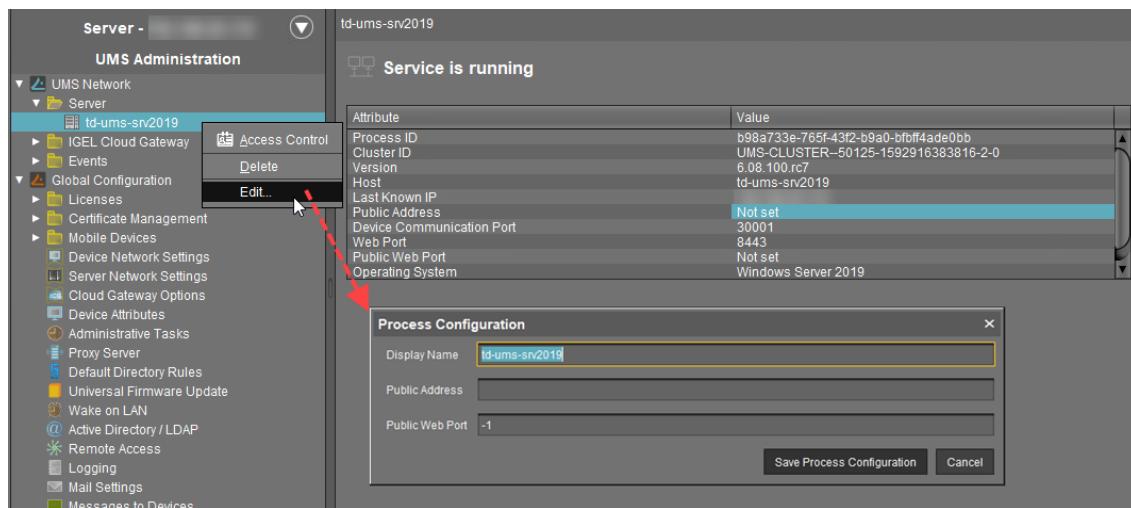
	The server is online.
--	-----------------------

	The server is offline.
	The server status is unknown (e.g. when a new server is being propagated in the network).

Process Configuration for the IGEL UMS Server

For each server, you can edit the process configuration, e.g. you can change the **Display Name** for the UMS Server. You can also configure here the **Public Address** and **Public Web Port**.

- To edit the process configuration, click **Edit** in the context menu of the required server.



If set, the **Public Address** and **Public Web Port** will be used

- when accessing files created in the UMS Console under **Files** (see [Files - Registering Files on the IGEL UMS Server and Transferring Them to Devices \(see page 366\)](#)) and Universal Firmware Updates (see [Universal Firmware Update \(see page 377\)](#))
- for internal communication between the UMS Servers (incl. WebDAV synchronization between the UMS Servers; see [Which Files Are Automatically Synchronized between the IGEL UMS Servers?, incl. the section "Connection Data Used during the Update"](#))
- for the automatically generated web certificates, see [Web \(see page 411\)](#)
- for HTTPS requests from devices if no **Cluster Address** is set (see [Server Network Settings in the IGEL UMS \(see page 420\)](#))

i As a **Public Address**, you can specify the IP address or FQDN of the UMS Server. The maximal length of the **Public Address** is restricted to 255 characters.

Process Tasks (for HA Installations Only)

In the case of the UMS HA installation, you can also start, stop, or restart the `IGEL_RMGUIServer` service:

The screenshot shows the UMS Administration interface for a server named td-ums-sv2012. The left sidebar lists various management categories like UMS Network, Server, Global Configuration, and Mobile Devices. Under the Server category, 'td-ums-sv2012' is selected. On the right, a detailed view of the service configuration is shown, including attributes such as Process ID, Cluster ID, Version, Host, Last Known IP, Public Address, Device Communication Port, Web Port, Public Web Port, and Operating System. Below this table, a section titled 'Process tasks' contains three buttons: 'Start service', 'Stop service', and 'Restart service', all highlighted with a red box.

For how you can start or stop services, see also [IGEL UMS HA Services and Processes](#).

Statistics for the IGEL UMS Server

An overview of **Requests** and **Failed and Waiting 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.

The screenshot shows the UMS Administration interface for a server named td-ums-sv2019. The left sidebar lists management categories. Under the Server category, 'td-ums-sv2019' is selected. On the right, the service configuration for td-ums-sv2019 is displayed, including attributes like Process ID, Cluster ID, Version, Host, Last Known IP, Public Address, Device Communication Port, Web Port, Public Web Port, and Operating System. At the bottom of this panel, there is a 'Show History' button. To the right, a 'Statistics' section displays two charts: 'Requests' and 'Failed and Waiting Requests'. Each chart has a 'Show History' button at its bottom. Red arrows in the image point to both of these 'Show History' buttons.

Load Balancer - View Your IGEL UMS Load Balancer Information

In the **Load Balancer** node of the IGEL Universal Management Suite (UMS) Console, you can find basic information on all load balancers that belong to your UMS installation. For an individual load balancer, additional details such as process information, service status, statistical data, etc. are available.

Menu path: **UMS Administration > UMS Network > Load Balancer**

"Load Balancer" Node in the IGEL UMS

The **Load Balancer** node 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).

The **Load Balancer** node lists all load balancers belonging to the UMS installation:

Load Balancer				
Process ID	Process Name	Timestamp	Service status	Mode
ums-broker-49849-163455...	td-ums-sn2012	Oct 19, 2021 15:55	Service is running	Normal Mode
ums-broker-49649-123655...	td-ums-sn2016	Oct 19, 2021 15:55	Service is running	Normal Mode

Normal Mode means that the load balancer is running with the normal "run configuration". Note that it does not serve as an indicator of the overall proper functioning of load balancers. If you want to check your HA environment, see UMS HA Health Check - Analyse Your IGEL UMS High Availability and Distributed UMS Systems.

Individual Load Balancer

Status Displays for the UMS Load Balancer

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 (e.g. when a new load balancer is being propagated in the network).

Process Configuration for the UMS Load Balancer

For each load balancer, you can edit the process configuration, e.g. you can change the **Display Name** for the load balancer.

- ▶ To edit the process configuration, click **Edit** in the context menu of the required load balancer.

Process Tasks for the UMS Load Balancer

Under **Process tasks**, you can also start, stop, or restart the **IGEL UMS Load Balancer** service. For how you can start or stop services, see also [IGEL UMS HA Services and Processes](#).

Statistics for the UMS Load Balancer

An overview of **Requests** and **Failed and Waiting 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.

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 For renewing the end certificate, see Renewing a Signed Certificate for the ICG . For exchanging the root certificate, see Exchanging the Root Certificate for ICG .
	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. <div style="border: 2px solid red; padding: 5px; margin-top: 10px;"> ! 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. </div>
	Edit the settings of the selected IGEL Cloud Gateway
	Navigate to the ICG instance view
	Set a limit for ICG connections (ICG 2.02 or higher required)

Add an IGEL Cloud Gateway to the UMS Database

- **Display name:** Display name of the gateway. The maximal length of the name is restricted to 200 characters.
- **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 \(see page 479\)](#)
 - **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 436), integrate user data from the [Active Directory](#) (see page 497), set up [Universal Firmware Updates](#) (see page 492) and manage [licenses](#) (see page 397).

- [Licenses](#) (see page 397)
- [Certificate Management](#) (see page 407)
- [Device Network Settings for the IGEL Universal Management Suite \(UMS\)](#) (see page 415)
- [Server Network Settings in the IGEL UMS](#) (see page 420)
- [First-authentication Keys](#) (see page 430)
- [Managing Device Attributes for IGEL OS Devices](#) (see page 432)
- [Administrative Tasks - Configure Scheduled Actions for the IGEL UMS](#) (see page 436)
- [UMS ID](#) (see page 477)
- [Proxy Server](#) (see page 479)
- [Default Directory Rules](#) (see page 481)
- [Universal Firmware Update](#) (see page 492)
- [Wake on LAN](#) (see page 494)
- [Active Directory / LDAP](#) (see page 497)
- [Remote Access](#) (see page 499)
- [Logging](#) (see page 501)
- [Mail Settings](#) (see page 507)
- [Messages to Devices](#) (see page 509)
- [Misc Settings](#) (see page 510)
- [UMS Features](#) (see page 512)

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 Licenses \(see page 398\)](#)
- [Device Licenses \(see page 399\)](#)
- [Deployment - Deploying Licenses through the IGEL UMS \(see page 401\)](#)

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

Select Filter / Reset Filter

IGEL Licenses (17)

Set filters: Category: Add-on Expiration Date: Between May 1, 2020 and Aug 20, 2020

Matching licenses (2)

Order Number	Category	Pack ID	Expiration Date
69-4578788	Add-on	90M-CDHOP	Jun 5, 2020
69-3467788	Add-on	TER-WOLRE	Jun 4, 2020

Hardware

00E0C51C5087

To get an overview that is suitable for your needs, you can filter the display of existing licenses. A maximum of 20,000 licenses can be displayed.

You can create a filter by combining several criteria or create a separate filter for each criterion. When you have created several filters, you can remove each one separately.

- ▶ To configure a filter, click **Select filter**.
- ▶ To remove all existing filters, click **Reset filter**.

The following criteria are available:

Category

Possible options:

- "All": No selection of categories is made.

- "Maintenance": Selects maintenance licenses.
- "Subscription": Selects subscription licenses.
- "Add-on": Selects add-on licenses.
- "Evaluation": Selects evaluation licenses.

Order Number: Selects all licenses which belong to the given order number.

Pack ID: Selects all licenses which belong to the Product Pack with the given Product Pack ID.

Expiration Date: Selects the licenses with the given expiration date.

Possible options:

- "All"
- "Date range"
- "Date"
- "Endless"

Unit ID: Selects the licenses that are assigned to the device with the given unit ID. The unit ID can be selected from the structure tree by clicking .

Table Columns

Order Number: Order number under which the license was ordered

Category: Category to which the license belongs; possible categories: "Maintenance", "Subscription", "Add-on" or "Evaluation"

Pack ID: ID of the Product Pack to which the license belongs

Expiration Date: Expiry date of the license

Hardware

Here, you can view device lists or export them for the Igel Licensing Portal (ILP).

Export unit ID list: Opens the export wizard.

Device lists: Opens the end device list with a filter option.

Deployment - Deploying Licenses through the IGEL UMS

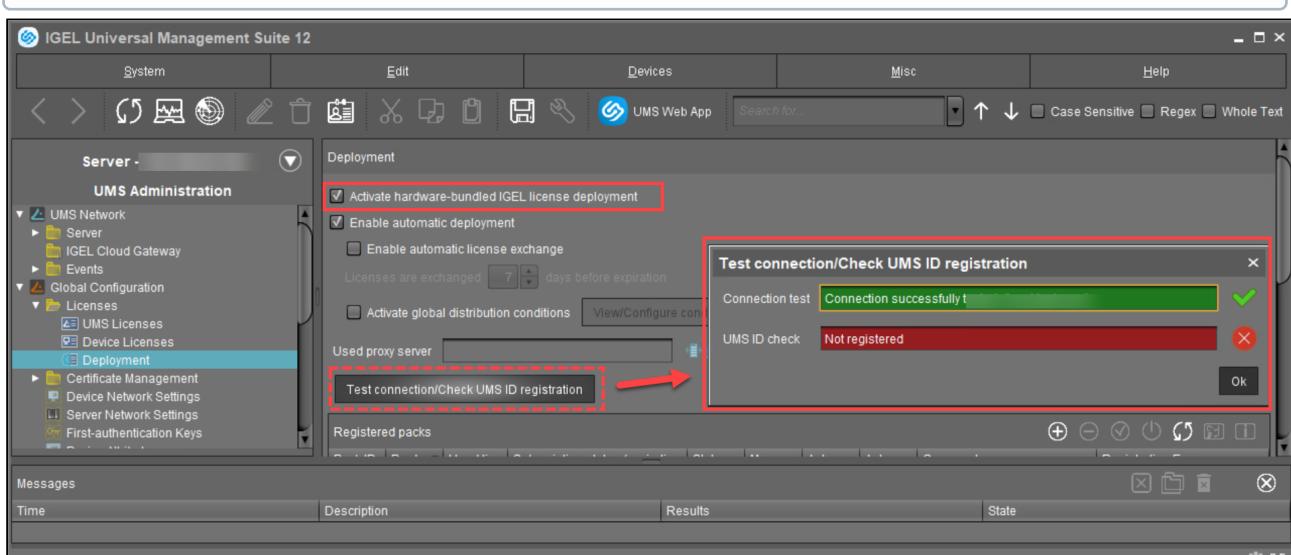
Here, you can enable and configure the automatic deployment of licenses by the IGEL Universal Management Suite (UMS). The automatic license deployment includes licenses for OSC/UDC3, UMA and UD Pocket. Once commercially available, the UMS can also deploy hardware-bundled IGEL licenses automatically.

Menu path: **UMS Console > UMS Administration > Global Configuration > Licenses > Deployment**

Hardware-Bundled IGEL License Deployment

A hardware-bundled IGEL license is purchased together with hardware manufactured by an IGEL Hardware Partner. This type of license, once commercially available, will be a COSMOS PAS (Platform Access Subscription) which is deployed based on the serial number of the device it is sold with. The license can be deployed automatically through the UMS or manually through the IGEL Licensing Portal (ILP). The license can be separated from its hardware and deployed on a different device.

- i Once commercially available, the hardware-bundled deployment function is available in UMS 12.2.120 or higher and for devices with version 11.08.440 / 12.2.0 or higher.



Activate hardware-bundled IGEL license deployment

- Hardware-bundled licenses are automatically deployed through the UMS.
- Hardware-bundled licenses are not deployed through the UMS; manual deployment is needed. (Default)

- i For the automatic hardware-bundled license deployment to work, the UMS ID needs to be registered in the IGEL Licensing Portal (ILP). To verify the registration, click **Test connection/Check UMS ID registration**.

Automatic License Deployment

- i** As of UMS 12, demo licenses for IGEL OS 12 and IGEL OS 11 devices are also supported by Automatic License Deployment.

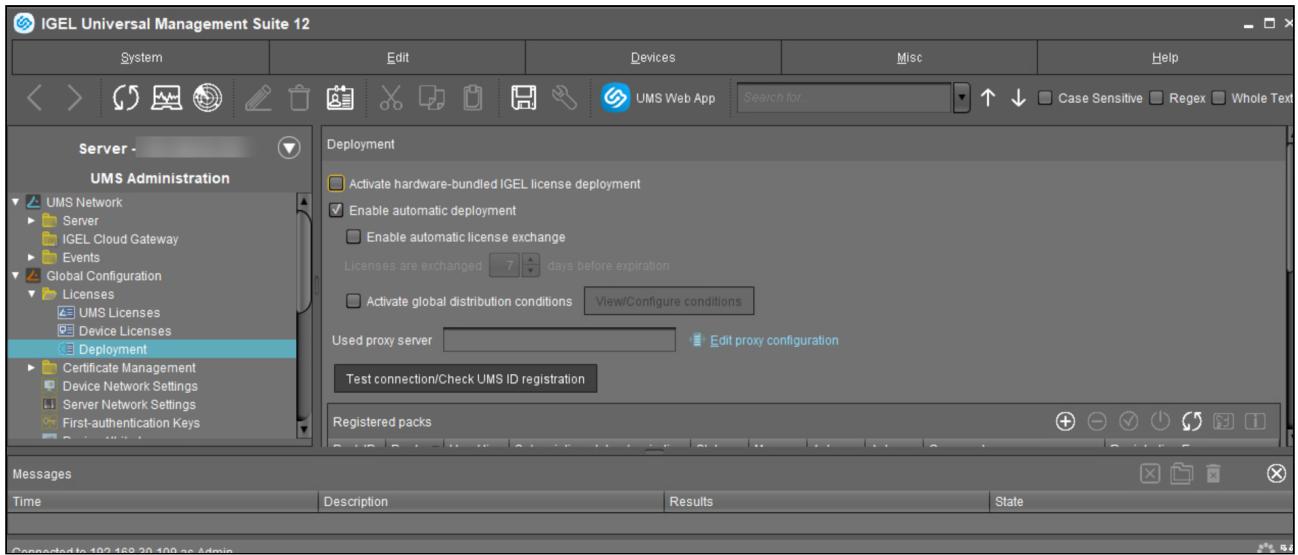
Automatic license deployment requires a connection between the UMS and the IGEL license server as well as the IGEL update server. This connection can be established via a proxy.

For details about the process of automatic license deployment, see [Intervals for Automatic License Deployment](#).

- i** 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.

- i** 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. (Default)

Enable automatic license exchange

- The automatic exchange of expiring device licenses is activated. If the current Product Pack was not renewed and the current device license expires, a device will be licensed from another Product Pack. This means it will be checked if a Product Pack with a later expiration date is registered in the UMS (see "Registered Packs" below), and in this case, the new licenses from this Product Pack are distributed to the devices. Old licenses will not be removed from the devices.

Specify when the new licenses should be deployed to the devices under **Licenses are exchanged [number] days before expiration**.

- The automatic exchange of expiring device licenses is disabled. (Default)

Licenses are exchanged [number] days before expiration

Defines how many days before the expiration date a new license should be deployed. (Default: 7)

Activate global distribution conditions

- Only devices that fulfill the conditions defined under **View / Configure conditions** are considered for the automatic license deployment. These conditions apply globally to the automatic license deployment. However, you can still configure pack-specific distribution conditions (see "Registered Packs" below).

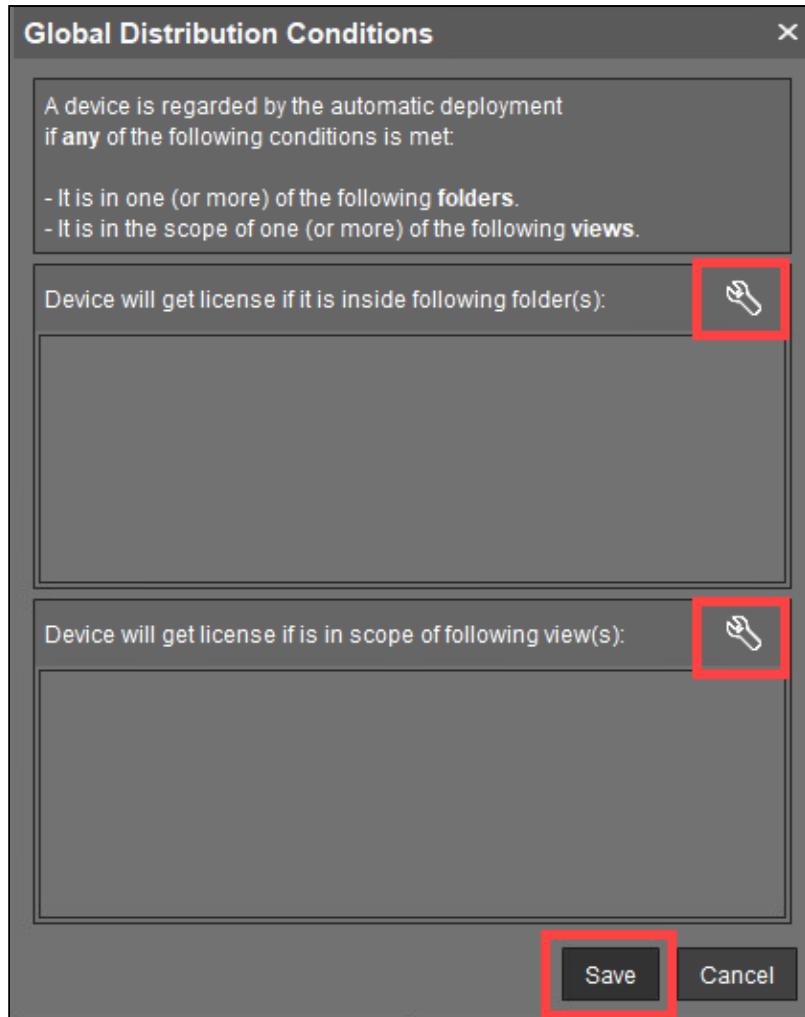
i Global Distribution Conditions vs. Pack-specific Distribution Conditions

The global distribution conditions specify which devices are generally considered for the automatic license deployment. This set of devices can further be limited by the pack-specific distribution conditions. Thus, pack-specific distribution conditions are an additional restriction to the global distribution conditions. This also means if a device has already been excluded by the global distribution conditions, it cannot be "added" to the automatic license deployment by the pack-specific distribution conditions.

- Global distribution conditions are disabled. (Default)

View / Configure conditions

Opens a dialog allowing you to select one or several directories or views as global distribution conditions:



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. Note that this proxy will also be used for all IGEL Cloud Services, including IGEL Onboarding Service, IGEL Insight Service, IGEL App Portal as well as for UMS as an Update Proxy.

- ⓘ Under **UMS Administration > Global Configuration > Proxy Server**, one or more proxies must be configured; see [Proxy Server](#) (see page 479).

Possible options:

- **No proxy server:** No proxy server will be used.

- **Use default proxy server:** The default proxy server defined under [Proxy Server](#) (see page 479) will be used.
- **Use selected proxy server:** A server from the **Configured Proxy Servers** list can be selected.

Test connection/Check UMS ID registration

Tests the connection between UMS or the proxy and the IGEL license server as well as the IGEL update server (<http://fwu.igel.com/>) and verifies if the UMS ID is registered in the IGEL Licensing Portal (ILP).

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 Packs. The current information will be obtained from the license server
	Shows and configures the distribution conditions for the selected Product Pack. For more information, see Configuring the Distribution Conditions .
	Show Product Pack details: <ul style="list-style-type: none"> • 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 period):** 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**
- **Automatic Distribution Condition:** Configures the distribution conditions for the selected Product Pack. For more information, see Configuring the Distribution Conditions.
- **Comment:** Product Pack comments created in the IGEL License Portal
- **Registration Error:** If the registration of the 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

If the action is connected to a hardware-bundled IGEL license, this is indicated in the action description with a "(OEM)".
Example: Deploy Workspace Edition license (OEM)

- **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

Certificate Management

Menu path: **UMS Administration > Global Configuration > Certificate Management**

Here, you can manage certificates for communication with endpoint devices, for communication over the Web Port (default: 8443), and for communication with the IGEL Cloud Gateway (ICG).

- [Device Communication](#) (see page 408)
- [Web](#) (see page 411)
- [Cloud Gateway](#) (see page 413)

Device Communication

In the section **Device Communication**, you can manage certificates for the communication between the IGEL Universal Management Suite (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.

No Support

Certificate chains and expired certificates cannot be imported. Certificates that use the MD5 algorithm are also not supported.

Menu path: **UMS Administration > Global Configuration > Certificate Management > Device Communication**

-  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 **Device Communication**, 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 of a key pair, generation of a new key pair, deletion, activation/deactivation of a certificate, changes of a certificate's priority), a new network token is automatically generated and you will have to define a location in which the new network token should be stored. The changes are then automatically synchronized within a HA network, and no restart of the IGEL RMGUIServer/igelRMserver services is required.

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 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.



Using certificates with SHA1 signature algorithms is NOT recommended because of security reasons.

Supported Keystore Types

The following keystore types are supported: JCEKS, JKS, PKCS#12, BKS-V1, BKS, UBER, and BCFKS.



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. 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.

Web

Menu path: **UMS Administration > Global Configuration > Certificate Management > Web**

Overview

Here, you can manage the certificates for communication via the Web Port (default: 8443).

The Web Port is used for the following tasks:

- Device management and communication for devices with IGEL OS 12
- Provide data for the endpoint devices (WebDAV etc.)
- Provide data for other servers (High Availability; WebDAV etc.)
- Provide data for the UMS Web App
- Provide an entry point for IMI and WebStart

Use

- UMS Web App: Providing the browser with the certificate; see [UMS Web App: The Browser Displays a Security Warning \(Certificate Error\)](#)
- If you need to use an alternative certificate chain instead of the pre-installed one, see [Using Your Own Certificates for Communication over the Web Port \(Default: 8443\)](#)

 New root web certificates are deployed to IGEL OS 12 devices on reboot, see the section "If You Exchange a Root Web Certificate for IGEL OS 12 Devices" under [Using Your Own Certificates for Communication over the Web Port \(Default: 8443\)](#).

Possible Actions



Open the dialog **Change Automatic Renewal Setting** to toggle

automatic certificate renewal.

The private key of the parent certificate (root CA or intermediate CA) must be known. The renewed certificate is assigned to the servers automatically.

Possible options:

- **ACTIVATE automatic renewal:** The end certificates in use will be renewed according to the number specified in **Renew a used end certificate [number] days ahead of its expiration date**.
- **DEACTIVATE automatic renewal:** The end certificates will not be renewed automatically.



Create a root certificate.



Create a signed certificate from the CA certificate (root or intermediate) that is currently selected.



Remove the selected certificate from the UMS. Only certificates that are not currently in use can be removed.



Renew the selected certificate; the dialog **Create signed certificate** is opened.

All settings except the expiry date (**Valid until**) can be left unchanged. The public key of the parent certificate (root CA or intermediate CA) must be known. Also, the expiry date of the parent certificate must be later than the new expiry date for the end certificate.



Show the content of the selected certificate.



Import a root CA certificate.



Import a signed certificate for which the currently selected certificate is a parent certificate (root CA or intermediate CA).



Import the decrypted private key for the selected certificate.



The private key is encrypted again when saved into the UMS Database.



Import a certificate chain from a keystore.



Export the certificate and its child certificates as a certificate chain to a keystore.



Assign the selected certificate to one or more servers. For more information, see [Using Your Own Certificates for Communication over the Web Port \(Default: 8443\)](#).

Cloud Gateway

Menu path: **UMS Administration > Global Configuration > Certificate Management > Cloud Gateway**

Overview

Here, you can manage the certificates for the communication between the IGEL Cloud Gateway (ICG) and the endpoint devices.

For details of how to set up all components for a connection to the ICG, read Installation and Setup.

Use

- Renewing a Signed Certificate for the ICG
- Exchanging the Root Certificate for ICG

Possible Actions



Create a root certificate.



Import a root CA certificate.



Create a signed certificate from the CA certificate (root or intermediate) that is currently selected.



Remove the selected certificate from the UMS. Only certificates that are not currently in use can be removed.



Export the selected end certificate and its complete certificate chain to a keystore in the IGEL Cloud Gateway keystore format.



Show the content of the selected certificate.



Navigate to an IGEL Cloud Gateway that is using the selected certificate.

Generate root certificate

Display name: Name in the root certificate (common name, CN).

Your organization: Organization, company, government agency.

Your locality (or random identifier): 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 20 years)

Import root certificate

The file selection window opens, allowing you to select the certificate file.

Create a signed certificate

Display name: Name in the certificate (common name, CN).

Your first and last name: Name of the certificate holder.

Your organization: Organization, company, government agency.

Your locality (or random identifier): 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:

Expiring date	Status	Used
Apr 13, 2027 10:38:00 AM	✓	
Apr 13, 2018 10:38:47 AM	✗	
Apr 13, 2018 10:48:27 AM	✓	
Apr 18, 2018 10:12:12 AM		Subject and issuer of certificate are equal. This is not a valid certificate!

Your two-letter country code: ISO 3166 country code, e.g. DE for Germany.

Host name and/or IP of certificate target server: 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 cannot be used by the ICG.
- **End Entity:** The certificate can be used by the ICG, but it cannot be used to sign other certificates.

Context menu (root certificate)

Create signed certificate: Collects certificate data and signs them with the selected root certificate.

Import signed certificate: Imports a certificate 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`

Remove certificate: Deletes the certificate from the UMS.

Export certificate chain in the IGEL Cloud Gateway Keystore format: Produces a file for ICG installation program.

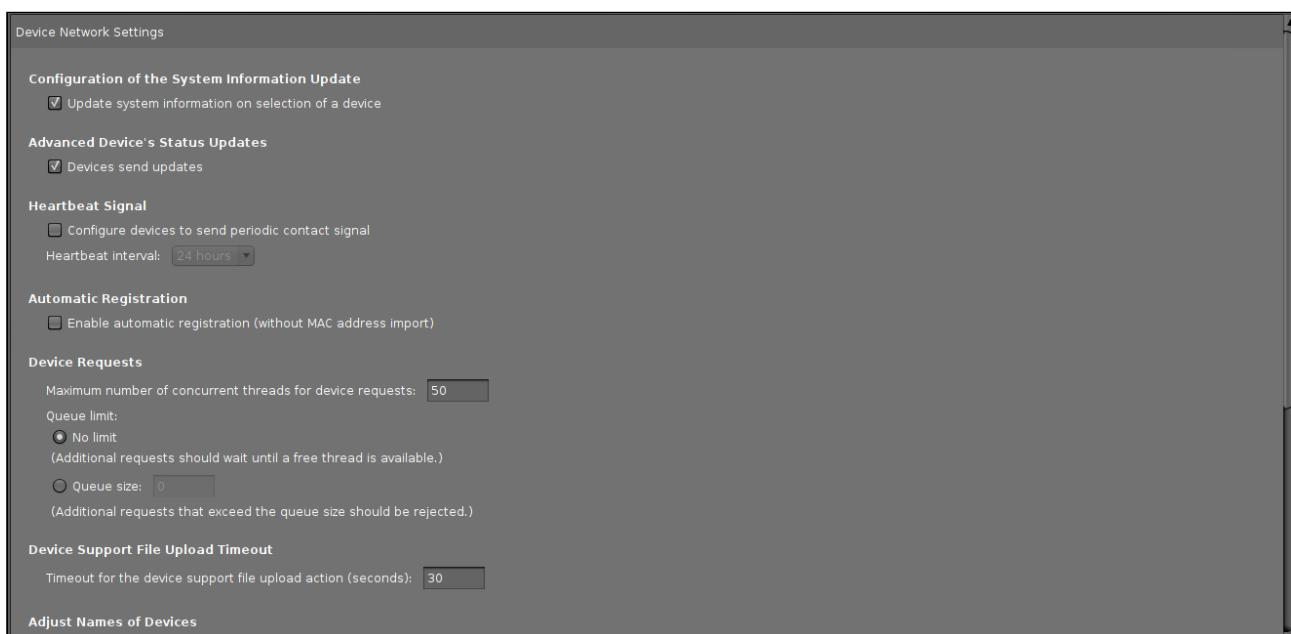
Export certificate: Exports certificate file.

Show certificate content: Shows the content of the certificate in a text window.

Device Network Settings for the IGEL Universal Management Suite (UMS)

Here, you can change the settings for the communication between the IGEL Universal Management Suite (UMS) and the devices that are controlled by the UMS.

Menu path: **UMS Administration > Global Configuration > Device Network Settings**



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.

Devices send updates

This setting defines if the devices report changes to the data shown under **Advanced System Information**; see [View Device Information in the IGEL UMS](#) (see page 288).

- The devices report changes in their advanced status. (Default)
- The only thing that is displayed is whether a device is online or offline.

Configure devices to send periodic contact signal

- The devices send a regular heartbeat signal according to the setting of **Heartbeat interval**.

Heartbeat interval

The interval between each heartbeat signal

Possible values: 1 ... 6 hours, 12 hours, 24 hours

For more information, see Monitoring Device Health and Searching for Lost Devices.

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 \(see page 173\)](#).

- 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)

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).

Queue limit

- **No limit:** When the **Maximum number of concurrent threads for device requests** is reached and another device sends a request, the UMS responds to the device that the request will be accepted when a free thread is available. The current request is put into a queue with an infinite size. (Default)
- **Queue size:** When the **Maximum number of concurrent threads for device requests** is reached and another device sends a request, the UMS responds to the device that the request will be accepted when a free thread is available. The current request is put into a queue whose size is defined here. When the queue size is reached and another request comes in, this request is rejected. Default 0

Timeout for the device support file upload action (seconds)

 **Rolling Release Info: UMS 6.10.110**

This parameter is available with UMS version 6.10.110 or higher.

This timeout should be adapted if the upload of the support file to the UMS should fail. The reason for this failure might be very large log file sizes and/or slow hardware.

The unit is seconds; the value range is 30 to 9000. Default: 30

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. If this setting is enabled, the maximum length of the device name is restricted to 15 characters.

 If you enable **Naming Convention**, the input of non-standard characters for **Prefix** will be limited.

- The network name of the device will not be set to the UMS-internal name. (Default)

Enable naming convention for new devices

- 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

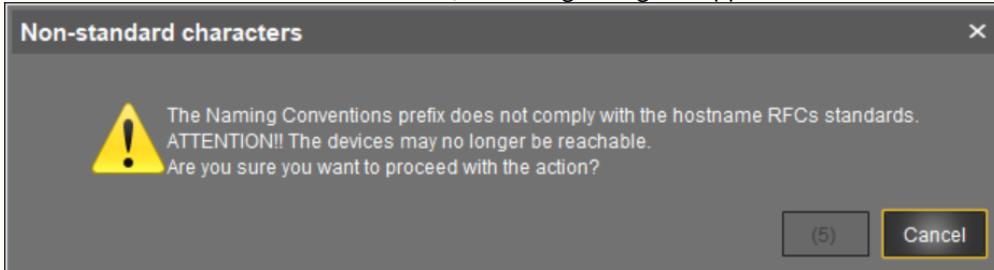
Prefix for automatically allocating names. The prefix can be between 1 and 7 characters long; if no prefix is specified, the default prefix "UMS-" will automatically be added.

 If **Adjust network name if UMS-internal name has been changed** has been enabled, the input of non-standard characters is limited. Example: "&", "/", "!", etc. will not be accepted.

To comply with the network naming standard, a prefix

- must contain letters or numbers: "A" to "Z", "a" to "z", or "0" to "9".
- can start or end with a letter or a number: "A" to "Z", "a" to "z", or "0" to "9".
- can contain a dash "-" but must not start with it.

If **Adjust network name if UMS-internal name has been changed** is enabled after a non-standard character has been entered under **Prefix**, a warning dialog will appear:



Confirm the dialog after the countdown only if you are sure that your devices will be reachable with new network names based on the prefix entered.

Identifier

i Available with UMS 12.02.120 or Higher

This parameter is available with UMS 12.02.120 or higher.

Possible options:

- **Sequential Number:** The device name will be made unique by a sequential number that is provided by the UMS.
- **Unit ID:** The device name will be made unique by the device's unit ID or a part of it.
 - **Use only the last [N] characters**
 - Only the last N characters of the unit ID are used.
 - The complete unit ID is used.
- **Serial Number:** The device name will be made unique by the device's serial number or a part of it.
 - **Use only the last [N] characters**
 - Only the last N characters of the serial number are used.
 - The complete serial number is used.

Minimum digits

i Note for UMS 12.02.120 or Higher

This setting is only available if the **Identifier** is set to **Sequential Number**.

A minimum number of digits for the sequential number added to the prefix. 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.

- i** If the number of devices exceeds the value defined here, the numbering will simply continue without an error occurring.

Suffix

i Available with UMS 12.02.120 or Higher

This parameter is available with UMS 12.02.120 or higher.

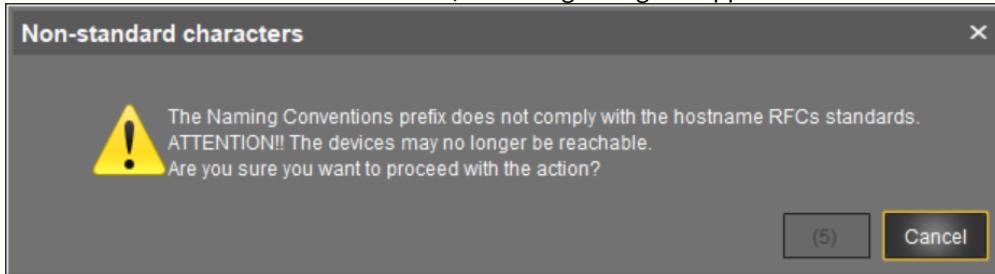
Suffix for automatically generated names. The suffix can be between 1 and 7 characters long;

⚠ If Adjust network name if UMS-internal name has been changed has been enabled, the input of non-standard characters is limited. Example: "&", "/", "!", etc. will not be accepted.

To comply with the network naming standard, a suffix

- must contain letters or numbers: "A" to "Z", "a" to "z", or "0" to "9".
- can start or end with a letter or a number: "A" to "Z", "a" to "z", or "0" to "9".
- can contain a dash "-" but must not end with it.

If **Adjust network name if UMS-internal name has been changed** is enabled after a non-standard character has been entered under **Suffix**, a warning dialog will appear:



Confirm the dialog after the countdown only if you are sure that your devices will be reachable with new network names based on the suffix entered.

Preview

Displays the current naming convention based on an example.

Rename all devices

All devices registered in the UMS will be renamed in accordance with the naming convention.

Rename and renumber all devices

All devices will be renamed in accordance with the naming convention. All names will be reallocated. If **Identifier** is set to **Sequential Number** or your UMS version is 12.02.100 or lower, the following applies: If numbers have become free because devices were taken out of service, these numbers will be used for other devices.

Server Network Settings in the IGEL UMS

In this area of the IGEL Universal Management Suite (UMS) Console, you can configure settings for the online check for your devices, parameters for the device scan, activate the Distributed UMS feature, specify the Cluster Address for the load distribution of specific device requests, etc.

Menu path: **UMS Console > UMS Administration > Global Configuration > Server Network Settings**

The screenshot shows the UMS Administration interface with the 'Server Network Settings' page selected. The left sidebar lists various configuration categories. The main panel contains several sections:

- Online Check Parameters:** Includes checkboxes for 'Disable online check' and 'Specify online check port (UDP)', and a slider for 'Online Check Response Timeout' set to 1000 ms.
- Scheduled Jobs:** Includes a checkbox for 'Scheduled jobs never expire' and a slider for 'Expiration time for scheduled jobs' set to 40 minutes.
- Scan Parameters:** Includes a slider for 'Timeout (ms)' set to 6000, a broadcast IP field (255.255.255.255), and a checkbox for 'Specify scan reply port (UDP)'.
- Cluster Address:** Includes a checkbox for 'Enable common cluster address for all UMS servers' and a field for 'Devices and other external services can reach the UMS cluster at' with a 'Set Address' button.
- OS 12 device enrollment address:** Includes a checkbox for 'Enable customize OS 12 device enrollment address' and a field for 'Devices can reach the enrollment service at' with a 'Set Address' button.
- Export Client Certificate Chain:** A 'Export' button.
- UMS High Availability / Distributed UMS:** Includes a checkbox for 'Distributed UMS enabled (restart of UMS Servers needed on change)'.

Online Check Parameters

Disable online check

- The online check is disabled.
- The online check is enabled. (Default)

Online Check Response Timeout

Specifies how long in milliseconds the system will wait for a response to an online status query message. The UMS 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”. Minimum: 100; maximum: 10000; default: 1000.

Changed Values on Update

The maximum and minimum value and the new default value have been introduced with UMS 6.04.100. If you update to version 6.04.100 from an older version, the value will be handled as follows:

- If the value was between 100 and 10.000, it remains unchanged.
- If the value was lower than 100, it is changed to 100.
- If the value was the old default value of 100, it is changed to the new default value 1.000.
- If the value was higher than 10.000, it is changed to 10.000.

Specify online check port (UDP)

- You specify the port to which the devices respond if the UMS checks their online status.
 The UMS will select any free port. (Default)

Scheduled Jobs

Scheduled jobs never expire

- No time limit for scheduled jobs. (Default)

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)

- You specify the port to which the devices respond if the UMS scans for devices.

- The UMS will select any free port. (Default)

Cluster Address

In the IGEL UMS High Availability (HA) and Distributed UMS installations, you can use **Cluster Address** to balance the incoming traffic. If no **Cluster Address** is set, the **Public Address** is used for HTTPS requests from devices (if defined). For more information on the Public Address, see [Server - View Your IGEL UMS Server Information \(see page 388\)](#).



- The Cluster Address is only for communication via the [web server port \(see page 552\)](#) (default: 8443).
- SSL can be terminated at the reverse proxy / external load balancer or at the UMS Server. For more on Reverse Proxies, see [IGEL Universal Management Suite Network Configuration](#).

Enable common cluster address for all UMS servers

- The address and port defined by clicking **Set Address** are used for the following HTTPS requests from devices:
- file transfer from the UMS to IGEL OS 11 devices
 - onboarding and device communication of IGEL OS 12 devices
 - app download for IGEL OS 12 devices if **Download from UMS** is set in the **UMS Web App > Apps >**  **Settings** > **UMS as an Update Proxy**

The **Cluster Address** does NOT affect:

- download of firmware updates for IGEL OS 11 devices
- device communication with the UMS Servers (IGEL OS 11 devices)
- internal communication between the UMS Servers (incl. the WebDAV synchronization between the UMS Servers)
- IGEL Cloud Gateway communication, i.e. devices connected to the UMS via ICG do not use the Cluster Address

- The Cluster Address is not used. (Default)

Devices and other external services can reach the UMS cluster at

The address defined by the following parameters. The parameters appear in a dialog when you click **Set Address**:

- FQDN or IP**

FQDN of your external load balancer / reverse proxy such as NGINX, Citrix Netscaler, etc. The maximal length is restricted to 255 characters.

- i** When a reverse proxy / load balancer is assigned to the cluster address, it can handle both external and internal network traffic. For information on Cluster Address and FQDNs, see also Troubleshooting: Error 38 during the Onboarding of an IGEL OS 12 Device.

- **Port**

Port of your external load balancer / reverse proxy

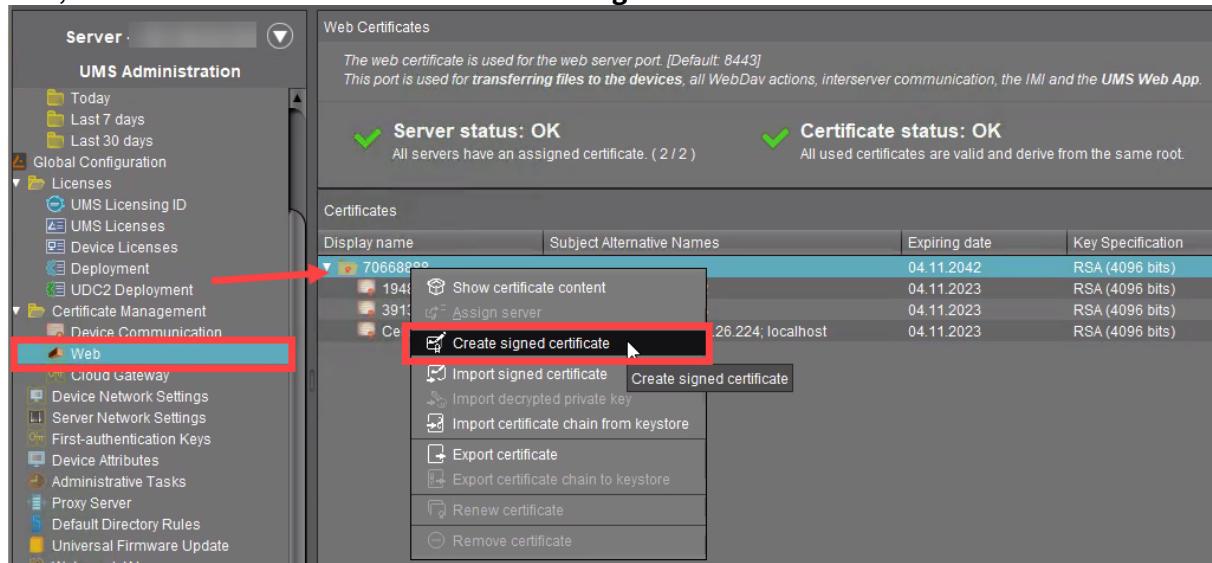
Configure a Web Certificate for All Servers...

If you have a UMS HA or Distributed UMS installation and configured the **Cluster Address**, you must define a web certificate for all servers:

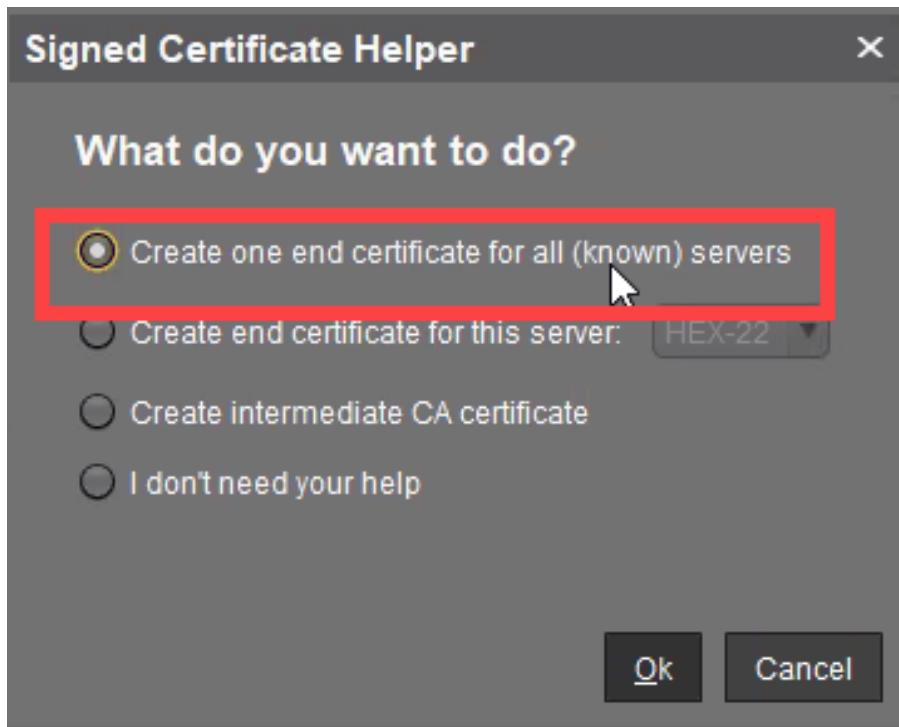
- The certificate must contain the cluster address and all server addresses
- The certificate must be assigned to all servers

To define a web certificate for all servers, proceed as follows:

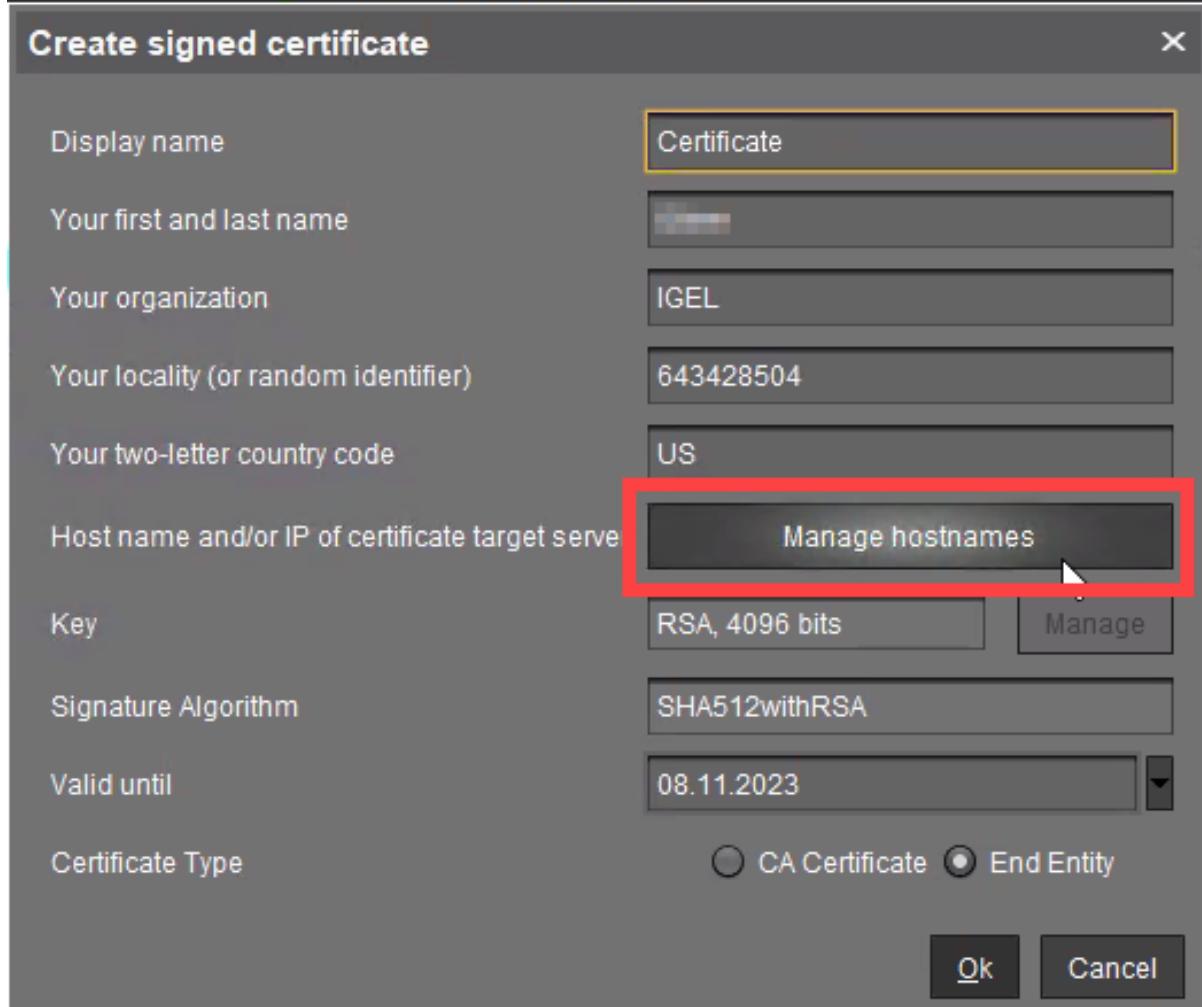
1. In the **UMS Console > UMS Administration > Global Configuration > Certificate Management > Web**, select the root certificate and click **Create signed certificate** in the context menu.



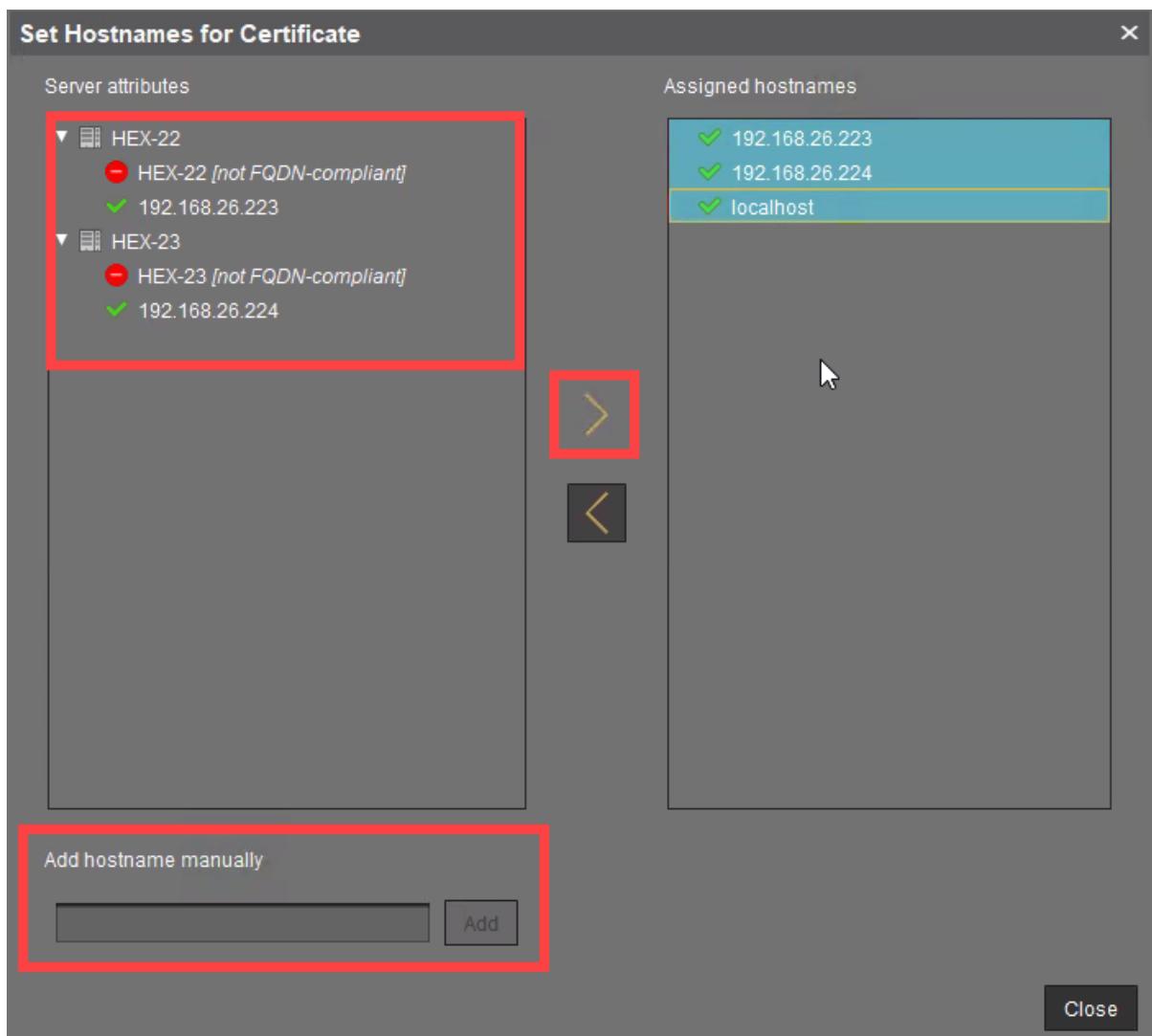
2. In the **Signed Certificate Helper** dialog, select **Create one end certificate for all (known) servers**.



3. In the **Create signed certificate dialog**, click **Manage hostnames**.



4. In the dialog **Set Hostnames for Certificate**, check if Cluster Address, "localhost", all IP addresses, and FQDNs (Fully Qualified Domain Names) under which your servers are reachable are displayed under **Assigned hostnames**. If not, add the missing IP addresses and FQDNs under **Add hostname manually**.



5. Close the dialog **Create Signed Certificate** with **Ok**.

The signed server certificate is created.

6. Select the created certificate and click **Assign server** in the context menu.

The screenshot shows the UMS Administration interface. On the left, there is a navigation tree with several collapsed categories like 'UMS Licensing ID' and 'UMS Licenses'. The 'Web' category is expanded, and its sub-items are listed. A red box highlights the 'Web' category. To its right is a table titled 'Certificates' with columns: Display name, Subject Alternative Names, Expiring date, Key Specification, and Signature. There are four entries in the table. The fourth entry, 'Certificate' (with values '192.168.26.223; localhost' and '04.11.2023'), has a context menu open over it. The context menu items are: 'Show certificate content', 'Assign server' (which is highlighted with a red box), 'Create signed certificate', 'Import signed certificate', 'Import decrypted private key', 'Import certificate chain from keystore', 'Export certificate', 'Export certificate chain to keystore', 'Renew certificate', and 'Remove certificate'. Below the table, there is a detailed view for 'HEX-23' with fields like Host, Process ID, Cluster ID, Version, Device Communication Port, and Public Address. A red box highlights the 'Assign server' option in the context menu.

7. Assign the certificate to all servers.

The screenshot shows the 'Assign Server(s) to Certificate' dialog box. It has two main sections: 'Available Servers' on the left and 'Assigned Servers' on the right. In the 'Available Servers' section, 'HEX-22' and 'HEX-23' are listed. A red box highlights both of them. In the center, there are two large yellow arrows: a right-pointing arrow above a left-pointing arrow. At the bottom right of the dialog box, there are 'Ok' and 'Cancel' buttons, with 'Ok' being highlighted by a red box.

OS 12 Device Enrollment Address

- i** This configuration allows the separation of the device onboarding endpoint from the Websocket (Management) endpoint. This option can be required for implementing a reverse proxy / external load balancer without optional Client Certificate verification option, like Azure Application Gateway. For more information, see [Azure Application Gateway: Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading](#).

Enable customize OS 12 device enrollment address

- The address and port defined by clicking **Set Address** are used for device onboarding.
- The Cluster Address is used for device onboarding in the reverse proxy / external load balance configuration. (Default)

Devices can reach the enrollment service at

The address defined by the parameters accessed by clicking **Set Address**:

- **FQDN or IP**

FQDN of the configured listener for device onboarding.

- **Port**

Port of the configured listener for device onboarding.

- **Path Prefix**

Path Prefix to the EST service. The defined path in the EST protocol is ".well-known/est". This prefix should be used to customize it. For example: `/device-connector/device/.well-known/est`
This value must only be set when the Path was customized. Default is empty.

Export Client Certificate Chain

Click **Export** to export the Client Certificate Chain.

- i** You need the Client Certificate Chain to configure the reverse proxy / external load balancer. For more information, see [IGEL Universal Management Suite Network Configuration](#).

UMS High Availability / Distributed UMS

Distributed UMS enabled (restart of UMS Server needed on change)

- The standalone UMS Servers will work just as if they were installed as a High Availability environment if connected to the same external database. Messages between the UMS Servers will be transferred via database entries. For detailed information on the Distributed UMS, see [IGEL UMS Installation](#) (see page 13).

For how to install the Distributed UMS or extend an existing standard UMS installation to the Distributed UMS, see [Installing the Distributed IGEL UMS](#) (see page 59).

- ⓘ If you have a UMS High Availability installation, the checkbox **Distributed UMS enabled (restart of UMS Server needed on change)** will not be present.

- The Distributed UMS is disabled. (Default)

- ⚠ If you activated the Distributed UMS feature and have multiple UMS Servers, take care in case you decide to disable the feature. If the Distributed UMS feature is deactivated but more than one UMS Server is using the same database, no synchronization will be done between the UMS Servers.

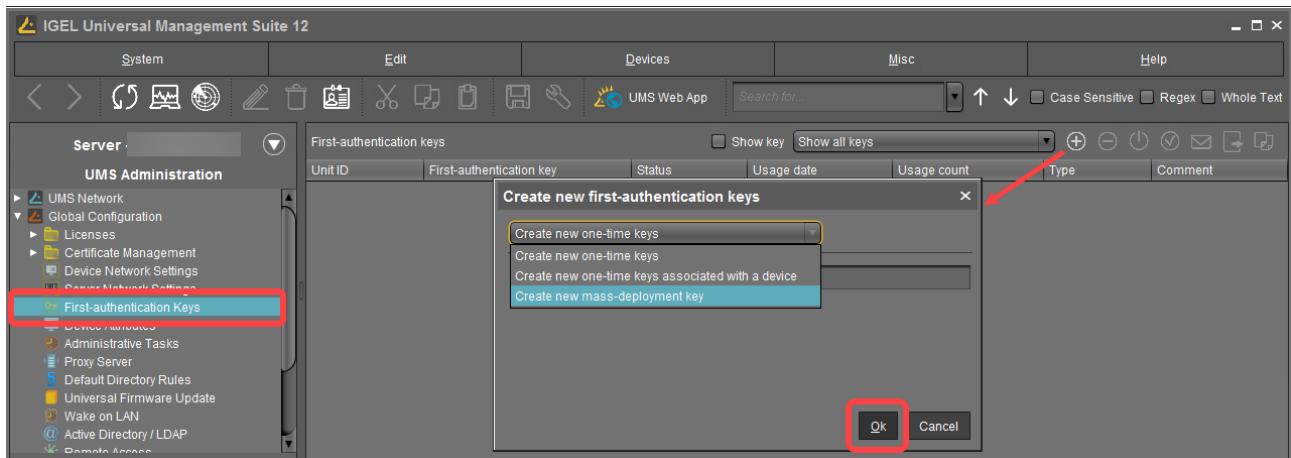
First-authentication Keys

Menu path: **UMS Administration > Global Configuration > First-authentication Keys**

	Create new first-authentication keys
	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 keys 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.

 It is not possible to create more than one first-authentication key with the same password.

Managing Device Attributes for IGEL OS Devices

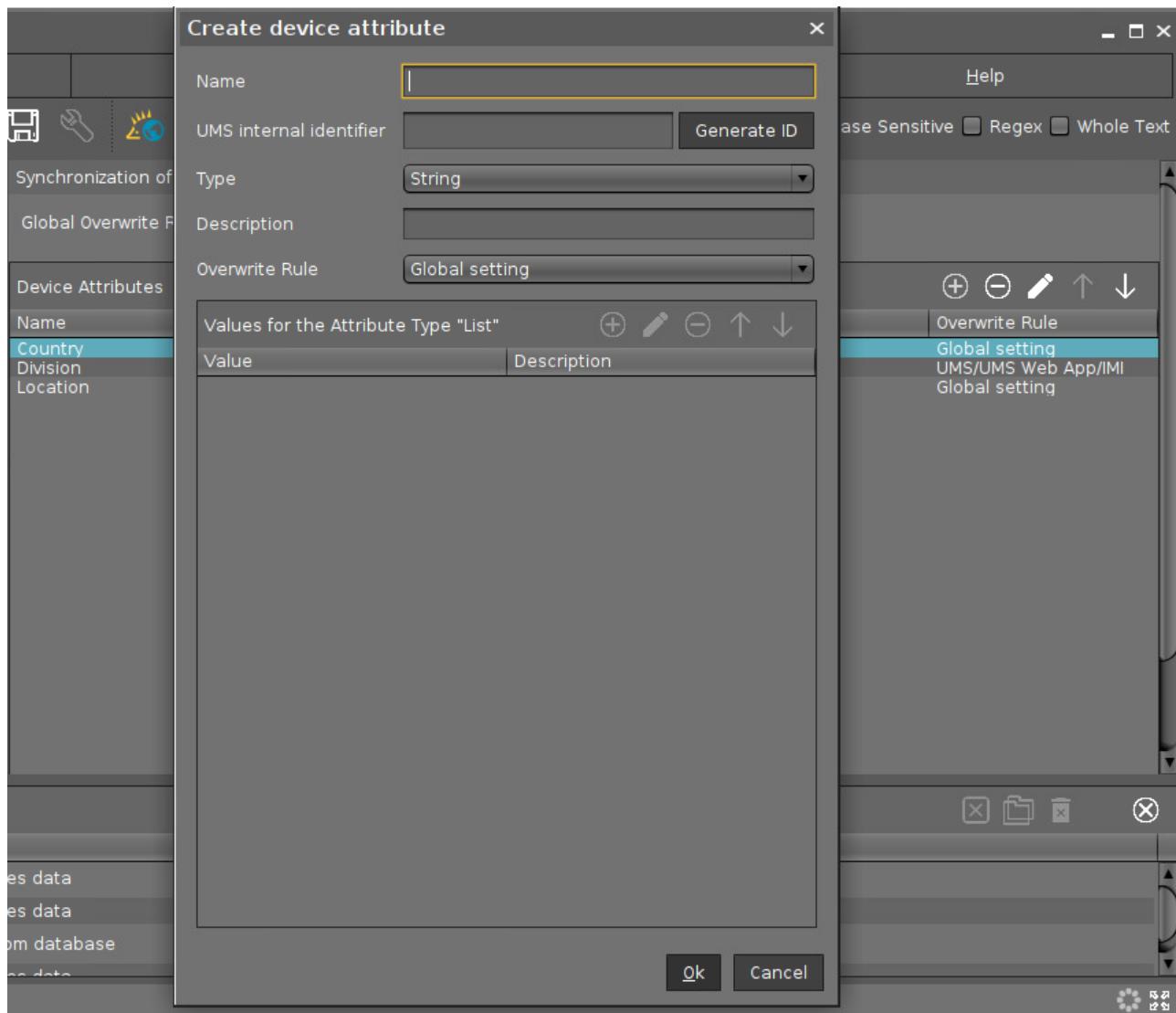
In this area, you can set up additional attributes for IGEL OS devices using the IGEL Universal Management Suite (UMS). These attributes are displayed together with the default device attributes, see [View Device Information in the IGEL UMS \(see page 288\)](#). They can also be used in:

- Searches in the [UMS Console \(see page 205\)](#) and the UMS Web App
- [Views \(see page 328\)](#)
- [Default directory rules \(see page 481\)](#)

Known Limitations

Device attributes can only be managed within the UMS; there is no export or import facility.

Menu path: **UMS Administration > Global Configuration > Device Attributes**



► Click on to set up a new device attribute:

Global Overwrite Rule

This parameter is relevant for devices with IGEL OS 11.07 or higher.

Defines the default overwrite rule for those device attributes whose overwrite rule is set to **Global setting**. The overwrite rule defines how the values of device attributes can be set and changed.

Possible options:

- **UMS/UMS Web App/IMI:** Only the UMS can set and change the values of the device attributes. This is true regardless of which interface is used for UMS control, i.e. UMS Console, UMS Web App, or IGEL Management Interface (IMI).
- **Devices:** Only the devices can set and change the values of the device attributes. See also Managing IGEL OS Devices by Device Specific Data - What Device Attributes Can Do for You.
- **All:** Both the UMS and the devices can set and change the values of the device attributes. New values overwrite older values.

Name

Display name of the attribute

UMS internal identifier

This identifier is required for creating/editing views or editing searches in text mode (see [How to Create a New View in the IGEL UMS \(see page 333\)](#)) and also for enabling the devices to set and change attribute values. If you do not plan to use any of these features, you can leave this field empty.

You can either generate the internal identifier automatically by clicking **Generate ID** or specify it manually.

- i** The **UMS internal identifier** must start with a lower-case letter. Only the following characters are allowed:
a-z, A-Z, 0-9.

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:
Values for the Attribute Type "List"
 - **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**, you can set the values for the attributes.

The screenshot shows the UMS Administration interface. On the left is a tree view of the UMS structure. In the center, a device named 'td-RD03' is selected. A 'System Information' dialog is open, displaying a table of attributes and their values. One row, 'DeviceAttribute_Subdepartments', is highlighted with a blue background. A red arrow points from this row to a 'Set value' dialog box that is overlaid on the main window. The 'Set value' dialog has a dropdown menu with 'KB' selected. At the bottom right of the dialog are 'Ok' and 'Cancel' buttons.

Attribute	Value
Name	
Site	
Comment	
Department	
Cost Center	
Asset ID	
In-Service Date	
Serial Number	
DeviceAttribute_Subdepartments	

Overwrite Rule

This parameter is relevant for devices with IGEL OS 11.07 or higher.

Defines how the value of this device attribute can be set and changed.

- **Global setting:** The **Global Overwrite Rule** is valid for this device attribute.
- **UMS/UMS Web App/IMI:** Only the UMS can set and change the value of this device attribute. This is true regardless of which interface is used for UMS control, i.e. UMS Console, UMS Web App, or IGEL Management Interface (IMI).
- **Devices:** Only the device can set and change the values of this device attribute. See also Managing IGEL OS Devices by Device Specific Data - What Device Attributes Can Do for You.
- **All:** Both the UMS and the devices can set and change the values of this device attribute. New values overwrite older values.

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 \(see page 567\)](#)), 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. For details, see [Performance Optimizations in IGEL UMS \(see page 78\)](#) and [IGEL UMS Maintenance Tasks \(see page 80\)](#).

Menu path: **UMS Administration > Global Configuration > Administrative Tasks**

Name	Job	Last Execution	Next Execution	Execution Status	Active	Send result as mail
Send notification info	Send notification info...	Feb 8, 2022 6:17 PM	Feb 8, 2022 6:22 PM	failed	✓	
Backup	Create backup	Feb 4, 2022 6:37 PM	Feb 11, 2022 6:37 PM	completed	✓	
Logs	Delete logging data	Feb 7, 2022 1:30 PM	Feb 14, 2022 1:30 PM	completed	✓	
Delete admin task logs	Delete administrative t...	Feb 7, 2022 12:57 PM	Feb 14, 2022 12:57 PM	completed	✓	
Delete process events...	Delete process events	Feb 8, 2022 12:58 PM	Feb 15, 2022 12:58 PM	completed	✓	

Last Execution	Execution Status	Result Message	Processed by
Feb 4, 2022 6:37 PM	completed	Database backup was successfully created.	
Jan 28, 2022 6:37 PM	completed	Database backup was successfully created.	
Jan 21, 2022 6:37 PM	completed	Database backup was successfully created.	
Jan 14, 2022 6:37 PM	completed	Database backup was successfully created.	
Nov 26, 2021 6:37 PM	completed	Database backup was successfully created.	
Nov 19, 2021 6:37 PM	completed	Database backup was successfully created.	
Nov 12, 2021 6:37 PM	completed	Database backup was successfully created.	
Nov 5, 2021 6:37 PM	completed	Database backup was successfully created.	
Oct 29, 2021 6:37 PM	completed	Database backup was successfully created.	
Oct 22, 2021 6:37 PM	completed	Database backup was successfully created.	

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 \(see page 438\)](#)
 - [Remove Unused Firmwares \(see page 441\)](#)

- [Delete Logging Data \(see page 444\)](#)
- [Delete Job Execution Data \(see page 448\)](#)
- [Delete Administrative Task Execution Data \(see page 451\)](#)
- [Delete Process Events \(see page 454\)](#)
- [Delete Devices \(see page 457\)](#)
- [Export View or Advanced Search Result via Mail \(see page 460\)](#)
- [Save View or Advanced Search Results in the File System \(see page 463\)](#)
- [Assign Objects to the Devices of Views or Device Searches \(see page 466\)](#)
- [Detach Assigned Objects from Devices of Views or Device Searches \(see page 469\)](#)
- [Delete Asset Information History \(see page 472\)](#)
- [Send Notification Information via Email \(see page 474\)](#)

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

You can define a scheduled backup of the database as an administrative task.

Menu path: **UMS Administration > Administrative Tasks > Dialog "Create Administrative Task" > Action "Create backup"**

General

Name

Name for the task.

Action

- ▶ Select **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 \(see page 507\)](#).

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 for created backup

Local directory path on the UMS Server in which the backup files are saved.

- i** 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)**
- **Configurations**
- **Transfer files (embedded DB only)**

Server Assignment

- i** The **Server Assignment** settings page is displayed only if you deploy [High Availability or Distributed UMS](#) (see page 13) environment.

Assignment type

Possible options:

- **One server (random)**: The server for this task will be automatically selected from the servers listed under **Assigned servers**. (Default)
- **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

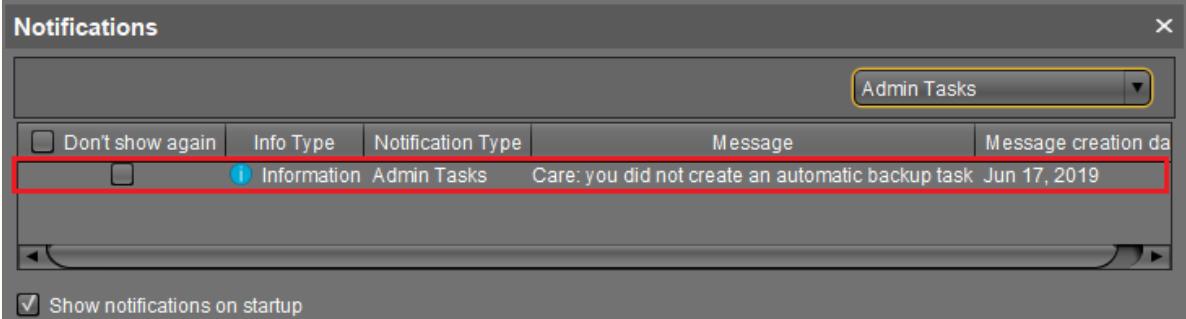
The task will not be executed on the days listed in the public holiday lists selected via  . Further information on the public holiday lists can be found in the menu bar under **Misc > Scheduled Jobs**, see [Menu Bar of the IGEL UMS Console \(see page 185\)](#).

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 \(see page 438\)](#)", 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

You can define the removal of unused firmware as an administrative task. The deletion helps with performance optimization, see [Performance Optimizations in IGEL UMS](#) (see page 78).

- (i) The first firmware that was registered in your UMS installation can not be removed.

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Remove unused firmwares"**

General

Name

Name for the task.

Action

- ▶ Select **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 507).

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 or Distributed UMS** (see page 13) environment.

Assignment type

Possible options:

- **One server (random)**: The server for this task will be automatically selected from the servers listed under **Assigned servers**. (Default)
- **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 in the menu bar under **Misc > Scheduled Jobs**, see [Menu Bar of the IGEL UMS Console](#) (see page 185).

Expiration

Point in time as of which the task will no longer be repeated.

Delete Logging Data

You can define the deletion of UMS message and event logs as an administrative task. The deletion helps with performance optimization, see [Performance Optimizations in IGEL UMS](#) (see page 78).

- ⓘ The logs for [Secure Shadowing](#) (see page 325) as well as [performance logs](#) (see page 502) will not be deleted as a result of this administrative task.

Menu path: **UMS Administration > Administrative Tasks > Dialog "Create Administrative Task" > Action "Delete logging data"**

General

Name

Name for the task.

Action

- ▶ Select **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 507).

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 or Distributed UMS](#) (see page 13) environment.

Assignment type

Possible options:

- **One server (random)**: The server for this task will be automatically selected from the servers listed under **Assigned servers**. (Default)
- **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 in the menu bar under **Misc > Scheduled Jobs**, see [Menu Bar of the IGEL UMS Console \(see page 185\)](#).

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 \(see page 444\)](#)", after the start of the UMS Console, the following notification pop-up will be shown:

Notifications				
<input type="checkbox"/> Don't show again	Info Type	Notification Type	Message	Message creation date
<input type="checkbox"/>	i Information	Admin Tasks	Care: you did not create an automatic backup task	May 22, 2019
<input type="checkbox"/>	i Information	Admin Tasks	Care: you did not create a cleanup task for Delete job execution data	May 22, 2019
<input type="checkbox"/>	i Information	Admin Tasks	Care: you did not create a cleanup task for Delete logging data	May 22, 2019

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

You can define an administrative task to delete the results of Jobs. The deletion helps with performance optimization, see [Performance Optimizations in IGEL UMS](#) (see page 78).

For more information on Jobs, see [Jobs - Sending Automated Commands to Devices in the IGEL UMS](#) (see page 355).

Menu path: **UMS Administration > Administrative Tasks > Dialog "Create Administrative Task" > Action "Delete job execution data"**

General

Name

Name for the task.

Action

- ▶ Select **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 507).

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 or Distributed UMS](#) (see page 13) environment.

Assignment type

Possible options:

- **One server (random):** The server for this task will be automatically selected from the servers listed under **Assigned servers**. (Default)
- **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 in the menu bar under **Misc > Scheduled Jobs**, see [Menu Bar of the IGEL UMS Console \(see page 185\)](#).

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 \(see page 448\)](#)", after the start of the UMS Console, the following notification pop-up will be shown:

Notifications					
	Info Type	Notification Type	Message	Message creation date	
<input type="checkbox"/>	Information	Admin Tasks	Care: you did not create an automatic backup task	May 22, 2019	
<input type="checkbox"/>	Information	Admin Tasks	Care: you did not create a cleanup task for Delete job execution data	May 22, 2019	
<input type="checkbox"/>	Information	Admin Tasks	Care: you did not create a cleanup task for Delete logging data	May 22, 2019	

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 Task Execution Data

You can define an administrative task to delete of the results of a (see page 436) dministrative tasks. The deletion helps with performance optimization, see [Performance Optimizations in IGEL UMS \(see page 78\)](#).

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Delete administrative task execution data"**

General

Name

Name for the task.

Action

- ▶ Select **Delete administrative task 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 \(see page 507\)](#).

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 or Distributed UMS](#) (see page 13) environment.

Assignment type

Possible options:

- **One server (random)**: The server for this task will be automatically selected from the servers listed under **Assigned servers**. (Default)
- **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 in the menu bar under **Misc > Scheduled Jobs**, see [Menu Bar of the IGEL UMS Console](#) (see page 185).

Expiration

Point in time as of which the task will no longer be repeated.

Delete Process Events

You can define the deletion of process events as an administrative task. The deletion helps with performance optimization, see [Performance Optimizations in IGEL UMS](#) (see page 78).

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Delete process events"**

General

Name

Name for the task.

Action

- ▶ Select **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 507).

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 or Distributed UMS \(see page 13\)](#) environment.

Assignment type

Possible options:

- **One server (random)**: The server for this task will be automatically selected from the servers listed under **Assigned servers**. (Default)
- **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 in the menu bar under **Misc > Scheduled Jobs**, see [Menu Bar of the IGEL UMS Console](#) (see page 185).

Expiration

Point in time as of which the task will no longer be repeated.

Delete Devices

You can define an administrative task that deletes specific devices from the UMS database. The devices can be specified through the criteria of a view created in the UMS Console or an advanced search created in the UMS Web App. For example, you can filter for devices that have not been booted for more than a year and then create an administrative task to delete them.

For more information on the advanced search in the UMS Web App, see [Search for Devices in the IGEL UMS Web App](#).

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action Delete devices**

General

Name

Name for the task.

Action

- ▶ Select **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 \(see page 507\)](#).

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

Delete devices of following view / advanced search

View / advanced search which specifies the criteria for deleting devices. The view / advanced search is selected via the  button.

View ID / Advanced search ID

ID of the selected view / advanced search.

Server Assignment

-  The **Server Assignment** settings page is displayed only if you deploy [High Availability or Distributed UMS](#) (see page 13) environment.

Assignment type

Possible options:

- **One server (random)**: The server for this task will be automatically selected from the servers listed under **Assigned servers**. (Default)
- **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 in the menu bar under **Misc > Scheduled Jobs**, see [Menu Bar of the IGEL UMS Console \(see page 185\)](#).

Expiration

Point in time as of which the task will no longer be repeated.

Export View or Advanced Search Result via Mail

You can define an administrative task to export the results of a view or advanced search as a mail attachment.

For more information on the advanced search in the UMS Web App, see [Search for Devices in the IGEL UMS Web App](#).

- ⓘ In order for emails to be sent, the UMS mail settings must be correct. Further information can be found under [Mail Settings \(see page 507\)](#).

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action Export view / advanced search result via mail**

General

Name

Name for the task.

Action

- ▶ Select **Export view / advanced search 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 \(see page 507\)](#).

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 / Advanced search ID**

ID of the selected view / advanced search. The view / advanced search is selected via the  button.

Visible columns configuration

Data fields which the email will contain.

View / Advanced search export name

Custom name for the export file (optional). Date and time will be added automatically, separated by an underscore.

Example: `CUSTOMNAME_2021-05-02_10-34.xml`

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 or Distributed UMS](#) (see page 13) environment.

Assignment type

Possible options:

- **One server (random)**: The server for this task will be automatically selected from the servers listed under **Assigned servers**. (Default)
- **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 in the menu bar under **Misc > Scheduled Jobs**, see [Menu Bar of the IGEL UMS Console](#) (see page 185).

Expiration

Point in time as of which the task will no longer be repeated.

Save View or Advanced Search Results in the File System

In the IGEL Universal Management Suite (UMS), you can define an administrative task to save the results of a view created in the UMS Console or the results of an advanced search created in the UMS Web App. The results will be saved in the file system of the UMS Server.

For more on administrative tasks, see [Administrative Tasks - Configure Scheduled Actions for the IGEL UMS \(see page 436\)](#). For more information on the advanced search in the UMS Web App, see [Search for Devices in the IGEL UMS Web App](#).

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action Save view / advanced search results in the file system**

General

Name

Name for the task.

Action

- ▶ Select **Save view / advanced search 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 \(see page 507\)](#).

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 / Advanced search ID

ID of the selected view / advanced search. The view / advanced search 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.

View / Advanced search export name

Custom name for the export file (optional). Date and time will be added automatically, separated by an underscore.

Example: `CUSTOMNAME_2021-05-02_10-34.xml`

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. Example: `C:\Program`

`Files\IGEL\RemoteManager\rmguiserver\temp`

-  If a network drive directory is accepted as a target directory depends on the configuration of the network drive. Example: if authentication is required to access the network drive directory, the execution of the administrative task will fail.

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 in the menu bar under **Misc > Scheduled Jobs**, see [Menu Bar of the IGEL UMS Console](#) (see page 185).

Expiration

Point in time as of which the task will no longer be repeated.

Assign Objects to the Devices of Views or Device Searches

You can assign objects to devices that you have filtered via a view or search in the UMS Console, or via advanced search in the UMS Web App. You can update this assignment regularly using a schedule.

For more information on the advanced search in the UMS Web App, see Search for Devices in the IGEL UMS Web App.

See also the instructions in [Assigning Objects to a View](#) (see page 354).

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Assign objects to the devices of views / advanced searches"**

General

Name

Name for the task.

Action

- ▶ Select **Assign objects to the devices of views / advanced searches**.

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 507).

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

► Select a view / search / advanced search and click on  to add them to the list that will be assigned to one or more objects.

Select Objects

► Select an object and click on  to add them to the list 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 or Distributed UMS](#) (see page 13) environment.

Assignment type

Possible options:

- **One server (random)**: The server for this task will be automatically selected from the servers listed under **Assigned servers**. (Default)
- **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 in the menu bar under **Misc > Scheduled Jobs**, see [Menu Bar of the IGEL UMS Console](#) (see page 185).

Expiration

Point in time as of which the task will no longer be repeated.

Detach Assigned Objects from Devices of Views or Device Searches

In the IGEL Universal Management Suite (UMS), you can create a scheduled administrative task to detach assigned objects from devices that you have filtered via a view or search in the UMS Console or via an advanced search in the UMS Web App. You can detach objects from the devices of the view or search also on a one-off basis, see [Assigning Objects to a View \(see page 354\)](#).

For general information on administrative tasks, see [Administrative Tasks - Configure Scheduled Actions for the IGEL UMS \(see page 436\)](#).

For more information on the advanced search in the UMS Web App, see [Search for Devices in the IGEL UMS Web App](#).

Menu path: **UMS Administration > Administrative Tasks > Dialog "Create Administrative Task" > Action "Detach assigned objects from devices of views / advanced searches"**

General

Name

Name for the task.

Action

- ▶ Select **Detach assigned objects from devices of views / advanced searches**.

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 \(see page 507\)](#).

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

► Select a view / search / advanced search and click on  to add them to the list of objects from which the assigned object(s) have to be detached.

Select Objects

► Select an object and click on  to add them to the list of objects which you would like to detach from 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 or Distributed UMS](#) (see page 13) environment.

Assignment type

Possible options:

- **One server (random):** The server for this task will be automatically selected from the servers listed under **Assigned servers**. (Default)
- **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 in the menu bar under **Misc > Scheduled Jobs**, see [Menu Bar of the IGEL UMS Console](#) (see page 185).

Expiration

Point in time as of which the task will no longer be repeated.

Delete Asset Information History

You can define the deletion of the history of asset information as an administrative task. The deletion helps with performance optimization, see Performance Optimizations in IGEL UMS.

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Delete asset information history"**

General

Name

Name for the task.

Action

- ▶ Select **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 507).

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` will 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 in the menu bar under **Misc > Scheduled Jobs**, see [Menu Bar of the IGEL UMS Console \(see page 185\)](#).

Expiration

Point in time as of which the task will no longer be repeated.

Send Notification Information via Email

In the IGEL Universal Management Suite (UMS), you can define an administrative task as a result of which a notification information will be sent via email. For details on notifications, see [How to Configure Notifications](#) in the IGEL UMS.

For general information on administrative tasks, see [Administrative Tasks - Configure Scheduled Actions for the IGEL UMS](#) (see page 436).

Menu path: **UMS Administration > Global Configuration > Administrative Tasks > Dialog Create Administrative Task > Action "Send notification information via email"**

General

Name

Name for the task.

Action

- ▶ Select **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 507).

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 notifications generated after the last administrative task execution**

Export notifications about

Defines the type of notifications that will be exported. For more information on notification types, see How to Configure Notifications in the IGEL UMS.

Possible options:

- **Universal Firmware Updates (up to 11.07)**
- **Universal Firmware Updates - Stable Releases**
- **Universal Firmware Updates - Rolling Releases**

 Existing administrative tasks with **Universal Firmware Updates** enabled (i.e. created before the update to UMS 12) are automatically converted to **Universal Firmware Updates (up to 11.07)** and **Universal Firmware Updates - Stable Releases**. **Universal Firmware Updates - Rolling Releases** is disabled by default.

- **Universal Management Licenses**
- **Device Licenses**
- **Disk Usage**

- **Global Notifications**
- **Admin Tasks**
- **Packs**
- **Certificates**

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 in the menu bar under **Misc > Scheduled Jobs**, see [Menu Bar of the IGEL UMS Console](#) (see page 185).

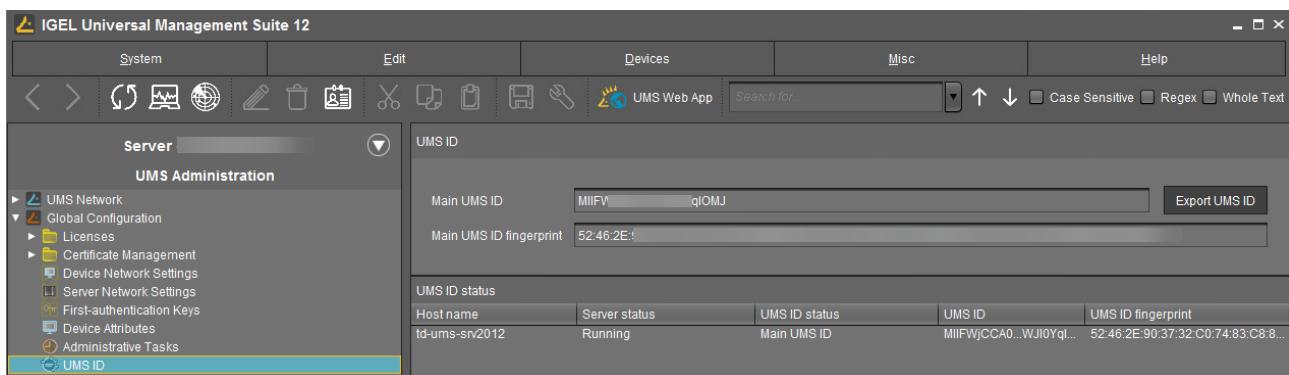
Expiration

Point in time as of which the task will no longer be repeated.

UMS ID

In the following article, you will learn about the UMS ID (called "UMS Licensing ID" before UMS 12) that you can find in your IGEL Universal Management Suite (UMS) installation.

Menu path: **UMS Administration > Global Configuration > UMS ID**



The UMS ID is used, for example, for the communication of your UMS with the IGEL Cloud Services.

The UMS ID also enables the communication between the UMS and the IGEL License Portal (ILP).

The UMS 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 ID must be registered with the IGEL License Portal. For further information, see [Setting up Automatic License Deployment \(ALD\)](#).

The UMS ID consists of a public/private key pair. The public key is a certificate and can be exported as a `.crt` file. The registration of the UMS ID is done by uploading the certificate file to the IGEL License Portal.

A UMS ID is not affected or changed when the UMS database is restored from a backup. The UMS 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.

For the backup options of the UMS ID, see [UMS ID Backup in the IGEL Administrator \(see page 556\)](#) or [IGEL UMS Administrator Command-Line Interface \(see page 582\)](#).

UMS ID

- ⓘ The UMS ID is generated upon each UMS Server installation. Therefore, if you have a High Availability or Distributed UMS (see [IGEL UMS Installation \(see page 13\)](#)) environment, each of the servers has its own UMS ID, i.e. **Local UMS ID**. For the communication of all UMS Servers with the ILP and IGEL Cloud Services, a **Main UMS ID** is used. Therefore, the **Main UMS ID** must be synchronized between all servers, see [UMS ID status \(see page 478\)](#) below.

Main UMS ID: The UMS ID used for communication with the ILP and IGEL Cloud Services. The first and last 10 characters are displayed.

Export UMS ID: Export the UMS ID as a `.crt` file.

Main UMS ID fingerprint: The SHA-256 fingerprint of the UMS ID.

UMS ID Status

If you are operating a single server, this area shows the status of the UMS ID for your server.

If you are operating a UMS High Availability or Distributed UMS environment, this area lists the UMS ID status for each server of the UMS installation. Each server gets the UMS ID on startup or restart.

Host name: Name of the host server as shown under **UMS Administration > UMS Network > Server**.

Server status: Status of the server, e.g. "Running"

Possible values:

- 'Running'
- 'Not running'

UMS ID status: Indicates whether the server has the current main UMS ID or not. If it has the main UMS ID, the field reads "Main UMS ID" or "in sync". If not, the server must be restarted to get synchronized.

Possible values:

- 'Main UMS ID'
- 'In sync'
- 'Not in sync, please restart server'

 If the restart was unhelpful, the UMS ID has to be synchronized manually, see [Manual Synchronization of the UMS ID](#).

UMS ID: The UMS ID currently used on the server. The first and last 10 characters are displayed.

UMS ID fingerprint: The SHA-256 fingerprint of the UMS ID.

Proxy Server

In the IGEL Universal Management Suite (UMS), you can configure proxy servers.

Menu path: **UMS Console > UMS Administration > Global Configuration > Proxy Server**

Name	Host	Port	User	Password	Default Proxy
proxy_test1				*****	<input checked="" type="checkbox"/>
proxy_test2				*****	<input type="checkbox"/>

In this area, you can add and configure proxy servers in order to use them in the following scenarios:

- [IGEL Cloud Gateway](#) (see page 393)
- IGEL Cloud Services (Note that a proxy set under **UMS Administration > Global Configuration > Licenses > Deployment > Edit proxy configuration** is used not only for the [automatic license distribution](#) (see page 401), i.e. not only for the communication with the IGEL License Portal, but for all IGEL Cloud Services, including IGEL Onboarding Service, IGEL Insight Service, IGEL App Portal as well as for UMS as an Update Proxy)
- [Universal Firmware Update](#) (see page 492) (if configured, this proxy is also used for [UMS update check](#) (see page 194))

i The IGEL Cloud Services and Universal Firmware Update 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.

Proxy Server

All configured proxy servers are shown in this list.

Show password

Passwords are made visible in the list.

- Passwords are not shown. (Default)

	Add proxy server
	Delete proxy server
	Edit proxy server
	Define the selected proxy server as a default server

 Only proxy servers that are not used can be deleted. The proxy server added first will automatically be the default proxy server.

Proxy Server Usages

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 \(see page 483\)](#)
- [Using Structure Tags with IGEL OS 11 Devices](#)

► Go to **UMS Administration > Global Configuration > Default Directory Rules**.

The user interface looks like this:

Default Directory Rule Configuration		Find:													
Rule	Directory	Overriding	Apply on boot	Leave in Subdirectory											
▼ DS Default Directory Rules															
▼ DS Product name is like (?i).*LX.*	/Thin Clients/Linux/				Double-click to edit item										
▼ DS OS type is like (?i).*Windows.*															
DS Product ID is like (?i).*64bit.*	/Thin Clients/Windows/64bit/	✓	✓												
DS Product ID is like (?i).*W7*	/Thin Clients/Windows/32bit/	✓	✓												

- ⓘ** 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 \(see page 482\)](#)
- [Creating a Default Directory Rule \(see page 483\)](#)
- [Finding Default Directory Rules \(see page 486\)](#)
- [Applying Rules \(see page 487\)](#)
- [Editing a Rule \(see page 488\)](#)
- [Combining Conditions \(see page 489\)](#)
- [Using the Netmask \(see page 491\)](#)

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:



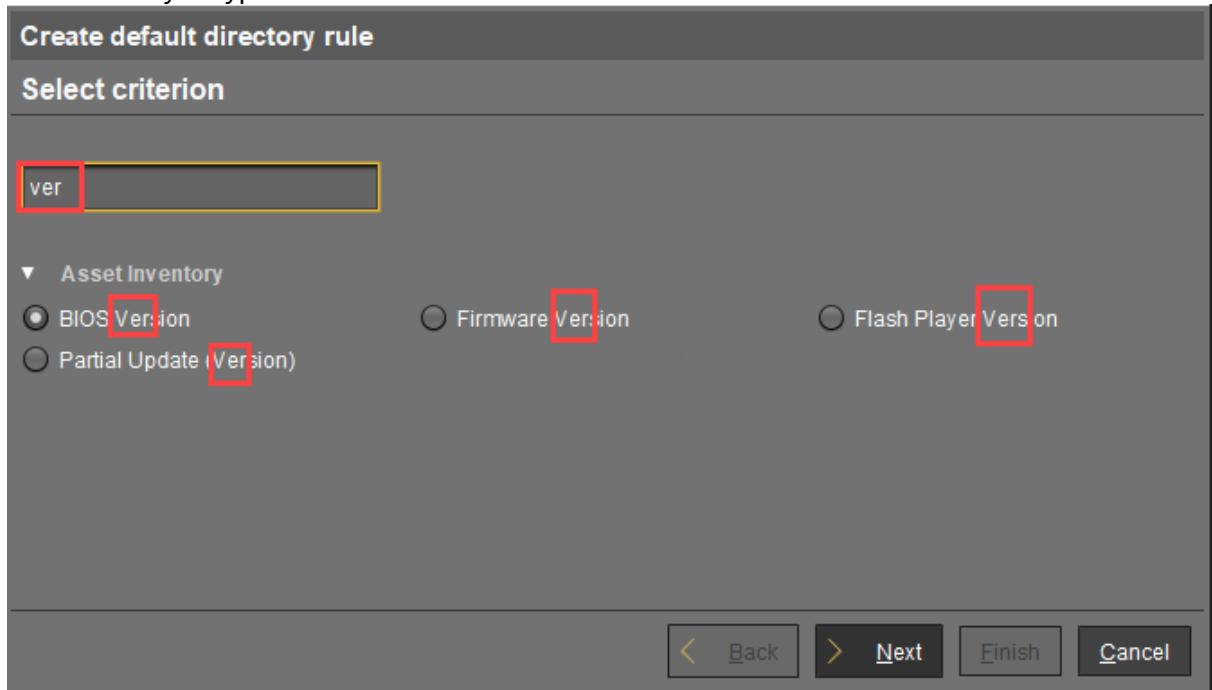
The symbols are as follows (in the correct order):

	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.

Create default directory rule

Version search

Version number exact above below Not like

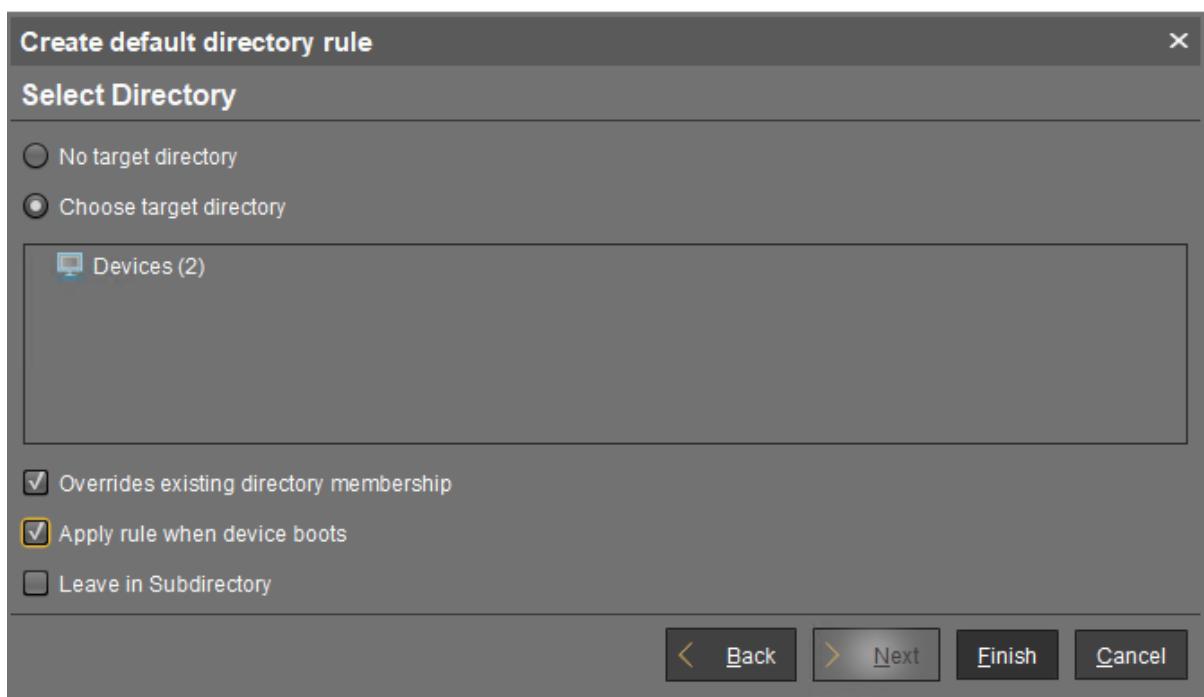
Use regular expression

- i** 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:

- **Overrides 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**.

- i** 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 **Overriding, Apply on boot** or **Leave in subdirectory** column in order to change these options.

Rule	Directory	Overriding	Apply on boot
▼ Default Directory Rules			
▼ Product name is like (?i).*LX.*	/Thin Clients/Linux/		
▼ OS type is like (?i).*Windows.*			
Double-click to edit item	/Thin Clients/Windows/64bit/	✓	✓
Product ID is like (?i).*W7*	/Thin Clients/Windows/32bit/	✓	✓

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.

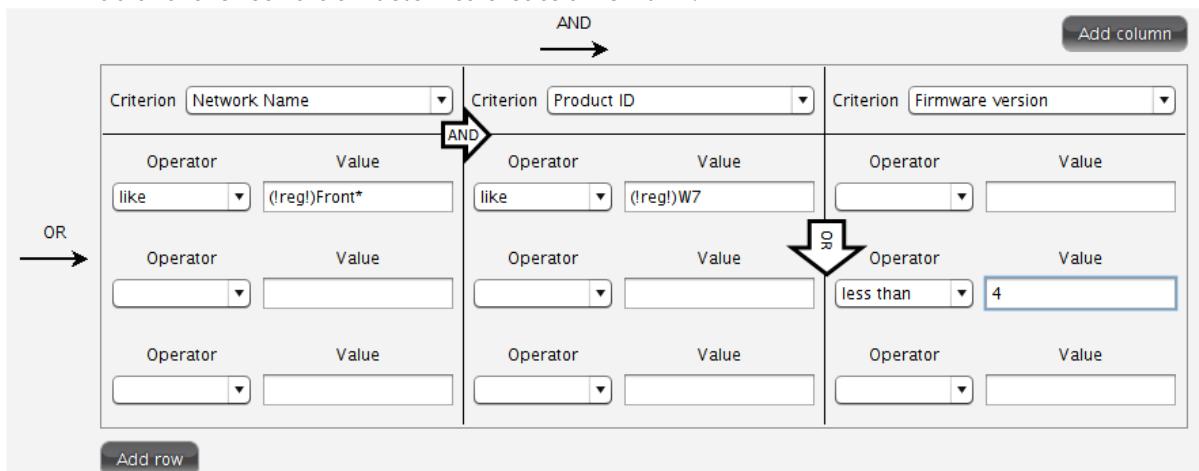
Rule	Directory	Overriding
Default Directory Rules		
Product name is like (?i).*LX.*	/Thin Clients/Linux/	
OS type is like (?i).*Windows.*		
OR		
Product ID is like (?i).*64bit.*	/Thin Clients/Windows/64bit/ ✓	
Product ID is like (?i).*W10*	/Thin Clients/Windows/64bit/ ✓	
Product ID is like (?i).*W7*	/Thin Clients/Windows/32bit/ ✓	

Example: In the illustration, devices whose **product ID** contains 64bit OR W10 are moved to the / devices/Windows/64bit/ directory.

- i** 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**

Here, you can configure the connection to the IGEL firmware server and the connection to an FTP server.

You can use an FTP server for distributing firmware updates to devices, as an alternative to the WebDAV capability of the UMS. If your devices are connected via ICG, an FTP server is required.

Edit....: Changes the Universal Firmware Update settings and the FTP server settings.

Proxy server: Optional proxy server to access the IGEL firmware server.

The FTP server settings where the files are downloaded to (optional): Changes the settings of the FTP server which is used by the devices for the firmware downloads.

Protocol: Protocol and mode to be used.

Possible options:

FTP: FTP in active mode (Default)

FTP passive: FTP in passive mode

FTPS: FTPS in active mode

FTPS passive: FTPS in passive mode

SFTP: SFTP

Host: Hostname of the server

Port: Port number. (Default: 21 for FTP and 22 for SFTP)

User name: Name of the user

Password: User password

Directory: Path of the FTP server

- ⓘ For the SFTP protocol, the path must be defined as an absolute path on the SFTP server. For FTP and FTPS, relative paths are also valid.

Edit proxy configuration:

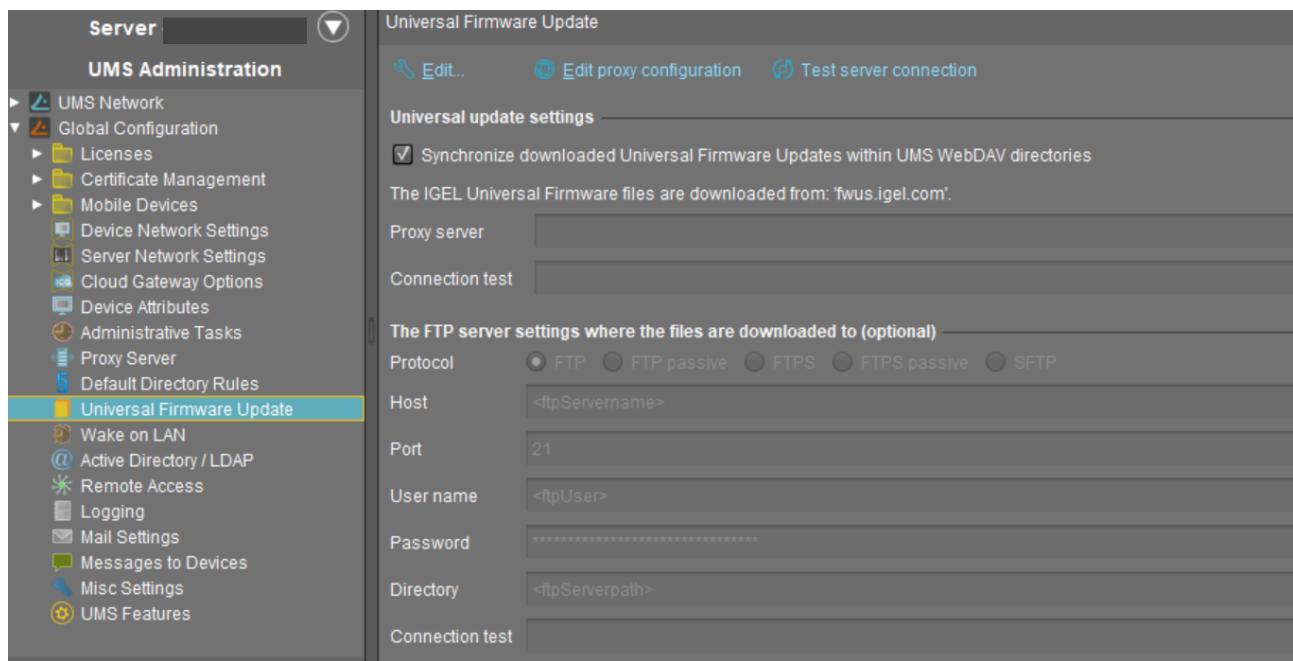
Possible options:

- **No proxy server:** Direct connection to the configured server.
- **Use default proxy server:** Use the proxy server which is configured as default in [Proxy Server](#). (see [page 479](#))
- **Use selected proxy server:** Select a proxy server from the list.

Test server connection: Tests communication between the IGEL server and your FTP server.

Synchronize downloaded Universal Firmware Updates within UMS WebDAV directories

- Downloaded Universal Firmware Updates are automatically synchronized between the servers in a High Availability (HA) network. This applies only if a WebDAV directory is configured as the target path for the download. See [Which Files Are Automatically Synchronized between the IGEL UMS Servers?](#).
- The Universal Firmware Updates are not synchronized between the HA servers.



The screenshot shows the UMS Administration interface with the left sidebar expanded. The 'Universal Firmware Update' option is selected and highlighted in blue. The main panel displays the 'Universal Firmware Update' configuration settings.

Universal Firmware Update

Universal update settings

Synchronize downloaded Universal Firmware Updates within UMS WebDAV directories
The IGEL Universal Firmware files are downloaded from: 'fwus.igel.com'.

Proxy server: [empty input field]

Connection test: [empty input field]

The FTP server settings where the files are downloaded to (optional)

Protocol: FTP FTP passive FTPS FTPS passive SFTP

Host: <ftpServername>

Port: 21

User name: <ftpUser>

Password: [redacted]

Directory: <ftpServerpath>

Connection test: [empty input field]

Further information regarding the Universal Firmware Update can be found under [Universal Firmware Update](#) (see page 377).

Wake on LAN

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 Universal Management Suite (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 (WoL) proxy.

- i The Wake-On-LAN proxy function is supported by Linux devices from *Version 5.09.100*.

Menu path: **UMS Administration > Global Configuration > Wake on LAN**

Broadcast address

- The magic packet is sent to the broadcast address of the network. (Default)

Last known IP address of the device

- The magic packet is sent to the last known IP address of the device. (Default)

Automatic Wake On LAN proxy detection

- Other clients in the subnet are not used as WoL proxy.
- If any other client in the subnet is online, this client is automatically used as WoL proxy. (Default)

All defined subnets

- The magic packet is sent to the network addresses of all subnets that are defined for the UMS.
- The magic packet is not sent to the network addresses of all subnets that are defined for the UMS. (Default)

To add a subnet, proceed as follows:

1. Enable **All defined subnets**.
2. Click  in the area below **All defined subnets**.
The **Define subnets** dialog is displayed.
3. In the **Subnet** field, enter the network address of the subnet.
4. Under **CIDR** (Classless Inter-Domain Routing), select the suitable suffix for the network mask.

- i** 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`.

5. If you wish, add a **Comment**.

6. Click **OK**.

Network address of 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.
- The magic packet is not sent to the network address of the network in which the last known IP address of the device is located. (Default)

To add a network mask, proceed as follows:

1. Click on  in the area below **Network address of last known IP address**.
The **Define network mask** dialog is displayed.
2. Enter the **Network Mask**.
3. If you wish, add a **Comment**.
4. Click on **OK**.

Dedicated Wake On LAN Proxies

- The magic packet is 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.
- i** The **Broadcast address**, **Last known IP address of the device**, **All defined subnets** and **Network address of last known IP** settings have no effect on the Wake-on-LAN proxy.
- The magic packet is not be sent to the devices defined as Wake-On-LAN proxies.

- ⓘ Devices configured as Wake-on-LAN proxies will retain their role, even if **Dedicated Wake On LAN Proxies** is disabled.

To define one or more devices as Wake-On-LAN proxies, proceed as follows:

1. Click on  in the area below **Dedicated Wake On LAN Proxies**.
The **Edit Wake On LAN Proxies** dialog will open.
2. Highlight the desired device in the left-hand column.
3. Click on  to select the device.
4. 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:

1. Click on  in the area below **Dedicated Wake On LAN Proxies**.
The **Edit Wake On LAN proxies** dialog will open.
2. Highlight the desired device in the right-hand column.
3. Click on  to deselect the device.
4. 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.

1. If you have user and group dependencies between different configured domains/subdomains, you might want to activate **Include all configured AD domains for search and import of AD users / groups**. This option activates the group search for a user within all configured domains. On activation, a confirmation dialog is shown.

 If this option is activated, a user may gain additional permissions. This will be the case if

- the user is in a group that has been discovered due to this option,
- this group has been imported under **System > Administrator accounts**,
- and permissions have been assigned to this group i.e. permissions the user would not have otherwise.

Please note that, due to the additional lookups, this option might have an impact on the performance in the following areas:

- UMS login
- Permission dialogs
- Shared Workplace (SWP)

2. Add a new entry to the list of linked Active Directories by selecting **Add (+)**.
3. Specify the **Domain Name**.
4. 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.

5. 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.
6. Activate **Use LDAPS connection** to secure the connection with the provided certificate.
The **Port** changes automatically to the default value "636".
7. 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.

i If more than one domain controller is used, the root certificate of the domain must be configured.

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

8. Enter valid user data under **User name** and **Password**.

i For the user, the read permission is sufficient since no changes will be made to the AD data.

9. Specify aliases under **UPN Suffix** if they have been configured (semicolon separated list). Example:
`domain.local;test.local`

10. Click **Test connection** to check the connection.

i 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).

i 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.

11. Click **Ok** to save the changes.

Remote Access

In the IGEL Universal Management Suite (UMS), you can enable a secure terminal session and a secure VNC connection globally.

Menu path: **UMS Console > UMS Administration > Global Configuration > Remote Access**

Secure terminal

Enable secure terminal globally

- Access via the secure terminal is enabled for all registered devices.
- Access via the secure terminal cannot be enabled for all registered devices. However, it can be enabled for individual devices. (Default)

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. (Default)

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. (Default)

i Secure Shadowing and IGEL OS 12

Shadowing of IGEL OS 12 devices through the UMS is always via Unified Protocol and therefore secure, i.e. communication is always encrypted. By default, shadowing over plain VNC protocol is denied. However, you can deactivate the **Deny shadowing via external VNC tool** option under **System > Remote Access > Shadow** if you want that the devices could be shadowed by the [external VNC viewer](#) (see page 324) via plain VNC protocol.

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. (Default)

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. (Default)

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. (Default)

Logging

In this area, you can specify the logging behavior of the UMS for messages and events as well as activate performance logging.

UMS Web App

Log messages for actions done in the UMS Web App are displayed only in the UMS Web App. For details on logging in the UMS Web App, see Logging in the IGEL UMS Web App.

Menu path: **UMS Administration > Global Configuration > Logging**

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.

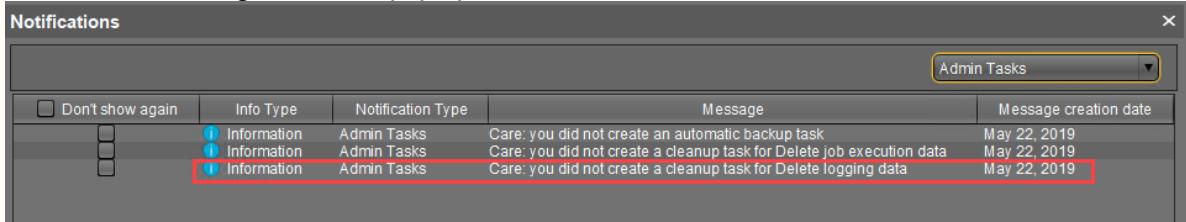
i Logs can be viewed via:
 1) Menu Bar > **System** > **Logging** > **Event Messages**
 2) Context menu of an object in the structure tree > **(Logging)** > **Logging: Event Messages**

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 \(see page 444\)](#)", 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**.

Security Log Settings

Activate security logging

- Security relevant events of the ICG, UMS and IMI are logged in files, that can be picked up by a configured log collector (for example, Graylog). For more information, see [Remote Security Logging in IGEL \(see page 504\)](#).
- Security relevant events of the ICG, UMS and IMI are not logged. (Default)

⚠ The feature logs personally identifiable information of UMS administrators, such as usernames and IP addresses. Ensure that the use of the feature is in accordance with the applicable data protection regulations before enabling it.

Performance Log Settings

Activate performance logging

- The monitoring of the UMS Server and, if available, the UMS Load Balancer is started. The monitoring provides statistical data and information on the methods called internally and their parameters, e.g. number of calls, total time execution, etc. The collected data are to be analyzed by IGEL Support.

For the proper data collection: wait for 3 minutes after enabling the performance logging and then you can either perform normal operations or start the actions you want to monitor. After stopping the monitoring, wait for 5 minutes to allow the system to collect all data.

- ⚠** Always consult IGEL Support before activating performance logging. The collected data can be sent to IGEL Support via UMS Console > **Help** > **Save support information** (see page 545).

- The monitoring is disabled. (Default)

In the case of High Availability installation: when you deactivate performance logging, check that a semaphore file `[Installation directory]/umsbroker/etc/conf/statistics.lck`, which is created by the UMS Load Balancer upon monitoring startup, is deleted.

Remote Security Logging in IGEL

This article describes the remote security logging feature for the IGEL Universal Management Suite (UMS), the IGEL Cloud Gateway (ICG) and the IGEL Management Interface (IMI). The remote security logging feature logs security relevant events in a separate log files that can be picked up by a configured log collector/SIEM.

- ⓘ Remote security logging is independent from the normal logging and is disabled by default.
-

Enable Remote Security Logging

You can enable the feature in the UMS Console, through **UMS Administration > Global Configuration > Logging > Activate security logging**. This will enable logging for all components, including UMS Server, UMS Console, UMS Web App, IMI, and ICG.

Where Are the Log Files Stored?

You can find the UMS Server log file created by remote security logging:

- On Windows:

```
C:\Program Files\IGEL\RemoteManager\rmguiserver\logs\ums-server\ums-server-security.log
```

- On Linux:

```
/opt/IGEL/RemoteManager/rmguiserver/logs/ums-server/ums-server-security.log
```

You can find the UMS Administrator log file created by remote security logging:

- On Windows:

```
C:\Program Files\IGEL\RemoteManager\rmguiserver\logs\ums-admin\ums-admin-security.log
```

- On Linux:

```
/opt/IGEL/RemoteManager/rmguiserver/logs/ums-admin/ums-admin-security.log
```

You can find the ICG log file created by remote security logging:

- On Linux:

```
/opt/IGEL/icg/usg/logs/icg-security.log
```

You can find the UMS Web App log file created by remote security logging:

- On Windows:

```
C:\Program Files\IGEL\RemoteManager\rmguiserver\logs\wums-app-security.log
```

- On Linux:

```
/opt/IGEL/RemoteManager/rmguiserver/logs/wums-app-security.log
```

Logged Events

- i** In the log file, some logged events are marked with source tags:

- UMS Server events contain the source tag: `UMS-Server` .
- ICG events contain the source tag: `ICG` .
- IMI events contain the source tag: `IMI` .
- UMS Web App events contain the source tag: `UMS-Webapp` .

Logged UMS Events

- UMS user login and logoff
- UMS user successful and failed logons
- UMS user password change
- All direct and indirect assignment changes to devices ("privileged policy changes")
- All config changes to devices
- Shut down of UMS or ICG services/processes
- UMS Administrator user account creation/deletion
- UMS Administrator user password change

Logged UMS Web App Events

- Authentication events
- Deletion of a search
- Update or deletion of a profile or priority profile
- Assignment or detachment of the following objects to a folder or a device:
 - profiles
 - priority profiles
 - variables
 - firmware customizations
- Device commands:
 - reset to factory default
 - update device settings

Logged ICG Events

- User creation and deletion

- Successful and failed authentication
- File uploads

Logged IMI Events

- Authentication events
- Add operations
- Update operations
- Delete operations

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 353)
- [Export view result as mail](#) (see page 460)
- Export results of the following administrative tasks as mail:
 - [Database backup \(only for embedded DB\)](#) (see page 438)
 - [Remove unused firmwares](#) (see page 441)
 - [Delete logging data](#) (see page 444)
 - [Delete job execution data](#) (see page 448)
 - [Delete Devices](#) (see page 457)
 - [Assigning Objects to a View](#) (see page 354)
- Mailing of one-off passwords for IGEL Cloud Gateway (ICG)

If you would like to use Gmail for sending mails, see E-Mail Settings for Gmail Accounts.

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.
- **Activate 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 port is 465; for STARTTLS, it is port 587.
- **Activate SMTP-SSL**
 - The mails will be sent with SMTPS encryption.
- **Activate SMTP-STARTTLS**
 - TLS encryption for transporting mails will be enabled in accordance with the STARTTLS procedure.
- **TLS Protocols Available:** Defines the protocols used for communication with the SMTP server.

i If no protocol is selected, TLS 1.0 is used. At least one protocol has to be selected. If more than one version is selected, the best choice selected (starting from left) which is accepted by the SMTP server is used.

- **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 ";".

Messages to Devices

Menu path: **UMS Administration > Global Configuration > Messages to Devices**

Here you can create, change or remove templates for messages to the devices.

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**. For further information, see [Send Message](#) (see page 313).

Allowed Format for Messages to Device

Possible options:

- "Rich messages": The message text can be formatted. Templates can be used. Common formats like font styles and sizes, bullet lists, icons and many more are available.
- "Plain text messages only": The message text is written in plain text. A template can be selected, but the message is converted to plain text.
- "No message allowed": The sending of messages is disabled.

Misc Settings

Menu path: **UMS Administration > Global Configuration > Misc Settings**

The following global parameters can be found here:

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)

i In the event of configuration changes, the page will need to be reloaded by clicking on  in order for the settings to be applied.

i You can view the user login history for a device both in the UMS Console and the UMS Web App:

- UMS Console:
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**. For details, see [View Device Information in the IGEL UMS](#) (see page 288).
- UMS Web App:
Click on the relevant device in the structure tree under **Devices**. All information regarding the device will now be shown in the right hand panel. Go to the **User Login History** tab to see the user login information. For details, see [Devices - View and Manage Your Endpoint Devices](#) in the IGEL UMS Web App.

Notifications

Enable notifications

- Notifications are enabled and will be shown on each connection to the UMS Console; see also settings under **Menu bar > Misc > Settings > Notifications**. (Default)

For detailed information on notifications, see [How to Configure Notifications in the IGEL UMS](#).

- The notification function is disabled for all users.

For each license, certificate, or Product Pack, a new notification will be created [...] day(s) before expiration: Sets a time limit for a notification to remind you about the expiration of your license, certificate, or Product Pack.

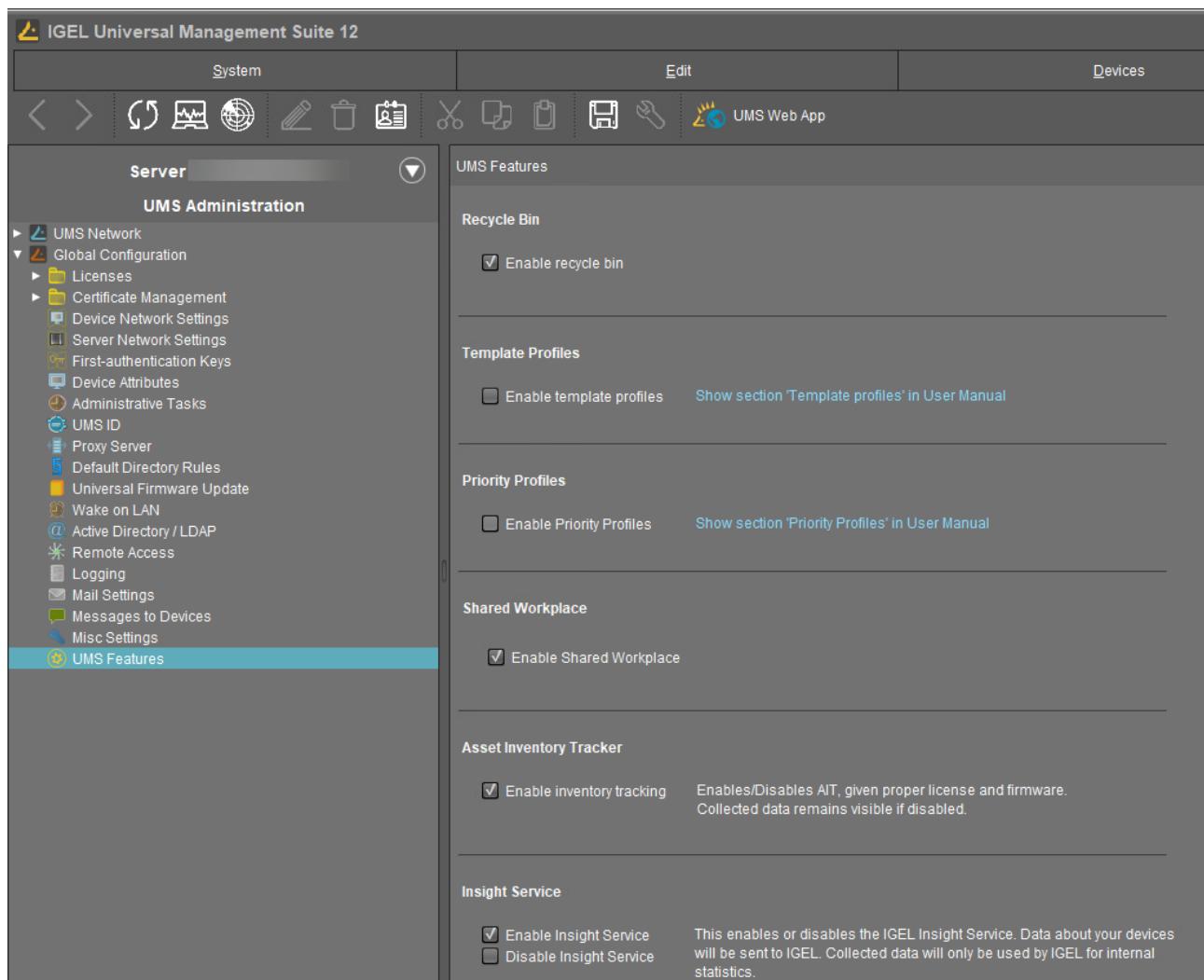
A notification will be created when the free disk space is below [...] GB: When the free disk space is below this value, a warning will be created.

For each license or Product Pack, a new notification will be created when the amount of used licenses is above [...] %: If the number of used licenses in a Product Pack is higher than this limit (integer percentage), a notification is created.

UMS Features

In the IGEL Universal Management Suite (UMS), you can activate / deactivate such features as recycle bin, template or priority profiles, IGEL Shared Workplace, IGEL Insight Service, etc.

Menu path: **UMS Console > UMS Administration > Global Configuration > UMS Features**



The screenshot shows the UMS Administration interface with the "Global Configuration" section selected. Under "UMS Features", several options are listed with checkboxes:

- Recycle Bin:** Enable recycle bin
- Template Profiles:** Enable template profiles [Show section 'Template profiles' in User Manual](#)
- Priority Profiles:** Enable Priority Profiles [Show section 'Priority Profiles' in User Manual](#)
- Shared Workplace:** Enable Shared Workplace
- Asset Inventory Tracker:** Enable inventory tracking
Enables/Disables AIT, given proper license and firmware.
Collected data remains visible if disabled.
- Insight Service:** Enable Insight Service
 Disable Insight Service
This enables or disables the IGEL Insight Service. Data about your devices will be sent to IGEL. Collected data will only be used by IGEL for internal statistics.

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)

i If the recycle bin is disabled, the objects are removed permanently straight away.

See also [Recycle Bin - Deleting Objects in the IGEL UMS](#) (see page 383).

Template Profiles

Enable template profiles

- Template profiles are enabled. For information on template profiles, see [Template Profiles in the IGEL UMS](#) (see page 256).
- Template profiles are disabled. (Default)

Priority Profiles

Enable priority profiles

- Priority profiles are enabled. For information on priority profiles, see [Priority Profiles in the IGEL UMS](#) (see page 253).
- Priority profiles are disabled. (Default)

Shared Workplace

Enable Shared Workplace

- IGEL [Shared Workplace \(SWP\)](#) (see page 327) is enabled. (Default)

i **Licensed Feature**

This feature requires a valid license from the IGEL Enterprise Management Pack (EMP).

! If you deactivate **Enable Shared Workplace**, the structure tree node **Shared Workplace Users** will be hidden and Shared Workplace users will NOT be able to log in!

Asset Inventory Tracker

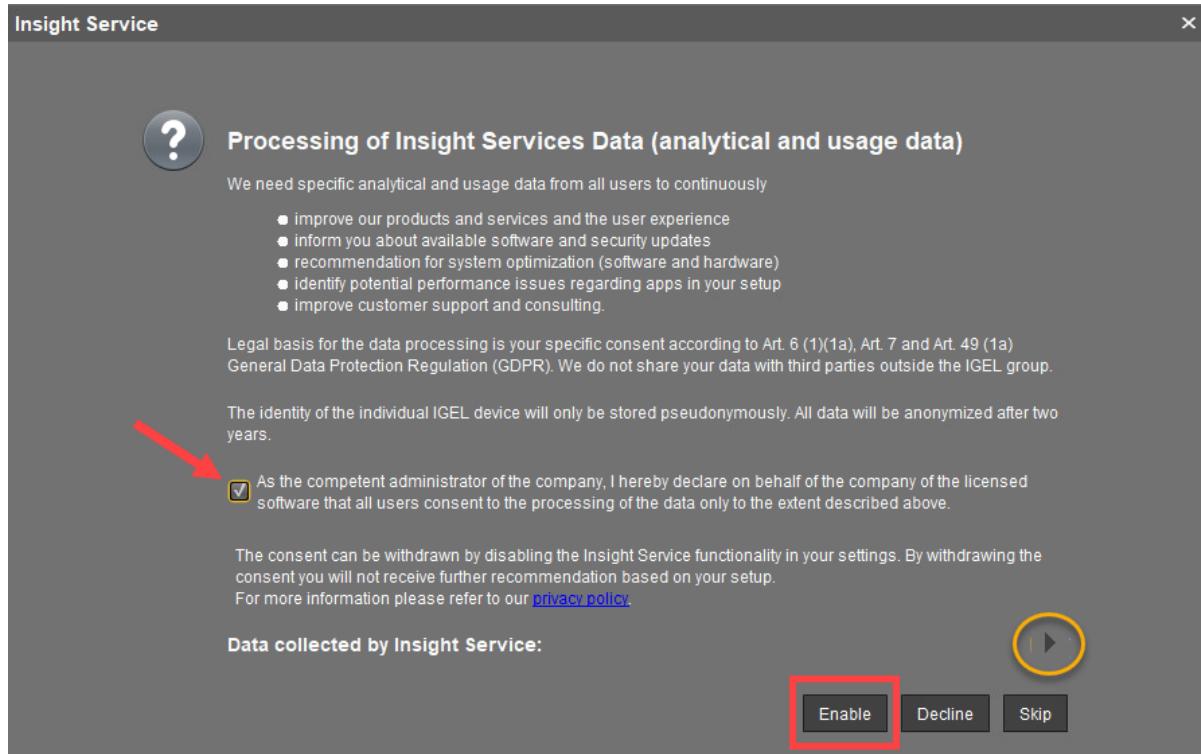
Enable inventory tracking

- [Inventory tracking](#) (see page 291) is enabled. (Default)

Insight Service

Enable Insight Service

- Enables IGEL Insight Service if you accept the privacy policy in the dialog opened and click **Enable**. When you activate the IGEL Insight Service, IGEL collects specific analytical and usage data; see IGEL Insight Service.



Disable Insight Service

- Disables IGEL Insight Service if you click **Decline** in the dialog opened.

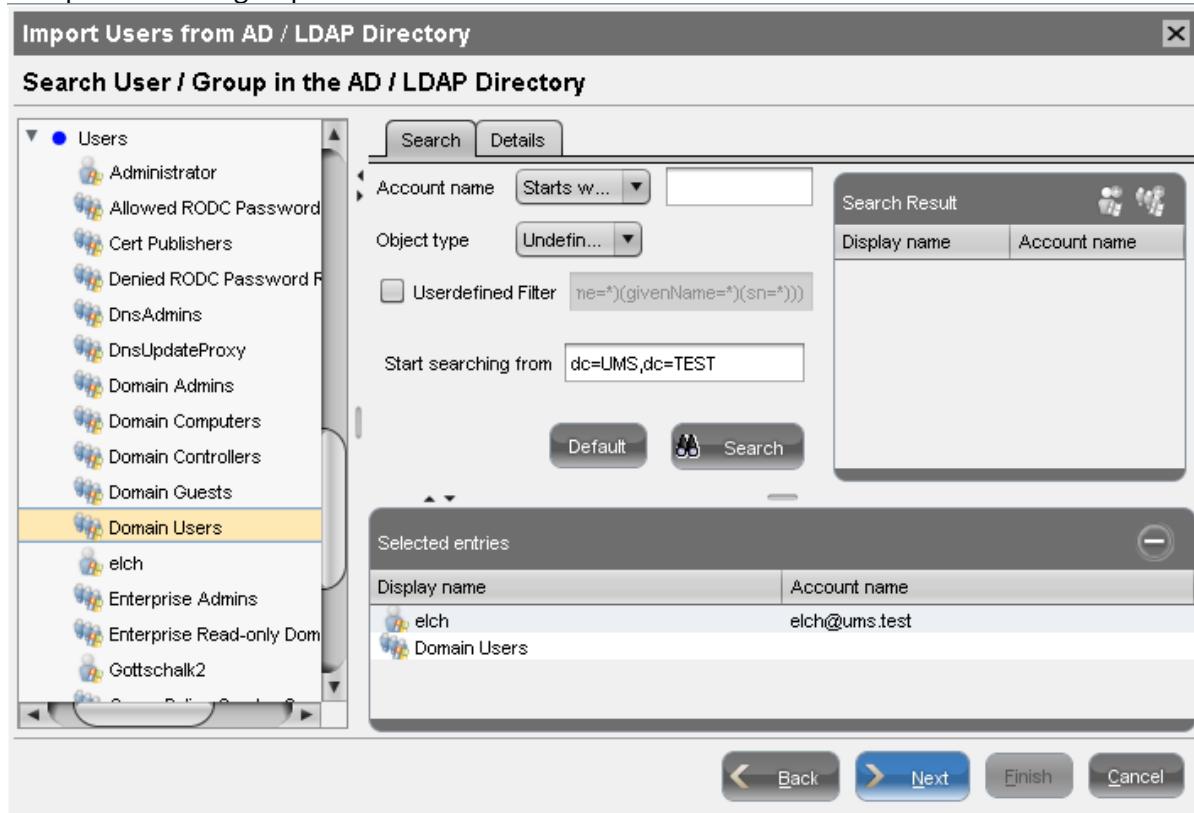
Importing Active Directory Users

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 497). 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 or 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:

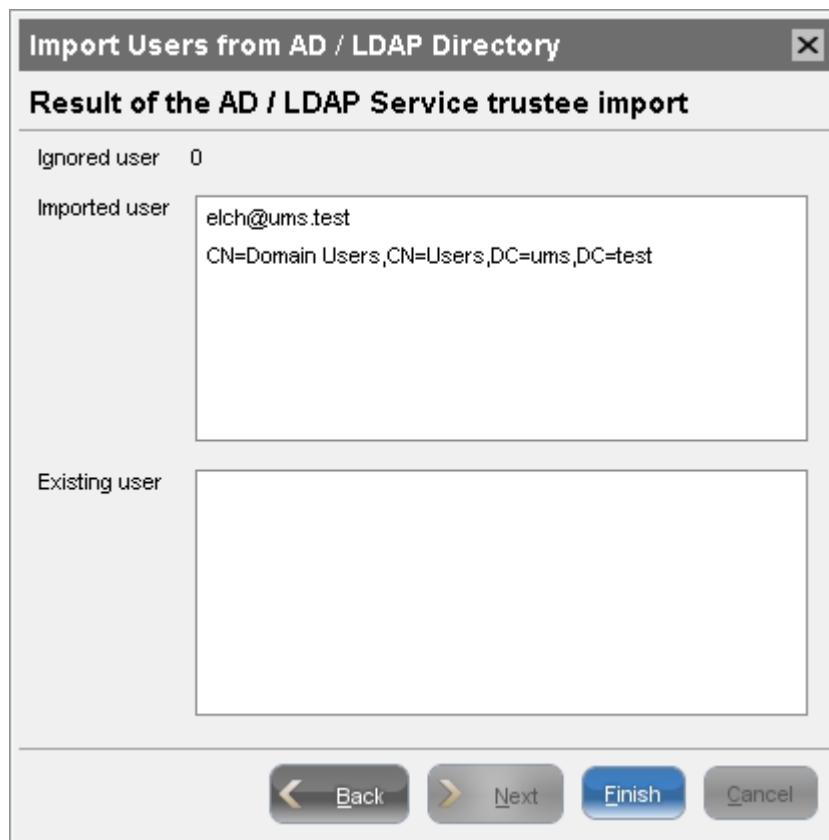
- **Add user**
- **Add group**
- **Start searching from**
- **Details...**

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 / UMS Web App](#) (see page 6), 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 the UMS superuser that was created during the installation (see [IGEL UMS Installation under Linux](#) (see page 20) or [IGEL UMS Installation under Windows](#) (see page 50)) cannot be restricted. The UMS superuser always has full access rights in the UMS.

UMS Web App

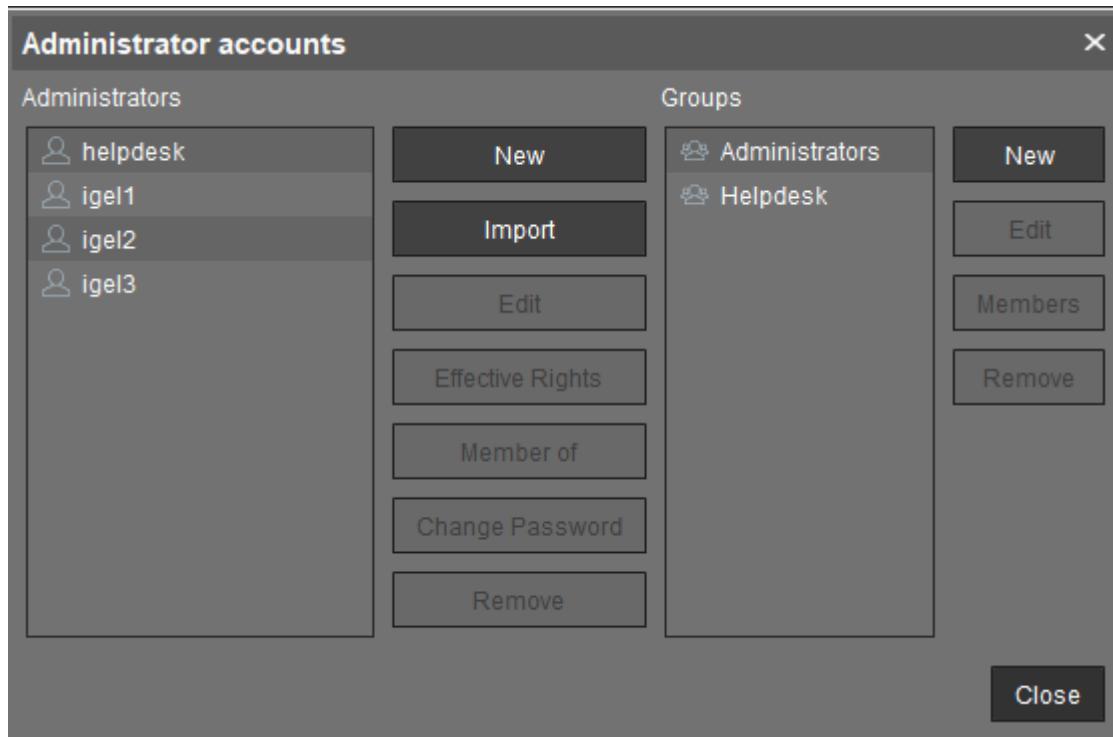
The UMS Web App supports the same permissions as the UMS Console. To get access to devices in a directory, read permissions on this directory are required; permissions to devices only are not sufficient. More information on permissions in the UMS Web App can be found under [Important Information for the IGEL UMS Web App](#).

- [Administrators and Groups](#) (see page 520)
- [Access Rights](#) (see page 521)

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
- Access rights to the nodes within the UMS Administration area of 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.

 Take notice:

1. Permissions that were granted directly have precedence over those granted indirectly.
2. Nevertheless, the withdrawal of permissions ALWAYS overrides the granting of permissions.

The precedence of the **Deny** permission over the **Allow** permission means:

- If an administrator is a member of several groups with permissions contradicting each other, the **Deny** permission will overrule the **Allow** permissions from other groups. Also, if the permission is granted to an administrator directly, it will be nevertheless denied via a group.

Administrator

Edit administrator permissions

User name	Edit administrator permissions	
	Allow all	Deny all
'System' Menu	Allow	Deny
Administrator accounts	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Firmware management	<input type="checkbox"/>	<input checked="" type="checkbox"/>
License management	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Logging (events and messages)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
WebDAV access (ums-filetransfer)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
'Device' Menu	Allow	Deny
Scan for devices	<input checked="" type="checkbox"/>	<input type="checkbox"/>
'Misc' Menu	Allow	Deny
Host Assignment (Jobs)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Public Holidays Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SQL Console	<input checked="" type="checkbox"/>	<input type="checkbox"/>
'Help' Menu	Allow	Deny
Save support information	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Ok Cancel

Permissions for an administrator take precedence over permissions for a group

Effective Rights

Permission	Reason
Administrator accounts	denied for support
Firmware management	denied for Helpdesk1
License management	denied for Helpdesk1
Logging (events and messages)	denied for Helpdesk1
WebDAV access (ums-filetransfer)	denied for Helpdesk1
Scan for devices	denied for Helpdesk1
Host Assignment (Jobs)	denied for Helpdesk1
Public Holidays Management	denied for Helpdesk1
SQL Console	denied for Helpdesk1
Save support information	denied for Helpdesk1

Ok Cancel

Group 1

Edit group permissions

Group Name	Edit group permissions	
	Allow all	Deny all
'System' Menu	Allow	Deny
Administrator accounts	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Firmware management	<input type="checkbox"/>	<input checked="" type="checkbox"/>
License management	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Logging (events and messages)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
WebDAV access (ums-filetransfer)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
'Device' Menu	Allow	Deny
Scan for devices	<input type="checkbox"/>	<input checked="" type="checkbox"/>
'Misc' Menu	Allow	Deny
Host Assignment (Jobs)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Public Holidays Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SQL Console	<input type="checkbox"/>	<input checked="" type="checkbox"/>
'Help' Menu	Allow	Deny
Save support information	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Ok Cancel

Group 2

Edit group permissions

Group Name	Edit group permissions	
	Allow all	Deny all
'System' Menu	Allow	Deny
Administrator accounts	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Firmware management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
License management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Logging (events and messages)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
WebDAV access (ums-filetransfer)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
'Device' Menu	Allow	Deny
Scan for devices	<input checked="" type="checkbox"/>	<input type="checkbox"/>
'Misc' Menu	Allow	Deny
Host Assignment (Jobs)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Public Holidays Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SQL Console	<input checked="" type="checkbox"/>	<input type="checkbox"/>
'Help' Menu	Allow	Deny
Save support information	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Ok Cancel

Deny permissions always override Allow permissions

- If a prohibition is issued for an object in the structure tree or a node in the UMS Administration area, it will apply for all subobjects/subnodes and cannot be withdrawn directly for these

subobjects/subnodes.

Permission	Allow	Deny	Effective Rights
Browse	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for group Helpdesk
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for group Helpdesk
Move	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Helpdesk
Edit Configuration	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Helpdesk
Write	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Helpdesk

Permission	Allow	Deny	Effective Rights
Browse	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for group Helpdesk (inherited from /ROOT/Devices/)
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for group Helpdesk (inherited from /ROOT/Devices/)
Move	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Helpdesk (inherited from /ROOT/Devices/)
Edit Configuration	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Helpdesk (inherited from /ROOT/Devices/)
Write	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Helpdesk (inherited from /ROOT/Devices/)

Generally speaking, the same permission settings are used for groups and administrators. The following description of individual configuration options therefore applies equally to administrators and groups.

- **Basic Access Rights** (see page 524)
- **General Administrator Rights** (see page 525)
- **Object-Related Access Rights** (see page 530)
- **Access Rights in the Administration Area** (see page 536)

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

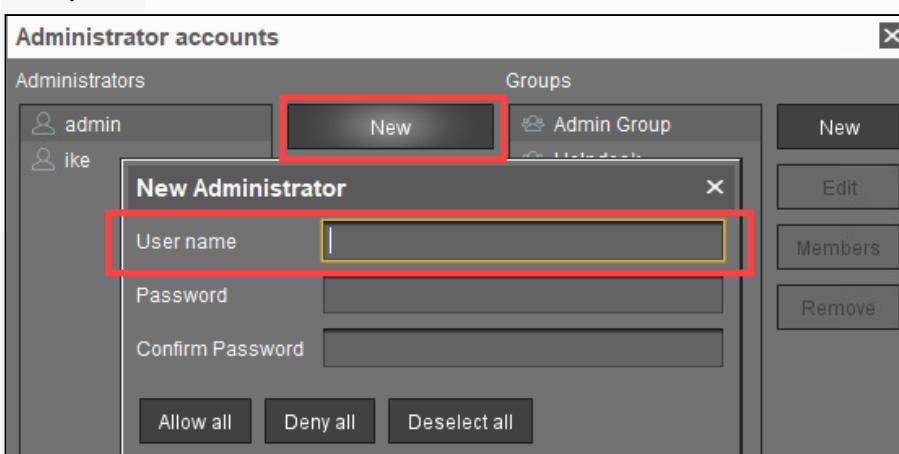
Menu path: Menu bar > **System > Administrator accounts**

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.

- ⓘ The following characters are not allowed for user names of UMS administrators: "/ \ [] : ; | = , + * ? < >



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 515).

- **Domain:** Domain in which the AD/LDAP service runs
- **User:** Name of the user
- **Password:** Password of the user

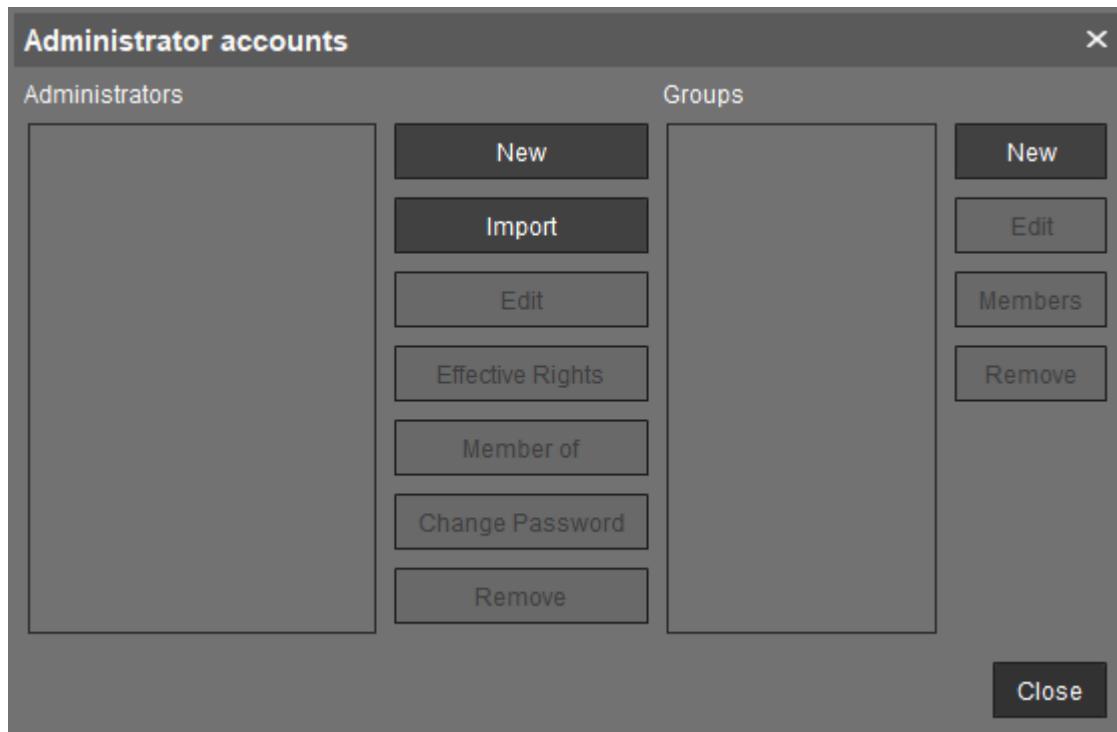
Edit: Existing administrator or group settings can be edited.

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**.

New Administrator

User name	<input type="text"/>																		
Password	<input type="password"/>																		
Confirm Password	<input type="password"/>																		
<input type="button" value="Allow all"/> <input type="button" value="Deny all"/> <input type="button" value="Deselect all"/>																			
'System' Menu <table border="1"> <thead> <tr> <th></th> <th>Allow</th> <th>Deny</th> </tr> </thead> <tbody> <tr> <td>Administrator accounts</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Firmware management</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>License management</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Logging (events and messages)</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>WebDAV access (ums-filetransfer)</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>			Allow	Deny	Administrator accounts	<input type="checkbox"/>	<input type="checkbox"/>	Firmware management	<input type="checkbox"/>	<input type="checkbox"/>	License management	<input type="checkbox"/>	<input type="checkbox"/>	Logging (events and messages)	<input type="checkbox"/>	<input type="checkbox"/>	WebDAV access (ums-filetransfer)	<input type="checkbox"/>	<input type="checkbox"/>
	Allow	Deny																	
Administrator accounts	<input type="checkbox"/>	<input type="checkbox"/>																	
Firmware management	<input type="checkbox"/>	<input type="checkbox"/>																	
License management	<input type="checkbox"/>	<input type="checkbox"/>																	
Logging (events and messages)	<input type="checkbox"/>	<input type="checkbox"/>																	
WebDAV access (ums-filetransfer)	<input type="checkbox"/>	<input type="checkbox"/>																	
'Device' Menu <table border="1"> <tbody> <tr> <td>Scan for devices</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>		Scan for devices	<input type="checkbox"/>	<input type="checkbox"/>															
Scan for devices	<input type="checkbox"/>	<input type="checkbox"/>																	
'Misc' Menu <table border="1"> <tbody> <tr> <td>Host Assignment (Jobs)</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Public Holidays Management</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>SQL Console</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>		Host Assignment (Jobs)	<input type="checkbox"/>	<input type="checkbox"/>	Public Holidays Management	<input type="checkbox"/>	<input type="checkbox"/>	SQL Console	<input type="checkbox"/>	<input type="checkbox"/>									
Host Assignment (Jobs)	<input type="checkbox"/>	<input type="checkbox"/>																	
Public Holidays Management	<input type="checkbox"/>	<input type="checkbox"/>																	
SQL Console	<input type="checkbox"/>	<input type="checkbox"/>																	
'Help' Menu <table border="1"> <tbody> <tr> <td>HA Health Check</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Save support information</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>		HA Health Check	<input type="checkbox"/>	<input type="checkbox"/>	Save support information	<input type="checkbox"/>	<input type="checkbox"/>												
HA Health Check	<input type="checkbox"/>	<input type="checkbox"/>																	
Save support information	<input type="checkbox"/>	<input type="checkbox"/>																	
General - WebApp <table border="1"> <tbody> <tr> <td>App Management</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Delete Log Messages</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Device Bulk Action</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>		App Management	<input type="checkbox"/>	<input type="checkbox"/>	Delete Log Messages	<input type="checkbox"/>	<input type="checkbox"/>	Device Bulk Action	<input type="checkbox"/>	<input type="checkbox"/>									
App Management	<input type="checkbox"/>	<input type="checkbox"/>																	
Delete Log Messages	<input type="checkbox"/>	<input type="checkbox"/>																	
Device Bulk Action	<input type="checkbox"/>	<input type="checkbox"/>																	
<input type="button" value="Ok"/> <input type="button" value="Cancel"/>																			

'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

Host Assignment (Jobs)

- Scheduled jobs can be assigned to various hosts.

Public Holidays Management

- Public holidays can be defined to plan jobs.

SQL Console

- The SQL Console may be run. **Warning:** The SQL Console can cause considerable damage to the database.

'Help' Menu

HA Health Check

- The **UMS HA Health Check - Analyse Your IGEL UMS High Availability and Distributed UMS Systems** feature for an overall check of the High Availability environment can be used.

Save support information

- Database and server log files can be exported for support purposes.

General - WebApp

App Management

- The **Apps** area of the UMS Web App is displayed. The user is authorized to manage apps.

Delete Log Messages

- Log messages can be deleted with the UMS Web App.

Device Bulk Action

- Actions can be performed for any number of devices with the UMS Web App, e.g. by using directories.
- With the UMS Web App, actions can only be performed for one device at a time.

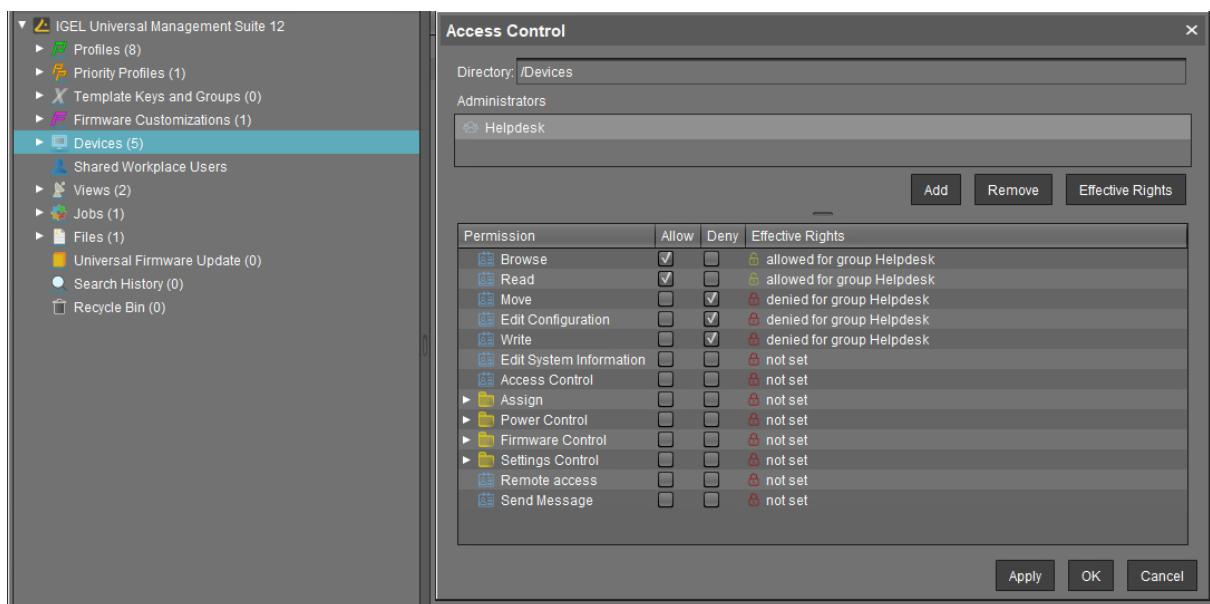
⚠ This only applies to the UMS Web App; bulk actions can still be performed from the UMS Console.

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 symbol bar
- 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 withdrawal of permissions, i.e. **Deny**, always overrides the granting of permissions, i.e. **Allow**.

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.

Create Administrator Accounts



The screenshot shows the IGEL Universal Management Suite (UMS) interface. On the left, the navigation tree displays the server structure under 'Server'. A specific device, 'ITC005056938D22', is selected and highlighted in blue. The main pane shows the 'Access Control' dialog for this device. The 'Administrators' tab is selected, showing the 'Helpdesk' group assigned to it. A red arrow points from the 'Effective Rights' button at the bottom right of the dialog to the 'Effective Rights' column in the permission table. The table lists various permissions and their effective status for the 'Helpdesk' group.

Permission	Allow	Deny	Effective Rights
Browse	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for group Helpdesk
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for group Helpdesk
Move	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Helpdesk
Edit Configuration	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Helpdesk
Write	<input type="checkbox"/>	<input checked="" type="checkbox"/>	denied for group Helpdesk
Edit System Information	<input type="checkbox"/>	<input type="checkbox"/>	not set
Access Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign	<input type="checkbox"/>	<input type="checkbox"/>	not set
Power Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Firmware Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Settings Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
Remote access	<input type="checkbox"/>	<input type="checkbox"/>	not set
Send Message	<input type="checkbox"/>	<input type="checkbox"/>	not set

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 (Setup)
	Write	Write permission in respect of folders and object attributes (not Setup)
	Edit System Information	The system information of a device (device attributes) can be edited.
	Access Control	The permission settings for the object can be changed.
	Remote access	VNC / secure terminal access to the device
	Send message	Messages may be sent to devices.
Assignment	Assign (priority) profile	A profile may be assigned to the object. This permission is required for the assignment of apps for IGEL OS 12 devices.
	Assign file	A file may be assigned to the object.
	Assign Base System / Firmware Update	An IGEL OS Base System app / firmware update may be assigned to the object.
	Assign FWC	A firmware customization can be assigned to the object.
	Assign Template Value / Value Group	A template value / value group can be assigned to the object.
Power Control	Reboot	Rebooting the device.
	Suspend	Putting the device into the idle state.
	Shutdown	Shutting down the device
	Wake up	Waking up the device using wake-on-LAN.

Firmware Control	Update	The app / firmware update may be carried out.
	Reset	Resetting the device to the factory defaults.
	Flash player	Downloading a Flash Player plugin for Firefox
	File transfer	An assigned file may be transferred to the device.
	Generic command	Generic commands (e.g. specific device commands like Deploy Jabra Xpress package) can be sent to the device.
Settings Control	UMS -> Device	The configuration of the UMS may be sent to the device.
	Device -> UMS	The local configuration of the device may be read to the UMS.

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

Permission	Allow	Deny	Effective Rights
Browse	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike (inherited from /ROOT/Profiles/)
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike (inherited from /ROOT/Profiles/)
Write	<input type="checkbox"/>	<input type="checkbox"/>	not set
Access Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
▼ Assign	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign File	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike
Assign device	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign Shared Workplace ...	<input type="checkbox"/>	<input type="checkbox"/>	not set

Permissions on the File

Permission	Allow	Deny	Effective Rights
Browse	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike (inherited from /ROOT/Files/)
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike (inherited from /ROOT/Files/)
Write	<input type="checkbox"/>	<input type="checkbox"/>	not set
Access Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
▼ Assign	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign Profile	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike
Assign Priority Profile	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign FWC	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign device	<input type="checkbox"/>	<input type="checkbox"/>	not set

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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike (inherited from /ROOT/Profiles/)
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike (inherited from /ROOT/Profiles/)
Write	<input type="checkbox"/>	<input type="checkbox"/>	not set
Access Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
▼ Assign	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign File	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign device	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike
Assign Shared Workplace U...	<input type="checkbox"/>	<input type="checkbox"/>	not set

Permissions on the Device

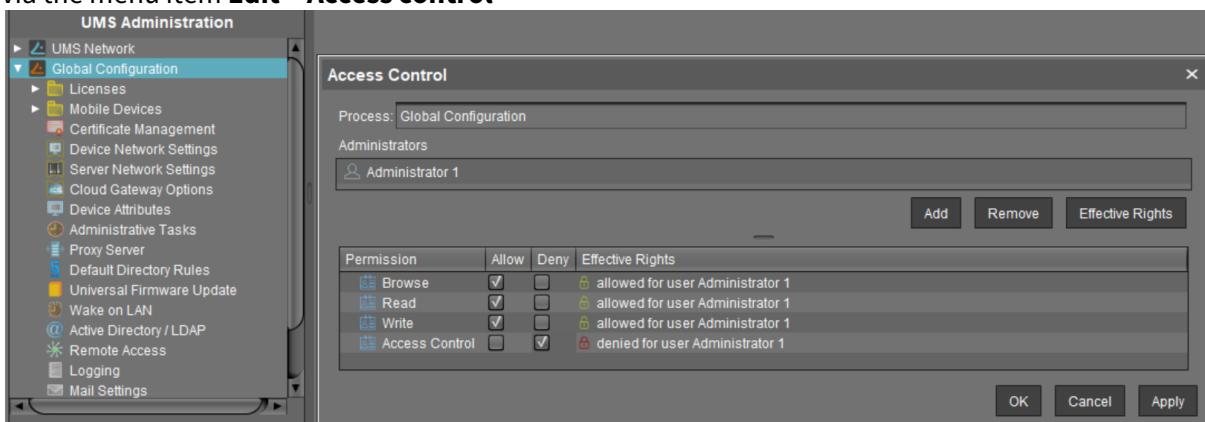
Permission	Allow	Deny	Effective Rights
Browse	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike (inherited from /ROOT/Devices/)
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike (inherited from /ROOT/Devices/)
Move	<input type="checkbox"/>	<input type="checkbox"/>	not set
Edit Configuration	<input type="checkbox"/>	<input type="checkbox"/>	not set
Write	<input type="checkbox"/>	<input type="checkbox"/>	not set
Edit System Information	<input type="checkbox"/>	<input type="checkbox"/>	not set
Access Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
▼ Assign	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign Profile	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike
Assign Priority Profile	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign File	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign Base System...	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign FWC	<input type="checkbox"/>	<input type="checkbox"/>	not set
Assign Template Val...	<input type="checkbox"/>	<input type="checkbox"/>	not set
► Power Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
► Firmware Control	<input type="checkbox"/>	<input type="checkbox"/>	not set
▼ Settings Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike
UMS -> Device	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike
Device -> UMS	<input checked="" type="checkbox"/>	<input type="checkbox"/>	allowed for user ike
Remote access	<input type="checkbox"/>	<input type="checkbox"/>	not set
Send Message	<input checked="" type="checkbox"/>	<input type="checkbox"/>	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

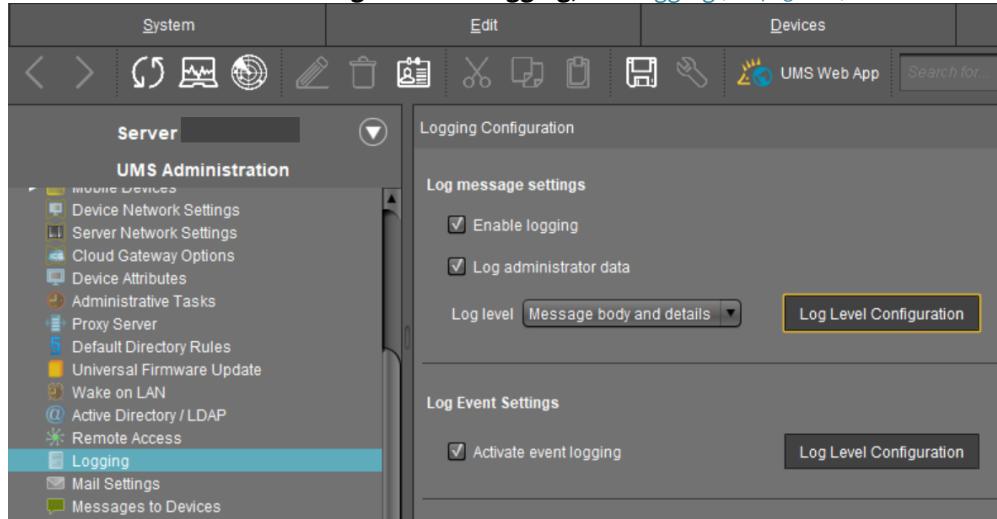
The logging system is used by the UMS and the registered devices in order to record all changes to the database. Only successful actions are logged. You will not find details of any errors in the log file of the UMS GUI Server.

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 \(see page 501\)](#).



- **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 539)

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.

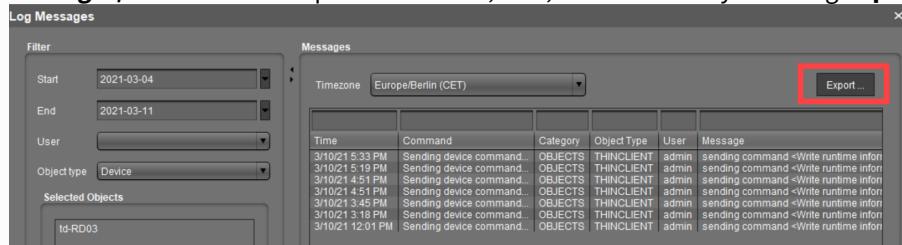
All filter fields are combined with the operator **AND**.

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**.

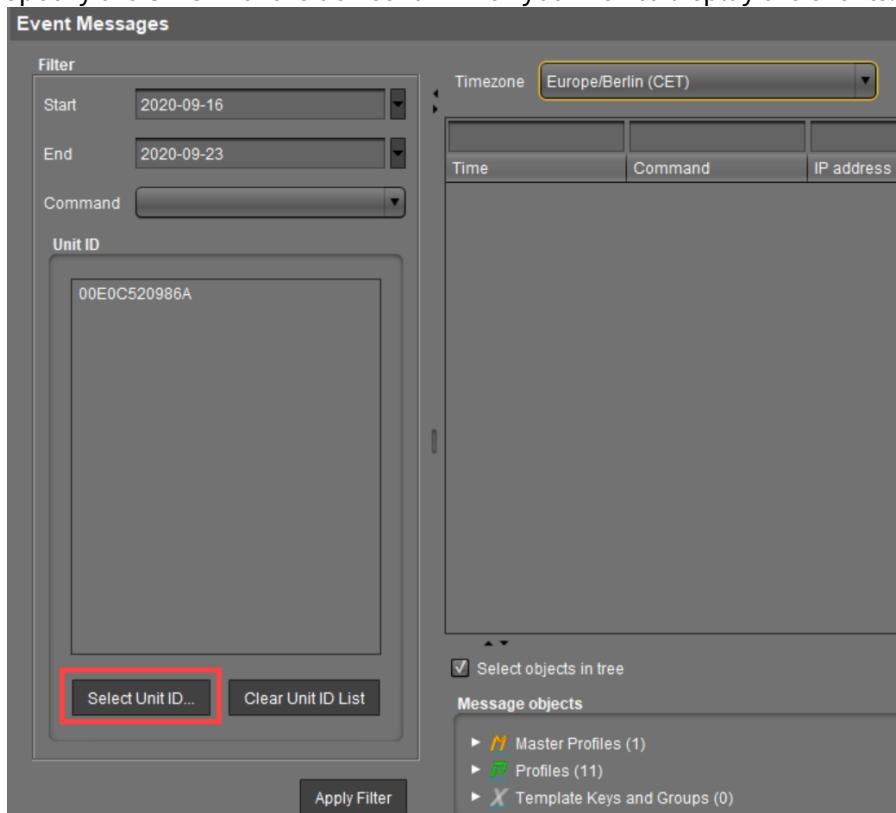


- [Setting a Filter for Events \(see page 540\)](#)
- [Filter for Messages \(see page 541\)](#)
- [Setting a Filter for Categories \(see page 542\)](#)
- [Notes \(see page 543\)](#)

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.

Log Messages

Filter

Start: 2021-03-04

End: 2021-03-11

User:

Object type: Device

Selected Objects

- td-RD03

Details

Select objects in tree

- ▶ Master Profiles (1)
- ▶ Profiles (13)
- ▶ Template Keys and Groups (2)
- ▶ Firmware Customizations (1)
- ▶ Devices (2)
- ▶ Mobile Devices (0)
- ▶ Views (2)
- ▶ Jobs (1)
- ▶ Files (2)
- ▶ Universal Firmware Update (1)

Messages

Timezone: Europe/Berlin (CET) Export ...

Time	Command	Category	Object Type	User	Message
3/10/21 5:33 PM	Sending device command...	OBJECTS	THINCLIENT	admin	sending command <Write runtime info
3/10/21 5:19 PM	Sending device command...	OBJECTS	THINCLIENT	admin	sending command <Write runtime info
3/10/21 4:51 PM	Sending device command...	OBJECTS	THINCLIENT	admin	sending command <Write runtime info
3/10/21 4:51 PM	Sending device command...	OBJECTS	THINCLIENT	admin	sending command <Write runtime info
3/10/21 3:45 PM	Sending device command...	OBJECTS	THINCLIENT	admin	sending command <Write runtime info
3/10/21 3:18 PM	Sending device command...	OBJECTS	THINCLIENT	admin	sending command <Write runtime info
3/10/21 12:01 PM	Sending device command...	OBJECTS	THINCLIENT	admin	sending command <Write runtime info

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 in the IGEL UMS](#) (see page 545) 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](#)¹⁹.

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](#)²⁰ too.

¹⁹ <https://cosmos.igel.com/>

²⁰ <https://www.igel.com/wp-content/uploads/2019/11/F-501-EN.pdf>

Support Wizard in the IGEL UMS

With the Support Wizard in the IGEL Universal Management Suite (UMS), you can collect the log files which are important for your support case and send them via e-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 in use, log files from the connected ICGs and the basic information of the used ICG certificates will also be saved. If the IGEL Management Interface (IMI) extension is used, its API log file will be saved too. In the case of performance logging (to be activated only upon recommendation of IGEL Support; see [Logging \(see page 502\)](#)), monitoring data for the UMS Server and UMS Load Balancer will be collected too.

Menu path: **Menu Bar > Help > Save support information**

- i** In order to send log files using the Support Wizard, the mail settings must be correct; further information can be found under [Mail settings \(see page 507\)](#). The support ID must also be valid.

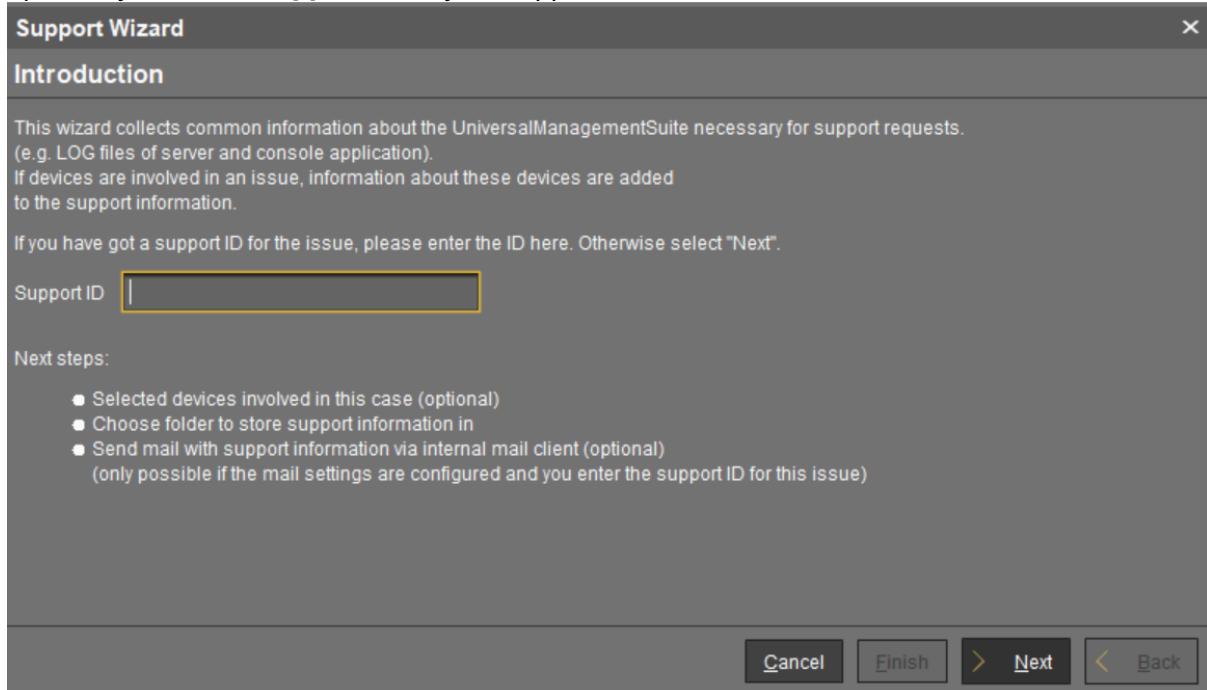
How to Send Log Files via Support Wizard in the IGEL UMS

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**.

Related Topics

[Debugging / How to Collect and Send Device Log Files to IGEL Support](#)

[Exporting the Local Device Configuration](#)

Save Device Files for Support

You can use the IGEL Universal Management Suite (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.

Menu path: **Menu bar > Help > Save device files for support**

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 Debugging / How to Collect and Send Device Log Files to IGEL Support.

Log Files Collected from IGEL OS 11 Devices

The following log files are collected from the device 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 from IGEL OS 12 Devices

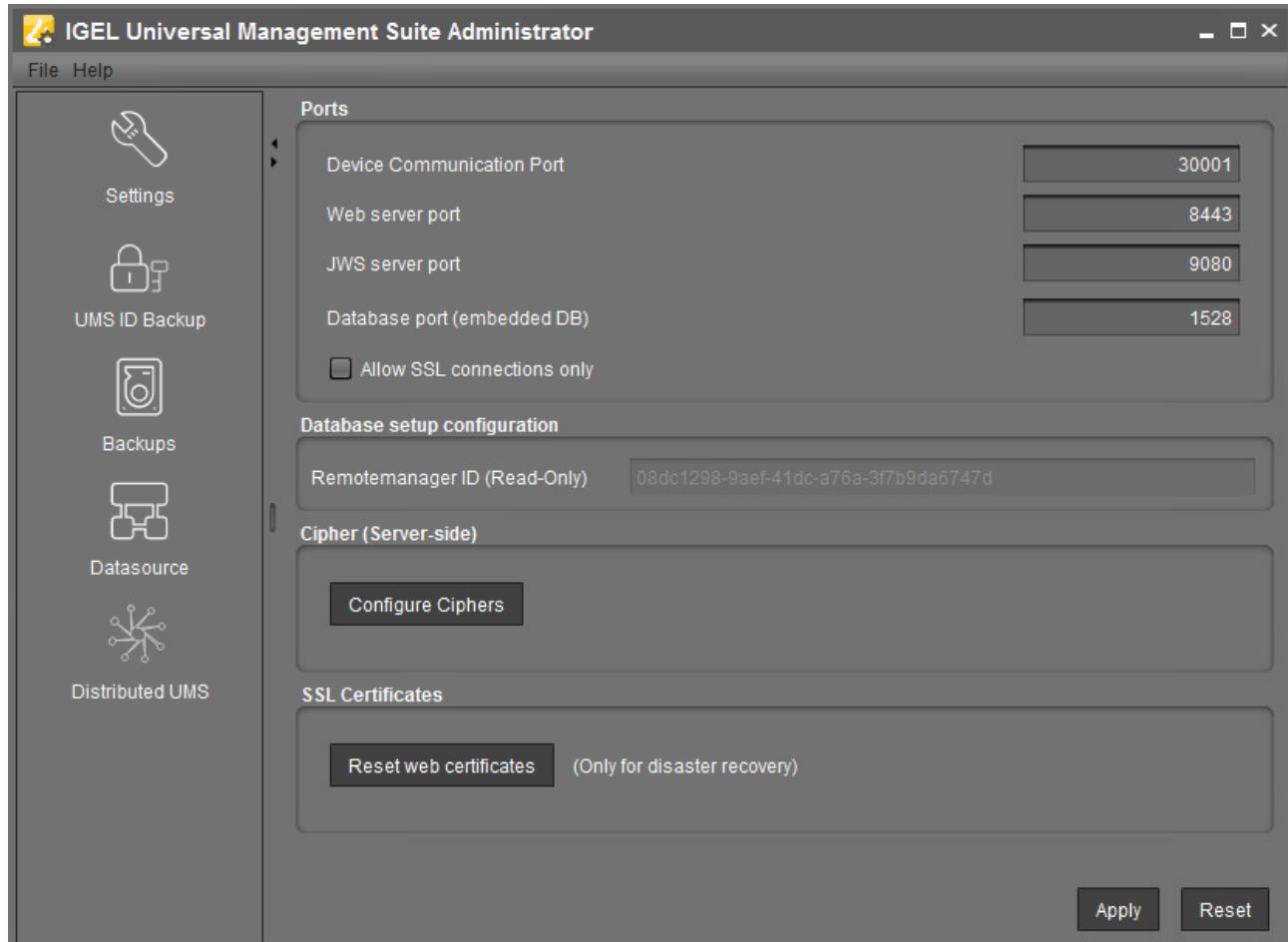
The following log files are collected from the device by default:

- /config/Xserver/card0
- /config/Xserver/monitor-info
- /config/Xserver/xorg.conf-0
- /var/log/Xorg.0.log
- /var/log/auth.log
- /var/log/daemon.log
- /var/log/igfmount.log
- /var/log/kern.log
- /var/log/syslog
- /var/log/tcsetup.log
- /wfs/user/setup-assistant.log

You can add more log files locally on the device through IGEL Setup or through the UMS Web App under **Accessories > System Log Viewer**. For further information, see System Log Viewer.

The IGEL UMS Administrator

The IGEL UMS Administrator application is only available on a UMS Server as it enables you to change the communication between the services directly. You can edit basic settings such as the ports to be used or the data sources to be connected. 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 with the following command: `/[IGEL installation directory]/RMAdmin.sh` (when the default installation directory is used: `/opt/IGEL/RemoteManager/RMAdmin.sh`)
It is NOT recommended to execute `RMAdmin.sh` with `sudo`. On Red Hat Enterprise Linux 8, `RMAdmin.sh` can be executed only without `sudo`.
- ⓘ 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 - Change Server Settings in the IGEL UMS Administrator \(see page 552\)](#)
- [UMS ID Backup in the IGEL Administrator \(see page 556\)](#)
- [Backups \(see page 562\)](#)
- [Data Source \(see page 571\)](#)
- [Distributed UMS - Perform Local UMS Actions in the IGEL UMS Administrator \(see page 580\)](#)
- [IGEL UMS Administrator Command-Line Interface \(see page 582\)](#)

Settings - Change Server Settings in the IGEL UMS Administrator

Using the IGEL Universal Management Suite (UMS) Administrator, you can edit various server settings, e.g. web server port, ciphers, etc.

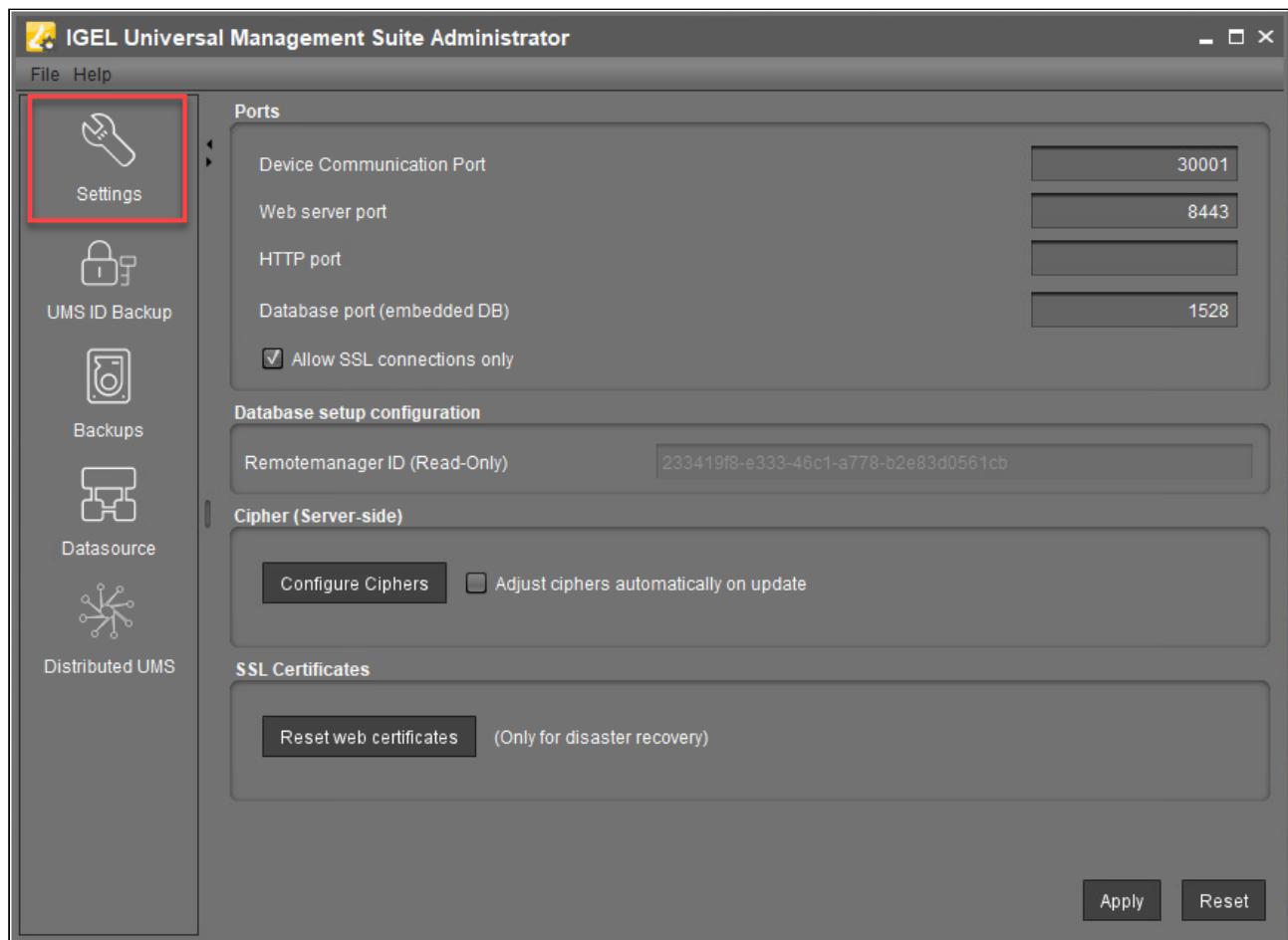
- i** Default path to the UMS Administrator:

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.

Menu path: **UMS Administrator > Settings**



Ports

Device Communication Port: The devices connect to this port. (Default: 30001)

- i** Changes to this port can only be made if you ensure that devices will establish a connection to the new port. For more information on ports, see IGEL UMS Communication Ports.

Web server port: Establishes the connection to the server. This port must be entered in the login window for the IGEL UMS Console or in the URL for the UMS Web App. (Default: 8443)

- i** If the port is changed, the service IGEL RMGUIServer/igelRMServer must be restarted.

- ⚠** If no [Cluster Address](#) (see page 420) is configured, the already registered IGEL OS 12 devices won't be manageable anymore after the change of the web server port. Therefore, you will have to register these devices again.
If the change of the web server port is required, it is thus recommended to change the port before registering IGEL OS 12 devices.

HTTP port: If **Allow SSL connections only** is deactivated, this port is used to reach the UMS via a non-encrypted connection via HTTP. For this to be possible, this port must be specified in the connection URL, e.g. `http://<server>:9080/ums_filetransfer/`. (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 SSL connections only

- A connection will only be allowed via SSL. This parameter is activated by default only for new UMS installations starting with UMS version 12.02.100. (Default)

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.

The List of Default Cipher Suites

```
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
```

- **Ok:** Save the changes.
- **Cancel:** Discard all changes.

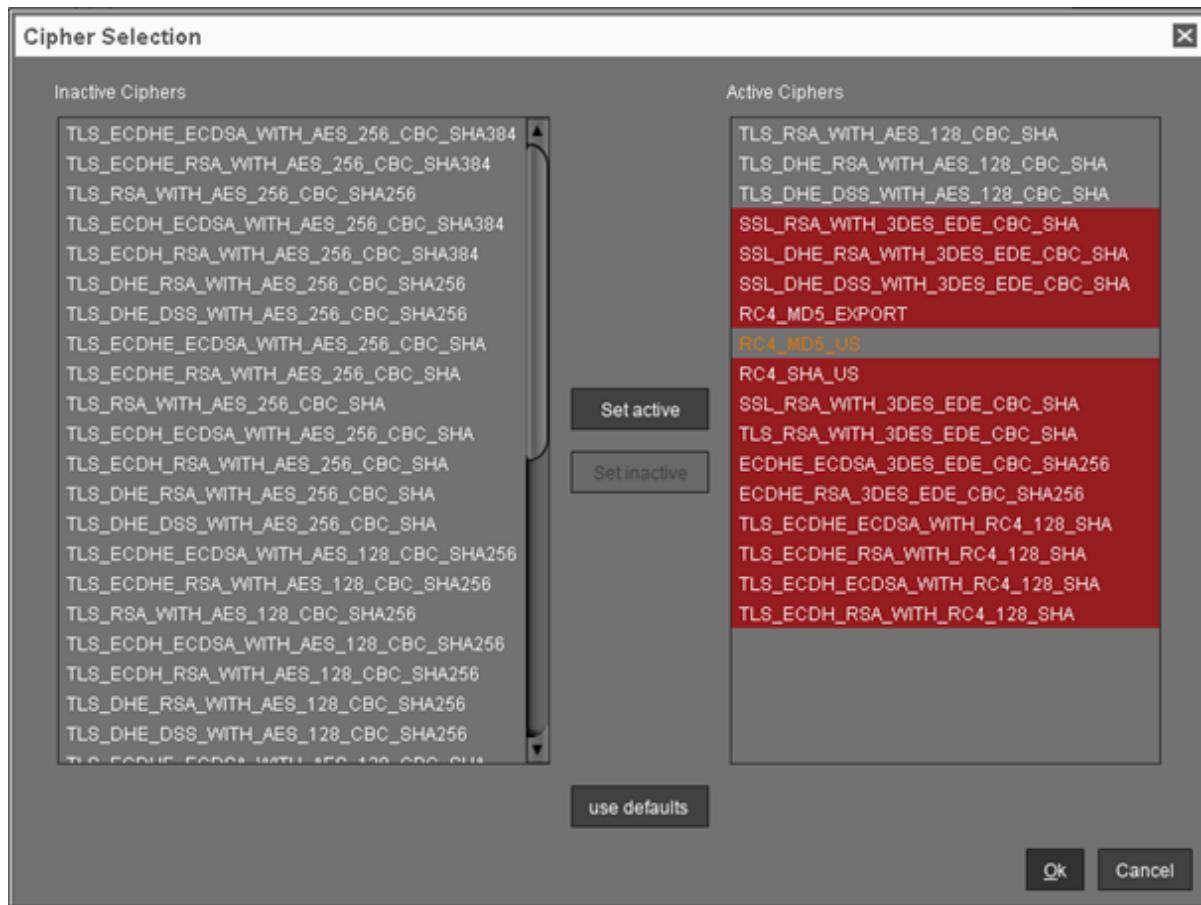
 On new UMS installations, only the [default ciphers \(see page 554\)](#) are activated. By updating the existing UMS installations, the already configured ciphers are kept.

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:



Adjust ciphers automatically on update

- All new ciphers get activated and all weak ciphers get deactivated automatically on every update.
- Cipher configuration is not automatically adjusted on an update.

SSL Certificates

Reset web certificates (Only for disaster recovery): Use this only if you cannot access the UMS Server from the UMS Console or the UMS Web App. This function deactivates the certificate chain that was previously used for communication over the Web Port (i.e. the port used for HTTPS; default: 8443; for more information, see IGEL UMS Communication Ports). Also, it creates a new certificate chain which is then used for HTTPS.

- i** If you want to use your own certificate or certificate chain after the reset, see Using Your Own Certificates for Communication over the Web Port (Default: 8443).

UMS ID Backup in the IGEL Administrator

In the IGEL UMS Administrator, you can create a backup of the UMS ID (called "UMS Licensing ID" before UMS 12). For information on the UMS ID, see also [UMS ID \(see page 477\)](#).

- i** 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.

Menu path: **UMS Administrator > UMS ID Backup**

- i** The UMS ID is generated upon each UMS Server installation. Therefore, if you have a High Availability or Distributed UMS environment (see [IGEL UMS Installation \(see page 13\)](#)), each of the servers has its own UMS ID, i.e. **Local UMS ID**. For the communication of all UMS Servers with the ILP and IGEL Cloud Services, a **Main UMS ID** is used.

Main UMS ID: The first and last 10 characters of the main UMS ID are displayed here.

Main UMS ID fingerprint: The SHA-256 fingerprint of the main UMS ID.

Local UMS ID: The first and last 10 characters of the local UMS ID are displayed here.

- ⚠** In a High Availability environment, the local UMS ID can differ from the main UMS ID. If this is the case, restart the server to get it synchronized. See also [Manual Synchronization of the UMS ID](#). This is also relevant for the Distributed UMS installations.

Local UMS ID fingerprint: The SHA-256 fingerprint of the local UMS ID.

Create new Main UMS ID: If the installation does not have a UMS ID, then this was not created during the installation and the creation must be triggered manually.

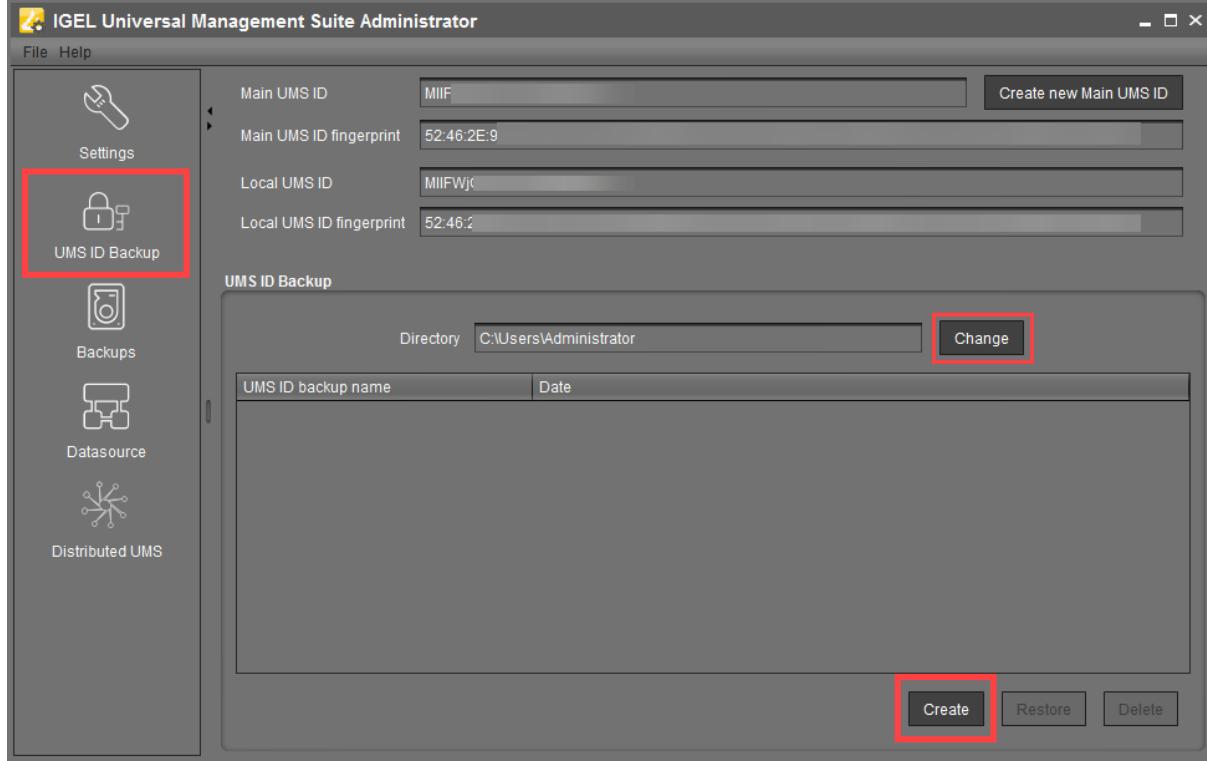
Directory: Path where to store the backup.

UMS ID backup name: The name of the backup which you have defined during the creation.

Date: Date of the backup.

How to Create a Backup of the UMS ID

1. Open the UMS Administrator and go to **UMS ID Backup**.



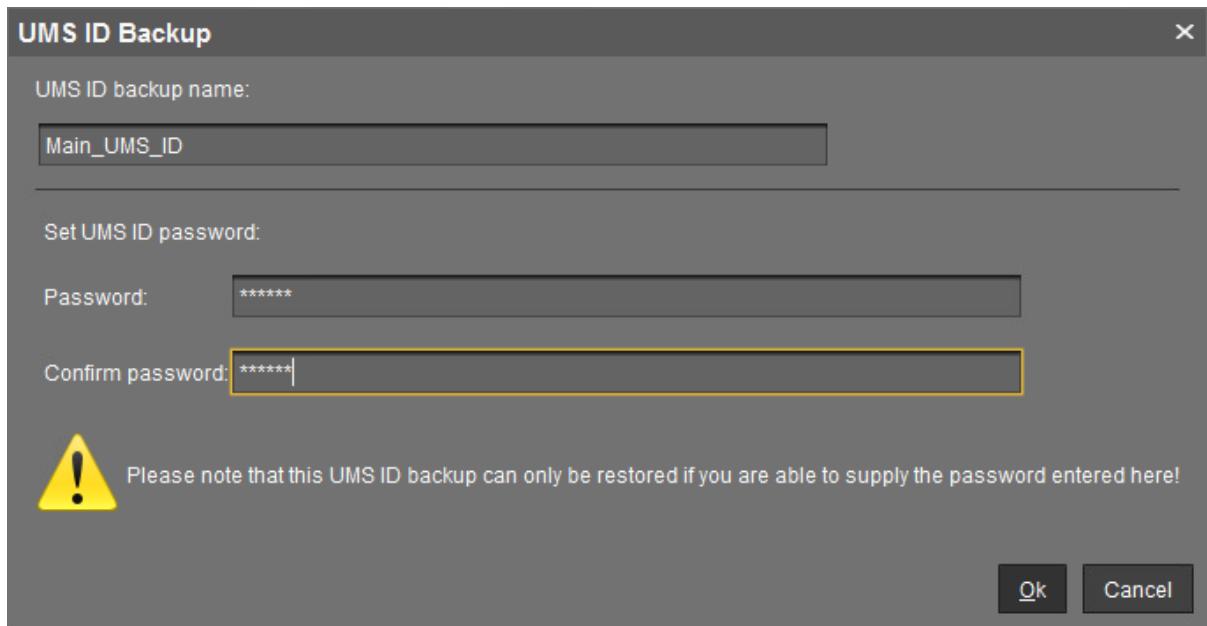
2. Click **Change** if you want to change the directory for storing the backup.

3. Click **Create**.

The **UMS ID Backup** dialog opens.

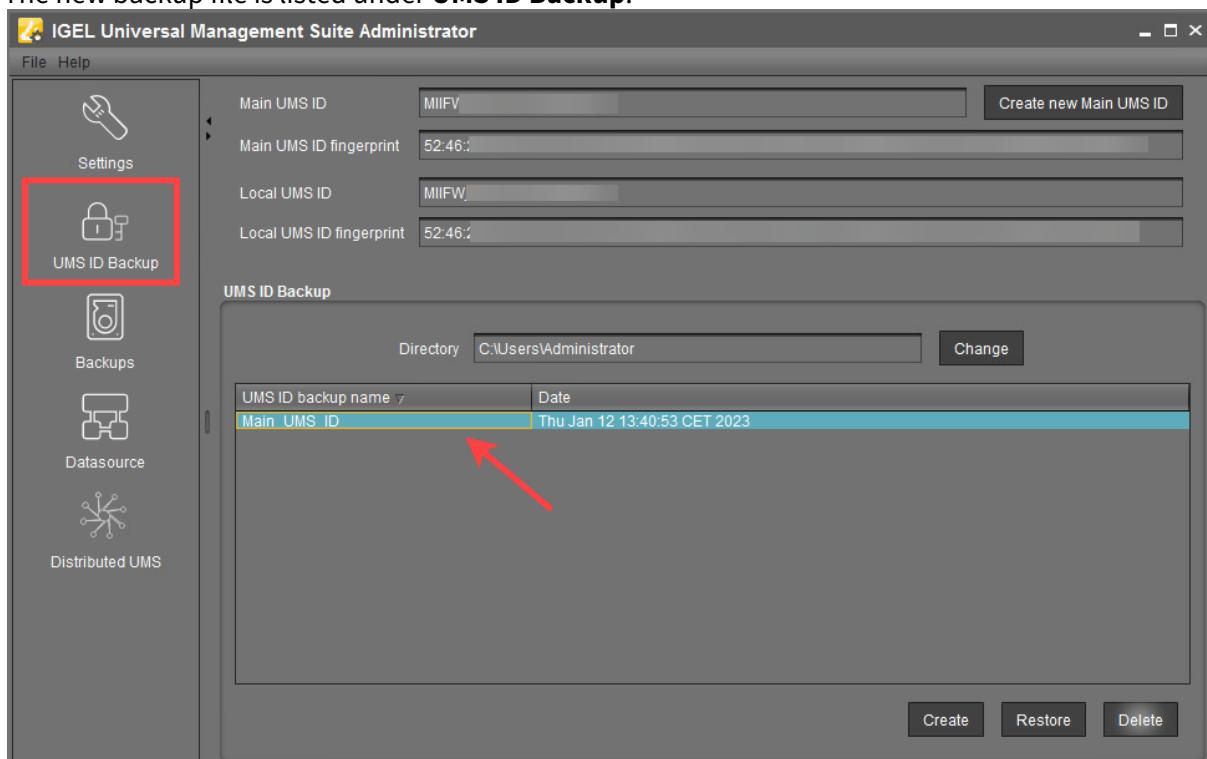
i If you are using a High Availability or Distributed UMS environment, note the following:
It is always the UMS ID of the local server that is backed up. Therefore, make sure at first that the **local UMS ID** is the same as the **main UMS ID**. If not, restart the UMS Server to synchronize the local UMS ID with the main UMS ID and then proceed with creating the backup. See also Manual Synchronization of the UMS ID.

4. Enter a **name** for the UMS ID backup and a **password**. Remember the password, otherwise you won't be able to restore the backup.



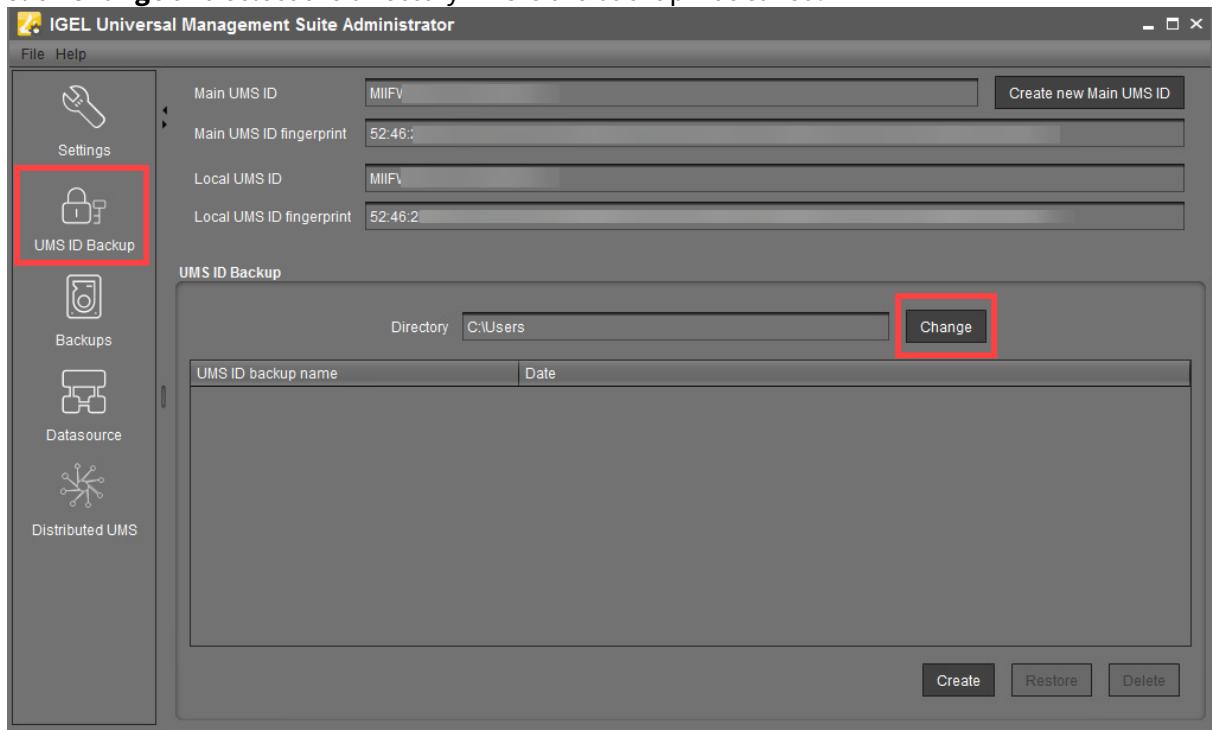
5. Click **OK**.

The new backup file is listed under **UMS ID Backup**.

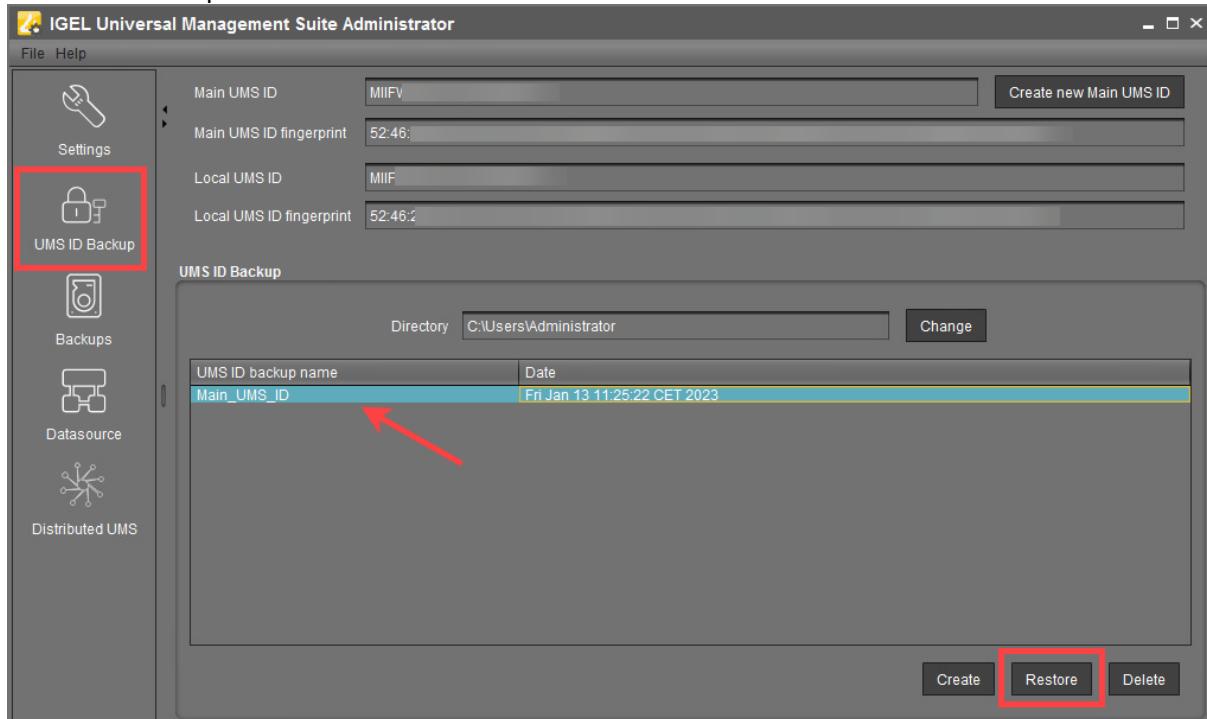


How to Restore a Backup of the UMS ID

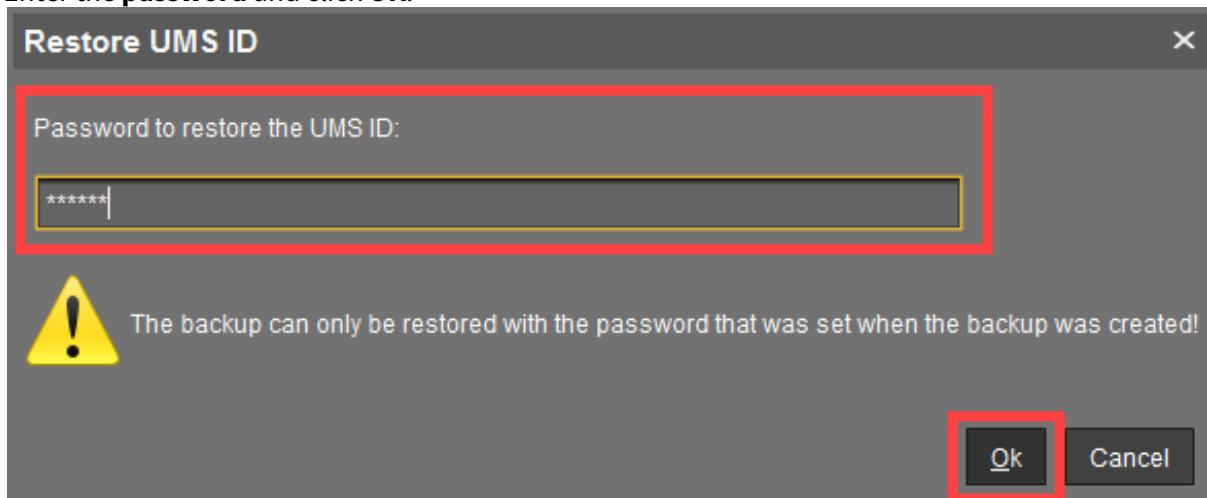
1. Open the UMS Administrator and go to **UMS ID Backup**.
2. Click **Change** and select the directory where the backup was saved.



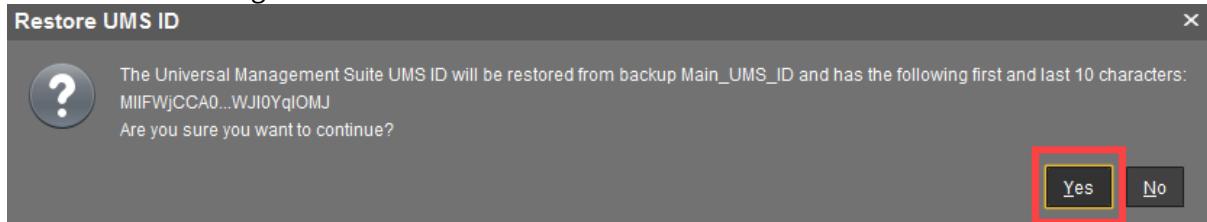
The backup appears in the list of the available UMS ID backups.

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

The **Restore UMS ID** dialog opens.

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

5. Confirm the restoring.



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 of the IGEL UMS \(see page 563\)](#)
- [Restoring a Backup \(see page 567\)](#)
- [Deleting a Backup \(see page 569\)](#)
- [Planned Backup \(see page 570\)](#)

- ⚠ For external database systems, please use the backup and recovery procedures recommended by the DBMS manufacturer. For more information, see [Creating a Backup of the IGEL UMS \(see page 563\)](#).

Creating a Backup of the IGEL UMS

The following article explains how you can create a backup of your IGEL Universal Management Suite (UMS) installation.

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:

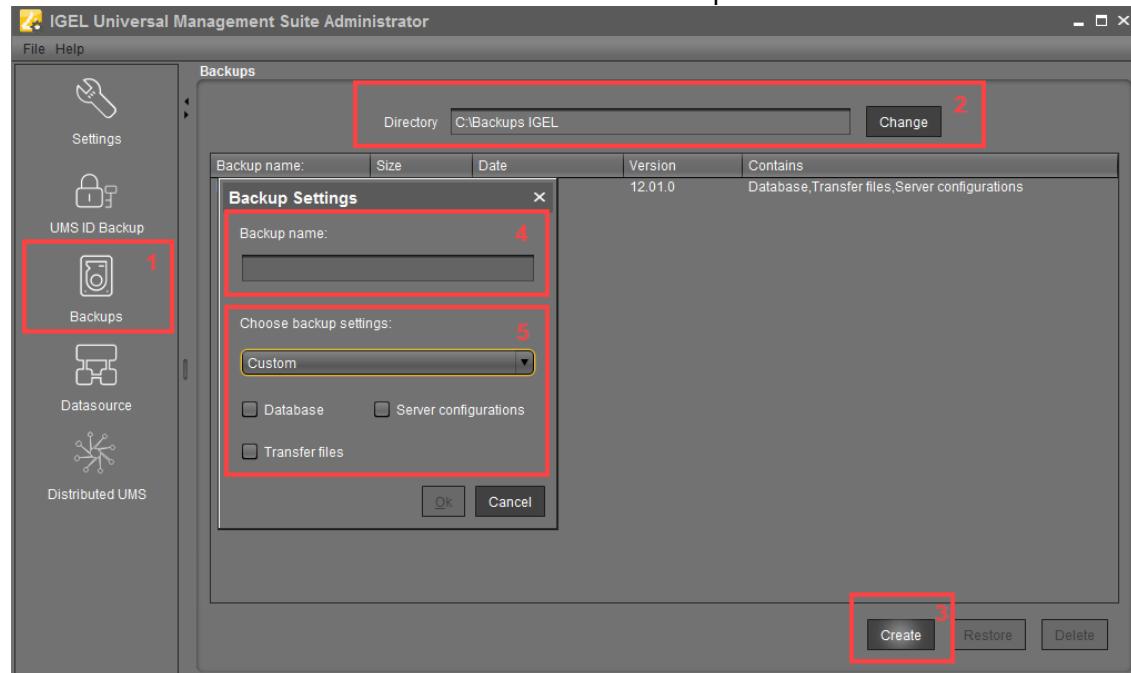
1. Open the UMS Administrator and select **Backups**.
2. Click **Change** to change the storage location for your backups.
3. Click **Create**.
4. Under **Backup name**, enter a name for the backup.

5. Select the backup settings under **Choose backup settings**:

The following can be selected:

- **Select all** (Default): Database, [server configurations](#) (see page 564), and transfer files (normally, you'll use this option to ensure that no components are missing from the backup)
- **Embedded Database**: Database
- **All files**: Transfer files (e.g. images, session certificates, etc.)
Note that files which have not been registered in the UMS, but are only stored in the system web resources (e.g. were manually placed in the folder `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.
- As of UMS version 6.08, all device licenses are included in the database backup. Backups of licenses made with the previous UMS versions are supported: Restore the backup, and the license files stored in the backup will eventually be saved in the database; see [Restoring a Backup](#) (see page 567).



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 552) area in the UMS Administrator application. Exceptions: **Web 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 ID, see [UMS ID Backup in the IGEL Administrator \(see page 556\)](#).

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 \(see page 98\)](#), 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.

Certificates

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/*

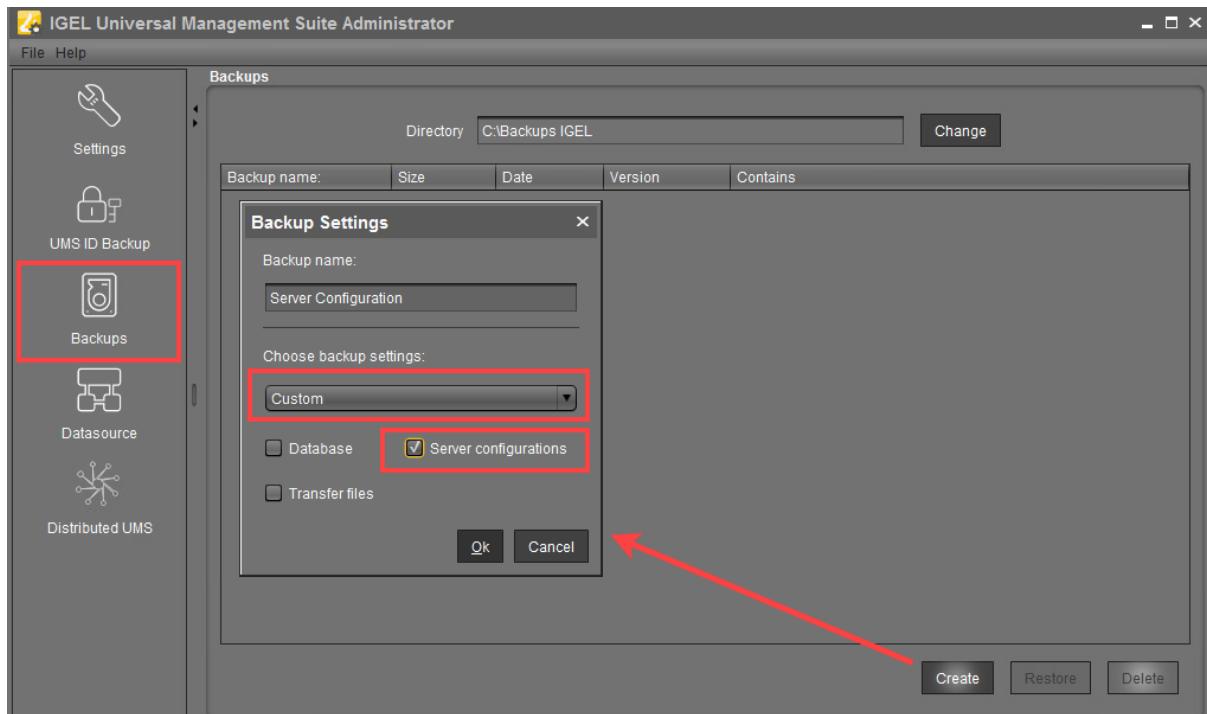
It includes the `tc.keystore` file, which is necessary for the communication with the endpoint devices. The certificate of this keystore can also be exported via the UMS Console under **UMS Administration > Global Configuration > Certificate Management > Device Communication > Export key pair** .

- [IGEL installation directory]/rmclient/cacerts
- [IGEL installation directory]/rmguiserver/
`https_cert_chain.keystore`

Licenses

As of UMS version 6.08, all device licenses are included in the database backup. Previously, they were stored in [IGEL installation directory]/rmguiserver/webapps/e08ce61-d6df-4d2b-b44a-14c1ec722c44 and had to be backed up separately, i.e. manually copied to a secure storage medium.

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 \(see page 564\)](#):



3. Files and firmware updates must be backed up separately, i.e. manually copied to a secure storage medium. You can find them here: [IGEL installation directory]/rmguiserver/webapps/ums_filetransfer
4. Back up also the UMS ID, see [UMS ID Backup in the IGEL Administrator](#) (see page 556).

i If you are using a High Availability or Distributed UMS environment, note the following:
It is always the UMS ID of the local server that is backed up. Therefore, make sure at first that the **local UMS ID** is the same as the **main UMS ID**. If not, restart the UMS Server to synchronize the local UMS ID with the main UMS ID and then proceed with creating the backup. See also [Manual Synchronization of the UMS ID](#).

5. For HA installations 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](#). If a new IGEL network token has been generated in the meantime, e.g. if changes to certificates were made (see "High Availability" under [Device Communication](#) (see page 408)), 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, see [Creating a Backup of the IGEL UMS](#) (see page 563).

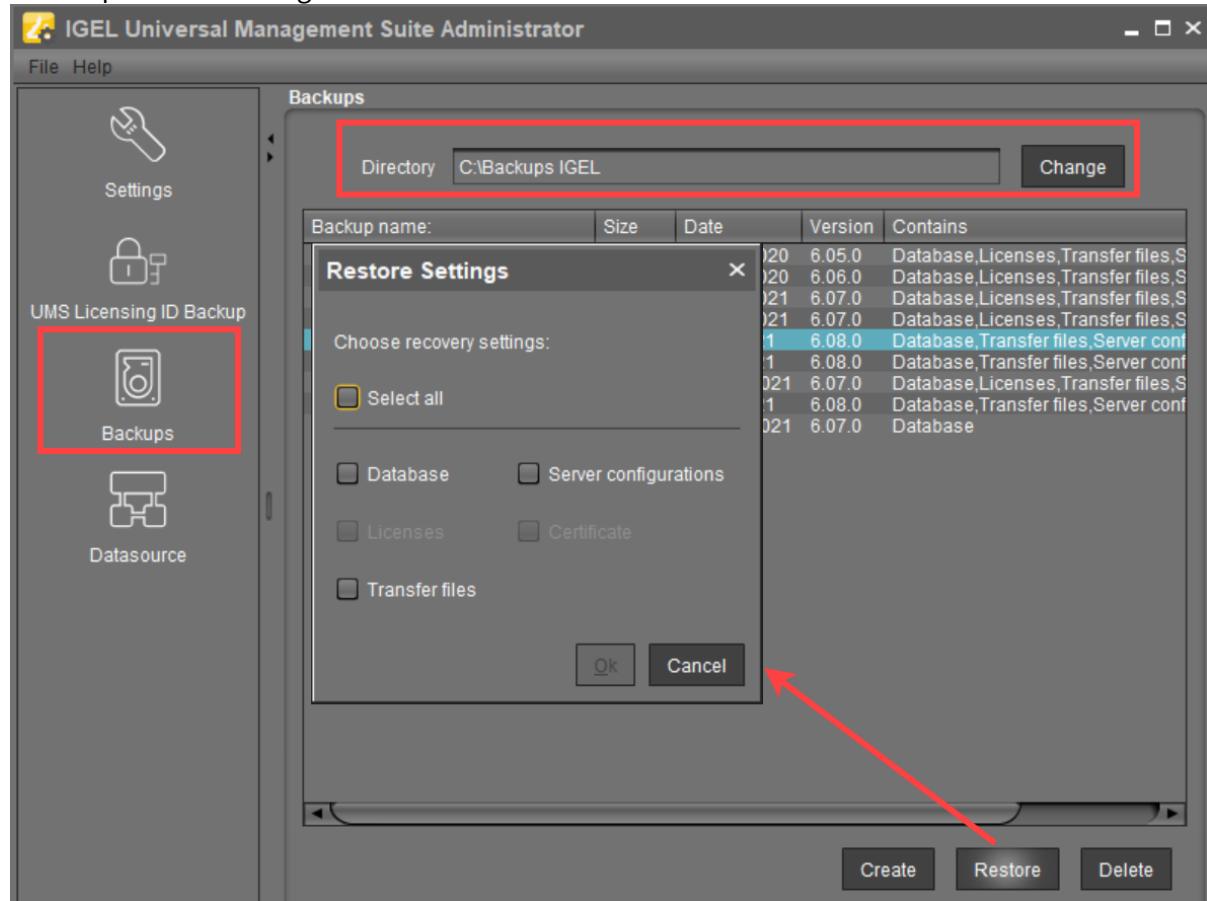
- ⓘ If you restore a database backup of an embedded database of a UMS version prior to 6.05, the superuser credentials are identical to the credentials of the database user. It is recommended to reset the superuser password.

For database backups of UMS versions 6.05 and higher, the superuser credentials have already been stored in the database backup and are taken from there.

To restore a saved backup, proceed as follows:

1. Check under **UMS Administrator > Backups** 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**.
4. Select the components to be restored.
In UMS installations with an external database, you can use the UMS Administrator only to restore

a backup of server configurations.



i The **Certificate** and **Licenses** options are greyed out since they are included in the database backup as of UMS version 5.09 and 6.08 respectively.

Once your data have been restored, the login data for the database will be displayed.

Tip

To avoid problems with backup restoring and with UMS performance generally, 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; see [Administrative Tasks - Configure Scheduled Actions for the IGEL UMS](#) (see page 436). See also [Performance Optimizations in IGEL UMS](#) (see page 78).

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!

Planned Backup

You can define a scheduled backup under **UMS Administration > Administrative Tasks**, see [Create Data Backup](#) (see page 438).

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 98).

- [How to Set Up a Data Source in the IGEL UMS Administrator](#) (see page 572)
- [Activating a Data Source](#) (see page 576)
- [Copying a Data Source](#) (see page 577)
- [Optimizing the Active Embedded DB](#) (see page 578)
- [Changing the UMS Superuser](#) (see page 579)

How to Set Up a Data Source in the IGEL UMS Administrator

Menu path: **UMS Administrator > Datasource**

The following article details how to configure the IGEL Universal Management Suite (UMS) data source.

The IGEL UMS supports the following data source types:

- Embedded DB (installed via the IGEL UMS)
- Microsoft SQL Server
- Oracle
- PostgreSQL
- Apache Derby

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

For information on the external database systems, see also [Connecting External Database Systems](#) (see page 98).

i Default path to the UMS Administrator:

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

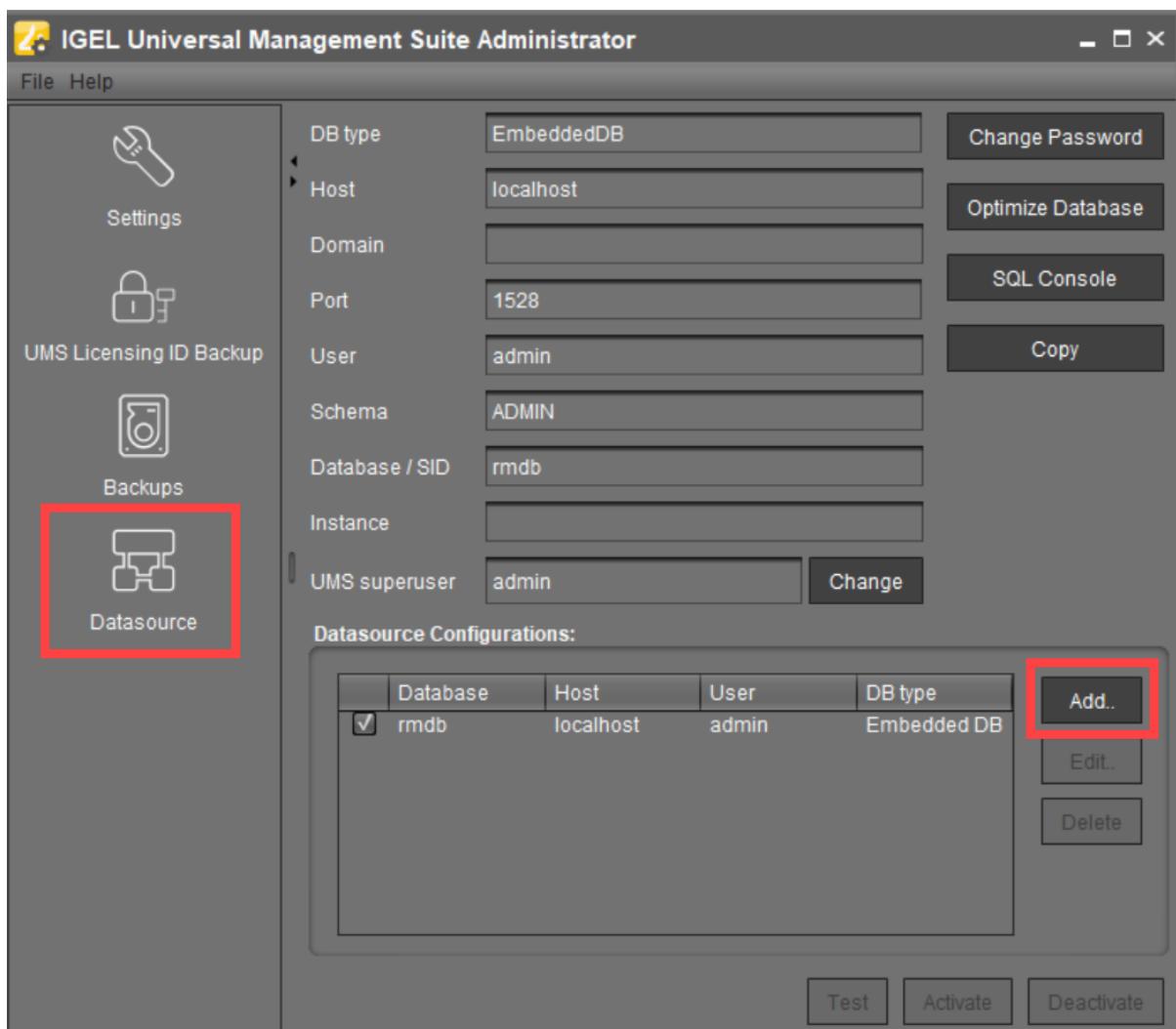
Windows: C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe

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

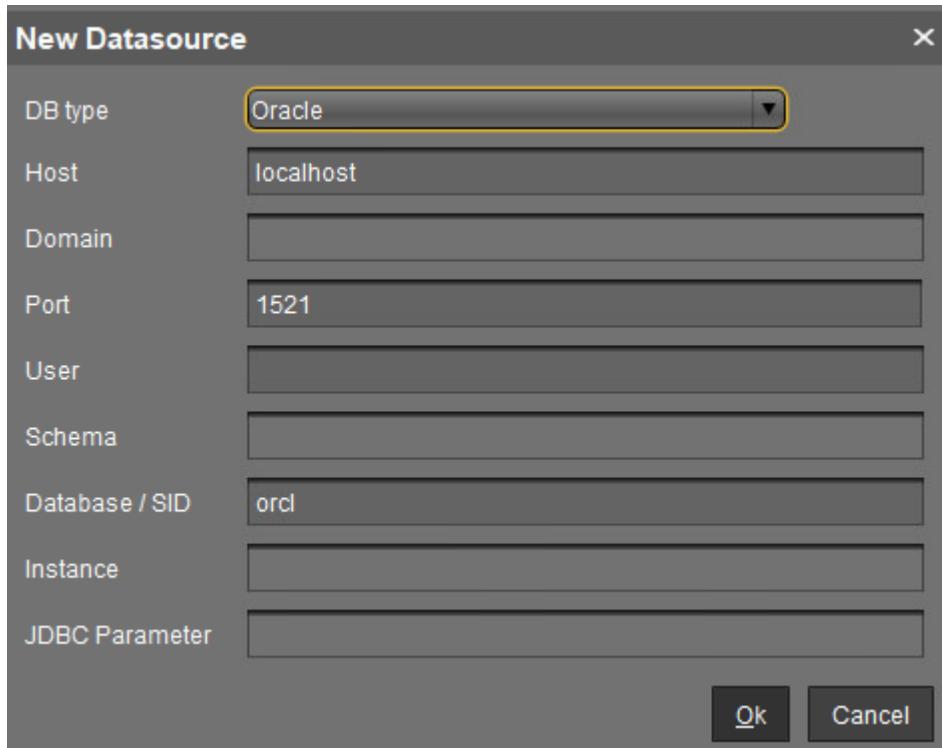
How to Add the Database Connection in the IGEL UMS Administrator

To set up a data source, proceed as follows:

1. Go to **UMS Administrator > Datasource** and click **Add** to add a first data source or an additional one.



A dialog window **New Datasource** will open.



2. Select the **DB type**, and enter the **Host**, and the **Port**, as well as the **User** that is set up on the DBMS. For SQL Server Cluster and Oracle RAC, specify the **Instance**.

i 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.

i 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.

i You can define additional parameters to be added to the JDBC URL via **JDBC Parameter**. Currently, only the following parameters are supported:

- Microsoft SQL Server: `sendStringParametersAsUnicode` (Default value: `true`)

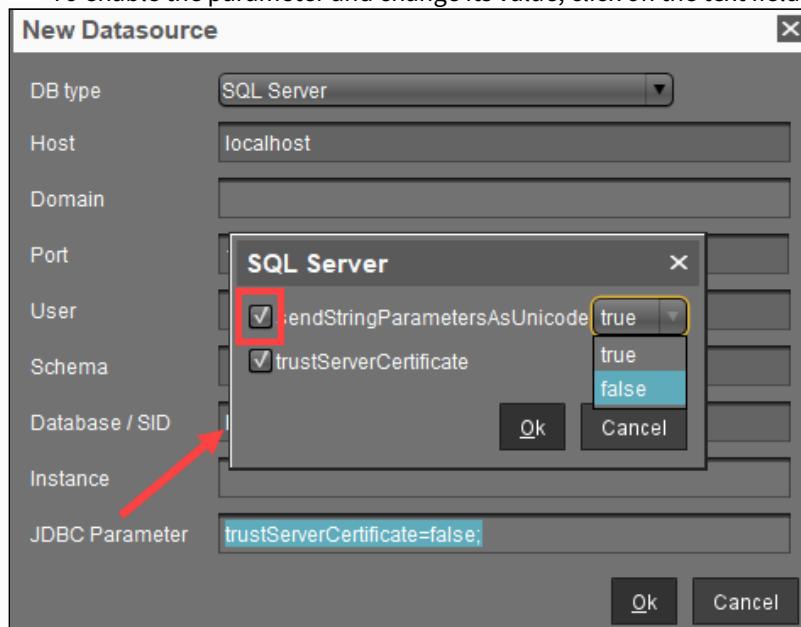
This parameter can be modified to improve the query performance in some cases.

See the Microsoft article [\(SQLServerDataSource\)²¹](https://docs.microsoft.com/en-us/sql/connect/jdbc/reference/setsendstringparametersasunicode-method-sqlserverdatasource?view=sql-server-ver16).

²¹ <https://docs.microsoft.com/en-us/sql/connect/jdbc/reference/setsendstringparametersasunicode-method-sqlserverdatasource?view=sql-server-ver16>

- Microsoft SQL Server: `trustServerCertificate` (Default value: `false`)
 This parameter can be modified to control the certificate check of connections from the UMS to the database. See the Microsoft article [Connecting with encryption - JDBC Driver for SQL Server](#)²².
 The UMS has no preinstalled certificates for MS SQL Server. Please follow the instructions in the Microsoft article if you want to set the property to '`false`'.
 For backward compatibility, the property is set to '`true`' if no value is specified in the field **JDBC Parameter** of the UMS Administrator. New data source definitions are created by default with the value '`false`' for the property.

► To enable the parameter and change its value, click on the text field **JDBC Parameter**.



- Click on **Test** to test the connection to the database.
 This is also possible when a data source is inactive.
- If required, **activate** the data source. See [Activating a Data Source](#) (see page 576).

²² <https://learn.microsoft.com/en-us/sql/connect/jdbc/connecting-with-ssl-encryption?view=sql-server-ver16>

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.

Changing the UMS Superuser

Menu path: **UMS Administrator > Datasource**

The UMS superuser is created initially during the installation process. This user is needed for the first login to the UMS Console and for further configuration tasks, in particular, the definition of additional administrator accounts with restricted rights. The UMS superuser user always has full access rights.

You can change the UMS superuser, which does not affect the user for database connections.

⚠ In an HA environment, changing the **UMS superuser** during operation can lead to issues when the servers are exchanging files. However, these issues are temporary.

- ▶ Click **Change** beside the **UMS superuser** field to change the **User name** and **Password** for the UMS superuser.

Distributed UMS - Perform Local UMS Actions in the IGEL UMS Administrator

In this area of the IGEL Universal Management Suite (UMS) Administrator, you can start or stop the local UMS Server, end its update mode, and activate the Distributed UMS.

For general information on the UMS Administrator, see [The IGEL UMS Administrator \(see page 550\)](#).

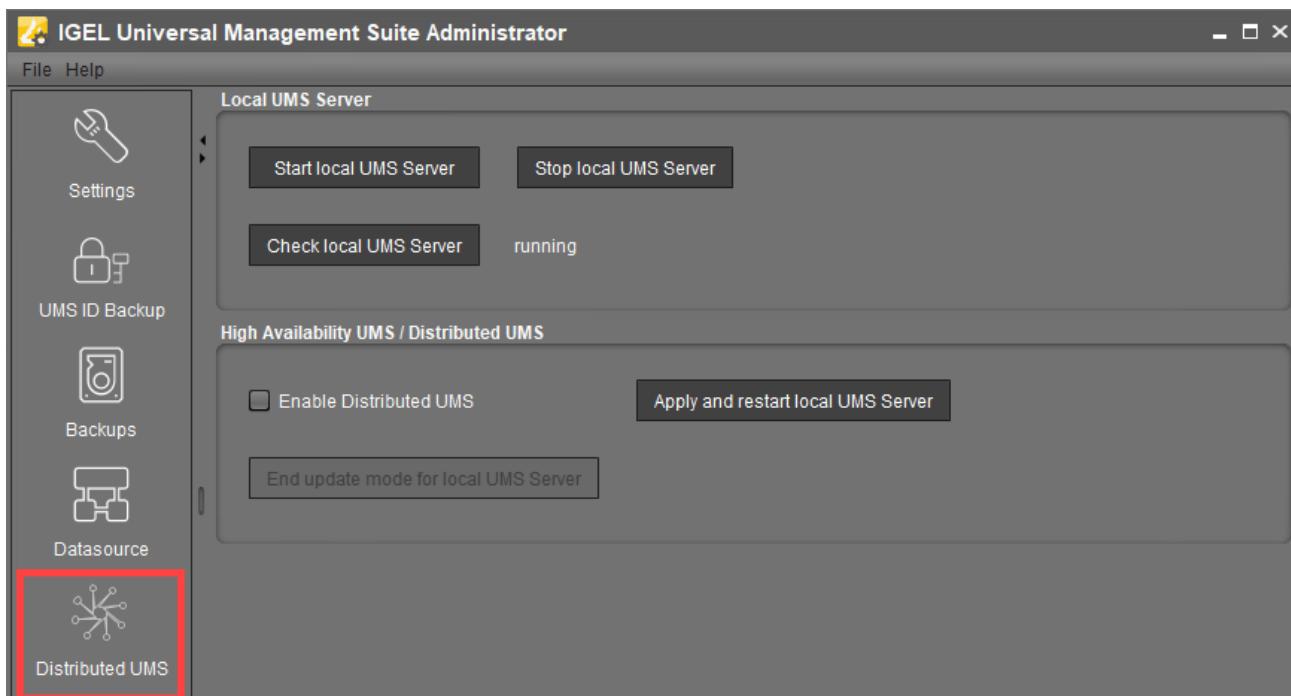
-  Default path to the UMS Administrator:

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.

Menu path: **UMS Administrator > Distributed UMS**



Start local UMS Server

Starts the UMS Server service on this machine. It can take some time till the UMS Server service is fully started.

For additional options for starting / stopping services, see [IGEL UMS HA Services and Processes](#).

Stop local UMS Server

Stops the UMS Server service on this machine. It can take some time till the UMS Server service is fully stopped.

Check local UMS Server

Checks the status of the UMS Server service on this machine.

Possible states:

- **running:** The local UMS Server is up and running.
- **stopped:** The local UMS Server is stopped.
- **unknown:** The status of the UMS Server service is unknown, e.g. when the `IGEL RMGUIServer` service has just been manually stopped/started/paused via Windows Services.

Enable Distributed UMS

The standalone UMS Servers will work just as if they were installed as a High Availability environment if connected to the same external database. Messages between the UMS Servers will be transferred via database entries. For detailed information on the Distributed UMS, see [IGEL UMS Installation \(see page 13\)](#).

For how to install the Distributed UMS or extend an existing standard UMS installation to the Distributed UMS, see [Installing the Distributed IGEL UMS \(see page 59\)](#).

⚠ If you activated the Distributed UMS feature and have multiple UMS Servers, take care in case you decide to disable the feature. If the Distributed UMS feature is deactivated but more than one UMS Server is using the same database, no synchronization will be done between the UMS Servers.

ⓘ If you have a UMS High Availability installation, this checkbox will be greyed out and cannot be activated.

Apply and restart local UMS Server

The changes under **Enable Distributed UMS** will be applied, and the UMS Server service on this machine will be restarted.

End update mode for local UMS Server

Use this feature if you have updated your Distributed UMS or UMS High Availability installation, but the update mode was not automatically stopped when the update procedure was complete.

IGEL UMS Administrator Command-Line Interface

The Universal Management Suite (UMS) Administrator command-line interface (CLI) allows you to control the IGEL UMS Administrator via a terminal and to automate UMS Administrator actions via scripting. Among these actions are creating and editing database connections for the UMS Server, backing up and restoring the embedded database, configuring communication ports and security, managing the UMS ID, configuring the superuser, and restarting the UMS Server.

As this feature allows complete control without any graphical desktop environment, it is possible to run the CLI application on headless Linux systems.

Basic Usage

Like the graphical UMS Administrator application, the CLI requires elevated privileges.

- ▶ Windows: Open a command prompt (`cmd.exe`) as Administrator.
- ▶ Linux: Become `root` or use `sudo`

You can run the main command `umsadmin-cli` from any directory, as the command is made available on the `PATH`.

▶ To see the global options and the primary subcommands, enter `umsadmin-cli`

```
root@'':~$ /home/ike/Downloads# umsadmin-cli -h
Usage: umsadmin-cli [-hV] [--machine-readable] [--no-header] [--quiet]
                      [--separator=<cliSeparator>] [COMMAND]
Configures UMS installation
  -h, --help          Show this help message and exit.
  --machine-readable Prints output machine-readable with ';' as default
                      separator.
  --no-header        Do not print a header line.
  --quiet            Suppress all output to stdout/stderr.
  --separator=<cliSeparator>
                      Define custom column separator for CLI output.
  -V, --version       Print version information and exit.
Commands:
  db                Provides commands for database operations
  ports             Configuration of ports
  cipher            Manage cipher configuration.
  license           View and change licensing ID data
  token             Install network token vor UMS server or broker.
  su                Configuration of superuser
  restart-server    Restart the server
  help              Displays help information about the specified command
```

- To get all possible options for a specific subcommand, enter `umsadmin-cli` followed by the subcommand, e.g. `umsadmin-cli db create`

```
root@td-: /home/ike# umsadmin-cli db create
Missing required options: '--type=TYPE', '--user=USER'
Usage: umsadmin-cli db create [-d=DOMAIN] [-H=HOST] [-I=INSTANCE] [-n=NAME]
                  [-p=PORT] [-S=SCHEMA] -t=TYPE -u=USER (-A |
                  (--password:file=<passwordFile> | --password:in))
Create a new database connection
-A, --no-activate      Skip activation of database (no password required)
-d, --domain=DOMAIN    The database domain
-H, --host=HOST         The database host
-I, --instance=INSTANCE The database instance
-n, --name=NAME         The database name
-p, --port=PORT         The database port
--password:file=<passwordFile>
                      Path to a file containing the password.
--password:in           Shows an interactive prompt to enter the password.
-S, --schema=SCHEMA     The database schema
-t, --type=TYPE          The database type. Valid values:
                        embedded    -> Embedded DB
                        oracle      -> Oracle
                        oracle-rac -> Oracle RAC
                        mssql       -> SQL Server
```

 Certain subcommands have no options and run immediately. Please refer to the [Command Reference](#) (see [page 586](#)).

- To get the complete online help with all commands, enter `umsadmin-cli fullhelp`

```
root@...:/home/ike# umsadmin-cli fullhelp
Usage: umsadmin-cli [-hV] [--machine-readable] [--no-header] [--quiet]
                     [--separator=<cliSeparator>] [COMMAND]
Configures UMS installation
-h, --help           Show this help message and exit.
--machine-readable Prints output machine-readable with ';' as default
                     separator.
--no-header         Do not print a header line.
--quiet             Suppress all output to stdout/stderr.
--separator=<cliSeparator>
                     Define custom column separator for CLI output.
-V, --version        Print version information and exit.
Commands:
db                  Provides commands for database operations
help                Displays help information about the specified command
activate            Activate a database connection
-i     --id           The database identifier
--password:file    Path to a file containing the password.
--password:in      Shows an interactive prompt to enter the password.
```

- ▶ To get the list of available commands, enter `umsadmin-cli help`

```
C:\Program Files\IGEL\RemoteManager\rmadmin>umsadmin-cli help
Usage: umsadmin-cli [-hV] [--machine-readable] [--no-header] [--quiet]
                     [--separator=<cliSeparator>] [COMMAND]
UMS Administrator CLI to configure UMS installation
-h, --help           Show this help message and exit.
--machine-readable Prints output machine-readable with ';' as default
                     separator.
--no-header         Do not print a header line.
--quiet             Suppress all output to stdout/stderr.
--separator=<cliSeparator>
                     Define custom column separator for CLI output.
-V, --version        Print version information and exit.
Commands:
db                  Provides commands for database operations
ports               Configuration of ports
cipher              Manage cipher configuration.
licensing            View and change UMS ID data
token               Install network token for UMS server or broker.
su                  Configuration of superuser
restart-server     Restart the UMS server (deprecated, use 'server restart')
server              Change the server run state
reset-certs         Reset the web certificates
ums-cluster         Set UMS cluster FQDN
web-certs           Provides commands for web certificates configuration
help                Displays help information about the specified command
fullhelp            Show full help with all commands
```

- ▶ To display help information about any command, use `help` as a subcommand. For example, enter
`umsadmin-cli web-certs help`

Global Options

If you intend to use the UMS Administrator CLI in a script, you may want to configure its output to stdout/stderr according to your needs. This makes it easy to further process the output of `umsadmin-cli` and extract any relevant data.

Please see the available options below.

--machine-readable

Prints output machine-readable with a semi-colon (;) as default separator.

Example:

```
root@machine:/home/locadmin# umsadmin-cli --machine-readable db list
ACTIVE;DATABASE;HOST;USER;DB-TYPE;ID
true;rmdb;localhost;root;Embedded DB;1
```

--no-header

No header line is printed. (Not all commands print a header.)

Example:

```
root@machine:/home/locadmin# umsadmin-cli --machine-readable --no-header db
list
true;rmdb;localhost;root;Embedded DB;1
```

--quiet

All output to stdout/stderr is suppressed for some commands which might take a long time to execute. These are, for instance, `db backup`, `db restore`, `db copy`, and `server-restart`.

Example:

```
root@machine:/home/locadmin# umsadmin-cli --quiet db backup -o /tmp/
mybackup02.pbak --full
root@machine:/home/locadmin#
```

It is still possible to redirect all output to a null device using operating system functions. For example, to redirect standard output and error output to the null device on Linux, use:

```
command ... >/dev/null 2>&1
```

--separator

Defines a custom column separator for output to stdout/stderr.

Example:

```
root@machine:/home/locadmin# umsadmin-cli --machine-readable --no-header --  
separator "||" db list  
true||rmdb||localhost||root||Embedded DB||1
```

- i Some separator characters, such as the pipe symbol (|), require quotes because they have special functions in terminals.

Exit Codes

Exit Code	Meaning
0	Successful execution
1	Internal error. An error number is outputted to stderr; for details, see Error Numbers (see page 617) .
2	Wrong usage of the CLI or invalid arguments

Command Reference

i General Usage of Password Options

Some commands require a password. Entering the password in plain text on the command line is not secure and therefore not possible. Therefore, one of the following password options must be used:

`--password:in` for interactively entering the password (possibly with confirmation)

`--password:file <FILE>` for providing a file containing the password

A password file must have the password as the first line and the passwords must not be pure whitespace. Additional lines with content are allowed but will not be evaluated.

i UMS Server Restart Required

Most of the commands in the sections "Ports", "Cipher", "Reset Certificates", and "Superuser" change the UMS configuration and a restart of the UMS server is required to make the new settings take effect. This can be done in two ways:

- Use the appropriate function of the OS (e.g. `systemctl` on Linux)
- Use the command `umsadmin-cli server restart`

Database

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
List all configured data sources	db	list					<p>Shows the ID of the data source, which is required by other commands.</p> <p>The lowest ID is 1.</p> <p>IDs may change upon the creation and deletion of data sources.</p> <p>It is strongly recommended to always extract the ID before using it in other commands with --id</p> <p>The ID is calculated like this: highest existing ID + 1</p>

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
Show all details of a database	db	show	-i	--id	integer	The ID of the database to show	<p>Run <code>umsadmin-cli db list</code> to get a list of current data sources and select the ID of a data source.</p> <p>Run <code>umsadmin-cli db show --id <ID></code> with that ID.</p>

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
Create a new database connection	db	create	-t	--type	string	The database type. For a list of the possible values, type <code>umsadmin-cli db create</code>	Type, user, and port are required. Other options may or may not be required depending on the DB type <code>db create</code> will activate the database by default; this can be prevented by using <code>-A</code> or <code>--no-activate</code> . A password option cannot be used then. If activation fails, the data source entry will still be present and is not active (same behavior as in the graphical UMS Administrator).

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
							'rmdb' is a reserved name for the embedded database type and cannot be used for other types.
			-H	--host	string	The database host	
			-d	--domain	string	The database domain	
			-p	--port	integer	The database port	
			-u	--user	string	The database username	
			-S	--schema	string	The database schema	
			-n	--name	string	The database name. Free text, except 'rmdb'; this name is reserved for the embedded database.	
			-I	--instance	string	The name of the database instance	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
			-A	--no-activate		The database will not be activated.	
				--password:file	string	The password is read from a file (plain text) whose path is provided after this option.	
				--password:in	string	The password is read from stdin; an interactive prompt is shown.	
Edit a data source	db	edit	-t	--type	string	The database type. For a list of the possible values, type <code>umsadmin-cli db create</code>	Embedded databases cannot be edited (as in the graphical UMS Administrator). All options are optional, except <code>--id</code>
			-H	--host	string	The database host	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
			-d	--domain	string	The database domain	
			-i	--id	integer	The identifier of the database to be edited	
			-I	--instance	string	The name of the database instance	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
				--jdbc-params	string	Additional JDBC parameter.	<p>For details on the JDBC parameters, see How to Set Up a Data Source in the IGEL UMS Administrator (see page 572).</p> <p>Examples:</p>

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
							<ul style="list-style-type: none"> • rmadmin\umsadmin -cli.exe db create --type=mssql --name=rmdb12_00 --host=122.30.229.1 --port=1433 --user=rmdb --password:in --jdbc-params sendStringParametersAsUnicode=false;

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
							<ul style="list-style-type: none"> • radmin/umsadmin-cli.bin db edit -i 1 --jdbc-params sendStringParametersAsUnicode=false;
			-n	--name	string	The database name. Free text, except 'rmdb'; this name is reserved for the embedded database.	
			-p	--port	integer	The database port	
			-S	--schema	string	The database schema	
			-u	--user	string	The database username	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
Activate a database connection	db	activate		--password:file	string	The password is read from a file (plain text) whose path is provided after this option. Example: umsadmin-cli db activate --password:file /home/ike/password.txt	
				--password:in	string	The password is read from stdin; an interactive prompt is shown.	
			-i	--id	integer	The identifier of the database to be activated	
Deactivate the active database connection	db	deactivate	-i	--id	integer	The identifier of the database to be deactivated	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
Test the active database connection	db	test		--password:file	string	The password is read from a file (plain text) whose path is provided after this option. Example: umsadmin-cli db test --password:file /home/ike/password.txt	
				--password:in		The password is read from stdin; an interactive prompt is shown.	
Optimize the active database	db	optimize					This command can only be applied to an embedded database or a Derby database.

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
Create a copy of the current database	db	copy	-t	--target	integer	The ID of the target database To get the database ID, enter umsadmin-cli db list	
				--password:file	string	The password is read from a file (plain text) whose path is provided after this option.	
				--password:in	string	The password is read from stdin; an interactive prompt is shown.	
Delete a database connection	db	delete	-i	--id	integer	The ID of the database connection that is to be deleted	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
Create a backup of the current embedded database	db	backup	-o	--outfile		Path to the target file. The file suffix .pbak is automatically added. Existing backup files are not overwritten.	
			-f	--full		Full backup. Database, server configurations, and transfer files are included.	
			-p	--parent		All directories for the specified path will be created if they are not already existing.	
Restore a backup into the embedded database	db	restore	-f	--file		Path to the backup file	

Ports

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value	Option Description
List all ports and SSL flag	ports	list				
Set new port numbers or SSL-only flag	ports	set	-d	--dev-comm	integer	Device communication port. For details, see Devices Contacting UMS.
			-j	--java-webstart	integer	Java Web Start port
			-w	--web-server	integer	UMS server port. For details, see UMS with Internal Database and UMS with External Database.
			-e	--embedded	integer	Embedded database port
				--ssl-only	boolean	Allow SSL connections only

Cipher

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description
List all ciphers, optionally filtered	cipher	list			List all ciphers
			-e	--enabled	List only enabled ciphers
			-d	--disabled	List only disabled ciphers
Enable ciphers	cipher	enable			Enable ciphers. The ciphers are separated by whitespaces. Example: umsadmin-cli cipher enable CIPHER1 CIPHER 2 CIPHER3
				--all	Apply for all; individual cipher names are ignored.
Disable ciphers	cipher	disable			Disable ciphers. The ciphers are separated by whitespaces. Example: umsadmin-cli cipher disable CIPHER1 CIPHER 2 CIPHER3
				--all	Apply for all; individual cipher names are ignored.

Manage Web Certificates

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description	Remarks
Reset web certificates	reset-certs		-y	--yes	The reset is only executed after confirmation	
Assign certificate to current or all servers	web-certs	assign-cert	-f	--fingerprint-sha1	SHA1 fingerprint of certificate	
				-s	--server Server to which the certificate is assigned. Possible values: <ul style="list-style-type: none">• ALL_SERVER• CURRENT_SERVERR (default)	
Create a root certificate	web-certs	create-root-cert	-a	--algorithm	Key pair algorithm; rsa or ec (default: rsa)	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description	Remarks
			-c	--country	Country code (two letters)	
			-d	--expiration-date	Expiration date (YYYY-MM-DD) (Current date plus 20 years if not specified.)	
				--key-size	Key size (4096, 8192, ... bits). Valid values : <ul style="list-style-type: none">• 4k (default)• 8k• 12k• 16k	
			-l	--locality	Locality (If not specified, the hash code of a random uuid is used.)	
			-n	--name	Certificate name (default: Root certificate)	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description	Remarks
				--named-curve	<p>Named curve. Valid values:</p> <ul style="list-style-type: none"> • nist-p-384 (default) • nist-p-256 • nist-p-521 	
			-o	--organization	<p>Organization (Mandatory option)</p>	
Create signed certificate	web-certs	create-signed-cert	-f	--fingerprint-sha1	SHA1 fingerprint of parent CA certificate	The parent CA certificate is specified by the SHA1 fingerprint. It doesn't matter whether you use no delimiter, '-' or ':' as the delimiter for the fingerprint.
			-n	--name	Certificate name (default: Certificate)	
				--cn	Common name	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description	Remarks
			-c	--country	Country code (two letters)	
			-o	--organization	Organization	
			-l	--locality	Locality (If not specified, the hash code of a random uuid is used.)	
			-d	--expiration-date	Expiration date (YYYY-MM-DD) (Current date plus 1 year if not specified.)	
				--ca	Certificate type: <ul style="list-style-type: none"> <code>true</code> = CA certificate <code>false</code> = End entity (default) 	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description	Remarks
			-h	--hostname	Hostname (hostname or one of these values: <ul style="list-style-type: none"> • ALL_SERVER • CURRENT_SERVER (default))	You can specify a list of hostnames for the subject alternative names (SAN) or you can specify, whether the current server (CURRENT_SERVER) or all servers (ALL_SERVER) should be listed in the SAN list.
Delete a certificate	web-certs	delete	-f	--fingerprint-sha1	SHA1 fingerprint of certificate	
Export certificate	web-certs	export-cert	-c	--cert-file	Path to which the certificate should be exported (Named <code>cert.cert</code> is used when only a directory is specified.)	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description	Remarks
			-f	--fingerprint-sha1	SHA1 fingerprint of certificate	
Export certificate chain to keystore (JKS)	web-certs	export-cert-chain	-f	--fingerprint-sha1	SHA1 fingerprint of certificate	
			-k	--keystore-file	Path to keystore to which certificate chain should be exported	
				--password:file	Path to a file containing the password	
				--password:in	Shows an interactive prompt to enter the password	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description	Remarks
Import certificate chain from keystore	web-certs	import-cert-chain	-k	--keystore-file	The keystore file	
				--password:file	Path to a file containing the password	
				--password:interactive	Shows an interactive prompt to enter the password	
Import decrypted private key	web-certs	import-private-key	-f	--fingerprint-sha1	SHA1 fingerprint of parent CA certificate	
			-p	--private-key-file	The file containing the private key	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description	Remarks
Import root certificate	web-certs	import-root-cert	-c	--cert-file	The root certificate (CERT, CER, CRT, PEM)	
Import signed certificate	web-certs	import-signed-cert	-c	--cert-file	The root certificate (CERT, CER, CRT, PEM)	A certificate can only be imported when no other certificate with the same fingerprint already exists; otherwise, you will get an error message.
				-f --fingerprint-sha1	SHA1 fingerprint of parent CA certificate	
List the assigned server of a certificate	web-certs	list-assigned-server	-f	--fingerprint-sha1	SHA1 fingerprint of certificate	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description	Remarks
List all web certificates or details of a certificate	web-certs	list	-f	--fingerprint-sha1	SHA1 fingerprint of certificate	When you specify a fingerprint, the details of the certificate with that fingerprint are shown.
Renew certificate	web-certs	renew-cert	-f	--fingerprint-sha1	SHA1 fingerprint of certificate	You only have to specify the fingerprint of the certificate that should be renewed. If the other parameters are not specified, the values from the old certificate are used (with a new expiration date).
			-n	--name	Certificate name	
				--cn	Common name	
			-c	--country	Country code (two letters)	
			-o	--organization	Organization	
			-l	--locality	Locality	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description	Remarks
			-d	--expiration-date	Expiration date (YYYY-MM-DD) (Current date plus 1 year if not specified)	
			-h	--hostname	Hostname (hostname or one of these values: <ul style="list-style-type: none"> ALL_SERVER CURRENT_SERVER R	

Superuser

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value	Option Description
Show UMS superuser	su	list				
Change UMS superuser	su	change	-u	--user	string	New superuser

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value	Option Description
			-p	--password:file	string	The password is read from a file (plain text) whose path is provided after this option.
				--password:in	string	The password is read from stdin; an interactive prompt is shown.

UMS ID

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value	Option Description
Show the current UMS IDs	licensing	list				
Create a new UMS ID	licensing	create				
Backup the UMS ID	licensing	backup	-o	--outfile	string	Path to the target file (file suffix: .ksbak)
			-p	--parent		All directories for the specified path will be created if they are not already existing.
				--password:file	string	The password is read from a file (plain text) whose path is provided after this option.

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value	Option Description
				--password:in	string	The password is read from stdin; an interactive prompt is shown.
Restore a UMS ID from a backup	licensing	restore	-f	--file	string	Path to the backup file
				--password:file	string	The password is read from a file (plain text) whose path is provided after this option.
				--password:in	string	The password is read from stdin; an interactive prompt is shown.

Network Token

Action	Primary Subcommand	Short Option	Long Option	Value	Option Description	Remarks
Install a network token for the UMS Server or a broker (UMS HA)	token	-f	--token-file	string	Path to token file	This command is also available as a standalone command named <code>umstokeninstall-cli</code> in broker-only installations. It is equivalent to <code>umsadmin-cli token</code> .

Action	Primary Subcommand	Short Option	Long Option	Value	Option Description	Remarks
			--server	boolean	Install token for UMS Server	
			--broker	boolean	Install token for broker	

UMS Cluster

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description
Show the current UMS cluster FQDN	ums-cluster	list			
Set a new UMS cluster FQDN	ums-cluster	create	-n	--name	Name for the new UMS cluster FQDN
Delete the current UMS cluster FQDN	ums-cluster	remove			

Server

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description
Start the local UMS Server	server	start			
Stop the local UMS Server	server	stop			
Restart the local UMS Server	server	restart			
End the update mode of the local UMS Server	server	end-update-mode			
Set the distributed mode (see page 13) of the UMS installation	server	distributed	-e	--enable	Enable Distributed UMS
			-d	--disable	Disable Distributed UMS

Error Numbers

The error numbers are printed in the following format:

<E-NNNN> : <HUMAN READABLE MESSAGE>

Some error descriptions in the following table contain the phrase „[param]“. These will be replaced during runtime with details for the relevant error, e.g. the problematic path for E-1030.

Error number	Error description
1000	Unable to connect to database. UMS server may be down.
1001	Cannot get database configurations.
1002	Cannot create database.
1003	Cannot activate database. [param]
1004	Internal error while activating database.
1005	Database already exists in this configuration.
1006	Database type is unknown.
1007	Database is already activated.
1008	Cannot edit database configurations.
1009	Internal error while optimizing database.
1010	The active data source type is not Embedded or Derby and does not support optimization.
1011	Test of the active data source failed.
1012	No database is activated.
1013	Cannot deactivate database.
1014	No database is active or the active database is not of type 'Embedded' or 'Derby'.
1020	Database could not be deleted.
1030	The specified directory for the backup does not exist: [param]
1031	Internal error while attempting database backup.
1040	The specified backup file was not found.
1041	The specified backup file has an invalid file type.
1042	Unable to read the specified backup file.

Error number	Error description
1043	Internal error while activating data source after restore.
1044	Internal error while attempting to restore database.
1045	The active data source is not embedded or there is no active data source.
1051	Authentication error or internal error when an attempt was made to copy the database
1052	Error Accessing credentials of source database
1090	A name is required for non-embedded database types.
1091	Activation failed, incorrect password provided.
1092	Backup failed, the specified file already exists.
1093	Port number is required for non-Embedded database.
1094	A data source of the Embedded type cannot be edited.
1095	No such data source with this ID.
1100	The name 'rmdb' is reserved for the Embedded database.
2000	Internal error while reading port configuration.
2001	Internal error while setting port configuration.
2002	Internal error while restarting UMS server.
2003	Invalid port number provided.
2004	Port number [param] already configured.
3000	Internal error while reading cipher data.
3001	Internal error while changing cipher configuration.
3002	Invalid ciphers provided: [param]
4000	Resetting web certificates requires '--yes' option for confirmation.
4001	Internal error while resetting web certificates.
5000	Internal error while reading superuser credentials.
5001	Internal error while writing superuser credentials.
5002	No username was provided for new credentials.

Error number	Error description
5003	Unable to set superuser credentials. There is no active data source.
6000	Unable to create a new UMS ID.
6001	The specified file for the license key backup already exists.
6002	No internal license keystore found.
6003	Internal error while creating license key backup.
6004	Internal error while restoring license key backup.
6005	The specified file for the license key backup does not exist.
6006	The specified password for the license key backup is incorrect.
6007	The specified path for the license key backup does not exist: [param]
7000	Token file was not found.
7001	Setup type not defined, token not installed.
7501	Unable to set UMS cluster FQDN.
7502	Unable to show UMS cluster FQDN.
7503	Unable to delete the cluster FQDN.
8000	Internal error while restarting the UMS server.
8001	Internal error while starting the UMS server.
8002	Internal error while stopping the UMS server.
8003	Internal error while ending the update mode of the UMS Server.
8004	Internal error while setting the distributed mode of the UMS installation.
8005	Either --enable or --disable must be provided in the options.
8006	Distributed UMS not recommended for Derby Embedded Database.
9000	An error with the password file occurred: [param]
9001	The provided passwords did not match. Aborted.

Error number	Error description
9002	The provided password exceeds the maximum character limit ([param]) or contains only whitespace.
9700	File [param] doesn't exist!
9701	Keystore contains no certificate entries!
9702	Keystore password is invalid!
9703	Keystore couldn't be read!
9704	Could not import certificate chain!
9705	Internal error while importing certificate chain!
9706	No SHA1 fingerprint specified!
9707	Could not delete certificate(s) with SHA1 fingerprint [param]!
9708	Certificate must not be deleted because it is currently in use!
9709	Root certificate creation failed!
9710	Certificate could not be created! Private key of CA certificate is not known.
9711	Certificate could not be created! CA certificate is not valid.
9712	Could not find CA certificate with specified fingerprint.
9713	Certificate could not be created! CA certificate does not meet the requirements.
9714	Certificate could not be created! Requirements for CA certificate creation are not met.
9715	Creation of signed certificate failed!
9716	Certificate could not be created! Certificate name too long (only 200 characters are allowed)!
9717	Could not find certificate with specified fingerprint!
9718	Certificate could not be renewed! Certificate has no CA parent.
9719	Certificate file [param] doesn't exist!
9720	Certificate is invalid!
9721	Import of certificate failed! No CA certificate.
9722	Import of certificate failed!

Error number	Error description
9723	Import of certificate failed! Certificate is not valid.
9724	Import failed! Certificate doesn't contain any subject alternative names.
9725	Import of private key failed! File [param] doesn't exist.
9726	Import of private key failed! Private key is encrypted. Decrypt it before importing it.
9727	Import of private key failed!
9728	Certificate already has private key!
9729	Import of private key failed! Private key does not match the specified certificate.
9730	Export of certificate failed! Directory [param] doesn't exist.
9731	Export of certificate failed!
9732	Export of certificate chain failed! Directory [param] doesn't exist.
9733	Certificate must not be a root or CA certificate!
9734	Export of certificate chain failed!
9735	Password must be at least 6 characters long!
9736	Assignment of certificate failed!
9737	Private key is not known!
9738	Could not read certificate info!
9739	Import failed! Certificate with same fingerprint already exists.
9740	Import failed! No valid root certificate.
9741	Import failed! Verification of signature failed.
9742	Import failed! No valid CA certificate available.
9743	Could not read assigned server info!
9744	Could not find certificate with specified fingerprint or no server is assigned to certificate!
9745	Common name is invalid! Only A-Z, a-z, 0-9, - and . are allowed.